NetBackup™ 重複排除ガイド

UNIX、Windows および Linux

リリース 11.0

VERITAS
now part of Cohesity

NetBackup™ 重複排除ガイド

最終更新日: 2025-04-24

法的通知と登録商標

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

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

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

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

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

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

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

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

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

https://www.veritas.com/support

次の URL で Cohesity Account の情報を管理できます。

https://my.veritas.com

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

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

マニュアル

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

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Cohesity Services and Operations Readiness Tools (SORT)

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

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

目次

1

NetBackup メディアサーバー重複排除オプションの概要

この章では以下の項目について説明しています。

NetBackup Deduplication のオプションについて

Cohesity NetBackup は、必要なかぎりデータソースに近い任意の場所でデータを重複排除できる重複排除オプションを提供します。

任意の場所での重複排除には、次の利点があります。

- 保存されるデータの量が減ります。
- バックアップ帯域幅が削減されます。
- バックアップ処理時間帯が短縮されます。
- インフラが縮小されます。

任意の場所での重複排除では、バックアップ処理のどの時点で重複排除を実行するかを選択できます。NetBackup は、バックアップストリーム内の実装されている場所で重複排除を管理できます。

表 1-1 に、重複排除のオプションの説明を示します。

表 1-1 NetBackup Deduplication のオプション

種類	説明
メディアサーバー重複排除	NetBackup クライアントは、バックアップデータを重複排除する NetBackup メディアサーバーにバックアップを送信します。NetBackup メディアサーバーは NetBackup Deduplication Engine をホストします。この Deduplication Engine はデータをターゲットストレージの［メディアサーバー重複排除プール (Media Server Deduplication Pool)］に書き込んで重複排除されたデータを管理します。 p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。
Client Deduplication	NetBackup MSDP Client Deduplication では、クライアントが自身のバックアップデータを重複排除してから直接ストレージサーバーに送信し、ストレージサーバーはストレージにそのデータを書き込みます。ネットワークトラフィックが非常に低減しています。 p.36 の「NetBackup Client Direct の重複排除について」を参照してください。
NetBackup Appliance の重複排除	Cohesity は NetBackup Deduplication を含むハードウェアとソフトウェアソリューションを提供します。 NetBackup Appliance には、それ自体のマニュアルセットが用意されています。 https://www.veritas.com/content/support/en_US/Appliances.html

2

配備の計画

この章では以下の項目について説明しています。

MSDP の配置計画

表 2-1 に、NetBackup 重複排除の配置計画の概要を示します。

表 2-1　　配置の概要

手順	配置タスク	情報の参照場所
手順 1	重複排除ノードとストレージの宛先についての理解	p.25 の「MSDP 重複排除ノードについて」を参照してください。 p.25 の「NetBackup 重複排除の宛先について」を参照してください。
手順 2	ストレージ容量の把握および要件	p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。 p.28 の「MSDP ストレージと接続性の必要条件について」を参照してください。
手順 3	使用する重複排除の種類の決定	p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。 p.36 の「NetBackup Client Direct の重複排除について」を参照してください。 p.38 の「MSDP リモートオフィスのクライアントの重複排除について」を参照してください。
手順 4	重複排除ホストの要件の確認	p.33 の「MSDP ストレージサーバーについて」を参照してください。 p.34 の「MSDP サーバーの必要条件について」を参照してください。 p.37 の「MSDP クライアントの重複排除の必要条件と制限事項について」を参照してください。 p.40 の「MSDP のネットワークインターフェースについて」を参照してください。 p.41 の「MSDP ポートの使用について」を参照してください。 p.50 の「MSDP の調整について」を参照してください。
手順 5	重複排除のクレデンシャルの確認	p.39 の「NetBackup Deduplication Engine のクレデンシャルについて」を参照してください。
手順 6	圧縮と暗号化についての確認	p.104 の「MSDP の圧縮について」を参照してください。 p.106 の「MSDP の暗号化について」を参照してください。
手順 7	最適化された合成バックアップについての確認	p.42 の「MSDP の最適化された合成バックアップについて」を参照してください。
手順 8	重複排除と SAN クライアントについての確認	p.43 の「MSDP と SAN クライアントについて」を参照してください。

手順	配置タスク	情報の参照場所
手順 9	最適化された複製とレプリケーションについての確認	p.43 の「MSDP の最適化複製とレプリケーションについて」を参照してください。
手順 10	ストリームハンドラについての確認	p.44 の「MSDP のストリームハンドラについて」を参照してください。
手順 11	実装のベストプラクティスについての確認	p.49 の「MSDP の配置のベストプラクティス」を参照してください。
手順 12	ストレージ要件の確認とストレージのプロビジョニング	p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。 p.28 の「MSDP ストレージと接続性の必要条件について」を参照してください。 p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。 p.89 の「MSDP のストレージパスのプロパティ」を参照してください。
手順 13	MSDP の構成	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。 p.64 の「MSDP クライアント側の重複排除の構成」を参照してください。
手順 14	他のストレージから NetBackup の重複排除への移行	p.751 の「別のストレージ形式から MSDP への移行」を参照してください。

NetBackup 命名規則

NetBackup には、クライアント、ディスクプール、バックアップポリシー、ストレージライフサイクルポリシーなどの論理構成を命名するための規則があります。一般的に、名前では大文字と小文字は区別されます。次の文字セットはユーザー定義の名前とパスワードに使うことができます。

- アルファベット (A から Z、a から z) (名前では大文字と小文字が区別されます)
- 数字 (0 から 9)
- ピリオド (.)
  WORM ボリューム名にピリオドを使用しないでください。
- プラス (+)
- ハイフン (-)
  最初の文字にはハイフンを使用しないでください。
- アンダースコア (_)

これらの文字はまた外国語のためにも使われます。

メモ: スペースは許可されません。

論理ストレージユニット (LSU) 名またはドメインボリューム名は、ハイフン (-) とアンダースコア (_) を含む 50 文字未満の ASCII 文字にする必要があります。空白を含めることはできません。

NetBackup 重複排除エンジンの命名規則はこれらの NetBackup の命名規則とは異なります。

p.39 の「NetBackup Deduplication Engine のクレデンシャルについて」を参照してください。

MSDP 重複排除ノードについて

メディアサーバーの重複排除ノードは、次で構成されています。

ストレージサーバー	ストレージサーバーはバックアップを重複排除し、ストレージにデータを書き込み、ストレージを管理します。 p.33 の「MSDP ストレージサーバーについて」を参照してください。
負荷分散サーバー	負荷分散サーバーはバックアップを重複排除することによってストレージサーバーを支援します。負荷分散サーバーは任意で使用できます。 p.34 の「MSDP 負荷分散サーバーについて」を参照してください。
ストレージ	p.25 の「NetBackup 重複排除の宛先について」を参照してください。
クライアント	クライアントには、自身のデータを重複排除するクライアント (Client Direct) が含まれる場合があります。 p.36 の「NetBackup Client Direct の重複排除について」を参照してください。

複数のメディアサーバー重複排除ノードを存在させることができます。ノードはサーバーまたはストレージを共有できません。

各ノードは自身のストレージを管理します。各ノード内の重複排除がサポートされます。ただし、ノード間の重複排除はサポートされません。

p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

NetBackup 重複排除の宛先について

メディアサーバー重複排除プール (Media Server Deduplication Pool)

NetBackup の[メディアサーバー重複排除プール (Media Server Deduplication Pool)]は、NetBackup メディアサーバーに接続されているディスクストレージまたはクラウドストレージを表します。NetBackup は、データの重複を排除し、ストレージをホスティングします。

この宛先を使用する場合は、このガイドに従って重複排除とストレージの計画、実装、構成および管理を行います。ストレージサーバーを構成するときに、ストレージ形式として[メディアサーバー重複排除プール (Media Server Deduplication Pool)]を選択します。

[メディアサーバー重複排除プール (Media Server Deduplication Pool)]は次のシステムでホスト可能です。

- NetBackup メディアサーバー。
- NetBackup 5200 シリーズアプライアンス、または NetBackup 5300 シリーズアプライアンス。

MSDP の容量のサポートとハードウェア要件について

MSDP ストレージには、1 つのローカル LSU または複数のクラウド LSU が含まれています。

NetBackup 10.2 では、予測/サンプリング (P/S) キャッシュと呼ばれる新しい重複排除フィンガープリントルックアップキャッシュが導入され、より大きい MSDP プールのサポートが可能になります。バージョン 10.2 以降で構成されている新しい MSDP プールは、デフォルトでこの P/S キャッシュを使用します。既存の MSDP プールをバージョン 10.2 にアップグレードする場合、既存の MSDP キャッシュアーキテクチャを使用することになり、MSDP の制限は変更されません。

NetBackup 10.4 にアップグレードする場合は、既存の MSDP プールを新しい P/S キャッシュアルゴリズムに変換し、ローカルストレージとクラウドストレージのサポート対象容量を増やすオプションがあります。

p.80 の「サンプリングと予測キャッシュについて」を参照してください。

p.81 の「サンプリングキャッシュの再構築」を参照してください。

次の表に、NetBackup 10.1.1 以前のバージョンの MSDP 容量を示します。

表 2-2 NetBackup 10.1.1 以前のバージョンの MSDP 容量

プラットフォーム	ローカルディスクプール	ローカルおよびクラウドディスクプール
BYO	400 TiB	1.2 PiB
クラウドのみ	該当なし	1.2 PiB
NBA	960 TiB	1.2 PiB

プラットフォーム	ローカルディスクプール	ローカルおよびクラウドディスクプール
Flex	960 TiB	1.2 PiB
Flex Scale (16 ノード)	1.8 PiB	8.8 PiB
Access	1.2 PiB	該当なし

次の表に、P/S キャッシュ MSDP プールを含む NetBackup バージョン 10.2 以降での MSDP 容量を示します。

表 2-3 NetBackup 10.2 以降の MSDP 容量

プラットフォーム	ローカルディスクプール	ローカルおよびクラウドディスクプール
BYO	400 TiB	2.4 PiB
クラウドのみ	該当なし	2.0 PiB
NBA	960 TiB	2.4 PiB
Flex	1.2 PiB	2.4 PiB
Flex Scale (16 ノード)	2.5 PiB	8.8 PiB
Access	2.4 PiB	該当なし
Cloud Scale (16 ノード)	該当なし	4.0 PiB

メモ: 増加したプールサイズは Access バージョン 8.4 でサポートされます。

メモ: 新しい P/S キャッシュでは、より大きい MSDP プールのサポートが有効になりますが、より大きいプールをサポートするために利用できる適切なリソースがあることを確認する必要があります。

Flex Appliance でサポートされるアプリケーションと使用状況の情報を識別するには、次の記事を参照してください。

https://www.veritas.com/support/ja_JP/article.100042995

NetBackup は、重複排除データベースとトランザクションログ用にストレージ領域の 4% を予約します。したがって、ストレージの完全な条件は 96% のしきい値でトリガされます。重複排除データベースに別のストレージを使った場合でも、データストレージが過負荷にならないように NetBackup は 96% のしきい値を使います。

ストレージ要件がメディアサーバー重複排除プールの容量を超えた場合、複数のメディアサーバーの重複排除ノードを使うことができます。

p.25 の「MSDP 重複排除ノードについて」を参照してください。

NetBackup で重複排除をサポートするオペレーティングシステムのバージョンについては、NetBackup ソフトウェア互換性リストを参照してください。

MSDP ストレージと接続性の必要条件について

以降の項では、NetBackup Media Server Deduplication Option のストレージと接続性の必要条件について説明します。

ストレージメディア

各ディスクボリュームの単一ストリームの読み取りまたは書き込みパフォーマンスの最小要件は次のとおりです。ディスクへの書き込みとディスクからの読み取りの目標値を満たすには、個々のデータストリーム能力または集計能力の拡大が必要な場合があります。

最大 32 TB のストレージ	130 MB/秒。 エンタープライズレベルパフォーマンスの場合は 200 MB/秒。
32 ～ 48 TB のストレージ	200 MB/sec。 Cohesity では、データと重複排除データベース (それぞれの読み込みまたは書き込み速度が 200 MB/sec) を別々のディスクボリュームに格納することをお勧めします。どちらもシステムディスクには保存しないでください。
48 ～ 64 TB のストレージ	250 MB/sec。 Cohesity では、データと重複排除データベース (それぞれの読み込みまたは書き込み速度が 250 MB/sec) を別々のディスクボリュームに格納することをお勧めします。どちらもシステムディスクには保存しないでください。
96 TB のストレージ	250 MB/sec。 96 TB のストレージでは、読み取りまたは書き込み速度がそれぞれ 250 MB/秒の 4 つの別々のボリュームが必要です。必要なボリュームのいずれにもストレージサーバーホストのシステムディスクは使用できません。
400 TB のストレージ	500 MB/秒

ローカルディスクストレージは災害時に脆弱な状態となることがあります。SAN ディスクは、同じ名前を持つ新しくプロビジョニングされたサーバーに再マウントされる可能性があります。

NetBackup を配備するときは、MSDP ストレージ専用のファイルシステムを指定します。MSDP ストレージに使用されているファイルシステムが、他のアプリケーションと共有されると、パフォーマンスが低下し、ストレージ使用率のレポートに影響する場合があります。別のアプリケーションが過剰な量のデータを書き込むと、ファイルシステムが予期せずいっぱいになることがあります。ストレージが容量の 96% に達すると、MSDP ストレージサーバーはバックアップジョブに利用できなくなります。

NetBackup［メディアサーバー重複排除プール (Media Server Deduplication Pool)］では、重複排除ストレージの以下のストレージ形式はサポートされません。

- CIFS や NFS のような (ファイルベースのストレージプロトコルである) ネットワーク接続ストレージ
- ZFS ファイルシステム

NetBackup 互換性リストはサポートされているオペレーティングシステム、コンピュータ、周辺機器の明確な情報源です。次の Web サイトで、利用可能な互換性リストを参照してください。

http://www.netbackup.com/compatibility

NetBackup で重複排除を構成する前にストレージをプロビジョニングして実行可能な状態にしておく必要があります。

p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。

ストレージ接続

ストレージは、直付けストレージ (DAS)、内部ディスク、または低レイテンシのストレージエリアネットワーク (ファイバーチャネルまたは iSCSI) で接続されたストレージである必要があります。

ストレージエリアネットワークは次の基準に一致する必要があります。

遅延	ラウンドトリップごとの遅延が最大 0.1 ミリ秒
帯域幅	スループット目標を達成するのに十分なストレージネットワーク帯域幅。 Cohesity はイーサネットネットワーク帯域幅が 10 Gb 以上であるストレージネットワークの iSCSI をサポートします。 Cohesity はネットワーク帯域幅が少なくとも 4 ギガビットあるファイバーチャネルのストレージネットワークを推奨します。
HBA	ストレージサーバーは、ストレージ専用の HBA を 1 つ以上備えている必要があります。これらの HBA には、スループット目標を達成するのに十分な帯域幅が必要です。

p.30 の「MSDP のファイバーチャネルおよび iSCSI の比較」を参照してください。
p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.89 の「MSDP のストレージパスのプロパティ」を参照してください。

p.23 の「MSDP の配置計画」を参照してください。

p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。

MSDP のファイバーチャネルおよび iSCSI の比較

重複排除は CPU およびメモリに負荷をかかる処理です。また、最適なパフォーマンスを得るために、専用かつ高速なストレージ接続を必要とします。そのような接続は次を確保するのに役立ちます。

- 一貫したストレージパフォーマンス。
- ネットワークの輻輳中にパケットロスを減少。
- ストレージのデッドロックを減少。

次の表は重複排除ストレージのパフォーマンスに影響するファイバーチャネルおよび iSCSI の両方の特徴を比較します。設計により、ファイバーチャネルはパフォーマンス目標を達成する絶好の機会を提供します。NetBackup MSDP ストレージに必要な結果を達成するため、iSCSI は次の表で記述されているその他の最適化を必要とします。

表 2-4　ファイバーチャネルおよび iSCSI の特性

項目	ファイバーチャネル (Fibre Channel)	iSCSI
起源	ストレージデバイスが使う同じブロックストレージの形式を処理するように設計されているストレージネットワークアーキテクチャ。	企業内で同じ配線を使うために TCP/IP 上に構築されたストレージネットワークプロトコル。
プロトコル	FCP はロスレス、正しい順序での配信および低遅延スイッチを提供するシン形式の、単一目的のプロトコルです。	iSCSI は、イントラネットや長距離のデータ転送を支援する多層実装です。SCSI プロトコルはロスレス、正しい順序での配信を求めますが、iSCSI はパケットロスおよび誤順序配信を経験する TCP/IP を使用します。
ホストの CPU 負荷	低。ファイバーチャネルフレームの処理は専用の低遅延な HBA にオフロードされます。	より高く。ほとんどの iSCSI 実装はストレージコマンドを作成、送信、解読するためにホストプロセッサを使います。したがって、ストレージサーバーの負荷を軽減し、遅延を減らすために、Cohesity はストレージサーバーの専用ネットワークインターフェースを必要とします。
遅延	低。	より高く。
フロー制御	デバイスでのデータの受信準備ができたときにデータが送信されることを確保するビルトインのフロー制御メカニズム。	ビルトインのフロー制御なし。Cohesity は IEEE 802.1Qbb の標準で定義されているとおりのイーサネット優先度ベースのフロー制御を使用することを推奨します。

項目	ファイバーチャネル (Fibre Channel)	iSCSI
配備	困難	ファイバーチャネルよりも容易であるが、MSDP の基準を満たすよう配備することはより困難です。必須の専用ネットワークインターフェースは配備をより困難にします。ストレージトラフィックを搬送するための他の最適化も配備をより困難にします。その他の最適化はフロー制御、ジャンボフレームおよびマルチパス I/O を含みます。

Cohesity は[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージへの接続用に iSCSI をサポートしていますが、Cohesity ではファイバーチャネルをお勧めします。Cohesity はファイバーチャネルが iSCSI よりもより良いパフォーマンスと安定性を提供すると考えています。iSCSI の不安定性は状態 83 と状態 84 のエラーメッセージとして顕在化することがあります。

p.735 の「MSDP メディアのオープンエラー (83)」を参照してください。

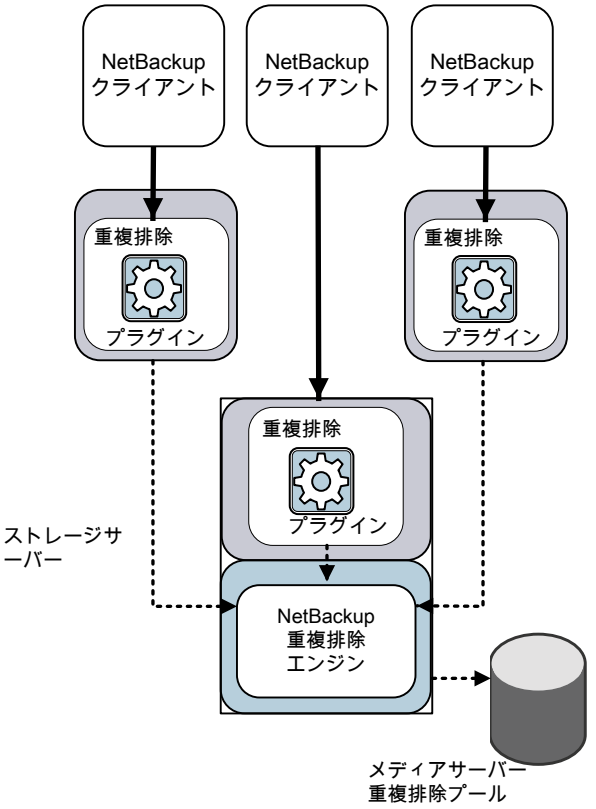
p.737 の「MSDP メディアの書き込みエラー (84)」を参照してください。

NetBackup メディアサーバー重複排除について

メディアサーバーの重複排除では、NetBackup クライアントソフトウェアは、通常のバックアップに関してはバックアップ済みファイルのイメージを作成します。クライアントはバックアップイメージをメディアサーバーに送信します。このメディアサーバーはバックアップデータを複製するプラグインをホストします。メディアサーバーは、ストレージサーバーまたは負荷分散サーバー (構成している場合) にできます。次に、重複排除プラグインはバックアップイメージをセグメントに分割し、その重複排除ノードに保存されているすべてのセグメントと比較します。さらにプラグインはストレージサーバーの NetBackup 重複排除エンジンに一意のセグメントのみを送信します。重複排除エンジンは、データをメディアサーバー重複排除プールに書き込みます。

図 2-1 は、NetBackup メディアサーバーの重複排除を示しています。重複排除ストレージサーバーは重複排除コアコンポーネントが有効になっているメディアサーバーです。ストレージの宛先は[メディアサーバー重複排除プール (Media Server Deduplication Pool)]です。

図 2-1 NetBackup メディアサーバーの重複排除



詳細情報が利用可能です。

p.25 の「MSDP 重複排除ノードについて」を参照してください。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

p.34 の「MSDP 負荷分散サーバーについて」を参照してください。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

p.36 の「MSDP のサポート外の構成について」を参照してください。

p.549 の「MSDP サーバーコンポーネント」を参照してください。

p.552 の「メディアサーバーの重複排除バックアップ処理」を参照してください。

MSDP 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。ストレージサーバーとしての 1 つのホスト機能と、1 つのみのストレージサーバーが各 NetBackup 重複排除ノードに存在します。ホストは NetBackup メディアサーバーである必要があります。ストレージサーバーのコンポーネントはメディアサーバーで動作しますが、ストレージサーバーは個別の論理的なエンティティです。

p.25 の「MSDP 重複排除ノードについて」を参照してください。

MSDP ストレージサーバーは、次のことを実行します。

- バックアップをクライアントから受信してデータを重複排除します。
- 重複排除されたデータをクライアントまたはメディアサーバーから受信します。NetBackup クライアントと他の NetBackup メディアサーバーもデータを重複排除するように構成できます。その場合、ストレージサーバーは重複排除された後のデータのみを受け取ります。

  p.36 の「NetBackup Client Direct の重複排除について」を参照してください。
  p.34 の「MSDP 負荷分散サーバーについて」を参照してください。
- ディスクストレージまたはクラウドストレージに重複排除されたデータを書き込み、ディスクストレージまたはクラウドストレージから重複排除されたデータを読み込みます。
- そのストレージを管理します。
- 重複排除プロセスを管理します。

何台ストレージサーバー (さらには、ノード) を構成するかは、ストレージの必要条件によって決まります。次のように、最適化複製とレプリケーションを使うかどうかにも依存します。

- 同じドメイン内にあるローカル LSU 間での最適化された複製では、同じドメインに少なくとも 2 つの重複排除ノードが必要になります。必須のストレージサーバーは次のとおりです。
  - バックアップストレージ用に 1 台のストレージサーバー。これが複製操作のソースになります。
  - 複製操作のターゲットとなるバックアップイメージのコピーを保存するためのもう 1 台のストレージサーバー。

  p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。
- 別のドメインへの自動イメージレプリケーションでは以下のストレージサーバーが必要になります。
  - レプリケート元の NetBackup ドメインのバックアップ用に 1 台のストレージサーバー。このストレージサーバーはストレージに NetBackup クライアントのバックアップを書き込みます。これは複製操作のソースになります。

- バックアップイメージのコピーを収めるためにリモート NetBackup ドメインにもう 1 台のストレージサーバー。このストレージサーバーは元のドメインで実行される複製操作のターゲットです。

p.134 の「NetBackup 自動イメージレプリケーションについて」を参照してください。

MSDP 負荷分散サーバーについて

データの重複排除を支援するように他の NetBackup メディアサーバーを構成できます。それらは重複排除についてファイル指紋の計算を実行し、ストレージサーバーに一意のデータセグメントを送ります。これらのヘルパーメディアサーバーは負荷分散サーバーと呼ばれます。

NetBackup メディアサーバーは次の 2 つの事が起きたときに負荷分散サーバーとして機能します。

- 重複排除を負荷分散するためにメディアサーバーを有効にする。
  ストレージサーバーを構成するときまたはそれ以降に、ストレージサーバーのプロパティを修正することによってそれを行います。
- ストレージユニットのメディアサーバーを重複排除プール用に選択する。

p.51 の「MSDP 負荷分散サーバーを徐々に導入する」を参照してください。

負荷分散サーバーはリストアと複製ジョブも実行します。

重複排除でサポートされるどの形式のサーバーでも負荷分散サーバーになれます。ストレージサーバーと同じ形式である必要はありません。

メモ: Cohesity アプライアンス構成で VMware バックアップにファイバーチャネルを使用する場合は、同じファイバーチャネルデータストア LUN をすべての負荷分散メディアサーバーにゾーン化する必要があります。

---

p.33 の「MSDP ストレージサーバーについて」を参照してください。

p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

p.495 の「MSDP サーバーの管理」を参照してください。

MSDP サーバーの必要条件について

同時に実行できるジョブの数は、ホストコンピュータの CPU とメモリによって制約されます。負荷分散サーバーに重複排除のいくつかをオフロードしないかぎり、ストレージサーバーは重複排除とストレージ管理のために十分な性能を必要とします。

表 2-5 に MSDP サーバーの最小必要条件を示します。NetBackup 重複排除サーバーは常に NetBackup メディアサーバーです。

重複排除のプロセッサには高いクロックレートと高い浮動小数点演算機能が必要です。さらに、コアごとの高いスループットが好ましいです。各々のバックアップストリームは別のコアを使います。

Intel と AMD のパフォーマンスは類似しており、単一コアのスループットでよく機能します。

SPARC64 VII のような、新しい SPARC プロセッサは、AMD と Intel に類似している単一コアのスループットを提供します。また、UltraSPARC T1 と T2 の単一コアのパフォーマンスは AMD と Intel のプロセッサには及びません。テストは UltraSPARC のプロセッサが高い集約スループットを達成できることを示します。ただし、そのためには AMD と Intel のプロセッサの 8 倍のバックアップストリームを必要とします。

表 2-5 MSDP サーバーの最小必要条件

コンポーネント	ストレージサーバー	負荷分散サーバー
CPU	Cohesity は少なくとも 2.2 GHz クロックレートを推奨します。64 ビットのプロセッサは必要になります。 少なくとも 4 つのコアが必要です。Cohesity は 8 つのコアを推奨します。 64 TB のストレージの場合、Intel x86-64 アーキテクチャでは 8 つのコアを必要とします。	Cohesity は少なくとも 2.2 GHz クロックレートを推奨します。64 ビットのプロセッサは必要になります。 少なくとも 2 つのコアは必要になります。スループットの要件によって、より多くのコアが有用なことがあります。
RAM	8 TB から 32 TB のストレージの場合は、Cohesity は 1 TB のストレージ用に 1 GB の RAM をお勧めします。ただし、32 TB を超えるストレージの場合は、Cohesity はより良いパフォーマンスを実現するため 32 GB 以上の RAM をお勧めします。	4 GB。
オペレーティングシステム	オペレーティングシステムは、サポートされている 64 ビット版のオペレーティングシステムである必要があります。 Cohesityのサポート Web サイトでご利用の NetBackup リリースの NetBackup ソフトウェア互換性リストを参照してください。	オペレーティングシステムは、サポートされている 64 ビット版のオペレーティングシステムである必要があります。 以下の Web サイトで、ご利用の NetBackup リリースの NetBackup ソフトウェア互換性リストを参照してください。

メモ: ある環境では、1 つのホストが NetBackup プライマリサーバーと重複排除サーバーの両方として機能できます。そのような環境は通常 1 日に合計 100 未満のバックアップジョブを実行します。(合計バックアップジョブ数は、重複排除と非重複排除のストレージを含むすべての宛先ストレージへのバックアップ数です) 1 日に 100 以上のバックアップを実行すると、重複排除の操作はプライマリサーバーの操作に影響することがあります。

p.517 の「MSDP キュー処理について」を参照してください。

p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.495 の「MSDP サーバーの管理」を参照してください。

MSDP のサポート外の構成について

次の項目では、サポートされていない構成をいくつか説明します。

- NetBackup メディアサーバーの重複排除と Cohesity Backup Exec の重複排除は、同じホストに配置できません。NetBackup と Backup Exec の両方の重複排除を使用する場合は、各製品が別々のホストに存在する必要があります。
- NetBackup は、重複排除のストレージサーバーまたは負荷分散サーバーのクラスタ化をサポートしません。
- 各メディアサーバーの重複排除ノード内の重複排除はサポートされますが、ノード間のグローバルな重複排除はサポートされません。

NetBackup Client Direct の重複排除について

NetBackup Client Direct の重複排除（クライアント側の重複排除としても知られます）では、クライアントがバックアップデータを複製するプラグインをホストします。NetBackup クライアントソフトウェアは、通常のバックアップに関してはバックアップ済みファイルのイメージを作成します。次に、重複排除プラグインはバックアップイメージをセグメントに分割し、その重複排除ノードに保存されているすべてのセグメントと比較します。さらにプラグインはストレージサーバーの NetBackup 重複排除エンジンに一意のセグメントのみを送信します。Engine は、データを[メディアサーバー重複排除プール (Media Server Deduplication Pool)]に書き込みます。

クライアントの重複排除では次の処理が実行されます。

- ネットワークの通信量を削減します。クライアントはストレージサーバーに一意のファイルセグメントのみを送信します。重複するデータは、ネットワークを介して送信されません。
- ストレージサーバーからクライアントに一部の重複排除処理の負荷を分散します。(NetBackup ではクライアント間の負荷は分散されません。各クライアントで自身のデータの重複排除が実行されます。)

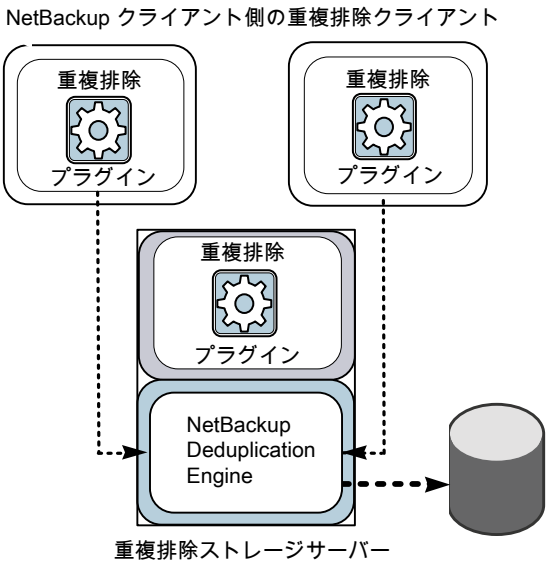
NetBackup のクライアント重複排除は次のためのソリューションです。

- リモートオフィスまたは支店のデータセンターへのバックアップ。
  NetBackup はリモートオフィスバックアップ用の耐性ネットワーク接続を提供します。
  p.38 の「MSDP リモートオフィスのクライアントの重複排除について」を参照してください。
- LAN に接続されたファイルサーバー。
- 仮想マシンのバックアップ。

クライアント側の重複排除は、クライアントホストに未使用の CPU サイクルがある場合、あるいはストレージサーバーまたは負荷分散サーバーが過負荷状態である場合にも有用なソリューションです。

図 2-2 はクライアントの重複排除を示しています。重複排除ストレージサーバーは重複排除コアコンポーネントが有効になっているメディアサーバーです。ストレージの宛先は［メディアサーバー重複排除プール (Media Server Deduplication Pool)］です

図 2-2 NetBackup クライアントの重複排除



詳細情報が利用可能です。

p.37 の「MSDP クライアントの重複排除の必要条件と制限事項について」を参照してください。

p.38 の「MSDP リモートオフィスのクライアントの重複排除について」を参照してください。

p.553 の「MSDP クライアントコンポーネント」を参照してください。

p.554 の「MSDP クライアント側の重複排除バックアップ処理」を参照してください。

MSDP クライアントの重複排除の必要条件と制限事項について

NetBackup のクライアント側の重複排除では、以下はサポートされません。

- ジョブあたりの複数コピー。複数のコピーを指定するジョブでは、バックアップイメージはストレージサーバーに送信され、そこで重複排除することができます。複数コピーは NetBackup バックアップポリシーで構成されています。
- NDMP ホスト。NDMP ホストにクライアント側の重複排除を使うとバックアップジョブは失敗します。

NetBackup がクライアント側の重複排除をサポートするシステムについては、NetBackup ソフトウェア互換性リストを参照してください。

自身のデータを重複排除するクライアントは、標準 NetBackup リリースレベルの互換性に準拠します。リリースごとの『NetBackup リリースノート』で NetBackup リリース間の互換性が定義されています。新機能、機能強化および修正を適切にご利用いただくため、Cohesity はクライアントとサーバーのリリースとバージョンを同一にすることをお勧めします。

p.36 の「NetBackup Client Direct の重複排除について」を参照してください。

p.20 の「NetBackup Deduplication のオプションについて」を参照してください。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

MSDP リモートオフィスのクライアントの重複排除について

WAN バックアップは自身のドメインのローカルバックアップよりも多くの時間を必要とします。ローカルバックアップと比較すると、WAN バックアップでは失敗のリスクが高くなります。WAN バックアップを容易にするために、NetBackup には耐性が高いネットワーク接続機能があります。耐性のある接続はクライアントと NetBackup メディアサーバー間のバックアップと復元トラフィックが WAN などの高遅延、低帯域幅ネットワークで効果的に機能できるようにします。

耐性が高い接続から最も恩恵を受ける使用例は、ローカルバックアップストレージがないリモートオフィスでのクライアント側の重複排除です。以下の項目は利点を示します。

- クライアントの重複排除では、転送する必要があるデータの量を減らすことによって WAN バックアップに必要な時間を短縮します。
- 耐性が高い接続により、(NetBackup がリカバリ可能なパラメータ範囲内の) ネットワークエラーと遅延から自動的にリカバリできます。

耐性が高い接続を構成すると、NetBackup はバックアップにその接続を使用します。耐性が高いネットワーク接続を使うには、NetBackup [耐性ネットワーク (Resilient Network)] ホストプロパティを使用して NetBackup を設定します。

p.166 の「[耐性ネットワーク (Resilient network)] プロパティ」を参照してください。

p.169 の「クライアントへの耐性のある接続の指定」を参照してください。

pd.confFILE_KEEP_ALIVE_INTERVAL パラメータで、アイドル状態であるソケットのキープアライブ操作の頻度を設定できます。

p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

リモートクライアントの最初のバックアップのパフォーマンスを向上できます。

p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。

MSDP のリモートクライアントのデータセキュリティについて

NetBackup は、接続トラフィックのバックアップデータまたはリストアデータを暗号化するため、移動中のデータの暗号化をサポートしています。『NetBackup セキュリティおよび暗号化ガイド』の「移動中のデータの暗号化」を参照してください。

移動中のデータの暗号化 (DTE) が有効でない場合、NetBackup の重複排除処理では WAN 経由で伝送する前にデータを暗号化できます。

p.106 の「MSDP の暗号化について」を参照してください。

MSDP は Client Direct Restore をサポートします。バックアップデータが暗号化されている場合、暗号化されたデータはクライアントに転送され、そこで復号されます。

Client Direct Restore について詳しくは、p.529 の「 MSDP のクライアントへの直接リストアの構成」を参照してください。

リモートクライアントのバックアップスケジュールについて

NetBackup のバックアップポリシーはジョブのスケジュールにプライマリサーバーのタイムゾーンを使います。リモートクライアントのタイムゾーンが NetBackup プライマリサーバーと異なる場合は、その相違を補正する必要があります。たとえば、プライマリサーバーがフィンランド (UTC+2) にあり、リモートクライアントがロンドン (UTC+0) にある場合を想定してください。バックアップポリシーに 6pm から 6am の時間枠がある場合、クライアントで 4pm にバックアップを開始できます。補正するには、バックアップ処理の時間帯を 8pm から 8am に設定する必要があります。または、リモートクライアントがある場所のタイムゾーンに応じて個別のバックアップポリシーを使うことも得策です。

NetBackup Deduplication Engine のクレデンシャルについて

NetBackup Deduplication Engine にはクレデンシャルが必要です。重複排除コンポーネントは、NetBackup Deduplication Engine との通信時にクレデンシャルを使用します。クレデンシャルは Deduplication Engine 用であり、実行されるホスト用ではありません。

ストレージサーバーを構成する際には、NetBackup Deduplication Engine のクレデンシャルを入力します。

クレデンシャルの規則は次のとおりです。

- ユーザー名とパスワードは、最大 62 文字で指定できます。ユーザー名とパスワードは空にできません。
- 次の文字を除く印刷可能な ASCII 範囲 (0x20-0x7E) の文字を使うことができます。
  - アスタリスク (*)
  - 円記号 (¥) とスラッシュ (/)
  - 二重引用符 (")
  - 左カッコ[(]と右カッコ[)]
  - 小なり記号 (<) と大なり記号 (>)。
  - 山形記号 (^)。
  - パーセント記号 (%)。
  - アンパサンド (&)
  - 空白。
  - 先頭および末尾の空白。
  - 角カッコ ([ ])
  - アットマーク (@)

重複排除エンジンを使用する Cohesity アプライアンス製品によっては、パスワード要件の制限がここの説明よりも多い場合があります。パスワードのガイドラインについては、アプライアンス固有のマニュアルを参照してください。

メモ: NetBackup Deduplication Engine のクレデンシャルは、入力した後に変更できません。そのため、慎重にクレデンシャルを選択し、入力します。クレデンシャルを変更する必要がある場合は、Cohesity のサポート担当者にお問い合わせください。

MSDP のネットワークインターフェースについて

MSDP ストレージサーバーに複数のネットワークインターフェースが含まれる場合、NetBackup はすべての重複排除トラフィックにデフォルトインターフェースを使用します。(重複排除トラフィックには、バックアップ、リストアおよびレプリケーションが含まれます)。ホストのオペレーティングシステムによって、どのネットワークインターフェースがデフォルトになるかが決定されます。ただし、ネットワークインターフェースまたは NetBackup が使用するインターフェースを次のように構成できます。

特定のインターフェースの構成	特定のインターフェースを使うためには、重複排除ストレージサーバーを構成するときにそのインターフェース名を入力します。複製とレプリケーション用に別のインターフェースを構成しない限り、NetBackup は、すべての重複排除トラフィックにこのインターフェースを使用します。 p.92 の「MSDP ネットワークインターフェースのプロパティ」を参照してください。 p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。
複製およびレプリケーショントラフィックのインターフェースの構成	複製およびレプリケーショントラフィック用に別のネットワークインターフェースを構成できます。バックアップおよびリストアトラフィックでは、デフォルトインターフェースまたは特定の構成済みインターフェースを引き続き使用します。 p.116 の「MSDP の複製およびレプリケーションに対する個別ネットワークパスについて」を参照してください。 p.117 の「MSDP 複製とレプリケーションに対する個別ネットワークパスの構成」を参照してください。

NetBackup の REQUIRED_INTERFACE の設定は、重複排除処理に影響しません。

p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.23 の「MSDP の配置計画」を参照してください。

p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。

MSDP ポートの使用について

次の表は NetBackup の重複排除に使われるポートを示したものです。ファイアウォールが各種の重複排除ホストの間にある場合は、その重複排除ホストで指定されているポートを開きます。重複排除ホストは、自身のデータを重複排除する重複排除ストレージサーバー、負荷分散サーバー、およびクライアントです。

ストレージサーバーが 1 つのみで、自身のデータを重複排除する負荷分散サーバーまたはクライアントがない場合、ファイアウォールポートを開く必要はありません。

表 2-6　　重複排除ポート

ポート	使用方法
10082	NetBackup Deduplication Engine (spoold)。データを重複排除するホスト間でこのポートを開いてください。ホストには、負荷分散サーバーと、自身のデータを重複排除するクライアントが含まれます。

ポート	使用方法
10102	NetBackup Deduplication Manager (spad)。データを重複排除するホスト間でこのポートを開いてください。ホストには、負荷分散サーバーと、自身のデータを重複排除するクライアントが含まれます。
443	MSDP サーバーと AWS や Azure などのクラウドストレージターゲット間でこのポートを開きます。

MSDP の最適化された合成バックアップについて

最適化された合成バックアップは合成バックアップのより効率的な形式です。メディアサーバーは、合成バックアップを作成するのにどの完全バックアップイメージと増分バックアップイメージを使うのかをメッセージを使ってストレージサーバーに指示します。ストレージサーバーは、ディスクストレージで直接、バックアップイメージを作成 (または合成) します。最適化された合成バックアップはネットワークをまたがるデータ移動を必要としません。

最適化された合成バックアップ方式には、次の利点があります。

- 合成バックアップより高速です。
  通常の合成バックアップはメディアサーバー上に作成されます。それらは、ストレージサーバーからメディアサーバーへネットワークを介して移動され、1 つのイメージに合成されます。その後、合成イメージがストレージサーバーに戻されます。
- ネットワークを介したデータの移動が必要ありません。
  通常の合成バックアップはネットワークトラフィックを使います。

p.116 の「最適化された合成バックアップの MSDP の構成」を参照してください。

NetBackup では、OptimizedImage 属性が最適化された合成バックアップを有効にします。これは、ストレージサーバーと重複排除プールの両方に適用されます。この属性はストレージサーバーとメディアサーバー重複排除プールでデフォルトで有効になっています。

p.496 の「MSDP ストレージサーバーの属性の設定」を参照してください。

p.507 の「メディアサーバー重複排除プールの属性の設定」を参照してください。

表 2-7　最適化された合成バックアップのための MSDP の要件と制限事項

内容	説明
要件	対象のストレージユニットの重複排除プールはソースイメージが存在するのと同じ重複排除プールである必要があります。

内容	説明
制限事項	NetBackup は最適化された合成バックアップの宛先としてストレージユニットグループをサポートしません。NetBackup が最適化された合成バックアップを生成できない場合、NetBackup はよりデータの移動に特化した合成バックアップを作成します。

MSDP と SAN クライアントについて

SAN クライアントは NetBackup クライアントの高速なバックアップとリストアを提供する NetBackup のオプション機能です。ファイバートランスポートは SAN クライアント機能の一部である NetBackup の高速データ転送方式の名前です。バックアップとリストアの通信は SAN を介して行われます。

SAN クライアントは重複排除オプションとともに使うことができます。ただし、重複排除はクライアントではなくメディアサーバーで行う必要があります。重複排除ストレージサーバー(または負荷分散サーバー)と FT メディアサーバーの両方になるようにメディアサーバーを構成します。それから、SAN クライアントバックアップは重複排除サーバー/FT メディアサーバーホストに SAN を介して送信されます。そのメディアサーバーで、バックアップストリームは重複排除されます。

SAN クライアントではクライアント側の重複排除を有効にしないでください。重複排除のデータ処理はファイバートランスポートの高速トランスポート方式と非互換です。クライアント側の重複排除はメディアサーバーとの LAN 経由の双方向通信に依存します。SAN クライアントは SAN を介して FT メディアサーバーにデータを高速でストリーム配信します。

MSDP の最適化複製とレプリケーションについて

NetBackup は重複排除されたデータの最適化複製とレプリケーションの複数の方式をサポートします。

次の表は、メディアサーバー重複排除プール間の NetBackup がサポートしている複製方式をリストしたものです。

表 2-8 NetBackup OpenStorage の最適化複製とレプリケーションの方式

最適化複製の方式	説明
同じ NetBackup ドメイン内	p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。 p.259 の「MSDP クラウドのサポートについて」を参照してください。

最適化複製の方式	説明
リモートの NetBackup ドメインへ	p.134 の「NetBackup 自動イメージレプリケーションについて」を参照してください。

MSDP のストリームハンドラについて

NetBackup は各種のバックアップデータストリームの形式を処理するストリームハンドラを提供します。ストリームハンドラは基礎となるデータストリームを処理することによってバックアップ重複排除率を改善します。

すでに重複排除されたデータの場合、新しいストリームハンドラによる最初のバックアップでは重複排除率が低くなります。最初のバックアップの後、重複排除率は新しいストリームハンドラの使用前の排除率を上回ります。

Cohesity はバックアップ重複排除のパフォーマンス向上のために、追加のストリームハンドラを開発し続けています。

Oracle ストリームハンドラ

Oracle ストリームハンドラは、NetBackup 8.3 の既存および新しい Oracle クライアントに対してはデフォルトで有効になりません。また、Oracle ストリームハンドラはストリームベースのバックアップのみをサポートし、`cacontrol` コマンドラインユーティリティを使用して `<client><policy>` の組み合わせごとに Oracle ストリームハンドラを有効または無効にできます。

NetBackup 10.0 では、既存のイメージがないすべての新しいクライアントで、Oracle ストリームハンドラが (デフォルトで) 有効になっています。以前のバージョンと同様に、Oracle ストリームハンドラはストリームベースのバックアップのみをサポートし、`cacontrol` コマンドラインユーティリティを使用して Oracle ストリームハンドラを構成できます。次に対してストリームハンドラを有効または無効にできます。

- ポリシーとクライアント
- ポリシーレベル
- ストリームの種類のレベル

メモ: Oracle ストリームハンドラを使用する場合、可変長の重複排除を使用することはお勧めしません。

`cacontrol` コマンドユーティリティで `--sth` フラグを使用して、構成ファイルでクライアント、ポリシー、またはストリームの種類に対する**マーカーエントリ**を作成することで、NetBackup のデフォルトの動作を上書きします。`cacontrol` コマンドユーティリティは次の場所にあります。

- Windows の場合: *install_path*¥Veritas¥pdde¥cacontrol
- UNIX の場合: /usr/openv/pdde/pdcr/bin/cacontrol

次の cacontrol の例では、Oracle ストリームハンドラを構成するため、*STHTYPE* を Oracle に設定する必要があります。

NetBackup 8.3 では、次のオプションを使用して cacontrol を構成できます。

- クライアントとポリシーごとにストリームハンドラの設定を問い合わせることができます。

```
cacontrol --sth get <STHTYPE> <CLIENT> <POLICY> [SPAUSER]
```

- クライアントとポリシーごとにストリームハンドラを有効にできます。

```
cacontrol --sth update
<STHTYPE> <CLIENT> <POLICY> [SPAUSER] <enabled>
```

- クライアントとポリシーの設定を削除できます (デフォルトの動作に戻ります)。

```
cacontrol --sth delete <STHTYPE> <CLIENT> <POLICY>
[SPAUSER]
```

- クライアントとポリシーでストリームハンドラを無効にできます。

```
cacontrol --sth update
<STHTYPE> <CLIENT> <POLICY> [SPAUSER] <disabled>
```

メモ: cacontrol を使用して **<*POLICY*>** または **<*STHTYPE*>** を enabled に設定すると、NetBackup は既存のイメージがあるすべての古いクライアントを有効にします。重複排除率は、有効にした後の最初のバックアップでのみ大幅に減少します。また、ストレージの使用状況は、有効にした後の最初のバックアップでのみ増加します。基本的には、NetBackup は最初の完全バックアップを実行したかのように動作します。ストリームハンドラの最初のアクティブ化後には、重複排除率とストレージ使用状況の両方が改善されます。

---

cacontrol コマンドユーティリティを使用して NetBackup 10.0 で**マーカーエントリ**を作成する際は、より詳細な構成が優先されます。例:

```
Marker Entry 1: <Client1> <Policy1> to enabled

Marker Entry 2: <Policy1> to disabled
```

構成がより詳細な**マーカーエントリ** 1 の優先度が高くなるため、ストリームハンドラが有効になります。

NetBackup 10.0 では、次のオプションを使用して cacontrol を構成できます。

- クライアントとポリシーごとにストリームハンドラの設定を問い合わせることができます。

  ```
  cacontrol --sth get <STHTYPE> <CLIENT> <POLICY> [SPAUSER]
  ```

- クライアントとポリシーごとにストリームハンドラを有効にできます。

  ```
  cacontrol --sth update
  <STHTYPE> <CLIENT> <POLICY> [SPAUSER] <enabled>
  ```

- クライアントとポリシーの設定を削除できます (デフォルトの動作に戻ります)。

  ```
  cacontrol --sth delete <STHTYPE> <CLIENT> <POLICY> [SPAUSER]
  ```

- クライアントとポリシーでストリームハンドラを無効にできます。

  ```
  cacontrol --sth update
  <STHTYPE> <CLIENT> <POLICY> [SPAUSER] <disabled>
  ```

- ポリシーごとにストリームハンドラの設定を問い合わせることができます。

  ```
  cacontrol --sth getbypolicy <STHTYPE> <POLICY> [SPAUSER]
  ```

- ポリシーごとにストリームハンドラを有効にできます。

  ```
  cacontrol --sth updatebypolicy
  <STHTYPE> <POLICY> [SPAUSER] <enabled>
  ```

- ポリシーごとにストリームハンドラの設定を削除できます (デフォルトの動作に戻ります)。

  ```
  cacontrol --sth deletebypolicy <STHTYPE> <POLICY> [SPAUSER]
  ```

- ポリシーごとにストリームハンドラを無効にできます。

  ```
  cacontrol --sth updatebypolicy
  <STHTYPE> <POLICY> [SPAUSER] <disabled>
  ```

- ストリームハンドラの種類ごとにストリームハンドラの設定を問い合わせることができます。

  ```
  cacontrol --sth getbytype <STHTYPE> [SPAUSER]
  ```

- ストリームハンドラの種類ごとにストリームハンドラを有効にできます。

  ```
  cacontrol --sth updatebytype <STHTYPE> [SPAUSER] <enabled>
  ```

- ストリームハンドラの設定を削除できます (デフォルトの動作に戻ります)。

  ```
  cacontrol --sth deletebytype <STHTYPE> [SPAUSER]
  ```

- ストリームハンドラの種類ごとにストリームハンドラを無効にできます。

  ```
  cacontrol --sth updatebytype <STHTYPE> [SPAUSER] <disabled>
  ```

Microsoft SQL Server ストリームハンドラ

Microsoft SQL ストリームハンドラは Microsoft SQL バックアップの重複排除率を改善します。Microsoft SQL Server のストリームハンドラは、Microsoft SQL Server のすべてのバージョンと Azure SQL Server に適用できます。

次の方法を使用して Microsoft SQL データベースを NetBackup で保護できます。

- MS-SQL-Server ポリシー
  Microsoft SQL データベースを保護するには、MS-SQL-Server ポリシー形式を使用します。このポリシー形式は Microsoft SQL データベースを保護するための推奨される方法です。
  この場合、Microsoft SQL ストリームハンドラは自動的に有効になります。このポリシーには、ユーザーが指定したバッチファイルの使用やインテリジェントポリシーなど、複数のオプションがあります。
- Standard ポリシー
  Microsoft SQL ダンプファイルを保護するには、Standard ポリシーを使用します。この場合、ユーザーは Microsoft SQL Server をファイルにダンプし、ダンプされたファイルをバックアップするための標準ポリシーを作成します。
  `cacontrol` コマンドを使用して、Microsoft SQL ストリームハンドラを手動で有効にする必要があります。

Microsoft SQL Server ストリームハンドラの管理に使用できる `cacontrol` オプションを次に示します。

表 2-9 cacontrol コマンドのオプション

オプション	説明
cacontrol --sth get <Oracle|MSSQL> <client> <policy>	指定したマーカーエントリの状態を取得します。
cacontrol --sth delete <Oracle|MSSQL> <client> <policy>	指定したマーカーエントリを削除します。
cacontrol --sth update <Oracle|MSSQL> <client> <policy> <enabled|disabled>	指定したマーカーエントリの状態を更新します。
cacontrol --sth getbypolicy <Oracle|MSSQL> <policy>	指定したポリシーについて、指定したマーカーエントリの状態を取得します。
cacontrol --sth deletebypolicy <Oracle|MSSQL> <policy>	指定したポリシーについて、指定したマーカーエントリを削除します。
cacontrol --sth updatebypolicy <Oracle|MSSQL> <policy> enabled|disabled	指定したポリシーについて、指定したマーカーエントリの状態を更新します。

Microsoft SQL Server ストリームハンドラを使用するには

1 ポリシーのストリームハンドラを有効または無効にします。

```
cacontrol --sth updatebypolicy MSSQL <POLICY name>
enabled/disabled
```

2 ポリシーのストリームハンドラ設定を削除します (デフォルトの動作に戻ります)。Microsoft SQL ストリームハンドラはデフォルトで有効になっています。

```
cacontrol --sth deletebypolicy MSSQL <POLICY name>
```

3 ポリシーについて、ストリームハンドラの設定を問い合わせます。

```
cacontrol --sth getbypolicy MSSQL <POLICY name>
```

4 ポリシーとクライアントについて、ストリームハンドラを有効または無効にします。

```
cacontrol --sth update MSSQL <Client name> <POLICY name>
enabled/disabled
```

5 ポリシーとクライアントのストリームハンドラ設定を削除します (デフォルトの動作に戻ります)。Microsoft SQL ストリームハンドラはデフォルトで有効になっています。

```
cacontrol --sth delete MSSQL <Client name> <POLICY name>
```

6 ポリシーとクライアントについて、ストリームハンドラの設定を問い合わせます。

```
cacontrol --sth get MSSQL <Client name><POLICY name>
```

7 Microsoft SQL ストリームハンドラが有効または無効であることを確認します。

NetBackup Web UI の[ジョブの詳細 (Job Details)]タブに、[MSSQL ストリームハンドラが有効 (MSSQL Stream Handler enabled)]が表示されます。

考慮すべき事項:

- Client Direct 設定を有効にすると、MS-SQL-Server ポリシー形式を使用しても Microsoft SQL ストリームハンドラは使用されません。pdplugin は、クライアント側で実行するときにポリシー形式を認識していません。
  ストリームハンドラを有効にするには、cacontrol コマンドを使用して、ポリシー、またはクライアントとポリシーに対して Microsoft SQL ストリームハンドラを有効にします。
- ストレージ形式が MSDP の場合は、NetBackup 圧縮設定を有効にしないでください。この設定は、Microsoft SQL ストリームハンドラが有効と無効のどちらになっていても、重複排除の損失を引き起こします。
- Microsoft SQL 圧縮設定は Microsoft SQL Server が提供する機能です。これは SQL データを圧縮します。Microsoft SQL ネイティブ圧縮が有効になっていると、重複排除率が低下することがあります。
- Microsoft SQL ストリームハンドラは、Microsoft SQL Server TDE (透過的なデータ暗号化) で正常に動作します。Microsoft SQL TDE は SQL データのみを暗号化し、SQL ページ構造は変わりません。Microsoft SQL Server TDE が有効な場合、重複排除は失われません。

MSDP の配置のベストプラクティス

Cohesity は、最小必要条件のホストとネットワークのみを推奨するので重複排除のパフォーマンスは環境に応じて大きく変わることがあります。Cohesity が提供するベストプラクティスのガイドラインに従うと、ホストの機能に関係なく重複排除を効果的に行うことができます。

Cohesity は NetBackup Deduplication を実装するとき次の方法を考慮することを推奨します。

完全修飾ドメイン名を使用する

Cohesity は NetBackup サーバー (さらには、重複排除サーバー) に完全修飾ドメイン名を使うことを推奨します。完全修飾ドメイン名は特にクライアント側の重複排除を使う場合、ホスト名解決問題を避けるうえで役立ちます。

重複排除サーバーはストレージサーバーと (ある場合) 負荷分散サーバーを含んでいます。

p.737 の「MSDP メディアの書き込みエラー (84)」を参照してください。

MSDP の調整について

負荷分散サーバーまたはクライアント重複排除あるいはその両方を使用して、パフォーマンスが向上するように重複排除処理を調整できます。

負荷分散サーバーを構成すると、それらのサーバーも重複排除を実行します。重複排除ストレージサーバーは引き続き重複排除サーバーおよびストレージサーバーの両方として機能します。NetBackup は、標準の負荷分散基準に従って各ジョブの負荷分散サーバーを選択します。ただし、重複排除のフィンガープリント計算は、負荷分散基準に含まれません。

重複排除の作業から重複排除ストレージサーバーを完全に除外するには、重複排除ディスクプールを使うすべてのストレージユニットに対して次の操作を行います。

- ［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。
- すべての負荷分散サーバーを選択します。

重複排除ストレージサーバーは、ストレージサーバーのタスク (重複排除されたデータの保存と管理、ファイルの削除、および最適化複製) のみを実行します。

クライアント重複排除を構成すると、クライアントは自身のデータを重複排除します。重複排除負荷の一部は、重複排除ストレージサーバーと負荷分散サーバーから除去されます。

Cohesity MSDP を調整するために次の方法を使うことをお勧めします。

- クライアントの初回の完全バックアップに、重複排除ストレージサーバーを使用します。2 回目以降のバックアップには、負荷分散サーバーを使用します。
- クライアント側の重複排除を徐々に有効にします。
  クライアントが重複排除処理の負荷に耐えることができない場合に、重複排除処理をサーバーに戻せるようにしておきます。

ストレージサーバーに初回の完全バックアップを送信する

負荷分散サーバーかクライアントの重複排除を使う場合は、クライアントの初回の完全バックアップにストレージサーバーを使います。それから、以降のバックアップを負荷分散サーバーを通して送信するか、またはバックアップにクライアントの重複排除を使います。そうすることで、重複排除の総負荷についての情報が提供されます。その後、ホスト間で最適に負荷を分散するようにジョブを割り当てることができます。

重複排除はどのホストが重複排除を実行するかにかかわらず、同じフィンガープリントリストを使います。従って最初にストレージサーバーのデータを重複排除できます。その後、以降の別ホストによるバックアップは同じフィンガープリントリストを使います。重複排除プラグインは、クライアントとポリシーの組み合わせの最新の完全バックアップを識別できる

場合、サーバーからフィンガープリントリストを取り込みます。リストは新しいバックアップのフィンガープリントキャッシュに配置されます。

p.72 の「MSDP のフィンガープリントについて」を参照してください。

Cohesity また、ベリタス社は負荷分散サーバーとクライアントの重複排除を徐々に実装することを推奨します。従って他のホストで重複排除を実装する間、バックアップにストレージサーバーを使うことは有利であることがあります。

MSDP ジョブ数を徐々に増やす

Cohesity は[最大並列実行ジョブ数 (Maximum concurrent jobs)]の値を徐々に増やすことをお勧めします([最大並列実行ジョブ数 (Maximum concurrent jobs)]はストレージユニットの設定です)。そうすることで、重複排除の総負荷についての情報が提供されます。初回のバックアップジョブ (初回シードとも呼ばれます) は、2 回目以降のジョブより多くの CPU とメモリを必要とします。初回シードの後、ストレージサーバーはより多くのジョブを同時に処理できます。それから徐々にジョブの値を増やすことができます。

MSDP 負荷分散サーバーを徐々に導入する

Cohesity ストレージサーバーが最大 CPU 使用率に達した後でのみ負荷分散サーバーを追加することをお勧めします。それから、負荷分散サーバーを 1 つずつ導入します。環境がどのように通信を処理するか評価したり、また重複排除のために加えられた少数のホストに関する問題をトラブルシュートすることを簡単にできることがあります。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

各種の要因のために、Cohesity は重複排除のために複数のサーバーを使うことについて現実的な予測をすることを推奨します。負荷分散サーバーとして 1 つのメディアサーバーを追加すれば、全体的なスループットはより速いはずです。ただし、1 つの負荷分散サーバーを追加しても全体的なスループット率が 2 倍にならなかったり、2 つの負荷分散サーバーを追加してもスループット率が 3 倍にならなかったりします。

次のすべてが MSDP 環境に該当する場合、その環境は負荷分散サーバーのよい候補であることがあります。

- 重複排除ストレージサーバーは複数のコアを持つ CPU に限定されています。
- メモリリソースはストレージサーバーで利用可能です。
- ネットワーク帯域幅はストレージサーバーで利用可能です。
- 重複排除プールへのバックエンドの I/O 帯域幅は利用可能です。
- 他の NetBackup メディアサーバーは重複排除に利用可能な CPU を備えています。

ギガビットイーサネットは多くの環境で十分なパフォーマンスを提供するはずです。パフォーマンス目標が負荷分散サーバーを使って、可能な限り早いスループットとした場合は、10 ギガビットイーサネットを考慮する必要があります。

p.23 の「MSDP の配置計画」を参照してください。

p.49 の「MSDP の配置のベストプラクティス」を参照してください。

MSDP クライアントの重複排除を徐々に実装する

自身のデータを重複排除するようにクライアントを構成した場合、それらのすべてのクライアントを同時に有効にしないでください。次のとおり、クライアントの重複排除を徐々に実装します。

- クライアントの初回バックアップにストレージサーバーを使います。
- 一度に少数のクライアントでのみ重複排除を有効にします。
  そうすることで、重複排除がクライアントの他のジョブに与える影響についての情報が提供されます。環境がどのように通信を処理するか評価したり、トラブルシューティングしたりすることを簡単にできることがあります。

クライアントが重複排除処理の負荷に耐えることができない場合に、重複排除処理をストレージサーバーに戻せるようにしておきます。

MSDP の圧縮と暗号化を使う

NetBackup ポリシーで圧縮か暗号化を使わないでください。むしろ、重複排除処理の一部である圧縮か暗号化を使ってください。

p.104 の「MSDP の圧縮について」を参照してください。

p.106 の「MSDP の暗号化について」を参照してください。

MSDP の最適なバックアップストリーム数について

バックアップストリームは NetBackup アクティビティモニターに別のジョブとして表示されます。ストリームを生成するために各種の方式が存在します。NetBackup では、複数のストリームを設定するためにバックアップポリシー設定を使うことができます。NetBackup for Oracle エージェントは複数のストリームを構成することを可能にします。また RMAN ユーティリティは Oracle に複数のバックアップチャネルを提供できます。

クライアントの重複排除の場合、最適なバックアップストリーム数は 2 です。

メディアサーバーの重複排除は複数のコアで複数のストリームを同時に処理できます。Oracle のようなアプリケーションの大きいデータセットの場合、メディアサーバーの重複排除は複数のコアと複数のストリームを利用します。従って、アプリケーションが複数のストリームかチャネルを提供できるとき、メディアサーバーの重複排除はより適切な解決策であることがあります。

MSDP のストレージユニットグループについて

NetBackup MSDP に対するバックアップ先としてストレージユニットグループを使えます。グループ内のすべてのストレージユニットには[メディアサーバー重複排除プール (Media Server Deduplication Pool)]がストレージの宛先としてある必要があります。

ストレージユニットグループは、バックアップサービスを中断することがある単一障害を回避します。

複数のディスクプールをまたがるのではなく、同じ重複排除の宛先ディスクプールにバックアップポリシーがデータを保存すると、ストレージの節約は最も大きくなります。したがって、[ストレージユニットの選択 (Storage unit selection)]の[フェールオーバー (Failover)]方式は最小限の量のストレージを使います。他のすべての方式はバックアップが実行される度に異なるストレージを使うように設計されています。Cohesity は[ストレージユニットの選択 (Storage unit selection)]形式で[フェールオーバー (Failover)]方式を選択することをお勧めします。

表 2-10　ストレージユニットグループの MSDP の必要条件と制限事項

内容	説明
要件	グループは 1 つのストレージ先の形式のみのストレージユニットを含む必要があります。つまり、1 つのグループが[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージユニットとその他のストレージ形式のストレージユニットの両方を含むことはできません。
制限事項	NetBackup のストレージユニットグループでは、以下はサポートされません。 ■ 重複排除されたデータの最適化複製。重複排除されたデータの最適化複製の宛先としてストレージユニットグループを使うと、NetBackup は通常の複製を使います。 p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。 ■ 最適化された合成バックアップ。NetBackup が最適化された合成バックアップを生成できない場合、NetBackup はよりデータの移動に特化した合成バックアップを作成します。 p.42 の「MSDP の最適化された合成バックアップについて」を参照してください。

MSDP データの保護について

Cohesity 次の方法を使って重複排除されたバックアップデータを保護することをお勧めします。

- 別の重複排除ノードのオフサイトの場所にイメージをコピーするために NetBackup の最適化複製を使います。

最適化複製は、別の重複排除プールにプライマリバックアップデータをコピーします。それは、同じ NetBackup ドメインに残ったままで、オフサイトにデータをコピーする最も簡単で効率的な方法を提供します。他の重複排除プールからイメージを取り込むことによって、プライマリコピーが存在するストレージを破壊する障害からリカバリできます。

p.124 の「同じ NetBackup ドメインでの MSDP 最適化複製の構成」を参照してください。

- 別の NetBackup ドメインオフサイトに重複排除されたデータをコピーするために NetBackup のレプリケーションを使います。

  p.132 の「異なる NetBackup ドメインへの MSDP レプリケーション設定」を参照してください。

Cohesity MSDP カタログをバックアップすることもお勧めします。

p.197 の「MSDP カタログの保護について」を参照してください。

MSDP ストレージサーバーの構成を保存する

Cohesity ストレージサーバーの構成を保存することをお勧めします。構成を取得して保存すると、環境のリカバリに役立つ場合があります。ディザスタリカバリでは、保存された構成ファイルの使用によってストレージサーバーの構成を設定する必要がある場合もあります。

ストレージサーバーの構成を保存する場合、リカバリに必要な情報のみが含まれるようにそれを編集してください。

p.191 の「MSDP ストレージサーバーの構成の保存について」を参照してください。

p.192 の「MSDP ストレージサーバーの構成の保存」を参照してください。

p.193 の「MSDP ストレージサーバーの構成ファイルの編集」を参照してください。

ディスクの書き込みのキャッシュ計画

ストレージコンポーネントは、読み込みと書き込みのパフォーマンスを向上させるためにハードウェアのキャッシュを使うことがあります。キャッシュを使うことがあるストレージコンポーネントには、ディスクアレイ、RAID コントローラ、ハードディスクドライブ自体などがあります。

ストレージコンポーネントがディスクの書き込み操作用にキャッシュを使用する場合、キャッシュが電源の変動または停電から保護されていることを確認します。電源の変動または停電から保護しない場合、データ破損またはデータ損失が発生することがあります。

保護には次も含まれます。

- 電源が復旧するまでの時間にも書き込み操作を継続できるように、キャッシュメモリに電源を供給するバッテリーバックアップ装置。

- コンポーネントが書き込み操作を完了できるようにする無停電電源装置。

キャッシュを備えているデバイスが保護されていない場合、Cohesity はハードウェアのキャッシュを無効にすることを推奨します。読み込みと書き込みのパフォーマンスは低下する可能性がありますが、データ損失は避けられます。

3

ストレージのプロビジョニング

この章では以下の項目について説明しています。

- MSDP 用のストレージのプロビジョニングについて
- MSDP のストレージディレクトリやファイルを変更しない
- NetBackup MSDP のボリューム管理について

MSDP 用のストレージのプロビジョニングについて

NetBackup では、ストレージがディレクトリパスとして公開されている必要があります。

次のようにストレージをプロビジョニングします。

最大 64 TB

400 TB

プロビジョニングするストレージインスタンスの数は、バックアップのストレージ要件によって決まります。要件が 1 つの重複排除ノードで対応できる範囲を超える場合は、複数のノードを構成できます。

p.25 の「MSDP 重複排除ノードについて」を参照してください。

最適化複製とレプリケーションも、プロビジョニングするノード数に影響を与える可能性があります。

p.43 の「MSDP の最適化複製とレプリケーションについて」を参照してください。

NetBackup の他の要件がストレージのプロビジョニング方法に影響を与えることがあります。

p.28 の「MSDP ストレージと接続性の必要条件について」を参照してください。

ストレージのプロビジョニング方法は、NetBackup のマニュアルの対象外となります。ストレージベンダーのマニュアルを参照してください。

p.25 の「NetBackup 重複排除の宛先について」を参照してください。

p.23 の「MSDP の配置計画」を参照してください。

最大 64 TB のストレージ

オペレーティングシステムの単一のマウントポイントとして表示されるように、バックアップストレージをプロビジョニングします。

ストレージにはディレクトリパスが必要であるため、root ノード (/) またはドライブ文字 (E:¥) のみをストレージパスとして使わないでください。つまり、ストレージを root ノード (/) またはドライブ文字 (E:¥) としてマウントしないでください。

重複排除データベースに別のディスクボリュームを使用する場合は、バックアップデータのストレージではなく、異なるマウントポイント上の 1 TB のボリュームをプロビジョニングします。

400 TB のストレージ

NetBackup は、特定のオペレーティングシステムでは 1 つのメディアサーバー重複排除プールで 400 TB のストレージをサポートしています。

p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。

MSDP ストレージサーバーを構成する前に、ボリュームをプロビジョニングする必要があります。各ボリュームは以下の項目に合致する必要があります。

- NetBackup で MSDP 用にサポートするファイルシステムでフォーマットされていること。すべてのボリュームで同じファイルシステムを使用する必要があります。
- MSDP ストレージに割り当てる他のボリュームとは別のディスクに置いてください。
- MSDP ストレージサーバーとして使用するコンピュータの別のマウントポイントにマウントされています。
  Cohesity では、マウントポイント名にわかりやすい命名規則を使用することを推奨します。

50 TB のボリュームを使用して 400 TB の MSDP を構成する手順

1. 9 つの新しいファイルシステムを作成、フォーマット、およびマウントします。1 つのファイルシステムには 1 TB のストレージ領域が、その他の 8 つのファイルシステムには 50 TB のストレージ領域がそれぞれ必要です。
2. 1 TB のファイルシステムを `/msdp/cat` にマウントし、50 TB のファイルシステムを `/msdp/vol0`、`/msdp/vol1` などにマウントして、各ボリュームがマウントされるまで続けます。

3 touch ファイル /etc/nbapp-release が存在しない場合は、作成します。

4 マウントされた各ボリュームの下に data という名前のサブディレクトリを作成します。たとえば、/msdp/vol0/data、/msdp/vol1/data、/msdp/vol2/data のようになります。

5 MSDP ストレージサーバーを構成します。[重複排除データベースに代替パスを使用 (Use alternate path for deduplication database)]オプションが選択されていることを確認します。ストレージパスに /msdp/vol0/data、データベースパスに /msd/cat を指定します。

6 重複排除プールに追加の 50 TB のファイルシステムを追加します:

```
/usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition
/msdp/vol1/data
/usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition
/msdp/vol2/data
till volume 07...
/usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition
/msdp/vol7/data
```

root 以外のユーザーが NetBackup メディアサーバーに使用されている場合は、次のコマンドを実行して、新しく作成されたボリュームの所有者を NetBackup メディアサーバーのサービスユーザーに変更します。

```
chown -R <NBU-service-user>:root <MSDP-volume-path>
```

7 次のコマンド出力を参照して、作成されたボリュームを確認します。

```
/usr/openv/pdde/pdcr/bin/crcontrol --dsstat 2 | grep Mount
Mount point count: 7
```

p.528 の「MSDP ストレージパーティションのサイズ調整」を参照してください。

MSDP のストレージディレクトリやファイルを変更しない

のマニュアルまたはベリタス社のサポート担当者によって指示されない限り、次の操作を実行しないでください。NetBackupCohesity

- 重複排除ストレージのディレクトリまたはデータベースのディレクトリにファイルを追加する。
- 重複排除ストレージのディレクトリまたはデータベースのディレクトリからファイルを削除する。
- 重複排除ストレージのディレクトリ内またはデータベースのディレクトリ内のファイルを変更する。

- 重複排除ストレージのディレクトリ内またはデータベースのディレクトリ内でファイルを移動する。
- 重複排除ストレージのディレクトリまたはデータベースのディレクトリ内にあるディレクトリとファイルの権限を変更します。

これらの指示に従わないと、操作に失敗したりデータ損失が起きることがあります。

NetBackup MSDP のボリューム管理について

NetBackup の［メディアサーバー重複排除プール (Media Server Deduplication Pool)］のストレージのボリューム管理にツールを使用する場合、Cohesityでは、Arctera InfoScale Storage を使用することをお勧めします。InfoScale Storage は Arctera Volume Manager と Arctera File System を含んでいます。

サポート対象のシステムについては、Arctera の Web サイトで、InfoScale ハードウェア互換性リストを参照してください。

http://www.veritas.com/

メモ: InfoScale Storage は NFS をサポートしていますが、NetBackup は［メディアサーバー重複排除プール (Media Server Deduplication Pool)］のストレージに対して NFS ターゲットをサポートしていません。従って、［メディアサーバー重複排除プール (Media Server Deduplication Pool)］は InfoScale Storage で NFS をサポートしません。

4

重複排除の構成

この章では以下の項目について説明しています。

- MSDP 最適化複製とレプリケーション帯域幅の構成について
- 大規模なイメージの最適化複製とレプリケーションのパフォーマンスチューニングについて
- MSDP クラウドの最適化複製とレプリケーションのパフォーマンスチューニングについて
- ストレージライフサイクルポリシーについて
- MSDP バックアップポリシーの構成について
- バックアップポリシーの作成
- [耐性ネットワーク (Resilient network)]プロパティ
- MSDP 負荷分散サーバーの追加
- NetBackup クライアントでの可変長の重複排除について
- MSDP pd.conf 構成ファイルについて
- MSDP contentrouter.cfg ファイルについて
- MSDP ストレージサーバーの構成の保存について
- MSDP ストレージサーバーの構成の設定
- MSDP ホストの構成ファイルについて
- MSDP ホストの構成ファイルの削除
- MSDP レジストリのリセット
- MSDP カタログの保護について
- MSDP の FIPS 準拠について
- MSDP の複数のインターフェースをサポートするための NetBackup クライアント側の重複排除の構成
- MSDP のマルチドメインのサポートについて
- MSDP アプリケーションのユーザーサポートについて
- MSDP マルチドメイン VLAN のサポートについて
- 変更不可および削除不可のデータの NetBackup WORM ストレージサポートについて
- root 以外のユーザーによる MSDP サービスの実行

- root 以外のユーザーによる MSDP コマンドの実行

NetBackup でのメディアサーバー重複排除の構成

表 4-1 に構成作業を記述します。

『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。

表 4-1 MSDP の構成タスク

タスク	手順
重複排除ストレージサーバーの構成	構成するストレージサーバーの台数は、ストレージ要件および複製またはレプリケーションを使うかどうかによって決まります。ストレージサーバーを構成するとき、ウィザードでディスクプールとストレージユニットも構成できます。 p.33 の「MSDP ストレージサーバーについて」を参照してください。 p.89 の「MSDP のストレージパスのプロパティ」を参照してください。 p.43 の「MSDP の最適化複製とレプリケーションについて」を参照してください。 構成するストレージサーバーの種類は、ストレージの宛先によって決まります。 p.25 の「NetBackup 重複排除の宛先について」を参照してください。 p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。
ディスクプールの構成	ストレージサーバー構成時にディスクプールをすでに構成した場合は、この手順をスキップできます。 構成するディスクプールの数は、ストレージ要件および複製またはレプリケーションを使うかどうかによって決まります。 p.92 の「NetBackup の重複排除用ディスクプールについて」を参照してください。 p.93 の「重複排除のディスクプールの構成」を参照してください。
ストレージユニットの構成	p.97 の「[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージユニットの構成」を参照してください。
バックアップポリシーの構成	重複排除ストレージユニットをバックアップポリシーの宛先として使用します。レプリケーションを構成した場合は、ストレージの宛先としてストレージライフサイクルポリシーを使います。 p.165 の「MSDP バックアップポリシーの構成について」を参照してください。 p.166 の「バックアップポリシーの作成」を参照してください。
最適化複製コピーの構成	最適化複製は、必要に応じて行います。 p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。

タスク	手順
レプリケーションの構成	レプリケーションは、必要に応じて行います。 p.131 の「異なるドメインへの MSDP レプリケーションについて」を参照してください。
MSDP クライアント側の重複排除の構成	p.64 の「MSDP クライアント側の重複排除の構成」を参照してください。
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.720 の「NetBackup MSDP ログファイル」を参照してください。 p.720 の「MSDP 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。
重複排除マルチスレッドエージェントの動作の構成	重複排除マルチスレッドエージェントは、デフォルトの構成値を使って動作を制御します。必要に応じてそれらの値を変更できます。 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。 p.66 の「重複排除マルチスレッドエージェントの動作の構成」を参照してください。 p.71 の「マルチスレッドエージェントによる重複排除プラグイン通信の構成」を参照してください。
指紋のキャッシュ動作の構成	指紋のキャッシュ動作の構成は省略可能です。 p.72 の「MSDP フィンガープリントのキャッシュについて」を参照してください。 p.73 の「MSDP フィンガープリントのキャッシュ動作の構成」を参照してください。
400 TB MSDP のサポートの有効化	400 TB メディアサーバー重複排除プールをホストするストレージサーバーを構成する前に、そのサイズのストレージのサポートを有効にする必要があります。 p.83 の「MSDP での 400 TB のサポートの有効化」を参照してください。
400 TB サポート用データディレクトリの作成	400 TB メディアサーバー重複排除プールの場合、ストレージディレクトリのマウントポイントの下にデータディレクトリを作成する必要があります。 p.83 の「400 TB MSDP サポート用データディレクトリの作成」を参照してください。
400 TB サポート用の他のボリュームの追加	400 TB メディアサーバー重複排除プールの場合、2 番目および 3 番目のボリュームをディスクプールに追加する必要があります。 p.84 の「400 TB メディアサーバー重複排除プールへのボリュームの追加」を参照してください。
暗号化を有効にする	暗号化は、必要に応じて行います。 p.106 の「MSDP ローカルストレージボリュームの暗号化の構成」を参照してください。
最適化された合成バックアップの構成	最適化された合成バックアップは、必要に応じて行います。 p.116 の「最適化された合成バックアップの MSDP の構成」を参照してください。

タスク	手順
MSDP リストア動作の構成	必要に応じて、NetBackup を構成し、リストア時にメディアサーバーを省略することができます。 p.529 の「MSDP のリストアのしくみ」を参照してください。 p.529 の「 MSDP のクライアントへの直接リストアの構成」を参照してください。
詳細な重複排除設定の指定	詳細設定は、必要に応じて行います。 p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。 p.175 の「MSDP pd.conf ファイルの編集」を参照してください。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。
MSDP データおよびカタログの保護	p.53 の「MSDP データの保護について」を参照してください。 p.197 の「MSDP カタログの保護について」を参照してください。

MSDP クライアント側の重複排除の構成

このトピックでは、NetBackup でクライアント重複排除を構成する方法について説明します。クライアント側の重複排除を構成できるようにするには、メディアサーバー重複排除を構成する必要があります。

p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

表 4-2　クライアント重複排除の構成作業

タスク	手順
メディアサーバー重複排除の構成	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。
クライアント重複排除について	p.36 の「NetBackup Client Direct の重複排除について」を参照してください。
リモートオフィスクライアント用の耐性が高い接続の構成	耐性が高い接続は任意です。 p.38 の「MSDP リモートオフィスのクライアントの重複排除について」を参照してください。 p.166 の「[耐性ネットワーク (Resilient network)]プロパティ」を参照してください。 p.169 の「クライアントへの耐性のある接続の指定」を参照してください。
クライアント側の重複排除の有効化	p.102 の「MSDP クライアント側重複排除のクライアント属性の構成」を参照してください。

タスク	手順
リモートクライアントの指紋キャッシュのシードの構成	リモートクライアントの指紋キャッシュのシードの構成は省略可能です。 p.77 の「クライアントでの MSDP フィンガープリントキャッシュのシードの構成」を参照してください。 p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。 p.78 の「ストレージサーバーでの MSDP フィンガープリントキャッシュのシードの構成」を参照してください。
クライアント主導リストアの構成	クライアント主導リストアの構成は任意です。構成しない場合、リストアは NetBackup メディアサーバーのコンポーネントを経由します。 p.529 の「 MSDP のクライアントへの直接リストアの構成」を参照してください。

MSDP 重複排除マルチスレッドエージェントについて

MSDP 重複排除処理では、ほとんどのデータソースでマルチスレッドエージェントを使うことができます。マルチスレッドエージェントは、クライアントサーバーとメディアサーバーの両方で重複排除プラグインとともに動作します。エージェントは、非同期ネットワーク I/O と CPU コア計算に複数のスレッドを使います。バックアップ中に、このエージェントは重複排除プラグインから共有メモリを介してデータを受信し、複数のスレッドを使って処理することでスループットパフォーマンスを改善します。無効な場合、エージェントは最小限のリソースを使います。

NetBackup 重複排除マルチスレッドエージェントは、データの重複排除を行うすべてのホスト、独自のデータの重複排除を行うストレージサーバー、負荷分散サーバー、クライアントのバックアップのパフォーマンスを改善します。マルチスレッドエージェントを使用するホストごとに、重複排除プラグインをマルチスレッドエージェントを使用するように構成する必要があります。

重複排除マルチスレッドエージェントは、デフォルトの構成値を使って動作を制御します。必要に応じてそれらの値を変更できます。次の表はマルチスレッドエージェントの動作を説明したものです。それはまたそれらの動作の設定方法について説明したトピックへのリンクを提供します。

表 4-3　　通信と動作

通信	手順
マルチスレッドエージェントの動作とリソース使用量。	p.66 の「重複排除マルチスレッドエージェントの動作の構成」を参照してください。

通信	手順
重複排除プラグインがマルチスレッドエージェントにバックアップを送信するかどうか	p.71 の「マルチスレッドエージェントによる重複排除プラグイン通信の構成」を参照してください。
バックアップに重複排除マルチスレッドエージェントを使う必要があるクライアント	p.71 の「マルチスレッドエージェントによる重複排除プラグイン通信の構成」を参照してください。
重複排除マルチスレッドエージェントを使う必要があるバックアップポリシー	p.71 の「マルチスレッドエージェントによる重複排除プラグイン通信の構成」を参照してください。

表 4-4は、MSDP マルチスレッドの操作上の注意事項を示します。マルチスレッドエージェントを使用しない場合、NetBackup は単一スレッドモードを使います。

表 4-4　マルチスレッドエージェントの要件と制限事項

項目	説明
サポートされているシステム	NetBackup は、Linux、Solaris、AIX および Windows のオペレーティングシステム上でマルチスレッドエージェントをサポートします。
サポート外のユースケース	NetBackup は、以下のユースケースではマルチスレッドエージェントを使用しません。 ■ 仮想合成バックアップ ■ SEGKSIZE が 128 を超える (pd.conf ファイル) ■ DONT_SEGMENT_TYPES が有効(pd.conf ファイル) ■ MATCH_PDRO = 1(pd.conf ファイル) p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。
ポリシーベースの圧縮または暗号化	NetBackup のポリシーベースの圧縮または暗号化がバックアップポリシーで有効になっている場合、NetBackup は重複排除マルチスレッドエージェントを使いません。 Cohesity では、NetBackup のポリシーベースの圧縮および暗号化よりも、MSDP の圧縮および暗号化を使用することをお勧めします。 p.104 の「MSDP の圧縮について」を参照してください。 p.106 の「MSDP の暗号化について」を参照してください。

重複排除マルチスレッドエージェントの動作の構成

mtstrm.conf 構成ファイルは、NetBackup 重複排除マルチスレッドエージェントの動作を制御します。

p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。

ホストの mtstrm.conf ファイルを変更すると、そのホストのみの設定が変更されます。データを重複排除するすべてのホストで同じ設定にするには、すべてのホストの mtstrm.conf ファイルを変更する必要があります。

マルチスレッドエージェントの動作を構成する方法

1. テキストエディタを使用して mtstrm.conf ファイルを開きます。

   mtstrm.conf 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/lib/ost-plugins/
   - Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins

2. 動作を変更するには、新しい値を指定します。

   p.67 の「MSDP mtstrm.conf ファイルパラメータ」を参照してください。

3. ファイルを保存して閉じます。
4. 次のようにホストのマルチスレッドエージェントを再起動します。

   - UNIX の場合:

     ```
     /usr/openv/pdde/pdag/bin/mtstrmd -terminate
     /usr/openv/pdde/pdag/bin/mtstrmd
     ```

   - Windows の場合、Windows サービスマネージャを使用します。サービス名は NetBackup 重複排除マルチスレッドエージェントです。

MSDP mtstrm.conf ファイルパラメータ

mtstrm.conf 構成ファイルは、重複排除マルチスレッドエージェントの動作を制御します。デフォルト値は、リソース使用量を用いてパフォーマンスを分散します。

これらのパラメータの構成方法を説明する手順があります。

pd.conf ファイルは、次のディレクトリに存在します。

- (UNIX) /usr/openv/lib/ost-plugins/
- (Windows) *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins

p.66 の「重複排除マルチスレッドエージェントの動作の構成」を参照してください。

mtstrm.conf ファイルは 3 つのセクションで構成されています。パラメータはセクション内にとどまる必要があります。パラメータの説明は、以降のセクションを参照してください。

- 「ログパラメータ」
- 「プロセスパラメータ」

- 「スレッドパラメータ」

mtstrm.conf 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/lib/ost-plugins/
- Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins

ログパラメータ

次の表は mtstrm.conf の設定ファイルのログパラメータを記述したものです。

表 4-5 ログパラメータ (mtstrm.conf ファイル)

ログパラメータ	説明
LogPath	mtstrmd.log ファイルがその中に作成されるディレクトリ。 デフォルト値: ■ Windows の場合: LogPath=*install_path*¥Veritas¥pdde¥¥..¥netbackup¥logs¥pdde ■ UNIX の場合: LogPath=/var/log/puredisk
Logging	何をログ記録するかを指定します。 デフォルト値: Logging=short,thread。 指定可能な値: minimal: Critical, Error, Authentication, Bug short : all of the above plus Warning long : all of the above plus Info verbose: all of the above plus Notice full : all of the above plus Trace messages (everything) none : disable logging 他のログ情報の有効と無効を切り替えるには、ログ値に次のいずれかをスペースを使わずに追加します。 ,thread : enable thread ID logging. ,date : enable date logging. ,timing : enable high-resolution timestamps ,silent : disable logging to console
Retention	NetBackup がログファイルを何日間保持してから削除するかを指定します。 デフォルト値: Retention=7。 有効値: 0～9。ログを永久に保持するときは 0 を使用します。

ログパラメータ	説明
LogMaxSize	NetBackup が新しいログファイルを作成するまでの最大ログサイズ(MB)。ロールオーバーされる既存のログファイルは、mtstrmd.log.<*date/time stamp*> と名前を変更されます。 デフォルト値: LogMaxSize=500。 有効値: 1～オペレーティングシステムの最大ファイルサイズ(MB)。

プロセスパラメータ

次の表は mtstrm.conf の設定ファイルのプロセスパラメータを記述したものです。

表 4-6　プロセスパラメータ (mtstrm.conf ファイル)

プロセスパラメータ	説明
MaxConcurrentSessions	マルチスレッドエージェントが処理する並行セッションの最大数。MaxConcurrentSessions 値に達したときにバックアップジョブを受信する場合、ジョブは単一スレッドジョブとして動作します。 デフォルトでは、重複排除プラグインは先入れ先出し方式でマルチスレッドエージェントにバックアップジョブを送信します。ただし、重複排除プラグインがどのクライアントやどのバックアップポリシーをマルチスレッドエージェントに送信するかを構成できます。pd.conf の MTSTRM_BACKUP_CLIENTS および MTSTRM_BACKUP_POLICIES パラメータは動作を制御します。マルチスレッドエージェントに送られるバックアップジョブをフィルタ処理すると、多くの並行バックアップジョブがあるシステムで非常に有用なことがあります。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。 デフォルト値: MaxConcurrentSessions=(NetBackup が計算。以下を参照)。 NetBackup は、インストールまたはアップグレード時にこのパラメータの値を構成します。値は、BackupFpThreads 値で割られるホストのハードウェア同時実行値です(表 4-7 を参照)。(このパラメータにおいて、同時ハードウェアは、CPU またはコアまたはハイパースレッディングユニットの数です) メディアサーバーでは、NetBackup は重複排除のためにすべてのハードウェア同時実行を使うとはかぎりません。一部は他のサーバープロセスのために予約される場合があります。 ハードウェア同時実行について詳しくは、pd.conf ファイルの MTSTRM_BACKUP_ENABLED パラメータの説明を参照してください。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。 指定可能な値: 1 から 32 までの整数。 **警告:** Cohesity ベリタス社では、変更がシステムリソースにどのように影響するかを慎重に考慮した後に限り、この値を変更することをお勧めしています。デフォルトの構成値で、各セッションは約 120～150 MB のメモリを使います。メモリ使用量は (BackupReadBufferCount * BackupReadBufferSize) + (3 * BackupShmBufferSize) + FpCacheMaxMbSize です(有効な場合)。

プロセスパラメータ	説明
BackupShmBufferSize	共有メモリのコピーのためのバッファサイズ(MB)。この設定は、共有メモリバッファ自体、mtstrmd プロセス内の共有メモリ受信バッファ、およびクライアントプロセスの共有メモリ送信バッファの 3 つのバッファに影響します。 デフォルト値: BackupShmBufferSize=2(UNIX)または BackupShmBufferSize=8(Windows)。 指定可能な値: 1 から 16 までの整数。
BackupReadBufferSize	バックアップ時にクライアントからのデータを読み取る操作で、セッションごとに使うメモリバッファのサイズ (MB)。 デフォルト値: BackupReadBufferSize=32。 指定可能な値: 16 から 128 までの整数。
BackupReadBufferCount	バックアップ時にクライアントからのデータを読み取る操作で、セッションごとに使うメモリバッファの数。 デフォルト値: BackupReadBufferCount=3。 有効値: 1〜10。
BackupBatchSendEnabled	バックアップのためストレージサーバーにデータを送るとき、バッチメッセージのプロトコルを使うかどうかを決めます。 デフォルト値: BackupBatchSendEnabled=1。 有効値: 0(無効)または 1(有効)。
FpCacheMaxMbSize	フィンガープリントキャッシュのためセッションごとに使用する最大メモリ量(MB)。 デフォルト値: FpCacheMaxMbSize=1024。 指定可能な値: 0 から 1024 までの整数。
SessionCloseTimeout	セッションが閉じられるときに、エージェントがタイムアウトでエラーになるまでにスレッドが待機する秒数。 デフォルト値: 180。 有効値: 1〜3600。
SessionInactiveThreshold	NetBackup が非アクティブと見なす前に、セッションをアイドル状態にする時間 (分単位)NetBackup がセッションを検査し、メンテナンス操作の間に非アクティブなものを閉じます。 デフォルト値: 480。 指定可能な値: 1 から 1440 までの整数。

スレッドパラメータ

次の表は mtstrm.conf の設定ファイルのスレッドパラメータを記述したものです。

表 4-7 スレッドパラメータ (mtstrm.conf ファイル)

スレッドパラメータ	説明
BackupFpThreads	受信データのフィンガープリントのためセッションごとに使うスレッドの数。 デフォルト値: BackupFpThreads=(NetBackup が計算。以下の説明を参照)。 NetBackup は、インストールまたはアップグレード時にこのパラメータの値を構成します。値は、以下のハードウェア同時実行しきい値と等しくなります。 ■ Windows と Linux の場合: しきい値は 2 です。 ■ Solaris の場合: しきい値は 4 です。 ハードウェア同時実行について詳しくは、pd.conf ファイルの MTSTRM_BACKUP_ENABLED パラメータの説明を参照してください。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。
BackupSendThreads	バックアップ処理中にストレージサーバーへデータを送るためセッションごとに使うスレッドの数。 デフォルト値: BackupSendThreads=1(サーバー)、BackupSendThreads=2(クライアント)。 指定可能な値: 1 から 32 までの整数。
MaintenanceThreadPeriod	NetBackup がメンテナンス操作を実行する頻度、分単位。 デフォルト値: 720。 指定可能な値: 1 から 10080 までの整数。ゼロ (0) はメンテナンス操作を無効にします。

マルチスレッドエージェントによる重複排除プラグイン通信の構成

NetBackup 重複排除プラグインとマルチスレッドエージェント間の通信を制御できます。ホストの pd.conf ファイルが通信を制御します。pd.conf ファイルの変更は、そのホストのみの設定を変更します。データを重複排除するすべてのホストで同じ設定にするには、すべてのホストの pd.conf ファイルを変更する必要があります。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

重複排除プラグインとマルチスレッドエージェントとの通信を構成する方法

1 テキストエディタを使用して pd.conf ファイルを開きます。

pd.conf ファイルは、次のディレクトリに存在します。

- (UNIX) /usr/openv/lib/ost-plugins/
- (Windows) *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins

2 設定を変更するには、新しい値を指定します。以下に、通信を制御する設定を示します。

- MTSTRM_BACKUP_CLIENTS
- MTSTRM_BACKUP_ENABLED
- MTSTRM_BACKUP_POLICIES
- MTSTRM_IPC_TIMEOUT

これらの設定は別のトピックで説明しています。

p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

3 ファイルを保存して閉じます。

4 ホストで NetBackup Remote Manager and Monitor Service (nbrmms) を再起動します。

MSDP のフィンガープリントについて

NetBackup は、一意の識別子を使って、バックアップする各ファイルと各ファイルセグメントを識別します。重複排除プラグインは、バックアップイメージを読み込み、これらのイメージを複数のファイルに分けます。プラグインはファイルをセグメントに分割します。各セグメントについて、プラグインは各データセグメントを識別するハッシュキー (またはフィンガープリント) を計算します。ハッシュを作成するために、セグメント内のデータのバイトがすべて読み込まれ、ハッシュに追加されます。

データの暗号化と保護が最高水準で行われるように、NetBackup は 8.1 リリースより AES 暗号化アルゴリズムと SHA-2 指紋アルゴリズムを導入しています。具体的には、MSDP は AES-256 および SHA-512/256 を使用します。

MSDP フィンガープリントのキャッシュについて

NetBackup はフィンガープリントを使ってバックアップデータのファイルセグメントを識別します。NetBackup はメディアサーバー重複排除プールに一意のデータセグメントのみを書き込みます。セグメントがすでにストレージにある場合、NetBackup は再格納しません。

p.72 の「MSDP のフィンガープリントについて」を参照してください。

ストレージサーバーは RAM のフィンガープリントのインデックスキャッシュを保持します。各バックアップジョブについては、サーバーからの最後のバックアップのフィンガープリントのリストをクライアントが要求します。

NetBackup 重複排除エンジンは (spoold) は、起動時にフィンガープリントのパーセントをキャッシュにロードします。起動後に、エンジンは残りのフィンガープリントをロードします。

キャッシュのロード動作を構成できます。

p.73 の「MSDP フィンガープリントのキャッシュ動作の構成」を参照してください。

また、クライアントへのフィンガープリントのキャッシュシーディングを制御できます。

p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。

MSDP フィンガープリントのキャッシュ動作の構成

キャッシュのロード動作を構成できます。

p.72 の「MSDP フィンガープリントのキャッシュについて」を参照してください。

p.190 の「MSDP contentrouter.cfg ファイルについて」を参照してください。

MSDP フィンガープリントのキャッシュ動作を構成するには

1. ストレージサーバーで、テキストエディタで `contentrouter.cfg` ファイルを開きます。それは次のディレクトリに存在します。
   - (UNIX) *storage_path*`/etc/puredisk`
   - (Windows) *storage_path*`¥etc¥puredisk`
2. 動作を制御するパラメータを編集します。

   p.73 の「MSDP フィンガープリントキャッシュの動作オプション」を参照してください。

MSDP フィンガープリントキャッシュの動作オプション

表 4-8 に、動作を制御するパラメータを示します。これらのオプションはすべて `contentrouter.cfg` ファイルにあります。

パラメータは `contentrouter.cfg` ファイルに格納されます。

p.190 の「MSDP contentrouter.cfg ファイルについて」を参照してください。

表 4-8　キャッシュロードパラメータ

動作	説明
`CacheLoadThreadNum`	残りのフィンガープリントをロードするのに使うスレッドの数。 `CacheLoadThreadNum` ファイル内の `contentrouter.cfg` は、スレッド数を制御します。NetBackup は、起動時にフィンガープリントをロードした後、次のコンテナ番号からフィンガープリントのロードを開始します。 デフォルトは 1 です。

動作	説明
MaxCacheSize	フィンガープリントキャッシュに使用する RAM の割合。 contentrouter.cfg ファイル内の MaxCacheSize は、RAM の割合を制御します。 デフォルト値は 50% です。 **メモ:** P/S キャッシュを使用する場合は、次の行で説明する UsableMemoryLimit パラメータを使用します。
UsableMemoryLimit	P/S キャッシュを使用するシステムの場合、ローカルボリュームとクラウドボリュームは同じ S キャッシュと P キャッシュのサイズを共有し、メモリ全体は UsableMemoryLimit によって制限されます。

リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて

Cohesity は新しいクライアント用のフィンガープリントキャッシュをシードする方法を提供します。シード処理が最も効果的な使用例は WAN のような大きな遅延のあるネットワーク上のリモートクライアントの最初のバックアップです。最初のバックアップのパフォーマンスは既存のクライアントのパフォーマンスに類似します。

キャッシュをシード処理するクライアントを考慮することが重要です。類似するクライアントを選択するときは次の点を考慮します。

- 情報のほとんどがオペレーティングシステムファイルの場合は、同じオペレーティングシステムを持つクライアントを使います。
- 情報のほとんどがデータの場合は、同じデータを持つクライアントを見つけられないことがあります。したがって、データセンターにデータのコピーを物理的に移動することを検討します。類似するクライアント上でそのデータをバックアップしてから、シード処理するクライアントとポリシーを使います。
- クライアントが類似しているほど、キャッシュのヒット率は大きくなります。

キャッシュのシード処理を構成するには 2 つの方法があります。どちらかの方法を使うことができます。次の表でシード処理の構成方法を説明します。

表 4-9　シード処理の構成方法

シード処理を構成するホスト	説明
クライアント	1 つまたは少数のクライアントのみのためのクライアント上でシード処理を構成します。 p.77 の「クライアントでの MSDP フィンガープリントキャッシュのシードの構成」を参照してください。
ストレージサーバー上	シード処理するクライアントが多く、1 つのホストからフィンガープリントキャッシュを使うような使用例が最大の利点を得ることができます。 p.78 の「ストレージサーバーでの MSDP フィンガープリントキャッシュのシードの構成」を参照してください。

NetBackup でシード値を設定したバックアップイメージを使うには、シード値を設定した後のクライアントの初回バックアップで単一ストリームの完全バックアップを作成する必要があります。具体的には、バックアップポリシーで次の 2 つの条件を満たす必要があります。

- [属性(Attributes)]ページにある[複数のデータストリームを許可する(Allow multiple data streams)]属性のチェックマークをはずす必要があります。
- バックアップ選択項目に、NEW_STREAM 指示句を含めることはできません。

これら 2 つの条件を満たしていない場合には NetBackup は複数のストリームを使うことがあります。[属性(Attributes)]ページにある[ポリシーごとにジョブ数を制限する(Limit jobs per policy)]をストリームの合計数より小さい数値に設定すると、これらのストリームでのみシード値を設定したイメージを使ってキャッシュをポピュレートします。[ポリシーごとにジョブ数を制限する(Limit jobs per policy)]の値より大きい値のストリームは、シード値を設定してもメリットがなく、キャッシュのヒット率は 0 % 近くになることがあります。

最初のバックアップ後に、元のバックアップポリシーパラメータの設定をリストアできます。

シードが発生したことを示す情報メッセージの例を以下に示します。

アクティビティモニターに表示されるジョブの詳細

```
1/2/2015 2:18:23 AM - Info nbmaster1(pid=6340)
StorageServer=PureDisk:nbmaster1; Report=PDDO
Stats for (nbmaster1): scanned: 3762443 KB, CR
sent: 1022 KB, CR sent over FC: 0 KB, dedup:
100.0%, cache hits: 34364 (100.0%)

1/2/2015 2:18:24 AM - Info nbmaster1(pid=6340)
StorageServer=PureDisk:nbmaster1; Report=PDDO
Stats for (nbmaster1): scanned: 1 KB, CR sent:
0 KB, CR sent over FC: 0 KB, dedup: 100.0%
```

クライアント上の重複排除プラグインログ (pdplugin.log)

```
01/02/15 02:15:17 [4452] [4884] [DEBUG] PDSTS:
cache_util_get_cache_dir: enter
db=/nbmaster1#1/2, scp='', bc=host1,
bp=seedfinal, bl=4096

01/02/15 02:15:17 [4452] [4884] [DEBUG] PDSTS:
cache_util_get_cache_dir: new backup, using
existing client seeding directory

01/02/15 02:15:17 [4452] [4884] [DEBUG] PDSTS:
cache_util_get_cache_dir: exit
db=/nbmaster1#1/2, scp='', bc=host1,
bp=seedfinal, bl=4096,
cachedir_buf='/nbmaster1#1/2/#pdseed/host1'
err=0
```

p.720 の「NetBackup MSDP ログファイル」を参照してください。

クライアント上の重複排除プロキシサーバーログ (nbostpxy.log)

```
02:15:17.417 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_get_cache_dir: enter
db=/nbmaster1#1/2, scp='', bc=host1,
bp=seedfinal, bl=4096

02:15:17.433 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_load_fp_cache_nbu: enter
dir_path=/nbmaster1#1/2/#pdseed/host1, t=16s,
me=1024

02:15:17.449 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_load_fp_cache_nbu: adding
'nbmaster1_1420181254_C1_F1.img' to cache list
(1)

02:15:17.449 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_load_fp_cache_nbu: opening
/nbmaster1#1/2/#pdseed/host1/nbmaster1_1420181254_C1_F1.img
for image cache (1/1)

02:15:29.585 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDVFS: pdvfs_lib_log: soRead: segment
c32b0756d491871c45c71f811fbd73af already
present in cache.

02:15:29.601 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDVFS: pdvfs_lib_log: soRead: segment
346596a699bd5f0ba5389d4335bc7429 already
present in cache.
```

p.720 の「NetBackup MSDP ログファイル」を参照してください。

p.72 の「MSDP フィンガープリントのキャッシュについて」を参照してください。

クライアントでの MSDP フィンガープリントキャッシュのシードの構成

クライアントのシードには、次が必要です。

- クライアント名
- ポリシー名
- 類似するクライアントのフィンガープリントキャッシュの使用を停止する日付

このシード方法をいつ使うかや、シードが利用可能なクライアントの選択方法についての情報。

p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。

警告: ストレージサーバーまたは負荷分散サーバー上ではこの手順を使わないでください。この手順を使うと、そのホストによってバックアップされるすべてのクライアントに影響します。

クライアントで MSDP フィンガープリントキャッシュをシードする方法

◆ リモートクライアントの最初のバックアップの前に、リモートクライアントの `FP_CACHE_CLIENT_POLICY` ファイルの `FP_CACHE_CLIENT_POLICY` パラメータを編集します。

次の形式で設定を指定します。

clienthostmachine,*backuppolicy*,*date*

clienthostmachine	キャッシュをシードする既存の類似クライアントの名前。 **メモ:** NetBackup では長い形式のホスト名と短い形式のホスト名は別のものとされるため、バックアップするポリシーに表示されるクライアント名を使用するようにします。
backuppolicy	そのクライアントのバックアップポリシー。
date	既存の類似クライアントからのフィンガープリントキャッシュを使う yyyy/mm/dd 形式の最新の日付。この日付の後、NetBackup はクライアント自体のバックアップからのフィンガープリントを使います。

p.175 の「MSDP pd.conf ファイルの編集」を参照してください。
p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

ストレージサーバーでの MSDP フィンガープリントキャッシュのシードの構成

ストレージサーバーでは、NetBackup `seedutil` ユーティリティによってクライアントの特別なシードディレクトリが作成されます。イメージ参照のシードディレクトリを別のクライアントとポリシーのバックアップイメージに事前設定します。シードディレクトリのパス名は次のとおりです。

`database_path``/databases/catalog/2/#pdseed/`*`client_name`*

デフォルトで、NetBackup ではストレージとカタログに同じパスが使用されます。*`database_path`* と *`storage_path`* は同じです。重複排除データベースに対し別のパスを構成する場合、パスは異なります。)

バックアップを実行する場合、NetBackup はクライアントの `#pdseed` ディレクトリからフィンガープリントをロードします(通常のカタログの場所にあるそのクライアントにフィンガープリントがないと想定)。

このシード方法をいつ使うかや、シードが利用可能なクライアントの選択方法についての情報。

p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。

ストレージサーバーからフィンガープリントキャッシュをシードする方法

1. リモートクライアントの最初のバックアップの前に、次の形式でクライアントとポリシーを指定します。

   UNIX の場合: `/usr/openv/pdde/pdag/bin/seedutil -seed -sclient` *`client_name`* `-spolicy` *`policy_name`* `-dclient` *`destination_client_name`*

   Windows の場合: *`install_path`*`¥Veritas¥pdde¥seedutil -seed -sclient` *`client_name`* `-spolicy` *`policy_name`* `-dclient` *`destination_client_name`*

   メモ: NetBackup では長い形式のホスト名と短い形式のホスト名は別のものとされるため、バックアップするポリシーに表示されるクライアント名を使用するようにします。

   p.79 の「NetBackup seedutil オプション」を参照してください。

2. フィンガープリントを使ってシードするクライアントごとにこのコマンドを繰り返します。
3. クライアントのシードディレクトリが次のコマンドを使って作成されたことを検証します。

   `seedutil -list_clients`

4 クライアントをバックアップします。

5 クライアントのバックアップ後に、クライアントのシードディレクトリを削除します。コマンドの構文は次のとおりです。

```
seedutil -clear client_name
```

クライアントの 1 つの完全バックアップの後、NetBackup ではシードディレクトリが自動的に消去されます。最初のバックアップが失敗すると、シードされたデータはそのまま残り、バックアップが連続的に試行されます。NetBackup でシードディレクトリが自動的に消去されますが、Cohesity ではクライアントシードディレクトリを手動で消去することを推奨します。

NetBackup seedutil オプション

次に、seedutil ユーティリティの使用方法の説明を示します。

```
seedutil [-v log_level] [-seed -sclient source_client_name -spolicy
policy_name -dclient destination_client_name [-backupid backup_id]]
[-clear client_name] [-clear_all] [-list_clients] [-list_images
client_name] [-dsid] [-help]
```

次の項目はオプションです。

-backupid *backup_id*	シードのためにデータをコピーするバックアップ ID。
-clear *client_name*	*client_name* で指定されたシードディレクトリの内容を消去します。
-clear_all	すべてのシードディレクトリの内容を消去します。
-dclient *destination_client_name*	データをシードしている新しいクライアントの名前。
-dsid	データ選択 ID。
-help	コマンドのヘルプを表示します。
-list_clients	シードのために構成されたクライアントをすべてリストします。
-list_images *client_name*	指定されたクライアントのシードディレクトリの内容をリストします。

-sclient *source_client_name*	シードのためにデータをコピーするクライアント。 **メモ:** NetBackup では長い形式のホスト名と短い形式のホスト名は別のものとされるため、バックアップするポリシーに表示されるクライアント名を使用するようにします。
-seed	シードを構成します。
-spolicy *policy_name*	シードデータに使用するクライアントをバックアップした NetBackup ポリシー。
-v *log_level*	ログレベル。

コマンドが存在するディレクトリは次のとおりです。

- UNIX の場合: `/usr/openv/pdde/pdag/bin`
- Windows の場合: `C:¥Program Files¥Veritas¥pdde`

サンプリングと予測キャッシュについて

MSDP は、効率的な重複排除のルックアップのために指紋をキャッシュする目的で、`MaxCacheSize` で構成されたサイズを上限としてメモリを使用します。NetBackup リリース 10.1 で導入された新しい指紋キャッシュのルックアップデータスキームによって、メモリの使用量が減少します。これにより、現在のメモリキャッシュは、サンプリングキャッシュ (S キャッシュ) と予測キャッシュ (P キャッシュ) の 2 つのコンポーネントに分割されます。S キャッシュは、各バックアップから指紋の一部をキャッシュに保存し、重複排除の以前のバックアップのサンプルから類似データを見つけるのに使用されます。P キャッシュは、重複排除のルックアップのために近い将来使用される可能性が高い指紋をキャッシュに保存します。

ジョブの開始時に、前回のバックアップから指紋の一部が初回シードとして P キャッシュにロードされます。指紋のルックアップは重複を見つけるために P キャッシュを使用して行われます。ルックアップミスが S キャッシュのサンプルで検索され、前回のバックアップデータに一致がないかどうかが検索されます。一致が検出されると、そのバックアップの指紋の一部が将来の重複排除のために P キャッシュにロードされます。

S キャッシュと P キャッシュによる指紋のルックアップ方法は、MSDP の非 BYO 配備 (Flex、Flex Worm、Flex Scale、NetBackup Appliance、AKS、EKS の配備を含む) を使用するローカルおよびクラウドのストレージボリュームで有効になっています。この方法は、MSDP BYO プラットフォームのクラウドのみのボリュームでも有効です。クラウドのみのボリュームをサポートするプラットフォームの場合、ローカルボリュームでは元のキャッシュルックアップ方法が引き続き使用されます。S キャッシュと P キャッシュの構成パラメータは、構成ファイル `contentrouter.cfg` の `Cache` セクションにあります。

NetBackup 10.2 以降、ローカルストレージの S キャッシュと P キャッシュの指紋ルックアップ方式は、Flex、Flex WORM、NetBackup Appliance の新しい設定で使用されます。アップグレードしても、S キャッシュと P キャッシュの指紋のルックアップ方式は変更されません。

S キャッシュと P キャッシュのデフォルト値:

構成	デフォルト値
`MaxCacheSize`	512MiB
`MaxPredictiveCacheSize`	40%
`MaxSamplingCacheSize`	20%
`contentrouter.cfg` の `EnableLocalPredictiveSamplingCache`	`true`
`spa.cfg` の `EnableLocalPredictiveSamplingCache`	`true`

P/S キャッシュを使用するシステムの場合、ローカルボリュームとクラウドボリュームは同じ S キャッシュと P キャッシュのサイズを共有し、メモリ全体は `UsableMemoryLimit` によって制限されます。

S キャッシュのサイズは、バックエンドの MSDP 容量またはバックエンドデータからの指紋の数によって決まります。セグメントの平均サイズを 32 KB と仮定する場合、S キャッシュのサイズはバックエンド容量の TB あたり約 100 MB です。P キャッシュのサイズは、同時実行ジョブの数、データの局所性、または受信データの作業セットによって決まります。作業セットはストリームあたり 250 MB (約 500 万の指紋) です。たとえば、100 の同時実行ストリームには 25 GB (100*250 MB) のメモリが最低限必要です。複数のストリームや大きいデータセットを伴う特定のアプリケーションでは、作業セットが大きくなる場合があります。指紋の重複排除ルックアップに P キャッシュが使用され、ロードされたすべての指紋は割り当てられた容量に達するまで P キャッシュに保持されるため、P キャッシュのサイズが大きいほど、ルックアップのヒット率は向上し、メモリ使用量も増えます。S キャッシュまたは P キャッシュのサイズを小さくすると重複排除率が低下し、大きくするとメモリコストが増加します。

サンプリングキャッシュの再構築

MSDP をアップグレードしても、指紋検索方法は変わりません。新しい指紋検索方法の予測キャッシュとサンプリングキャッシュを使用する場合は、手動で構成できます。保守期間中にサンプリングキャッシュを再構築するには、`rebuild_scache` スクリプトを使用します。ローカルの BYO、Flex、Flex Worm 環境で予測キャッシュとサンプリングキャッシュを手動で有効にすると、アップグレード後の環境でローカルの重複排除率が向上します。

スクリプトは次の場所に格納されます。

- UNIX の場合: `/usr/openv/pdde/pdag/scripts/rebuild_scache.sh`
- Windows の場合: `install_path¥Veritas¥pdde¥rebuild_scache.bat`

ログレベルを指定する必要はありません。ログは次の場所に保存されます。

- UNIX の場合: /var/log/puredisk/<date and time>-rebuild-scache.log
- Windows の場合: C:¥rebuild-scache.log

スクリプトを実行してサンプリングキャッシュを再構築する場合は、次の推奨事項を考慮してください。

- アップグレード後、バックアップタスクを実行する直前にこのスクリプトを実行して、サンプリングキャッシュを再構築します。
- スクリプトの実行時に、予測キャッシュとサンプリングキャッシュが有効になっていることを確認します。
- MSDP 環境とユニバーサル共有環境の S3 インターフェースでは、サンプリングキャッシュの再構築が重複排除率に影響することがあります。
- スクリプトの実行はすべてのバックアップジョブに影響するため、再構築の処理中にこれらが失敗するとバックアップジョブが実行されません。
  再構築処理の完了後にバックアップジョブを実行できない場合は、MSDP を再起動します。
- スクリプトが開始されたら、スクリプトが正常に実行されたことを確認します。何らかの理由で途中で終了した場合は、スクリプトを再実行します。
- 再構築処理中にエラーが発生した場合は、スクリプトを再実行します。

アップグレード後にサンプリングキャッシュを再構築するには

1. `contentrouter.cfg` と `spa.cfg` で予測キャッシュとサンプリングキャッシュを有効にします。

   p.80 の「サンプリングと予測キャッシュについて」を参照してください。

2. ストレージサーバーで、スクリプトを実行します。

   UNIX の場合: `/usr/openv/pdde/pdag/scripts/rebuild_scache.sh`

   Windows の場合: `install_path¥Program Files¥Veritas¥bin¥rebuild_scache.bat`

3. `y` と入力し、Enter キーを押して続行します。ジョブの状態に関する警告が表示されます。

4. `y` と入力し、Enter キーを押して、再構築するプロセスを開始します。スクリプトにより、再構築の状態と進捗率が表示されます。

Flex Worm 環境では、重複排除シェルを使用してサンプリングキャッシュの再構築を開始します。

重複排除シェルからサンプリングキャッシュを再構築するには

1 サーバーへの SSH セッションを開きます。

2 最初のサンプリングキャッシュの再構築について次のコマンドを実行します。

```
setting rebuild-scache rebuild-sampling-cache
```

3 サンプリングキャッシュの再構築の状態を確認します。

```
setting rebuild-scache rebuild-sampling-cache-status
```

MSDP での 400 TB のサポートの有効化

400 TB メディアサーバー重複排除プールにストレージサーバーを構成する前に、必要な複数のボリュームのサポートを有効にする必要があります。

p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。

p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。

400 TB MSDP サポート用データディレクトリの作成

NetBackup では、各ストレージボリュームに `data` という名前が付いたディレクトリが含まれている必要があります。

400 TB サポートに必要な 2 つ目と 3 つ目のボリュームに `data` ディレクトリを作成する必要があります (NetBackup は必要な `data` ディレクトリをボリュームに作成します。このボリュームは[ストレージサーバーの構成ウィザード (Storage Server Configuration Wizard)]で指定します)。

前提条件

- ボリュームは、NetBackup で MSDP に対してサポートされているファイルシステムでフォーマットし、ストレージサーバーでマウントする必要があります。
  p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。
- ストレージサーバーはすでに構成されている必要があります。
  p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。

400 TB MSDP サポート用データディレクトリを作成するには

◆ メディアサーバー重複排除プール用の 2 つ目のボリュームと 3 つ目のボリュームで、次のように、ボリュームのマウントポイントに data サブディレクトリを作成します。

mount_point/data

次に、3 つの必要なストレージボリュームに対するマウントポイントの例を示します。

```
/msdp/vol0  <--- Netbackup creates the data directory in this
volume
/msdp/vol1  <--- Create a data directory in this volume
/msdp/vol2  <--- Create a data directory in this volume
```

400 TB メディアサーバー重複排除プールへのボリュームの追加

400 TB メディアサーバー重複排除プールにストレージサーバーを構成する場合、最初のストレージボリュームのパス名を指定します。メディアサーバー重複排除プールを使用する前に、その他の 2 つのボリュームをディスクプールに追加する必要があります。

次に、400 TB MSDP にボリュームを追加するためのハードウェアの最小要件を示します。

- CPU: クロックレート 2.4 GHz 以上の 64 ビットプロセッサが必要です。最低 8 つのコアが必要です。16 コアを推奨します。
- メモリ: 256 GB 以上。同じメディアサーバーによって実行される追加の役割がある場合は、メモリを追加する必要がある場合があります。たとえば、メディアサーバーが VMware バックアップホスト、NDMP バックアップエージェント、プライマリサーバーとして使用される場合があります。
- スワップ: 64 GB
- ストレージ:
  - メタデータディスク: RAID 0+1 を推奨します。少なくとも 1 TB の容量が必要です。
  - Cohesity では 8 つのマウントポイント (各マウントポイントに個別の RAID グループが必要) を推奨します。RAID 6 を推奨します。メタデータディスクとデータディスクの両方に 250 MB/秒を超える読み取りまたは書き込み速度が必要です。
  - ファイルシステム: NetBackup は VxFS、XFS、Ext4 をサポートしますが、推奨されるのは VxFS です。ストレージボリュームの数は設定環境に応じて異なります。ストレージ領域の最大容量は 400 TB です。次の手順では、それぞれ 50 TB の 8 つのファイルシステムを例として使用します。

p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。

p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。

400 TB のメディアサーバー重複排除プールにボリュームを追加するには

1 MSDP ストレージサーバーで、新しいストレージボリュームを作成、フォーマット、およびマウントする必要があります。いずれかのストレージボリュームに 1 TB 以上のストレージ領域が必要です (このストレージはメタデータ用です)。それ以外のストレージボリュームのストレージ領域は最大 400 TB です。

次の手順では、それぞれ 50 TB の 8 つのファイルシステムを例として使用します。

メモ: ストレージボリュームの数は設定環境に応じて異なります。ストレージ領域の最大容量は 400 TB です。

---

2 次の場所で、1 TB のストレージボリューム (メタデータ用) をマウントします。

```
/msdp/cat
```

3 次の場所で、8 つのストレージボリュームをマウントします。

```
/msdp/vol1
...
/msdp/vol8
```

4 touch ファイルを `/etc/nbapp-release` に作成します (まだ作成していない場合)。

5 マウントされた各ボリュームの下に `data` という名前のサブディレクトリを作成します。

```
/msdp/vol1/data
...
/msdp/vol8/data
```

6 ストレージサーバーの構成ウィザードを使用して MSDP を構成し、[重複排除データベースの代替パスを使用 (Use alternate path for deduplication database)]オプションにチェックマークが付いていることを確認します。

7 ストレージパスに `/msdp/vol1/`、データベースパスに `/msdp/cat` を指定します。

8 重複排除プールにさらに 50 TB のストレージボリュームを追加します。

```
/usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition
/msdp/vol2/data
...
/usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition
/msdp/vol8/data
```

root 以外のユーザーが NetBackup メディアサーバーに使用されている場合は、次のコマンドを実行して、新しく作成されたボリュームの所有者を NetBackup メディアサーバーのサービスユーザーに変更します。

```
chown -R <NBU-service-user>:root <MSDP-volume-path>
```

9 次のコマンドを使用して、重複排除プールに新しいボリュームが含まれていることを確認します。

```
/usr/openv/pdde/pdcr/bin/crcontrol --dsstat 2 | grep Mount
Mount point count: 8
```

Windows MSDP サーバーでの 400 TB の構成

400 TB のサポートを有効にするには、次のファイルを作成します。

```
mkdir c:¥etc
echo Windows_BYO > "c:¥¥etc¥¥nbapp-release"
```

Windows に関するサイズの推奨値は Linux の場合と同じです。いずれかのストレージボリュームに 1 TB のストレージ領域が必要です。それ以外のストレージボリュームのストレージ領域は最大 400 TB です。Windows の場合は、さらにいくつかの要件があります。

- `<MSDP Storage DIR>¥etc¥puredisk¥contentrouter.cfg` ファイルの `DCHeaderHashSize` 設定は `2000000 / number_of_volumes` に変更する必要があります。たとえば、8 つのマウントポイントすべてについて、`DCHeaderHashSize` を 250000 に設定します。
- 使用するボリュームは、文字ドライブ (C: または E:) ではなく、ネストされたボリュームとして存在する必要があります。Cohesity は、NTFS ボリュームを使用してこのソリューションを認定します。

ボリュームレイアウトの例を次に示します。各 `data#` ディレクトリはネストされたマウントです。

```
"msdp_data" :["f:/msdp/data1" ,"f:/msdp/data2" ,"f:/msdp/data3" ,
"f:/msdp/data4","f:/msdp/data5","f:/msdp/data6", "f:/msdp/data7"],
"f:/msdp/data8"],
"msdp_cat" :["f:/msdp/cat" ]
```

crcontrol 構文は Linux と同じです。Windows の場合、crcontrol は <INSTALL_DRIVE>¥Program Files¥Veritas¥pdde¥ にあります。例:

```
C:¥Program Files¥Veritas¥pdde¥crcontrol --dsaddpartition f:¥msdp¥data2
```

メモ: MSDP ストレージ容量には最大値が定義されています。これらの設定に従わない場合、データがすべてのボリューム間で分散されないため、パフォーマンス関連の問題が発生する可能性があります。

MSDP ストレージ容量について詳しくは、次のセクションを参照してください。

p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。

メモ: NetBackup は、最大 400 TB のプールサイズをサポートします。プールのサイズを小さくし、後でボリュームを追加することで拡張することも可能です。

メディアサーバー重複排除プールのストレージサーバーの構成

ここで言う構成とは、メディアサーバー重複排除プールのストレージサーバーとして NetBackup メディアサーバーを構成することを意味します。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

ストレージの形式。	ディスクストレージの形式に対して[メディアサーバー重複排除プール (Media Server Deduplication Pool)]を選択します。
Deduplication Engine のクレデンシャル。	p.39 の「NetBackup Deduplication Engine のクレデンシャルについて」を参照してください。
ストレージのパス。	p.89 の「MSDP のストレージパスのプロパティ」を参照してください。
ネットワークインターフェース。	p.40 の「MSDP のネットワークインターフェースについて」を参照してください。
負荷分散サーバー (存在する場合)。	p.33 の「MSDP ストレージサーバーについて」を参照してください。

ストレージサーバーを構成するとき、ウィザードでディスクプールとストレージユニットを作成することもできます。

前提条件

96-TB メディアサーバー重複排除プールの場合、ストレージサーバーを構成する前に必要なディレクトリを作成する必要があります。

p.83 の「400 TB MSDP サポート用データディレクトリの作成」を参照してください。

メディアサーバー重複排除プールの NetBackup ストレージサーバーを構成する方法

1. Web UI を開きます。
2. 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。[ストレージサーバー (Storage servers)]タブを選択し、[追加 (Add)]をクリックします。
3. [ストレージ形式 (Storage type)]リストで、[ディスクストレージサーバー (Disk storage servers)]を選択します。
4. [カテゴリ (Category)]のオプションから、[メディアサーバー重複排除プール (MSDP, MSDP Cloud, MVG) (Media Server Deduplication Pool (MSDP, MSDP Cloud, MVG))]を選択します。
5. [開始 (Start)]をクリックします。
6. [基本プロパティ (Basic properties)]タブで、適切な情報を選択または入力します。

メディアサーバー (Media server)	ストレージサーバーとして構成するメディアサーバーを選択します。 次のウィザードパネルで重複排除負荷分散サーバーを追加できます。
ユーザー名 (Username)	NetBackup Deduplication Engine のユーザー名を入力します。 p.39 の「NetBackup Deduplication Engine のクレデンシャルについて」を参照してください。
パスワード (Password)	NetBackup 重複排除エンジンのパスワードを入力します。
パスワードを再入力してください。(Re-enter password)	パスワードを確認するために、パスワードを再入力します。

7. [ストレージサーバーのオプション (Storage server options)]ページで、[ストレージパス (Storage path)]にストレージパスを検索または入力します。
8. [重複排除データベースの代替パスの使用 (Use alternate path for deduplication database)]フィールドに代替パスを入力します。
9. [特定のネットワークインターフェースを使用する (Use specific network interface)]フィールドに、インターフェースを入力します。

10 必要に応じて、[暗号化を有効にする (Enable encryption)]チェックボックスにチェックマークを付けます。

11 [次へ (Next)]をクリックします。

12 [メディアサーバー (Media servers)]ページで、[追加 (Add)]をクリックします。

13 追加のメディアサーバーを選択します。

14 [追加 (Add)]をクリックします。

15 [次へ (Next)]をクリックします。

16 [確認 (Review)]ページで、すべての情報を確認して[保存 (Save)]をクリックします。

MSDP のストレージパスのプロパティ

NetBackup では、ストレージがディレクトリパスとして公開されている必要があります。次の表に、ストレージサーバーの[メディアサーバー重複排除プール (Media Server Deduplication Pool)]のストレージパスのプロパティを示します。

表 4-10 MSDP のストレージパスのプロパティ

プロパティ	説明

ストレージパス (Storage path)	ストレージのパス。ストレージパスは NetBackup が未加工のバックアップデータを保存するディレクトリです。バックアップデータはシステムディスクに保存しないでください。
	
	ストレージにはディレクトリパスが必要であるため、ルートノード (/) またはドライブ文字 (E:¥) のみをストレージパスとして使わないでください。つまり、ストレージを root ノード (/) またはドライブ文字 (E:¥) としてマウントしないでください。
	
	400 TB のメディアサーバー重複排除プールでは、最初の 32 TB のストレージボリュームと見なしているボリュームのマウントポイントのパス名を入力する必要があります。次に、バックアップのマウントポイントのボリューム命名規則の例を示します。
	
	`/msdp/vol0  <--- The first volume`
	`/msdp/vol1`
	`/msdp/vol2`
	
	NetBackup は、サポート対象のシステムのサブセットで 400 TB の重複排除プールをサポートします。
	
	『NetBackup 重複排除ガイド』を参照してください。
	
	p.26 の「MSDP の容量のサポートとハードウェア要件について」を参照してください。
	
	p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。
	
	p.83 の「400 TB MSDP サポート用データディレクトリの作成」を参照してください。
	
	ストレージパス名には、次の文字を使用できます。
	
	■ 国際標準化機構 (ISO) のラテン文字アルファベット 26 文字の大文字と小文字の両方。これらは英語のアルファベットと同じ文字です。
	■ 0 から 9 までの整数。
	■ 空白文字。
	■ 次のいずれかの文字:
	UNIX: `_-:./¥`
	Windows の場合: `_-:.¥` (コロン (:) はドライブ文字の後にのみ許可されます (たとえば、`G:¥MSDP_Storage`))
	
	重複排除ストレージパスの NetBackup の必要条件はストレージの表示方法に影響することがあります。
	
	『NetBackup 重複排除ガイド』を参照してください。
	
	p.28 の「MSDP ストレージと接続性の必要条件について」を参照してください。

プロパティ	説明
重複排除データベースに代替パスを使用 (Use alternate path for deduplication database)	デフォルトでは、NetBackup は MSDP データベースの場所 (MSDP カタログ) のストレージパスを使います。MSDP データベースは、NetBackup カタログとは異なります。 重複排除データベースにデフォルト以外の場所を使用するには、このオプションを選択します。 400 TB のメディアサーバー重複排除プールでは、このオプションを選択する必要があります。 p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。 『NetBackup 重複排除ガイド』を参照してください。 パフォーマンスの最適化のために、重複排除データベースにバックアップデータとは別のディスクボリュームを使用することをお勧めします。
データベースパス (Database Path)	[重複排除データベースに代替パスを使用 (Use alternate path for deduplication database)] を選択した場合は、データベースのパス名を入力します。データベースはシステムディスクに保存しないでください。 400 TB のメディアサーバー重複排除プールでは、MSDP カタログのために作成したパーティションのパス名を入力する必要があります。たとえば、マウントポイントの命名規則が */msdp/vol*x の場合は、MSDP カタログディレクトリに対して次のパスをお勧めします。 `/msdp/cat` 『NetBackup 重複排除ガイド』を参照してください。 p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。 パフォーマンスの最適化のために、重複排除データベースにバックアップデータとは別のディスクボリュームを使用することをお勧めします。 パス名には、次の文字を使用できます。 ■ 国際標準化機構 (ISO) のラテン文字アルファベット 26 文字の大文字と小文字の両方。これらは英語のアルファベットと同じ文字です。 ■ 0 から 9 までの整数。 ■ 空白文字。 ■ 次のいずれかの文字: UNIX: `_-:./¥` Windows の場合: `_-:.¥` (コロン (`:`) はドライブ文字の後 (たとえば、`F:¥MSDP_Storage`) のみ許可されます)

ディレクトリが存在しない場合、NetBackup はそれらを作成して必要なサブディレクトリ構造を追加します。ディレクトリが存在する場合、NetBackup は必要なサブディレクトリ構造をそれらに追加します。

注意: NetBackup によって重複排除ストレージサーバーが構成された後にパスを変更することはできません。したがって、重複排除されたバックアップデータの保存場所および保存方法を計画段階で決定してからパスを慎重に入力してください。

p.23 の「MSDP の配置計画」を参照してください。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

p.25 の「NetBackup 重複排除の宛先について」を参照してください。

MSDP ネットワークインターフェースのプロパティ

次の表で、メディアサーバー重複排除プールストレージサーバーのネットワークインターフェースプロパティについて説明します。

注意: NetBackup によって重複排除ストレージサーバーが構成された後にパスまたはネットワークインターフェースを変更することはできません。したがって、プロパティは慎重に入力します。

表 4-11 MSDP ネットワークインターフェースのプロパティ

プロパティ	説明
特定のネットワークインターフェースを使用する (Use specific network interface)	重複排除トラフィックのネットワークインターフェースを指定するには、このオプションを選択します。ネットワークインターフェースを指定しない場合、NetBackup はオペレーティングシステムのホスト名の値を使います。 p.40 の「MSDP のネットワークインターフェースについて」を参照してください。
インターフェース (Interface)	[特定のネットワークインターフェースを使用する (Use specific network interface)]を選択した場合は、インターフェース名を入力します。

NetBackup の重複排除用ディスクプールについて

NetBackup 重複排除のディスクプールは、重複排除されたバックアップデータのストレージを表します。NetBackup サーバーまたは NetBackup クライアントは、重複排除ディスクプールに格納されているバックアップデータを重複排除します。

重複排除のプールには次の 2 つの形式があります。

- NetBackup の[メディアサーバー重複排除プール (Media Server Deduplication Pool)]は、NetBackup メディアサーバーに接続されているディスクストレージを表します。NetBackup は、データの重複を排除し、ストレージをホスティングします。NetBackup では、重複排除プールを構成するディスクリソースの所有権が排他的である必要があります。これらのリソースを他のユーザーと共有した場合、NetBackup では重複排除プールの容量またはストレージのライフサイクルポリシーを正しく管理できません。

いくつの重複排除プールを構成するかは、ストレージ要件に依存します。次の表に示すように、最適化複製またはレプリケーションを使うかどうかにも依存します。

表 4-12　　複製またはレプリケーションのための重複排除プール

形式	要件
同じ NetBackup ドメイン内での最適化複製	同じドメインの最適化複製では以下の重複排除プールが必要になります。 ■ バックアップストレージ用に少なくとも 1 つのディスクプール。これが複製操作のソースになります。ソース重複排除プールは 1 つの重複排除ノードにあります。 ■ バックアップイメージのコピーを保存するためにもう 1 つのディスクプール。これが複製操作のターゲットになります。ターゲット重複排除プールは異なる重複排除ノードにあります。 p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。
異なる NetBackup ドメインへの自動イメージレプリケーション	自動イメージレプリケーションの重複排除プールはレプリケーションソースにもレプリケーションターゲットにもなれます。レプリケーションのプロパティは重複排除プールの目的を示します。重複排除プールはボリュームからレプリケーションのプロパティを継承します。 p.139 の「自動イメージレプリケーションのレプリケーショントポロジーについて」を参照してください。 自動イメージレプリケーションでは以下の重複排除プールが必要になります。 ■ レプリケーションソースのドメインに、少なくとも 1 つのレプリケーションソース重複排除プール。レプリケーションソース重複排除プールはバックアップの送信先となる重複排除プールです。ソース重複排除プールのバックアップイメージは 1 つまたは複数のリモートドメインの重複排除プールにレプリケートされます。 ■ 1 つまたは複数のリモートドメインに、少なくとも 1 つのレプリケーションターゲットの重複排除プール。レプリケーションターゲット重複排除プールはレプリケートソースのドメインで実行される複製操作のターゲットです。 p.134 の「NetBackup 自動イメージレプリケーションについて」を参照してください。

p.508 の「メディアサーバー重複排除プールのプロパティの変更」を参照してください。

p.507 の「メディアサーバー重複排除プールの属性の設定」を参照してください。

重複排除のディスクプールの構成

NetBackup［ストレージサーバーの構成ウィザード (Storage Server Configuration Wizard)］によりストレージサーバーの構成中にディスクプールを 1 つ構成できます。追加のディスクプールを構成するには、［ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)］を起動します。NetBackup ディスクプールを構成するには、あらかじめ NetBackup 重複排除ストレージサーバーが存在している必要があります。

p.92 の「NetBackup の重複排除用ディスクプールについて」を参照してください。

重複排除ディスクプールを構成するときに、次を指定します。

- ディスクプールの形式:
  - [メディアサーバー重複排除プール (Media Server Deduplication Pool)]は NetBackup 重複排除メディアサーバーに接続するディスクストレージを表します。
- プールに使うディスクストレージを問い合わせるための重複排除ストレージサーバー。
- プールに含めるディスクボリューム。
  NetBackup は単一のボリュームとしてストレージを表示します。
- ディスクプールのプロパティ。

Cohesity ディスクプールの名前は、企業全体にわたって一意にすることをお勧めします。

ウィザードを使用して重複排除ディスクプールを構成する方法

1. 管理コンソールで、[NetBackup の管理 (NetBackup Management)]または[メディアおよびデバイスの管理 (Media and Device Management)]を選択します。
2. 右ペインのウィザードのリストで、[ディスクプールの構成 (Configure Disk Pool)]をクリックします。
3. ウィザードの[ようこそ (Welcome)]パネルで[次へ (Next)]をクリックします。

   [ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]パネルが表示されます。
4. [ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]パネルで、[ストレージサーバー形式 (Storage server type)]ウィンドウで構成するディスクプール形式を選択します。

   [ストレージサーバー形式 (Storage server type)]ウィンドウでディスクプールを選択したら、[次へ (Next)]をクリックします。
5. [ストレージサーバーの選択 (Storage Server Selection)]パネルで、このディスクプールのストレージサーバーを選択します。ウィザードにより、環境で構成されている重複排除ストレージサーバーが表示されます。

   [次へ (Next)]をクリックします。
6. [ボリュームの選択 (Volume Selection)]パネルで、このディスクプールのボリュームを選択します。

メディアサーバー重複排除プール (Media Server Deduplication Pool)	[ストレージサーバーの構成ウィザード (Storage Server Configuration Wizard)]で構成したストレージパスのすべてのストレージが 1 つのボリュームとして公開されます。 PureDiskVolume はそのストレージの仮想名です。

   ボリュームを選択したら、[次へ (Next)]をクリックします。

7 [ディスクプールの追加情報 (Additional Disk Pool Information)]パネルで、このディスクプールの値を入力します。

適切な情報を入力するか、必要なオプションを選択した後、[次へ (Next)]をクリックします。

8 [ディスクプールの構成の概略 (Disk Pool Configuration Summary)]パネルで選択項目を確認します。選択項目が正しければ、[次へ (Next)]をクリックします。

ディスクプールを構成するには、[次へ (Next)]をクリックします。

9 [ディスクプールの構成の状態 (Disk Pool Configuration Status)]パネルには、操作の進捗状況が表示されます。

ディスクプールを作成すると次が行えます。

ストレージユニットの構成	[作成したディスクプールを使用してストレージユニットを作成する (Create a storage unit using the disk pool that you have just created)]を選択していることを確認してから[次へ (Next)]をクリックします。[ストレージユニットの作成 (Storage Unit Creation)]ウィザードパネルが表示されます。次の手順に進みます。
終了 (Exit)	[閉じる (Close)]をクリックします。 後から 1 つ以上のストレージユニットを構成できます。

10 [ストレージユニットの作成 (Storage Unit Creation)]パネルで、ストレージユニットに関する適切な情報を入力します。

適切な情報を入力するか、必要なオプションを選択した後、[次へ (Next)]をクリックしてストレージユニットを作成します。

11 NetBackup でストレージユニットの構成が完了すると、[完了 (Finished)]パネルが表示されます。[完了 (Finish)]をクリックしてウィザードを終了します。

p.506 の「メディアサーバー重複排除プールの属性の表示」を参照してください。

[メディアサーバー重複排除プール (Media Server Deduplication Pool)] プロパティ

表 4-13 では、ディスクプールのプロパティについて説明します。

表 4-13 ［メディアサーバー重複排除プール (Media Server Deduplication Pool)］プロパティ

プロパティ	説明
ストレージサーバー (Storage server)	ストレージサーバーの名前。ストレージサーバーは、ストレージが接続されている NetBackup メディアサーバーと同じです。
ストレージサーバー形式 (Storage server type)	メディアサーバー重複排除プールの場合、ストレージ形式は PureDisk です。
ディスクボリューム (Disk volumes)	メディアサーバー重複排除プールでは、すべてのディスクストレージは単一のボリュームとして公開されます。 PureDiskVolume はストレージパスとデータベースパスに指定したディレクトリ内に含まれているストレージの仮想名です。
合計利用可能領域 (Total available space)	ディスクプール内で利用可能な領域の量。
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 サイズの合計。
ディスクプール名 (Disk Pool name)	ディスクプールの名前。企業全体にわたって一意の名前を入力します。
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)］はボリュームに空きがないことを示します。ボリュームが［高水準点 (High water mark)］に到達すると、NetBackup はストレージユニットに割り当てられているバックアップジョブに失敗します。また、NetBackup は、重複排除プールに空きがないストレージユニットに新しいジョブを割り当てません。 ［高水準点 (High water mark)］は他のジョブにコミットされているがまだ使われていない領域を含んでいます。 デフォルトは 98% です。
低水準点 (Low Water Mark)	［低水準点 (Low water mark)］は PureDiskVolume に影響しません。

プロパティ	説明
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。このプロパティを選択したら、ボリュームごとに許可するストリームの数も構成します。 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。
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。

p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.92 の「NetBackup の重複排除用ディスクプールについて」を参照してください。

p.93 の「重複排除のディスクプールの構成」を参照してください。

p.505 の「メディアサーバー重複排除プールの管理」を参照してください。

p.25 の「NetBackup 重複排除の宛先について」を参照してください。

［メディアサーバー重複排除プール (Media Server Deduplication Pool)］ストレージユニットの構成

NetBackup 重複排除ストレージユニットは、いずれかのメディアサーバー重複排除プールにあるストレージを表します。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。

p.92 の「NetBackup の重複排除用ディスクプールについて」を参照してください。

ディスクプールを作成したときにストレージユニットを作成した可能性があります。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を構成する方法

1. NetBackup Web UI を開きます。
2. 左側で[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。
3. [追加 (Add)]をクリックします。
4. ウィザードの指示に従います。

   最適化された複製先のストレージユニットに、[次のメディアサーバーのみを使用 (Only use the following media servers)]を選択します。それから 2 つの重複排除ノード間で共通であるメディアサーバーを選択します。

   p.98 の「[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージユニットのプロパティ」を参照してください。

[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージユニットのプロパティ

[メディアサーバー重複排除プール (Media Server Deduplication Pool)]をターゲットとするストレージユニットの構成オプションを次に示します。

表 4-14 [メディアサーバー重複排除プール (Media Server Deduplication Pool)]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)	[PureDisk]を[メディアサーバー重複排除プール (Media Server Deduplication Pool)]のディスク形式として選択します。
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。

プロパティ	説明
メディアサーバー (Media server)	［メディアサーバー (Media server)］設定はこのストレージユニット用のデータを重複排除できる NetBackup メディアサーバーを指定します。重複排除ストレージサーバーと負荷分散サーバーのみがメディアサーバーのリストに表示されます。 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。
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、Cohesity では、重複排除パフォーマンスを最適化するために、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お勧めします。 詳しくは、『NetBackup NAS 管理者ガイド』および『NetBackup Snapshot Manager for Data Center 管理者ガイド』を参照してください。

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されます。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使用できなくなります。
WORM を使用	このオプションが、WORM 対応のストレージユニットに対して有効になっています。 WORM は、Write Once Read Many の略語です。 ［WORM のロック解除時間 (WORM Unlock Time)］まで、このストレージユニットのバックアップイメージを変更不可および削除不可にする場合は、このオプションを選択します。

p.53 の「MSDP のストレージユニットグループについて」を参照してください。

p.97 の「［メディアサーバー重複排除プール (Media Server Deduplication Pool)］ストレージユニットの構成」を参照してください。

MSDP ストレージユニットの推奨事項

ストレージユニットのプロパティを使用して、次のように NetBackup の実行方法を制御できます。

「クライアントとサーバーの最適比率の構成」

「メディアサーバーへのスロットル通信」

クライアントとサーバーの最適比率の構成

クライアントとサーバーの比率を最適にするには、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。

---

p.31 の「NetBackup メディアサーバー重複排除について」を参照してください。

p.97 の「[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージユニットの構成」を参照してください。

メディアサーバーへのスロットル通信

ディスクプールのストレージユニットの[最大並列実行ジョブ数 (Maximum concurrent jobs)]設定を使って、メディアサーバーへの通信をスロットルで調整することができます。また、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。

p.97 の「[メディアサーバー重複排除プール (Media Server Deduplication Pool)]ストレージユニットの構成」を参照してください。

MSDP クライアント側重複排除のクライアント属性の構成

クライアントの重複排除を構成にするには、NetBackup プライマリサーバーの[クライアント属性 (Client attributes)]ホストプロパティで属性を設定します。クライアントは、ストレージ宛先が[メディアサーバー重複排除プール (Media Server Deduplication Pool)]であるバックアップポリシーに従っている場合は、独自のデータの重複を排除します。

バックアップの重複排除を行うクライアントを指定する方法

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Host)]、[ホストプロパティ (Host properties)]の順に選択します。
3. 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. [クライアント属性 (Client attributes)]をクリックします。
6. [一般 (General)]タブで、[クライアント (Clients)]リストに独自のデータを重複排除するクライアントを追加します。
   - [追加 (Add)]をクリックします。
   - クライアント名を入力するか、クライアントを参照して選択します。次に[追加 (Add)]をクリックします。
     追加するクライアントごとに繰り返します。

7 特定のクライアントの重複排除の場所を選択するには、そのクライアントを選択します。

8 次の[重複排除場所 (Deduplication location)]オプションから 1 つ選択します。

- 常にメディアサーバーを使用 (Always use the media server) - クライアントの重複排除を無効にします。デフォルトでは、すべてのクライアントに[常にメディアサーバーを使用する (Always use the media server)]オプションが設定されます。
- クライアント側の重複排除を優先して使用 (Prefer to use client-side deduplication) - 重複排除プラグインがクライアントでアクティブな場合にクライアントの重複排除を使用します。それがアクティブでない場合は、通常のバックアップが実行されます。クライアントの重複排除は実行されません。
- 常にクライアント側の重複排除を使用 (Always use client-side deduplication) - クライアントの重複排除を使用します。重複排除バックアップジョブが失敗した場合、NetBackup はジョブを再試行します。

バックアップポリシーの[クライアント側の重複排除を使用する (Prefer to use client-side deduplication)]または[常にクライアント側の重複排除を使用する (Always use client-side deduplication)]ホストプロパティを上書きできます。

『NetBackup 管理者ガイド Vol. 1』の「クライアント側の重複排除」を参照してください。

p.103 の「クライアントについての MSDP クライアント側の重複排除の無効化」を参照してください。

p.36 の「NetBackup Client Direct の重複排除について」を参照してください。

p.20 の「NetBackup Deduplication のオプションについて」を参照してください。

クライアントについての MSDP クライアント側の重複排除の無効化

各自のデータを重複排除するクライアントのリストからクライアントを削除できます。削除すると、重複排除サーバーはクライアントをバックアップし、データを重複排除します。

クライアントの MSDP クライアント重複排除を無効にする方法

1 Web UI を開きます。

2 左側で、[ホスト (Host)]、[ホストプロパティ (Host properties)]の順に選択します。

3 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 [クライアント属性 (Client attributes)]をクリックします。

6 データを重複排除するクライアントを選択します。

7 ［重複排除 (Deduplication)］リストから、［常にメディアサーバーを使用 (Always use the media server)］を選択します。

8 ［保存 (Save)］をクリックします。

ポリシー内のすべてのクライアントについてクライアント側の重複排除を無効にする

あるポリシーについてクライアント側の重複排除の使用を無効にするには、［属性 (Attributes)］タブで［すべてのクライアントで無効 (Disable for all clients)］を選択する必要があります。

ポリシー内のすべてのクライアントについてクライアント側の重複排除を無効にするには

1 Web UI を開きます。

2 ［保護 (Protection)］、［ポリシー (Policies)］の順に選択します。

3 編集するポリシーをクリックします。

4 ［属性 (Attributes)］タブをクリックします。

5 ［クライアント側の重複排除 (Client-side deduplication)］を見つけ、［すべてのクライアントで無効 (Disable for all clients)］をクリックします。

6 ［保存 (Save)］をクリックします。

MSDP の圧縮について

NetBackup 重複排除ホストは、重複排除されたデータの圧縮機能を提供します。それは NetBackup のポリシーベースの圧縮とは別の、異なるものです。

圧縮は、デフォルトですべての MSDP ホストで構成されます。したがって、バックアップ、複製トラフィック、およびレプリケーショントラフィックは、すべての MSDP ホストで圧縮されます。データもストレージ上で圧縮されます。

表 4-15 に、圧縮オプションを示します。

別のトピックでは、MSDP の暗号化と圧縮の設定の相互作用について説明します。

表 4-15 MSDP の圧縮オプション

オプション	説明
バックアップのための圧縮	バックアップでは、重複排除された後のデータを重複排除プラグインが圧縮します。データは、プラグインからストレージサーバーの NetBackup 重複排除エンジンに圧縮されたまま転送されます。重複排除エンジンは、暗号化されたデータをストレージに書き込みます。リストアジョブのプロセスは逆方向に動作します。 各 MSDP ホストの pd.conf ファイルの COMPRESSION パラメータは、そのホストの圧縮と解凍を制御します。デフォルトでは、バックアップ圧縮はすべての MSDP ホストで有効になっています。したがって、圧縮と解凍は必要に応じて次のホストで実行されます。 ■ 自身のデータ(つまり、クライアント側の重複排除)を重複排除するクライアント。 ■ 負荷分散サーバー。 ■ ストレージサーバー。 MSDP 圧縮は、通常の NetBackup クライアント (つまり、自身のデータを重複排除しないクライアント) では実行できません。 **メモ:** [ポリシー (Policy)]ダイアログボックスの[属性 (Attributes)]タブの[圧縮 (Compression)]オプションを選択して圧縮を有効にしないでください。それを行うと、データを重複排除するプラグインにデータが達する前に NetBackup はデータを圧縮します。その結果、重複排除率は非常に低くなります。また、ポリシーベースの暗号化が構成されている場合、NetBackup は重複排除マルチスレッドエージェントを使いません。 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。
複製とレプリケーションの圧縮	複製とレプリケーションでは、重複排除プラグインは転送するデータを圧縮します。データは、プラグインからストレージサーバーの NetBackup 重複排除エンジンに圧縮されたまま転送され、ストレージに圧縮されたまま保存されます。 OPTDUP_COMPRESSIONpd.conf ファイルの パラメータは、複製とレプリケーションの圧縮を制御します。デフォルトでは、複製とレプリケーションの圧縮はすべての MSDP ホストで有効になっています。したがって、複製とレプリケーションの圧縮は次の MSDP サーバーで実行されます。 ■ 負荷分散サーバー。 ■ ストレージサーバー。 複製とレプリケーションの圧縮は、クライアントには適用されません。 NetBackup は、最も使用率が低いホストを選択して、各複製ジョブとレプリケーションジョブを開始して管理します。最適化されたすべての複製ジョブとレプリケーションジョブに確実に圧縮を実行するために、OPTDUP_COMPRESSION パラメータのデフォルト設定は変更しないでください。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.52 の「MSDP の圧縮と暗号化を使う」を参照してください。

MSDP の暗号化について

NetBackup では重複排除データを暗号化できます。それは NetBackup のポリシーベースの暗号化とは別の、異なるものです。

NetBackup では、メディアサーバー重複排除プール (MSDP) に 256 ビットの CTR AES (Advanced Encryption Standard) 暗号化アルゴリズムが使用されます。AES 暗号化アルゴリズムが古い Blowfish 暗号化アルゴリズムに置き換わります。

p.781 の「Encryption Crawler について」を参照してください。

p.110 の「MSDP 暗号化の動作と互換性」を参照してください。

MSDP ローカルストレージボリュームの暗号化の構成

キーを別のキーを使用して暗号化することを、エンベロープ暗号化と呼びます。MSDP はエンベロープ暗号化を使用します。

KMS の構成方法と使用方法に関する詳細情報が利用可能です。

p.111 の「NetBackup Key Management Server サービスを使用した MSDP 暗号化について」を参照してください。

MSDP の初期設定では、NetBackup Web UI を使用して暗号化を構成できます。既存のシステムの暗号化を有効にするには、次の手順を手動で実行します。有効にすると、NetBackup メディアサーバー、opt-dup のサーバー、AIR のサーバー、Client Direct ホストを含む MSDP サーバーのローカルディスクボリュームへのすべてのデータが暗号化されます。他のどの場所でも暗号化を構成する必要はありません。

メモ: 次の手順は、MSDP のローカルディスクボリューム専用です。MSDP クラウドボリュームの暗号化については、次のトピックを参照してください。

p.107 の「MSDP クラウドストレージボリュームの暗号化の構成」を参照してください。

MSDP ローカルストレージボリュームのバックアップの暗号化を構成する方法

1 ストレージサーバーで、テキストエディタで `contentrouter.cfg` ファイルを開きます。それは次のディレクトリに存在します。

- (UNIX) *`storage_path`*`/etc/puredisk`

- (Windows) *storage_path*¥etc¥puredisk

2 ファイルの encrypt 行に ServerOptions を追加します。例:

```
ServerOptions=fast,verify_data_read,encrypt
```

MSDP ストレージサーバー、MSDP 負荷分散サーバー、NetBackup Client Direct 重複排除クライアントなど、サーバーに格納されているすべてのデータに対して暗号化が有効になります。

3 MSDP サービスを再起動します。

メモ: pd.conf ファイルを使用する暗号化構成は、NetBackup メディアサーバーまたはクライアントでの変更を必要とするため、使用は推奨されません。

MSDP クラウドストレージボリュームの暗号化の構成

MSDP クラウドボリュームの暗号化は、NetBackup Web UI またはコマンドラインオプションを使用して構成します。MSDP クラウドボリュームの作成時に、暗号化を構成できます。クラウドボリュームの場合、暗号化を構成するには常に KMS が必要です。KMS が有効になっていない場合、暗号化チェックボックスは利用できません。

メモ: 各 MSDP ストレージボリュームの暗号化は個別に構成されます。MSDP ディスクストレージプールの暗号化と同様に、一度構成すると、クラウドストレージボリュームへのすべてのデータがデータソースに関係なく暗号化されます。

p.265 の「クラウドストレージユニットの作成」を参照してください。

異なるプラットフォームでの MSDP 暗号化の構成

MSDP は、NetBackup BYO、NetBackup Appliance、Flex メディアサーバー、Flex WORM、Flex Scale、Cloud Scale、Access Appliance などの異なるプラットフォームに配備できます。一部のプラットフォームは閉じられており、構成ファイルを直接編集できません。このような場合は、プラットフォーム固有のサポートが必要です。たとえば、NetBackup Appliance の CLISH や、Flex WORM と Access Appliance の Deduplication Shell を使用して構成を変更できます。

ローリングデータ変換のモード

MSDP では、ローリングデータ変換のメカニズムを使用して、Blowfish で暗号化されたデータを AES-256 で暗号化されたデータに、MD5 に似たアルゴリズムの指紋を SHA-512/256 の指紋に並列で変換します。データ変換には、通常モードと高速モードの 2 種類のモードがあります。

- 通常モード: アップグレード済みのシステムでは、デフォルトでデータ変換プロセスが通常モードで開始されます。圧縮と同様に、データ変換は、バックアップ、リストア、または CRQP (Content Router Queue Processing) ジョブが実行中でない場合にのみ実行されます。
  通常モードでは、データ変換の所要時間は次の要因によって左右されます。
  - ストレージの合計サイズ
  - CPU 能力
  - システムに対する負荷

  通常モードのデータ変換には所要時間が長くなる場合があります。
  制御下の環境でCohesityが行ったテストによると、1 TB の単一マウントポイントでは、変換速度は通常モードで約 50 MB/秒であることが示されました。
- 高速モード: 高速モードでは、データ変換によって巡回冗長検査と圧縮が無効化されます。ローリングデータ変換は、バックアップ、リストア、複製、または CRQP ジョブの実行時に行われます。
  制御下の環境でCohesityが行ったテストによると、1 TB の単一マウントポイントでは、変換速度は高速モードで約 105 MB/秒であることが示されました。

メモ: パフォーマンスの数値はCohesityのテスト環境で計測されたものであり、お使いの環境でのパフォーマンスを保証するものではありません。

NetBackup 8.1 の新規インストールでは、ローリングデータ変換は[完了]としてマーク付けされ、その後開始されることはありません。NetBackup 8.1 へのアップグレードの場合、ローリングデータ変換はデフォルトでは有効であり、MSDP 変換の完了後にバックグラウンドで動作します。変換されるのは、アップグレードの前に存在していたデータのみです。すべての新しいデータは新しい SHA-512/256 の指紋を使用するため、変換の必要がありません。

高速モードでは、ローリングデータ変換はバックアップ、リストア、複製、およびレプリケーションジョブのパフォーマンスに影響します。この影響を最小限に抑えるには、通常モードを使用します。通常モードでは、システムがビジー状態のときに変換が一時停止されますが、変換プロセスは遅くなります。高速モードでは、システム状態に関係なく変換がアクティブになります。

次の `crcontrol` コマンドオプションを使うと、ローリングデータ変換を管理、監視できます。

表 4-16 ローリングデータ変換の MSDP crcontrol コマンドオプション

オプション	説明
--dataconverton	データ変換プロセスを開始するには、--dataconverton オプションを使用します。 Windows の場合: install_path¥Veritas¥pdde¥Crcontrol.exe --dataconverton UNIX の場合: /usr/openv/pdde/pdcr/bin/crcontrol --dataconverton
--dataconvertoff	データ変換プロセスを停止するには、--dataconvertoff オプションを使用します。 Windows の場合: install_path¥Veritas¥pdde¥Crcontrol.exe --dataconvertoff UNIX の場合: /usr/openv/pdde/pdcr/bin/crcontrol --dataconvertoff
--dataconvertstate	データ変換のモードと変換の進捗状況を確認するには、--dataconvertstate オプションを使用します。 Windows の場合: install_path¥Veritas¥pdde¥Crcontrol.exe --dataconvertstate UNIX の場合: /usr/openv/pdde/pdcr/bin/crcontrol --dataconvertstate
--dataconvertmode	データ変換の通常モードと高速モードを切り替えるには、--dataconvertmode オプションを使用します。 Windows の場合: install_path¥Veritas¥pdde¥Crcontrol.exe --dataconvertmode mode UNIX の場合: /usr/openv/pdde/pdcr/bin/crcontrol --dataconvertmode <mode> *<mode>* 変数のデフォルト値は 0 です。この値は通常モードを意味します。通常モードから高速モードにデータ変換を切り替えるには、*<mode>* 変数の値に 1 を入力します。

p.110 の「MSDP 暗号化の動作と互換性」を参照してください。

MSDP 暗号化の動作と互換性

MSDP は複数の暗号化アルゴリズムをサポートします。MSDP はデータ互換性を確保するため Blowfish と AES の両方の暗号化データを管理します。

リストア操作では、MSDP は Blowfish データと AES データを認識するため、古いバックアップイメージでもリストアできます。

次の表に、暗号化の進行中におけるバックアップ、重複排除、レプリケーション操作の暗号化の動作を示します。

表 4-17 NetBackup 8.0 ストレージサーバーへのバックアップ操作における暗号化の動作

クライアントの形式	データ暗号化形式
NetBackup 8.0 を備えるクライアント (Client Direct 重複排除を含む)	AES
8.0 より前の NetBackup バージョンを備えるクライアント (Client Direct 重複排除を除く)	AES
8.0 より前の NetBackup バージョンを備えるクライアント (Client Direct 重複排除を使用)	AES (インラインデータ変換を使用)
NetBackup バージョン 8.0 を備える負荷分散サーバー	AES
8.0 以前のバージョンの NetBackup を備える負荷分散サーバー	AES (インラインデータ変換を使用)

表 4-18 NetBackup 8.0 対象サーバーに対する最適化された重複排除操作と自動イメージレプリケーション操作における暗号化の動作

ソースストレージの形式	重複排除または **AES** で暗号化されたレプリケーションデータのデータ暗号化形式	重複排除または **Blowfish** で暗号化されたレプリケーションデータのデータ暗号化形式
NetBackup 8.0 を備えるソースサーバー	AES	AES (インラインデータ変換を使用)
8.0 以前のバージョンの NetBackup を備えるソースサーバー	なし	AES (インラインデータ変換を使用)

メモ: インラインデータ変換は、バックアップ、重複排除、レプリケーションの操作の進行中に同時に実行されます。

NetBackup Key Management Server サービスを使用した MSDP 暗号化について

NetBackup は、メディアサーバー重複排除プールに KMS (Key Management Server) を組み込んでいます。

NetBackup 10.1.1 および Flex WORM ストレージサーバー 17.1 以降、MSDP はキーの複数の階層が含まれるエンベロープ暗号化を使用してデータを暗号化します。新しい各 MSDP データセグメントは、MSDP によって生成される一意の DEK (データ暗号化キー) で暗号化されます。各 DEK は、MSDP によって生成される KEK (キー暗号化キー) によって暗号化またはラップされます。複数の DEK は、アクティブな KEK が新たに生成されるまで、同じ KEK を暗号化に使用できます。KEK は、NetBackup KMS または外部 KMS に存在するアクティブな root キーを使用して暗号化されます。root キーは MSDP に送信されません。代わりに、MSDP は KEK を NetBackup プライマリサーバーに送信します。このプライマリサーバーは、NetBackup KMS または外部 KMS に接続して KEK を暗号化または復号します。暗号化された DEK と暗号化された KEK は MSDP 内に格納されます。

以前のバックアップデータのレガシー KMS 暗号化を KEK ベースの KMS 暗号化に変換する方法については、「p.802 の「レガシー KMS の KEK ベースの KMS への変換」を参照してください。」を参照してください。

ユーザーは KMS サービスを管理してキーを作成し、アクティブ化します。KMS サービスでは、1 つのアクティブなキーが存在する必要があります。

KMS サービスは、ストレージサーバーの構成時に NetBackup Web UI または NetBackup コマンドラインから設定できます。

メモ: MSDP の KMS サービスを有効にしたら無効にすることはできません。

KMS サービスが MSDP で利用できない場合、または MSDP が使用する KMS サービスのキーが利用できない場合、MSDP は無限ループで待機し、バックアップジョブが失敗する場合があります。MSDP が無限ループに入ると、実行するコマンドのいくつかが応答しなくなることがあります。

KMS 暗号化を構成した後、または MSDP プロセスが再起動した後、最初のバックアップの完了後に KMS 暗号化の状態を確認します。

キー辞書のキーを削除したり、非推奨にしたり、終了したりしないでください。MSDP ディスクプールに関連付けられているすべてのキーは、アクティブまたは非アクティブの状態である必要があります。

KMS モードの状態は、次のコマンドを使用して取得できます。

- UNIX の場合:
  `/usr/openv/pdde/pdcr/bin/crcontrol --getmode`
  MSDP クラウドの場合は、次の `keydictutil` コマンドを実行して、LSU (論理ストレージユニット) が KMS モードかどうかを確認します。
  `/usr/openv/pdde/pdcr/bin/keydictutil --list`
- Windows の場合:
  `<install_path>¥Veritas¥pdde¥crcontrol.exe --getmode`

メモ: `nbdevconfig` コマンドを使用して、新しい暗号化されたクラウド LSU を追加するとき、暗号化された LSU がこの MSDP に存在する場合、`keygroupname` が暗号化済みの LSU の `keygroupname` と同じである必要があります。

KMS の有効化について詳しくは、次のトピックを参照してください。

p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。

ローカル LSU での KMS 暗号化の有効化

`nbdevconfig` コマンドを使用して、ローカル LSU の KMS 暗号化を有効にできます。

ローカル LSU での KMS 暗号化を有効にするには

1 次の形式でユーザー設定の名前を付けて、構成ファイルを作成します。例:
`sample_config.txt`

```
V7.5 "operation" "set-local-lsu-kms-property" string
V7.5 "encryption" "1" string
V7.5 "kmsenabled" "1" string
V7.5 "kmsservertype" "0" string
V7.5 "kmsservername" "xxxxxx" string
V7.5 "keygroupname" "xxxxx" string
```

構成設定	説明
`V7.5 "operation" "set-local-lsu-kms-property" string`	KMS の状態は無効から有効にのみ更新できます。
`V7.5 "encryption" "1" string`	暗号化の状態を指定します。この値は 1 にする必要があります。

構成設定	説明
`V7.5 "kmsenabled" "1" string`	KMS の状態を指定します。この値は 1 にする必要があります。
`V7.5 "kmsservertype" "0" string`	KMS のサーバー形式を指定します。この値は 0 にする必要があります。
`V7.5 "kmsservername" "" string`	すべての LSU 間で共有される KMS サーバー名。
`V7.5 "keygroupname" "" string`	キーグループ名には、次の有効な文字を含める必要があります。 ■ A から Z ■ a から z ■ 0 から 9 ■ アンダースコア (_) ■ ハイフン (-) ■ コロン (:) ■ ピリオド (.) ■ スペース

2 KMS 暗号化を有効にするには、次のコマンドを実行します。

```
nbdevconfig -setconfig -storage_server <storage server host name>
-stype PureDisk -configlist <configuration file name>
```

メモ: 1 台のストレージサーバーに存在するすべての暗号化された LSU は、同じ `keygroupname` と `kmsservername` を使用する必要があります。KMS サーバーを構成する必要があります。キーグループとキーは KMS サーバーに存在します。

MSDP 用の KMS のアップグレード

8.1.1 より前のバージョンの NetBackup の KMS 暗号化をアップグレードする前に、次の手順を実行します。NetBackup のアップグレード中、KMS ローリング変換が、MSDP 暗号化のローリング変換とともに実行されます。

8.1.1 より前のバージョンの NetBackup では、サポートされる NetBackup のアップグレードパスは次のとおりです。

- NetBackup 8.0 から 8.1.1 以降
- NetBackup 8.1 から 8.1.1 以降

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』にある KMS の構成に関するセクションを参照してください。

KMS をアップグレードする前に、次の手順を実行します。

メモ: 次の手順は Solaris OS ではサポートされません。Solaris については、次の記事を参照してください。

Solaris プラットフォームでの MSDP 用の KMS 暗号化のアップグレード (Upgrade KMS encryption for MSDP on the Solaris platform)

---

1 次のコマンドを使用して空のデータベースを作成します。

- UNIX の場合:

  ```
  /usr/openv/netbackup/bin/nbkms -createemptydb
  ```

- Windows の場合:

  ```
  <install_path>¥Veritas¥NetBackup¥bin¥nbkms.exe -createemptydb
  ```

  プロンプトが表示されたら、次のパラメータを入力します。

  - HMK パスフレーズの入力
    ホストマスターキー (HMK) のパスフレーズとして設定するパスワードを入力します。Enter キーを押して、ランダムに生成された HMK パスフレーズを使用します。パスフレーズは画面には表示されません。
  - HMK ID の入力
    ホストマスターキーと関連付ける一意の ID を入力します。この ID は、任意のキーストアに関連付けられた HMK を特定するのに役立ちます。
  - KPK パスフレーズの入力
    キー保護キー (KPK) のパスフレーズとして設定するパスワードを入力します。Enter キーを押して、ランダムに生成された HMK パスフレーズを使用します。パスフレーズは画面には表示されません。
  - KPK ID の入力
    キー保護キーと関連付ける一意の ID を入力します。この ID は、任意のキーストアに関連付けられた KPK を特定するのに役立ちます。

  操作が正常に完了したら、プライマリサーバーで次のコマンドを実行し、KMS を起動します。

- UNIX の場合:

  ```
  /usr/openv/netbackup/bin/nbkms
  ```

- Windows の場合:

  ```
  sc start NetBackup Key Management Service
  ```

2 次のコマンドを入力して、キーグループとアクティブなキーを作成します。

- UNIX の場合:

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -createkg -kgname
msdp
/usr/openv/netbackup/bin/admincmd/nbkmsutil -createkey -kgname
msdp -keyname name -activate
```

- Windows の場合:

```
<install_path>¥Veritas¥NetBackup¥bin¥admincmd¥nbkmsutil.exe
-createkg -kgname msdp
<install_path>¥Veritas¥NetBackup¥bin¥admincmd¥nbkmsutil.exe
-createkey -kgname msdp -keyname name -activate
```

キーのパスフレーズとして設定するパスワードを入力します。

3 MSDP ストレージを構成した NetBackup メディアサーバーの次の場所で、kms.cfg 構成ファイルを作成します。

- UNIX の場合:

```
/usr/openv/pdde/kms.cfg
```

- Windows の場合:

```
<install_path>¥Veritas¥pdde¥kms.cfg
```

kms.cfg ファイルに次の内容を追加します。

```
[KMSOptions]
KMSEnable=true
KMSKeyGroupName=YourKMSKeyGroupName
KMSServerName=YourKMSServerName
KMSType=0
```

KMSServerName には、KMS サービスが実行されているサーバーのホスト名を入力します。多くの場合、プライマリサーバーのホスト名です。

手順を完了したら、MSDP をアップグレードできます。

外部 KMS サーバーを使用した MSDP 暗号化について

MSDP ストレージの場合、NetBackup は外部キーマネージメントサービス (KMS) サーバーのキーをサポートします。キーは、MSDP から KEK (キー暗号化キー) を暗号化または復号するために、外部 KMS サーバーからプライマリサーバーに取得されます。

外部 KMS のサポートについて詳しくは、『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。

その他の情報は、次のトピックに記載されている内容と同じままです。

p.111 の「NetBackup Key Management Server サービスを使用した MSDP 暗号化について」を参照してください。

最適化された合成バックアップの MSDP の構成

最適化された合成バックアップの MSDP を構成するには、[合成バックアップ (Synthetic Backup)]ポリシー属性を選択する必要があります。

最適化された合成バックアップを MSDP 用に構成する方法

1 [標準 (Standard)]または[MS-Windows]バックアップポリシーを構成します。

p.166 の「バックアップポリシーの作成」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。

http://www.veritas.com/docs/DOC5332

2 バックアップポリシーの[スケジュールの属性 (Schedule Attributes)]タブで[合成バックアップ (Synthetic Backup)]属性を選択します。

p.496 の「MSDP ストレージサーバーの属性の設定」を参照してください。

p.166 の「バックアップポリシーの作成」を参照してください。

MSDP の複製およびレプリケーションに対する個別ネットワークパスについて

MSDP の複製とレプリケーションのトラフィックには MSDP バックアップに使っているネットワークと異なるネットワークを使えます。複製とレプリケーションのデータトラフィックと制御トラフィックの両方が個別のネットワーク上を移動します。MSDP トラフィックは、次のように 2 つの異なるネットワークを使います。

バックアップおよびリストア
: NetBackup は、バックアップとリストアで、ストレージサーバー構成時に設定したネットワークインターフェースを使います。

  バックアップおよびリストアのトラフィックと制御トラフィックの両方がバックアップネットワーク上で移動します。

p.40 の「MSDP のネットワークインターフェースについて」を参照してください。

複製とレプリケーション	複製およびレプリケーションのトラフィックの場合、バックアップおよびリストアに使用するネットワークとは異なるネットワークを使用するホストオペレーティングシステムを設定します。 複製およびレプリケーションのデータトラフィックと制御トラフィックの両方が複製およびレプリケーションネットワーク上を移動します。 p.117 の「MSDP 複製とレプリケーションに対する個別ネットワークパスの構成」を参照してください。 最適化された複製またはレプリケーションのレプリケーションターゲットを設定する際、必ず複製およびレプリケーションネットワークを表すホスト名を選択してください。

p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。

p.131 の「異なるドメインへの MSDP レプリケーションについて」を参照してください。

MSDP 複製とレプリケーションに対する個別ネットワークパスの構成

MSDP の複製とレプリケーションのトラフィックには MSDP バックアップに使っているネットワークと異なるネットワークを使えます。複製とレプリケーションのデータトラフィックと制御トラフィックの両方が個別のネットワーク上を移動します。

p.116 の「MSDP の複製およびレプリケーションに対する個別ネットワークパスについて」を参照してください。

この手順では個別ネットワークにトラフィックをルーティングするのにストレージサーバーの `hosts` ファイルを使う方法を記述します。

前提条件は次のとおりです。

- コピー元と宛先ストレージサーバーの両方に、その他のネットワーク専用のネットワークインターフェースカードが必要です。
- 個別ネットワークが稼働中で、コピー元と宛先ストレージサーバーで専用ネットワークインターフェースカードを使っている。
- UNIX の MSDP ストレージサーバーの場合には、ネームサービススイッチが DNS (ドメイン名システム) に問い合わせる前に必ずローカルの `hosts` ファイルを調べるように設定します。ネームサービススイッチについて詳しくはオペレーティングシステムのマニュアルを参照してください。

MSDP の複製とレプリケーションに対して個別のネットワークパスを構成する方法

1. コピー元ストレージサーバーで、宛先ストレージサーバーの専用ネットワークインターフェースをオペレーティングシステムの hosts ファイルに追加します。
   TargetStorageServer が複製専用の宛先ホストの名前である場合の IPv4 表記で書かれた hosts エントリの例は次のとおりです。

   ```
   10.10.10.1   TargetStorageServer.example.com   TargetStorageServer
   ```

   Cohesity ベリタス社では、ホストを指定するときは常に完全修飾ドメイン名を使用することをお勧めします。

2. 宛先ストレージサーバーで、コピー元ストレージサーバーの専用ネットワークインターフェースをオペレーティングシステムの hosts ファイルに追加します。
   SourceStorageServer が複製専用のネットワーク上にあるソースホストの名前である場合の IPv4 表記で書かれた hosts エントリの例は次のとおりです。

   ```
   10.80.25.66   SourceStorageServer.example.com
   SourceStorageServer
   ```

   Cohesity ベリタス社では、ホストを指定するときは常に完全修飾ドメイン名を使用することをお勧めします。

3. 変更を強制的にすぐに反映させるには DNS のキャッシュを消去します。DNS キャッシュの消去について詳しくはオペレーティングシステムのマニュアルを参照してください。

4. 各ホストで ping コマンドを使うことにより各ホストがその他のホストの名前を解決することを確認します。

   ```
   SourceStorageServer.example.com> ping
   TargetStorageServer.example.com
   TargetStorageServer.example.com> ping
   SourceStorageServer.example.com
   ```

   ping コマンドが陽性結果を返した場合は、個別ネットワークにわたり複製とレプリケーション用のホストが構成されます。

5. ターゲットストレージサーバーを設定するときには、代替のネットワークパスを表すホスト名を選択することを確認します。

同じドメイン内での MSDP の最適化複製について

同じドメイン内での最適化複製は同じドメイン内の［メディアサーバー重複排除プール (Media Server Deduplication Pool)］間で重複排除されたバックアップイメージをコピーします。つまり、コピー元とコピー先ストレージで同じ NetBackup プライマリサーバーを使用する必要があります。

最適化複製処理は、通常の複製より効率的です。一意の重複排除データセグメントのみが転送されます。最適化複製は、ネットワークを介して転送されるデータの量を減らします。

最適化複製はディザスタリカバリ用にバックアップイメージをオフサイトでコピーするよい方式です。

デフォルトでは、NetBackup は NetBackup Vault が `bpduplicate` コマンドを使用して起動した、失敗した最適化複製ジョブを再試行しません。その動作は変更できます。

p.128 の「NetBackup の最適化複製またはレプリケーション動作の設定」を参照してください。

複製トラフィックに対して個別のネットワークを使用できます。

p.116 の「MSDP の複製およびレプリケーションに対する個別ネットワークパスについて」を参照してください。

p.124 の「同じ NetBackup ドメインでの MSDP 最適化複製の構成」を参照してください。

次の必要条件と制限事項を確認します。

MSDP の最適化複製の必要条件について

次は同じ NetBackup ドメイン内での最適化複製の要件です。

- コピー元のストレージと宛先のストレージには少なくとも 1 つの共通のメディアサーバーがなければなりません。
  p.120 の「同じドメイン内での MSDP の最適化複製のメディアサーバーについて」を参照してください。
- 最適化複製の宛先に使うストレージユニットでは、共通のメディアサーバーのみ選択してください。
  複数選択すると、NetBackup は最もビジー状態でないメディアサーバーに複製ジョブを割り当てます。メディアサーバーや共通でないサーバーを選択すると、最適化複製ジョブは失敗します。
  メディアサーバーの負荷分散について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
- ソースストレージユニットを宛先ストレージユニットとして使用することはできません。

MSDP の最適化複製の制限について

次は同じ NetBackup ドメイン内での最適化複製の制限事項です。

- 設定された回数再試行した後、最適化複製ジョブが失敗した場合、NetBackup はジョブを再実行しません。
  デフォルトでは、NetBackup は最適化複製ジョブを 3 回再試行します。再試行の数は変更できます。

p.128 の「NetBackup の最適化複製またはレプリケーション動作の設定」を参照してください。

- NetBackup はストレージユニットグループの MSDP 最適化複製をサポートしません。最適化複製の宛先としてストレージユニットグループを使うと、NetBackup は通常の複製を使います。
- 最適化複製は複数コピーをサポートしません。バックアップイメージの (コピー元の) コピーから複数の新しいコピーを作成するように NetBackup が構成されている場合は、次が起きます。
  - ストレージライフサイクルポリシーでは、1 つの複製ジョブが 1 つの最適化複製コピーを作成します。最適化複製先が複数存在する場合、別々のジョブが宛先ごとに存在します。この動作は最適化複製先のデバイスがソースイメージが存在するデバイスと互換性があると仮定します。
    残りの複数のコピーが、最適化複製が可能でないデバイスに移動するように構成されている場合、NetBackup は通常の複製を行います。1 つの複製ジョブがそれらの複数コピーを作成します。
  - 他の複製の方式の場合、NetBackup は通常の複製を行います。1 つの複製ジョブがコピーすべてを同時に作成します。その他に、次の複製方法があります。
    NetBackup Vault、`bpduplicate` コマンドライン、NetBackup Web UI のカタログユーティリティの複製オプションが含まれます。
- コピー操作では、コピー先ストレージユニットの設定ではなく、コピー元ストレージユニットの最大フラグメントサイズが使用されます。最適化複製では、イメージフラグメントがそのままコピーされます。効率の向上を図るため、複製によってコピー先ストレージユニット上でイメージのサイズが変更されたり、イメージが別のフラグメントセットに移動されることはありません。

p.120 の「同じドメイン内での MSDP の最適化複製のメディアサーバーについて」を参照してください。

p.121 の「同じドメイン内での MSDP のプッシュ型の複製について」を参照してください。

p.123 の「同じドメイン内での MSDP のプル型の複製について」を参照してください。

p.43 の「MSDP の最適化複製とレプリケーションについて」を参照してください。

同じドメイン内での MSDP の最適化複製のメディアサーバーについて

同じドメイン内でのメディアサーバー重複排除プールの最適化複製の場合、ソーストレージと宛先ストレージには少なくとも 1 つの共通のメディアサーバーがなければなりません。共通のサーバーは複製操作を開始し、監視し、検証します。共通のサーバーはコピー元のストレージと宛先のストレージ両方のクレデンシャルを必要とします。(重複排除の場合、クレデンシャルは NetBackup Deduplication Engine 用であり、それが動作するホスト用ではありません。)

どのメディアサーバーが複製操作を開始するかによって、プッシュ型の複製かプル型の複製かが次のように決定されます。

- メディアサーバーがソースストレージサーバーと物理的に共存している場合は、プッシュ型の複製です。
- メディアサーバーが宛先ストレージサーバーと物理的に共存している場合は、プル型の複製です。

厳密には、プッシュ型の複製にもプル型の複製にも利点はありません。ただし、複製操作を開始するメディアサーバーは新しいイメージコピーの書き込みホストにもなります。

ストレージサーバーまたは負荷分散サーバーは共通のサーバーである場合があります。共通のサーバーはコピー元のストレージと宛先のストレージ両方のクレデンシャルを持ち、接続していなければなりません。

p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。

p.121 の「同じドメイン内での MSDP のプッシュ型の複製について」を参照してください。

p.123 の「同じドメイン内での MSDP のプル型の複製について」を参照してください。

同じドメイン内での MSDP のプッシュ型の複製について

図 4-1 は同じドメイン内での最適化複製のプッシュ型の構成を示します。ローカル重複排除ノードは通常のバックアップを含んでいます。リモート重複排除ノードは最適化複製のコピー先です。負荷分散サーバー LB_L2 は両方のストレージサーバーのクレデンシャルを持っており、共通のサーバーです。

図 4-1　　プッシュ型の複製環境

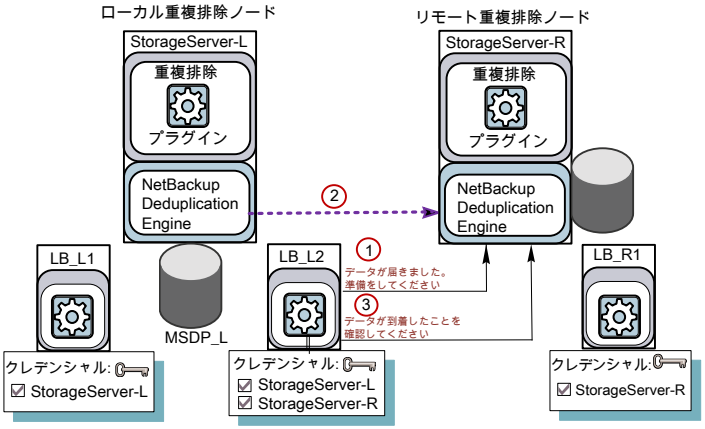


図 4-2 に、ローカル重複排除ノードの通常のバックアップに対するストレージユニットの設定を示します。ディスクプールはローカル環境の［MSDP_L］です。ローカルノードの

すべてのホストが同じ場所に配置されているので、バックアップに対して利用可能な任意のメディアサーバーを使用できます。

図 4-2　　MSDP_L へのバックアップに対するストレージユニットの設定

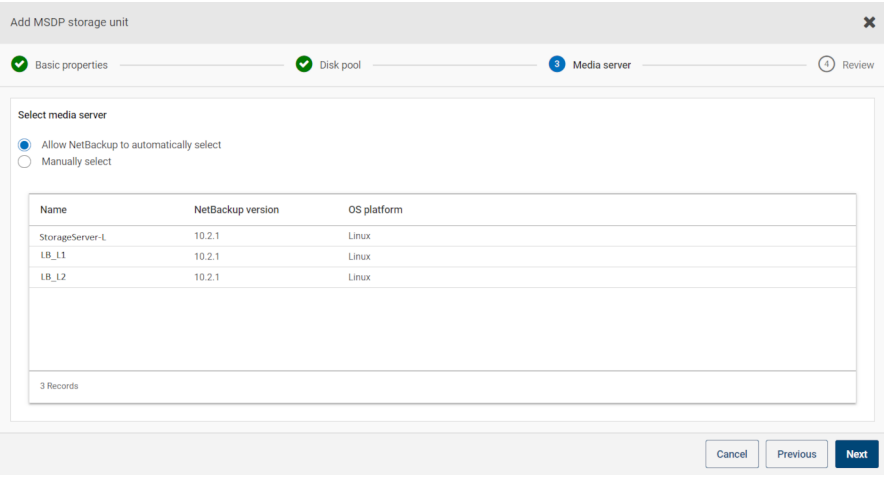
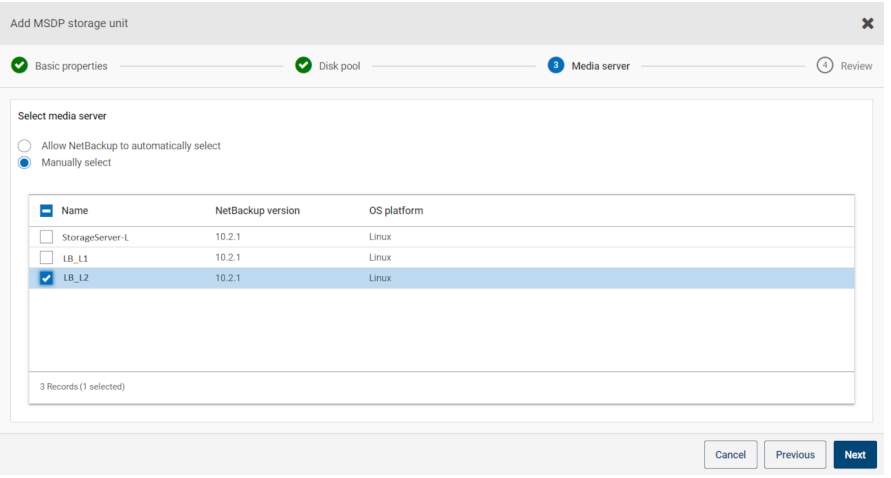


図 4-3 に、最適化複製のストレージユニットの設定を示します。宛先はリモート環境の [MSDP_R] です。負荷分散サーバー LB_L2 だけが選択されるように、共通のサーバーを選択する必要があります。

図 4-3　　MSDP_R への複製に対するストレージユニットの設定



リモートノードをバックアップにも使う場合は、リモートノードバックアップ用にストレージユニットの StorageServer-R と負荷分散サーバー LB_R1 を選択します。サーバー LB_L2

を選択すると、それがリモートの[メディアサーバー重複排除プール (Media Server Deduplication Pool)]の負荷分散サーバーになります。そのような場合、データは WAN を経由して移動します。

同じドメイン内での MSDP のプル型の複製について

図 4-4 は同じドメイン内での最適化複製のプル型の構成を示します。重複排除ノード B は最適化複製のコピー先です。ホスト B は両方のノードのクレデンシャルを持っており、共通のサーバーです。

図 4-4　　プル型の複製

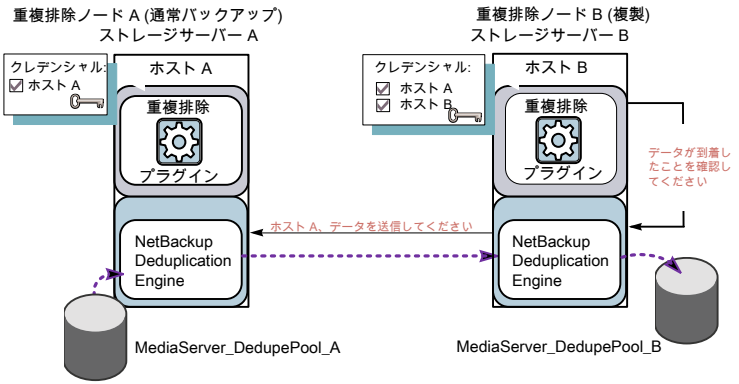
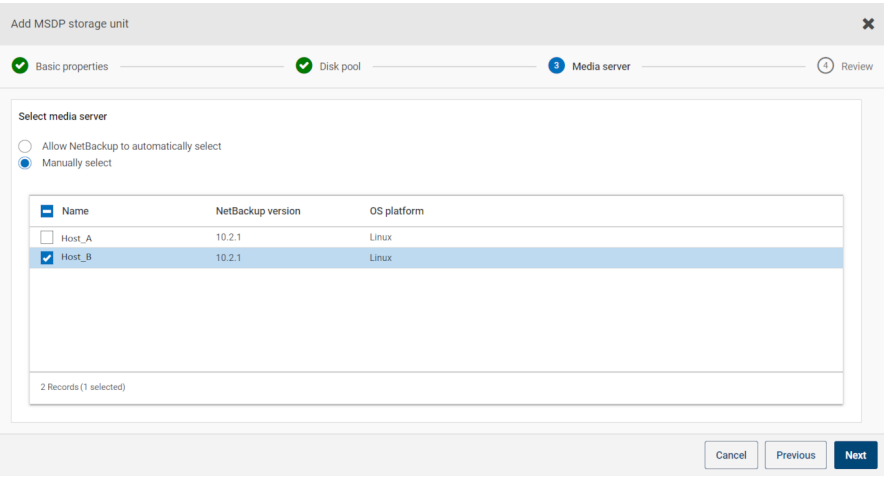


図 4-5 は、複製先のストレージユニットの設定を示します。それらはホスト B が選択されていること以外はプッシュ型の例に類似しています。ホスト B は共通のサーバーです。したがって、ストレージユニットで選択する必要があります。

図 4-5 プル型の複製のストレージユニットの設定



バックアップにもノード B を使う場合は、ストレージユニットのホスト A ではなくホスト B をノード B のバックアップ用に選択します。ホスト A を選択すると、それはノード B 重複排除プールの負荷分散サーバーになります。

同じ NetBackup ドメインでの MSDP 最適化複製の構成

あるメディアサーバー重複排除プールから同じ NetBackup ドメインのその他のメディアサーバー重複排除ストレージに最適化複製を構成できます。

表 4-19 重複排除されたデータの最適化複製を構成する方法

手順	処理	説明
手順 1	最適化複製の確認	p.118 の「同じドメイン内での MSDP の最適化複製について」を参照してください。

手順	処理	説明
手順 2	ストレージサーバーを構成します。	p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。 1 つのサーバーはコピー元のストレージと宛先のストレージ間で共通である必要があります。どれを選択するかはプッシュ型の構成にするかプル型の構成にするかに左右されます。 p.120 の「同じドメイン内での MSDP の最適化複製のメディアサーバーについて」を参照してください。 プッシュ型の構成の場合は、通常のバックアップ用のストレージサーバーの負荷分散サーバーとして共通のサーバーを構成します。プル型の構成の場合は、リモートサイトのコピー用のストレージサーバーの負荷分散サーバーとして共通のサーバーを構成します。または、どちらかの環境にサーバーを後で追加できます。(サーバーは重複排除プールのストレージユニットで選択すると負荷分散サーバーになります。)
手順 3	重複排除プールの構成	ストレージサーバーを構成したときに重複排除プールを構成しなかった場合は、[ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)]を使用して重複排除プールを設定します。 p.93 の「重複排除のディスクプールの構成」を参照してください。
手順 4	バックアップ用ストレージユニットの構成	**バックアップのストレージユニットで、以下を行います。** **1** [ディスク形式 (Disk type)]で、[PureDisk]を選択します。 **2** [ディスクプール (Disk pool)]で、[メディアサーバー重複排除プール (Media Server Deduplication Pool)]を選択します。 プル型の構成を使う場合は、バックアップストレージユニットで共通のメディアサーバーを選択しないでください。選択した場合、NetBackup はバックアップデータの重複排除にそれを使います。(つまり、ソース重複排除ノードの負荷分散サーバーにそれを使わない場合。)

手順	処理	説明
手順 5	複製用ストレージユニットの構成	Cohesity は最適化複製のターゲットにするストレージユニットを個別に構成することを推奨します。通常のバックアップを実行する重複排除ノードでストレージユニットを構成します。コピーを含んでいるノードでは構成しないでください。 **複製されたイメージの宛先であるストレージユニットで、以下を行います。** **1** ［ディスク形式 (Disk type)］で、［PureDisk］を選択します。 **2** ［ディスクプール (Disk pool)］で、宛先を［メディアサーバー重複排除プール (Media Server Deduplication Pool)］にできます。 また、［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。次に、ソースストレージサーバーと宛先ストレージサーバーの両方に共通のメディアサーバーを選択します。複数選択すると、NetBackup は最もビジー状態でないメディアサーバーに複製ジョブを割り当てます。 共通ではないメディアサーバーのみを選択すると、最適化複製ジョブは失敗します。
手順 6	最適化複製の帯域幅の構成	必要に応じて、レプリケーションの帯域幅を構成できます。 p.156 の「MSDP 最適化複製とレプリケーション帯域幅の構成について」を参照してください。
手順 7	最適化複製の動作の構成	必要に応じて、最適化複製の動作を構成できます。 p.128 の「NetBackup の最適化複製またはレプリケーション動作の設定」を参照してください。 p.156 の「MSDP 最適化複製とレプリケーション帯域幅の構成について」を参照してください。

手順	処理	説明
手順 8	複製のストレージライフサイクルポリシーの構成	イメージを複製するために使うときのみストレージライフサイクルポリシーを構成します。ストレージライフサイクルポリシーはバックアップジョブと複製ジョブを両方管理します。通常のバックアップを実行する重複排除環境でライフサイクルポリシーを構成します。コピーを含んでいる環境では構成しないでください。 ストレージライフサイクルポリシーを構成するとき、以下を行います。 ■ 最初の操作は[バックアップ (Backup)]である必要があります。[バックアップ (Backup)]操作の[ストレージ (Storage)]には、バックアップのターゲットであるストレージユニットを選択します。そのストレージユニットには[メディアサーバー重複排除プール (Media Server Deduplication Pool)]を使用できます。 これらのバックアップはプライマリバックアップコピーであり、複製操作のソースイメージです。 ■ 第 2 の子の[操作 (Operation)]には、[複製 (Duplication)]を選択します。その後、宛先の重複排除プールのストレージユニットを選択します。そのプールには[メディアサーバー重複排除プール (Media Server Deduplication Pool)]を使用できます。 p.159 の「ストレージライフサイクルポリシーについて」を参照してください。 p.161 の「ストレージライフサイクルポリシーの作成」を参照してください。
手順 9	バックアップポリシーの構成	クライアントをバックアップするためにポリシーを構成します。通常のバックアップを実行する重複排除環境でバックアップポリシーを構成します。コピーを含んでいる環境では構成しないでください。 ■ ストレージライフサイクルポリシーを使用してバックアップジョブと複製ジョブを管理する場合、ポリシーの[属性 (Attributes)]タブの[ポリシーストレージ (Policy storage)]フィールドでそのストレージライフサイクルポリシーを選択します。 ■ バックアップジョブと複製ジョブの管理にストレージライフサイクルポリシーを使わない場合には、通常のバックアップを含むストレージユニットを選択します。これらのバックアップはプライマリバックアップコピーです。 p.165 の「MSDP バックアップポリシーの構成について」を参照してください。 p.166 の「バックアップポリシーの作成」を参照してください。

手順	処理	説明
手順 10	NetBackup Vault の複製用の構成	イメージを複製するために NetBackup Vault を使うときのみ Vault 複製を構成します。 通常のバックアップを実行する重複排除環境で Vault を構成します。コピーを含んでいる環境では構成しないでください。 Vault のために、Vault プロファイルと Vault ポリシーを構成してください。 ■ Vault プロファイルを構成します。 ■ Vault の[プロファイル (Profile)]ダイアログボックスの[バックアップの選択 (Choose Backups)]タブで、ソースメディアサーバー重複排除プール内のバックアップイメージを選択します。 ■ [プロファイル (Profile)]ダイアログボックスの[複製 (Duplication)]タブで、[宛先ストレージユニット (Destination Storage Unit)]フィールドで宛先ストレージユニットを選択します。 ■ 複製ジョブをスケジュールするために Vault ポリシーを構成します。Vault ポリシーは Vault ジョブを実行するために構成される NetBackup ポリシーです。
手順 11	`bpduplicate`コマンドの使用による複製	NetBackup の `bpduplicate` コマンドは、イメージを手動で複製する場合にのみ使います。 [メディアサーバー重複排除プール (Media Server Deduplication Pool)]または[PureDisk 重複排除プール (PureDisk Deduplication Pool)]から、同じドメイン内の別の[メディアサーバー重複排除プール (Media Server Deduplication Pool)]に複製します。 『NetBackup コマンドリファレンスガイド』を参照してください。 http://www.veritas.com/docs/DOC5332

NetBackup の最適化複製またはレプリケーション動作の設定

NetBackup について、最適化複製とレプリケーション動作を設定できます。動作は、次の表で説明するように、NetBackup によるイメージの複製方法に応じて変わります。

表 4-20 最適化複製の動作

動作	説明
NetBackup Vault または bpduplicate コマンドを使った複製	NetBackup Vault または bpduplicate コマンドを使用して複製する場合は、次の動作を設定できます。 ■ 最適化複製の試行回数。 ジョブに失敗する前に、NetBackup が最適化複製ジョブを再試行する回数を変更できます。 p.129 の「複製の試行回数を構成する方法」を参照してください。 ■ 最適化複製のフェールオーバー。 デフォルトでは、最適化された複製ジョブが失敗した場合、NetBackup はジョブを再実行しません。 最適化複製ジョブが失敗した場合には、通常の複製を使うように NetBackup を構成できます。 p.130 の「最適化複製のフェールオーバーを構成する方法」を参照してください。
ストレージライフサイクルポリシーを使った複製またはレプリケーション	ストレージライフサイクルポリシーの最適化複製またはレプリケーションジョブが失敗すると、NetBackup は 2 時間待ってからジョブを再試行します。NetBackup は、ジョブが成功するまで、またはソースバックアップイメージが期限切れになるまで、再試行の動作を繰り返します。 待機期間の時間を変更できます。 p.130 の「ストレージライフサイクルポリシーの待機時間を設定する方法」を参照してください。

複製にストレージライフサイクルポリシーを使用する場合は、NetBackup Vault に対する最適化複製動作や bpduplicate コマンドは設定しないでください。また、その逆の操作も行わないでください。NetBackup の動作は予測できない場合があります。

注意: これらの設定は、特定の NetBackup ストレージオプションに限定されず、すべての最適化複製ジョブに影響します。

複製の試行回数を構成する方法

◆ プライマリサーバーで、OPT_DUP_BUSY_RETRY_LIMIT という名前のファイルを作成します。NetBackup でジョブが失敗するまでに行うジョブの再試行回数を示す整数をファイルに追加します。

このファイルは (オペレーティングシステムに応じて) プライマリサーバーの次のディレクトリに存在する必要があります。

■ UNIX の場合: /usr/openv/netbackup/db/config

- Windows の場合: *install_path*¥NetBackup¥db¥config

最適化複製のフェールオーバーを構成する方法

◆ プライマリサーバーで、次の構成オプションを追加します。

```
RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE
```

p.130 の「コマンドラインの使用による NetBackup 構成オプションの設定」を参照してください。

UNIX システムでは代わりに、NetBackup プライマリサーバーの `bp.conf` ファイルにエントリを追加できます。

ストレージライフサイクルポリシーの待機時間を設定する方法

1. NetBackup 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。
2. 編集するホストを選択し、[プライマリサーバーの編集 (Edit primary server)]をクリックします。
3. [SLP 設定 (SLP settings)]を選択します。
4. [拡張されたイメージの再試行間隔 (Extended image retry interval)]を新しい値に変更します。
5. [保存 (Save)]をクリックします。

コマンドラインの使用による NetBackup 構成オプションの設定

Cohesityでは、NetBackup Web UI を選択してホストのプロパティを構成することをお勧めします。

ただし、NetBackup Web UI からは設定できないプロパティもあります。次の NetBackup コマンドを使って、それらのプロパティを設定できます。

NetBackup サーバーの場合: `bpsetconfig`

NetBackup クライアントの場合: `nbsetconfig`

次の例に示すように、構成オプションはキーと値のペアです。

- `CLIENT_READ_TIMEOUT = 300`
- `LOCAL_CACHE = NO`
- `RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE`
- `SERVER = server1.example.com`

`SERVER` オプションのようなオプションを複数回指定できます。

コマンドラインを使って構成オプションを設定するには

1 プロパティを設定するホストのコマンドウィンドウまたはシェルウィンドウで、適切なコマンドを呼び出します。コマンドは、次のように、オペレーティングシステムと NetBackup ホストの種類 (クライアントまたはサーバー) によって異なります。

UNIX の場合
NetBackup クライアントの場合:
`/usr/openv/netbackup/bin/nbsetconfig`
NetBackup サーバーの場合:
`/usr/openv/netbackup/bin/admincmd/bpsetconfig`

Windows の場合
NetBackup クライアントの場合:
install_path¥NetBackup¥bin¥nbsetconfig.exe
NetBackup サーバーの場合:
install_path¥NetBackup¥bin¥admincmd¥bpsetconfig.exe

2 コマンドプロンプトで、設定する構成オプションのキーと値のペアを 1 行に 1 組ずつ入力します。

既存のキーと値のペアを変更できます。

キーと値のペアを追加できます。

追加する任意の新しいオプションの許可される値と形式を理解していることを確認してください。

3 構成の変更を保存するには、オペレーティングシステムに応じて、次のコマンドを入力します。

Windows の場合: `Ctrl + Z Enter`

UNIX の場合: `Ctrl + D Enter`

異なるドメインへの MSDP レプリケーションについて

NetBackup は異なるドメインにあるストレージのレプリケーションをサポートします。NetBackup 自動イメージレプリケーションは、バックアップイメージをレプリケートするのに使われる方法です。(バックアップイメージのレプリケーションは、同じドメイン内で発生する可能性のあるスナップショットレプリケーションとは同じではありません) レプリケーションは 1 つのソースから複数の宛先に実行できます。

表 4-21では、NetBackup がサポートする MSDP のレプリケーションソースとターゲットについて説明します。

表 4-21 NetBackup メディアサーバーの重複排除におけるレプリケーションターゲット

ソーススストレージ	ターゲットストレージ
メディアサーバー重複排除プール (Media Server Deduplication Pool)	次のシステムでホスト可能な[メディアサーバー重複排除プール (Media Server Deduplication Pool)]。 ■ NetBackup メディアサーバー。 ■ NetBackup 5200 シリーズアプライアンス、または NetBackup 5300 シリーズアプライアンス。

自動イメージレプリケーションは、ストレージユニットグループからのレプリケートをサポートしません。つまり、ソースコピーはストレージユニットグループにはありません。

レプリケーションジョブが失敗すると、NetBackup はジョブが成功するかソースイメージが期限切れになるまでレプリケーションを再試行します。試行間隔の動作を変更できます。

p.128 の「NetBackup の最適化複製またはレプリケーション動作の設定」を参照してください。

いくつかのイメージをレプリケートした後でジョブが失敗した場合、NetBackup は部分的にレプリケートされたイメージのために別途イメージのクリーンアップジョブを実行することはありません。このジョブは、次回レプリケーションが実行されるときに、イメージの断片をクリーンアップしてからイメージのレプリケーションを開始します。

複製トラフィックに対して個別のネットワークを使用できます。

p.116 の「MSDP の複製およびレプリケーションに対する個別ネットワークパスについて」を参照してください。

p.132 の「異なる NetBackup ドメインへの MSDP レプリケーション設定」を参照してください。

p.43 の「MSDP の最適化複製とレプリケーションについて」を参照してください。

異なる NetBackup ドメインへの MSDP レプリケーション設定

表 4-22では、あるメディアサーバー重複排除プールから、NetBackup ドメインの異なる、別のメディアサーバー重複排除プールにバックアップイメージをレプリケートするために必要なタスクを説明しています。

必要に応じて、最適化複製トラフィックに対して個別のネットワークを使用できます。

p.116 の「MSDP の複製およびレプリケーションに対する個別ネットワークパスについて」を参照してください。

表 4-22 NetBackup MSDP レプリケーション構成タスク

手順	作業	手順詳細
手順 1	MSDP レプリケーションについて	p.131 の「異なるドメインへの MSDP レプリケーションについて」を参照してください。 p.134 の「NetBackup 自動イメージレプリケーションについて」を参照してください。
手順 2	ターゲット NetBackup ドメインと信頼関係を構成する必要があるかを判断する	信頼関係は省略可能です。 p.142 の「自動イメージレプリケーションの信頼できるプライマリサーバーについて」を参照してください。
手順 3	リモートストレージサーバーをレプリケーションターゲットとして追加する	p.152 の「リモートドメインへの MSDP レプリケーションに対するターゲットの構成」を参照してください。 p.140 の「自動イメージレプリケーションのレプリケーショントポロジーの表示」を参照してください。
手順 4	ストレージライフサイクルポリシーの構成	SLP 操作を構成するときのオプションは以下のとおりです。 ■ ターゲットドメインとの信頼関係を構成した場合、次のオプションの 1 つを指定できます。 ■ すべてのレプリケーションターゲットストレージサーバー (異なる NetBackup ドメイン全体) レプリケーションジョブの実行中、NetBackup はターゲットドメイン内でインポート SLP を自動的に作成します。 ■ 特定のマスターサーバー (A specific Master Server)。このオプションを選択したら、次に[ターゲットマスターサーバー (Target master server)]および[ターゲットインポート SLP (Target import SLP)]を選択します。 ソースドメインで SLP を構成する前に、ターゲットドメインでインポート SLP を作成する必要があります。 ■ ターゲットドメインとの信頼関係を構成しなかった場合、[すべてのレプリケーションターゲットストレージサーバー (異なる NetBackup ドメイン全体) (All replication target storage servers (across different domains))]がデフォルトで選択されます。特定のターゲットストレージサーバーは選択できません。 レプリケーションジョブの実行中、NetBackup はターゲットドメイン内でインポート SLP を自動的に作成します。 p.159 の「ストレージライフサイクルポリシーについて」を参照してください。 p.159 の「自動イメージレプリケーションに必要なストレージライフサイクルポリシーについて」を参照してください。 p.161 の「ストレージライフサイクルポリシーの作成」を参照してください。

手順	作業	手順詳細
手順 5	レプリケーション帯域幅の構成	必要に応じて、レプリケーションの帯域幅を構成できます。 p.156 の「MSDP 最適化複製とレプリケーション帯域幅の構成について」を参照してください。

NetBackup 自動イメージレプリケーションについて

1 つの NetBackup ドメインで生成されたバックアップは、1 つ以上のターゲット NetBackup ドメインのストレージにレプリケートできます。この処理は自動イメージレプリケーションと呼ばれます。

さまざまな地理的なサイトにまたがる場合が多い、他の NetBackup ドメインのストレージにバックアップをレプリケートする機能は、次のようなディザスタリカバリのニーズへの対応を容易にするのに役立ちます。

- 1 対 1 モデル
  単一の本番データセンターは 1 つのディザスタリカバリサイトにバックアップできます。
- 1 対多モデル
  単一の本番データセンターは複数のディザスタリカバリサイトにバックアップできます。
  p.136 の「1 対多の自動イメージレプリケーションモデル」を参照してください。
- 多対 1 モデル
  複数のドメインのリモートオフィスは単一ドメインのストレージデバイスにバックアップできます。
- 多対多モデル
  複数のドメインのリモートデータセンターは複数のディザスタリカバリサイトをバックアップできます。

NetBackup は、ある NetBackup ドメインのメディアサーバー重複排除プールに含まれるディスクボリュームから、別のドメインのメディアサーバー重複排除プールに含まれるディスクボリュームへの自動イメージレプリケーションをサポートします。

自動イメージレプリケーションに関する注意事項

- 自動イメージレプリケーションは合成バックアップまたは最適化された合成バックアップをサポートしません。
- 自動イメージレプリケーションでは、ディスクプールのスパンボリュームはサポートされません。NetBackup では、バックアップジョブがレプリケーション操作も含むストレージライフサイクルポリシー内にある場合は、ボリュームをスパンするディスクプールへのバックアップジョブが失敗します。
- 自動イメージレプリケーションは、ストレージユニットグループからのレプリケートをサポートしません。つまり、ソースコピーはストレージユニットグループにはありません。

- NetBackup の異なるバージョン間で自動イメージレプリケーションを実行する機能は、ベーシックイメージの互換性ルールを却下しません。たとえば、ある NetBackup ドメインで取得されたデータベースバックアップは、以前のバージョンの NetBackup ドメインにレプリケートできます。ただし、古いサーバーでは、新しいイメージから正常にリストアできない場合があります。
  バージョンの互換性と相互運用性について詳しくは、次の URL で NetBackup Enterprise Server とサーバーソフトウェアの互換性リストを参照してください。
  http://www.netbackup.com/compatibility
- 準備ができたらすぐにターゲットドメインのプライマリサーバーがイメージをインポートできるように、ソースドメインとターゲットドメインのプライマリサーバーの時計を同期します。ターゲットドメインのプライマリサーバーは、イメージの作成日時になるまでイメージをインポートできません。イメージは協定世界時 (UTC) を使うので、タイムゾーンの違いを考慮する必要はありません。

処理の概要

表 4-23は、発生ドメインとターゲットドメインのイベントの概要を説明する処理の概要です。

NetBackup は、自動イメージレプリケーション操作を管理するソースドメインとターゲットドメインでストレージライフサイクルポリシーを使います。

p.159 の「自動イメージレプリケーションに必要なストレージライフサイクルポリシーについて」を参照してください。

表 4-23　　自動イメージレプリケーション処理の概要

イベント	イベントが発生するドメイン	イベントの説明
1	元のプライマリサーバー (ドメイン 1)	クライアントは[ポリシーストレージ (Policy storage)]の選択としてストレージライフサイクルポリシーを示すバックアップポリシーに従ってバックアップされます。SLP には、ターゲットドメインの類似ストレージに少なくともレプリケーション操作を 1 つ含める必要があります。
2	ターゲットプライマリサーバー (ドメイン 2)	ターゲットドメインのストレージサーバーはレプリケーションイベントが起きたことを認識します。ストレージサーバーはターゲットドメインの NetBackup プライマリサーバーに通知します。
3	ターゲットプライマリサーバー (ドメイン 2)	NetBackup は、インポート操作を含んでいる SLP に基づいてイメージをすぐにインポートします。NetBackup は、メタデータがイメージの一部としてレプリケートされるので、イメージをすばやくインポートできます。(このインポート処理は、[カタログ (Catalog)]ユーティリティで利用可能なインポート処理とは異なります。)
4	ターゲットプライマリサーバー (ドメイン 2)	イメージがターゲットドメインにインポートされた後、NetBackup はそのドメインのコピーを管理し続けます。構成によっては、ドメイン 2 のメディアサーバーはドメイン 3 のメディアサーバーにイメージをレプリケートできます。

1 対多の自動イメージレプリケーションモデル

この構成では、すべてのコピーが並行して作成されます。コピーは 1 つの NetBackup ジョブのコンテキスト内で作成されるのと同時に、レプリケート元のストレージサーバーのコンテキスト内でコピーが作成されます。1 つのターゲットストレージサーバーが失敗すると、ジョブ全体が失敗し、後で再試行されます。

すべてのコピーには同じ[ターゲットの保持 (Target Retention)]が設定されます。ターゲットのプライマリサーバードメインごとに異なる[ターゲットの保持 (Target Retention)]を設定するには、複数のソースコピーを作成するか、ターゲットのプライマリサーバーに複製をカスケードします。

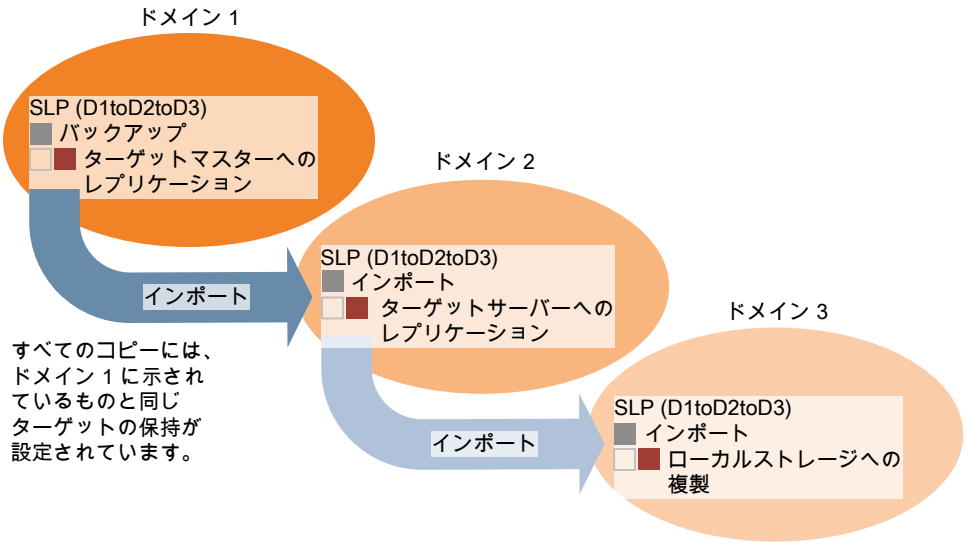
自動イメージレプリケーションモデルのカスケード

レプリケーションはレプリケート元のドメインから複数のドメインにカスケードできます。ストレージライフサイクルポリシーをドメインごとにセットアップして、レプリケート元のイメージを予想し、それをインポートしてから次のターゲットプライマリにレプリケートするようにします。

図 4-6 は、3 つのドメインに渡る次のようなカスケード構成を表します。

- イメージはドメイン 1 で作成されたのち、ターゲットのドメイン 2 にレプリケートされます。
- イメージはドメイン 2 でインポートされてから、ターゲットドメイン 3 にレプリケートされます。
- 次に、イメージはドメイン 3 にインポートされます。

図 4-6 自動イメージレプリケーションのカスケード



このカスケードモデルでは、ドメイン 2 とドメイン 3 の元のプライマリサーバーはドメイン 1 のプライマリサーバーです。

メモ: イメージがドメイン 3 にレプリケートされると、レプリケーション通知イベントはドメイン 2 のプライマリサーバーが元のプライマリサーバーであることを示します。ただし、イメージがドメイン 3 に正常にインポートされると、NetBackup は元のプライマリサーバーがドメイン 1 にあることを正しく示します。

カスケードモデルは、ターゲットプライマリにインポートされたコピーをレプリケートするインポート SLP の特殊な例です。(このプライマリサーバーは、ターゲットプライマリサーバーの文字列の先頭でも末尾でもありません。)

インポート SLP には、[固定 (Fixed)]の保持形式を使う 1 つ以上の操作と、[ターゲットの保持 (Target Retention)]形式を使う 1 つ以上の操作が含まれている必要があります。したがって、SLP のインポートがこれらの要件を満たすように、レプリケート操作は[ターゲットの保持 (Target Retention)]を使う必要があります。

表 4-24 にインポート操作のセットアップの違いを示します。

表 4-24 インポートされたコピーをレプリケートするように構成された SLP におけるレプリケート操作の違い

インポート操作の基準	カスケードモデルでのインポート操作
最初の操作はインポート操作である必要がある。	同じ、相違なし。

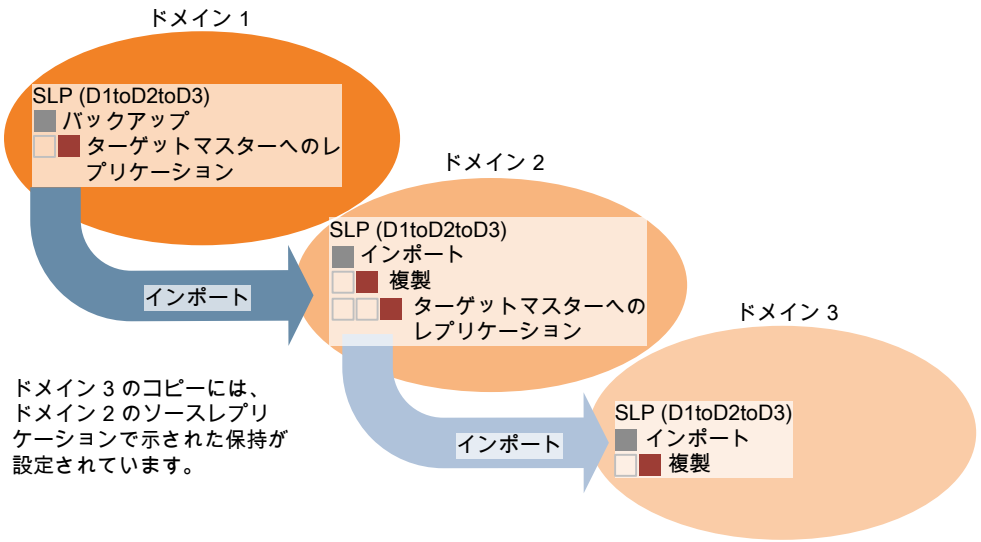
インポート操作の基準	カスケードモデルでのインポート操作
ターゲットプライマリへのレプリケーションは[固定 (Fixed)]の保持形式を使う必要がある。	同じ、相違なし。
1 つ以上のレプリケート操作が[ターゲットの保持 (Target retention)]を使う必要がある。	違いは次のとおりです。 基準を満たすには、レプリケート操作は[ターゲットの保持 (Target retention)]を使う必要があります。

ターゲットの保持はレプリケート元のイメージに埋め込まれます。

図 4-6 に示されているカスケードモデルでは、ドメイン 1 に示されている[ターゲットの保持 (Target Retention)]と同じ[ターゲットの保持 (Target Retention)]が設定されています。

ドメイン 3 のコピーが異なるターゲット保持を持つようにするには、ドメイン 2 のストレージライフサイクルポリシーに中間レプリケート操作を追加します。中間レプリケート操作は、ターゲットプライマリへのレプリケーションのソースとして機能します。ターゲットの保持がレプリケート元のイメージに埋め込まれているので、ドメイン 3 のコピーは中間レプリケート操作に設定されている保持レベルを優先します。

図 4-7 さまざまなターゲットの保持によるターゲットのプライマリサーバーへのレプリケーションのカスケード



複製用のドメインの関係について

メディアサーバーの重複排除プールがターゲットの場合: 元のドメインと (1 つ以上の) ターゲットドメイン間の関係は、元のドメインで確立されます。具体的には、ソースストレージサーバーの[ストレージサーバーの変更 (Change Storage Server)]ダイアログボックスにある[レプリケーション (Replication)]タブでターゲットストレージサーバーを構成します。

p.152 の「リモートドメインへの MSDP レプリケーションに対するターゲットの構成」を参照してください。

レプリケーション関係を設定する前に、信頼できるホストとしてターゲットプライマリサーバーを追加できます。

p.142 の「自動イメージレプリケーションの信頼できるプライマリサーバーについて」を参照してください。

注意: ターゲットストレージサーバーは慎重に選択してください。ターゲットストレージサーバーは元のドメインのストレージサーバーにならないようにする必要があります。

自動イメージレプリケーションのレプリケーショントポロジーについて

自動イメージレプリケーションの場合は、ディスクボリュームにボリューム間のレプリケーション関係を定義するプロパティがあります。ボリュームプロパティの認識が、デバイスのレプリケーショントポロジーです。ボリュームに含めることができるレプリケーションのプロパティは、次のとおりです。

ソース (Source)	ソースボリュームには、クライアントのバックアップが含まれます。このボリュームは、NetBackup のリモートドメインにレプリケートされるイメージのソースです。元のドメインの各ソースボリュームでは、ターゲットドメインに 1 つ以上のレプリケーションパートナーのターゲットボリュームがあります。
ターゲット (Target)	リモートドメインのターゲットボリュームは、元のドメインにあるソースボリュームのレプリケーションパートナーです。
なし (None)	ボリュームにレプリケーション属性がありません。

NetBackup は、[メディアサーバー重複排除プール (Media Server Deduplication Pool)]のストレージを単一ボリュームとして表示します。そのため、MSDP では常に 1 対 1 のボリューム関係があります。

ソースドメインのレプリケーション関係を構成します。これを行うには、ソースストレージサーバーの[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[レプリケーション (Replication)]タブでターゲットストレージサーバーを追加します。

p.152 の「リモートドメインへの MSDP レプリケーションに対するターゲットの構成」を参照してください。

レプリケーション関係を設定すると、NetBackup はレプリケーショントポロジを発見します。NetBackup は、[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスの[更新 (Refresh)]オプションを使うときにトポロジーの変更を検出します。

p.508 の「メディアサーバー重複排除プールのプロパティの変更」を参照してください。

NetBackup には、レプリケーショントポロジーを理解するうえで役に立つコマンドが含まれます。次の状況では、このコマンドを使ってください。

- レプリケーションターゲットを構成した後。
- ストレージサーバーを構成した後、ディスクプールを構成する前。
- ストレージを構成するボリュームに変更を加えた後。

p.140 の「自動イメージレプリケーションのレプリケーショントポロジーの表示」を参照してください。

自動イメージレプリケーションのレプリケーショントポロジーの表示

レプリケーションのソースであるボリュームは、レプリケーションのターゲットである少なくとも 1 つ以上のレプリケーションパートナーが必要です。NetBackup では、ストレージのレプリケーショントポロジーを表示できます。

p.139 の「自動イメージレプリケーションのレプリケーショントポロジーについて」を参照してください。

自動イメージレプリケーションのレプリケーショントポロジーを表示するには

◆ `bpstsinfo` コマンドを実行し、ストレージサーバー名とサーバーの形式を指定します。コマンドの構文は次のとおりです。

- Windows の場合: *install_path*¥NetBackup¥bin¥admincmd¥bpstsinfo -lsuinfo -storage_server *host_name* -stype *server_type*
- UNIX の場合: /usr/openv/netbackup/bin/admincmd/bpstsinfo -lsuinfo -storage_server *host_name* -stype *server_type*

コマンドのオプションおよび引数は次のとおりです。

host_name-storage_server	ターゲットストレージサーバーの名前。
-stype PureDisk	PureDisk を[メディアサーバー重複排除プール (Media Server Deduplication Pool)]に使います。

出力をファイルに保存して、現在のトポロジーを前のトポロジーと比較して変更箇所を判断できるようにします。

p.141 の「MSDP レプリケーション用ボリュームプロパティのサンプル出力」を参照してください。

MSDP レプリケーション用ボリュームプロパティのサンプル出力

次の 2 つの例は、2 つの NetBackup 重複排除ストレージサーバーに対する bpstsinfo-lsuinfo コマンドの出力を示します。最初の例は、元のドメイン内にあるソースディスクプールからの出力です。2 番目の例は、リモートプライマリサーバードメイン内にあるターゲットディスクプールからの出力です。

2 つの例では、次の情報を示します。

- 重複排除ディスクプール内にあるすべてのストレージが、1 つのボリュームとして表示されます。PureDiskVolume。
- 重複排除ストレージサーバー bit1.datacenter.example.com の PureDiskVolume は、レプリケーション操作のソースです。
- 重複排除ストレージサーバー target_host.dr-site.example.com の PureDiskVolume は、レプリケーション操作のターゲットです。

```
> bpstsinfo -lsuinfo -storage_server bit1.datacenter.example.com -stype PureDisk
LSU Info:
        Server Name: PureDisk:bit1.datacenter.example.com
        LSU Name: PureDiskVolume
        Allocation : STS_LSU_AT_STATIC
        Storage: STS_LSU_ST_NONE
        Description: PureDisk storage unit (/bit1.datacenter.example.com#1/2)
        Configuration:
        Media: (STS_LSUF_DISK | STS_LSUF_ACTIVE | STS_LSUF_STORAGE_NOT_FREED |
         STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE)
        Save As : (STS_SA_CLEARF | STS_SA_IMAGE | STS_SA_OPAQUEF)
        Replication Sources: 0 ( )
      Replication Targets: 1 ( PureDisk:target_host.dr-site.example.com:PureDiskVolume
 )
        Maximum Transfer: 2147483647
        Block Size: 512
        Allocation Size: 0
        Size: 74645270666
        Physical Size: 77304328192
        Bytes Used: 138
        Physical Bytes Used: 2659057664
        Resident Images: 0

> bpstsinfo -lsuinfo -storage_server target_host.dr-site.example.com -stype PureDisk
LSU Info:
        Server Name: PureDisk:target_host.dr-site.example.com
```

```
LSU Name: PureDiskVolume
Allocation : STS_LSU_AT_STATIC
Storage: STS_LSU_ST_NONE
Description: PureDisk storage unit (/target_host.dr-site.example.com#1/2)
Configuration:
Media: (STS_LSUF_DISK | STS_LSUF_ACTIVE | STS_LSUF_STORAGE_NOT_FREED |
 STS_LSUF_REP_ENABLED | STS_LSUF_REP_TARGET)
Save As : (STS_SA_CLEARF | STS_SA_IMAGE | STS_SA_OPAQUEF)
Replication Sources: 1 ( PureDisk:bit1:PureDiskVolume )
Replication Targets: 0 ( )
Maximum Transfer: 2147483647
Block Size: 512
Allocation Size: 0
Size: 79808086154
Physical Size: 98944983040
Bytes Used: 138
Physical Bytes Used: 19136897024
Resident Images: 0
```

自動イメージレプリケーションの信頼できるプライマリサーバーについて

NetBackup は、レプリケーションドメイン間の信頼関係を確立する機能を備えています。メディアサーバー重複排除プールをターゲットストレージにする場合、信頼関係の確立は省略できます。ストレージサーバーをターゲットストレージとして構成するには、まずソースの A.I.R. 操作とターゲットの A.I.R 操作間に信頼関係を確立します。

以下の項目は、信頼関係が自動イメージレプリケーションにどのように影響するかを示します。

信頼関係なし	NetBackup は、定義されたすべてのターゲットストレージサーバーにレプリケートします。特定のホストをターゲットとして選択することはできません。
信頼関係	信頼できるドメインのサブセットは、レプリケーションのターゲットとして選択できます。NetBackup は、構成されたすべてのレプリケーションターゲットよりもむしろ指定されたドメインのみにレプリケートします。この種類の自動イメージレプリケーションは「ターゲット型 A.I.R (Targeted A.I.R)」として知られます。

NetBackup CA が署名した証明書を使用した信頼できるプライマリサーバーの追加について

ターゲット型 A.I.R. では、ソースサーバーとリモートターゲットサーバー間で信頼を確立するときに、両方のドメインで信頼を確立する必要があります。

1. ソースプライマリサーバーで、信頼できるサーバーとしてターゲットプライマリサーバーを追加します。
2. ターゲットプライマリサーバーで、信頼できるサーバーとしてソースプライマリサーバーを追加します。

メモ: NetBackup Web UI は、外部 CA が署名した証明書を使用した、信頼できるプライマリサーバーの追加をサポートしていません。

---

p.147 の「信頼できるプライマリサーバーの追加」を参照してください。

p.146 の「信頼できるプライマリサーバーを追加するときに使用する証明書について」を参照してください。

次の図は、NetBackup CA が署名した証明書 (またはホスト ID ベースの証明書) を使用してソースプライマリサーバーとターゲットプライマリサーバー間の信頼を確立する場合に、信頼できるプライマリサーバーを追加する際のさまざまなタスクを示しています。

図 4-8 NetBackup CA が署名した証明書を使用して、ターゲット型 A.I.R. でプライマリサーバー間の信頼関係を確立するタスク

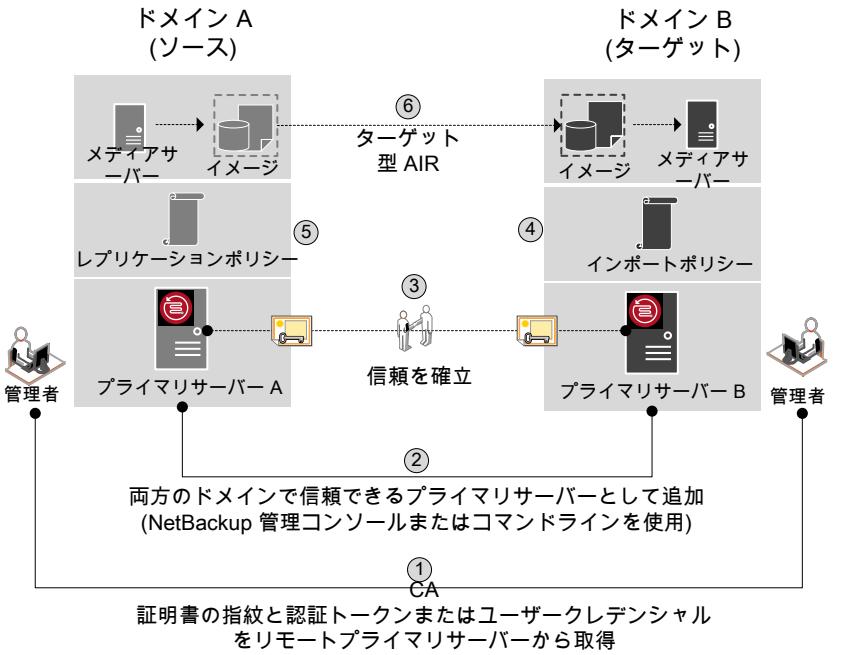


表 4-25 ターゲット型 A.I.R. でプライマリサーバー間の信頼関係を確立するタスク

手順	タスク	手順詳細
手順 1	ソースとターゲットの両方のプライマリサーバーの管理者は、お互いの CA 証明書指紋と認証トークンまたはユーザークレデンシャルを取得する必要があります。このアクティビティはオフラインで実行する必要があります。 **メモ:** 認証トークンを使用してリモートプライマリサーバーに接続することをお勧めします。認証トークンは制限付きアクセスを提供し、両方のホスト間のセキュア通信を可能にします。ユーザークレデンシャル (ユーザー名とパスワード) の使用はセキュリティ違反となることがあります。	認証トークンを取得するには、bpnbat コマンドを使用してログオンし、nbcertcmd で認証トークンを取得します。 root 証明書の SHA1 指紋を取得するには、nbcertcmd -displayCACertDetail コマンドを使用します。 このタスクを実行するには、『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:** コマンドを実行するときは、ターゲットをリモートサーバーとして保持します。
手順 2	ソースドメインとターゲットドメイン間の信頼を確立します。 ■ ソースプライマリサーバーで、信頼できるサーバーとしてターゲットプライマリサーバーを追加します。 ■ ターゲットプライマリサーバーで、信頼できるサーバーとしてソースプライマリサーバーを追加します。	NetBackup Web UI でこのタスクを実行するには、次のトピックを参照してください。 p.147 の「信頼できるプライマリサーバーの追加」を参照してください。 nbseccmd を使用してこのタスクを実行するには、『NetBackup コマンドリファレンスガイド』を参照してください。
手順 3	ソースとターゲットの信頼できるサーバーを追加したら、お互いのホスト ID ベースの証明書を持ちます。証明書は、それぞれの通信時に使用されます。 プライマリサーバー A はプライマリサーバー B が発行した証明書を持ち、その逆も同様にします。通信を行う前に、プライマリサーバー A はプライマリサーバー B が発行した証明書を提示します (その逆も同様です)。これで、ソースとターゲットのプライマリサーバー間の通信がセキュリティで保護されます。	ホスト ID ベースの証明書の使用について詳しくは『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。
手順 3.1	セキュリティ証明書とホスト ID の証明書をターゲットプライマリサーバーから取得するようにソースメディアサーバーを構成します。	p.150 の「ソースとターゲットの MSDP ストレージサーバー間で安全に通信を行うための NetBackup CA と NetBackup ホスト ID ベースの証明書の構成」を参照してください。 p.156 の「自動イメージレプリケーションに限定された権限を持つ NetBackup Deduplication Engine ユーザーの構成」を参照してください。

手順	タスク	手順詳細
手順 4	ターゲットドメインにインポートストレージライフサイクルポリシーを作成します。 **メモ:** インポートストレージライフサイクルポリシー名は 112 文字以下である必要があります。	p.159 の「ストレージライフサイクルポリシーについて」を参照してください。
手順 5	ソース MSDP サーバーで、[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[レプリケーション (Replication)]タブを使用してターゲットストレージサーバーのクレデンシャルを追加します。	p.152 の「リモートドメインへの MSDP レプリケーションに対するターゲットの構成」を参照してください。
手順 5.1	特定のターゲットプライマリサーバーとストレージライフサイクルポリシーを使用してソースドメインにレプリケーションストレージライフサイクルポリシーを作成します。 1 つの NetBackup ドメインで生成されたバックアップは、1 つ以上のターゲット NetBackup ドメインのストレージにレプリケートできます。	p.159 の「ストレージライフサイクルポリシーについて」を参照してください。
手順 6	1 つの NetBackup ドメインで生成されたバックアップは、1 つ以上のターゲット NetBackup ドメインのストレージにレプリケートできます。この処理は自動イメージレプリケーションと呼ばれます。	p.134 の「NetBackup 自動イメージレプリケーションについて」を参照してください。

ソースとターゲットの信頼できるサーバーで異なるバージョンの NetBackup を使用する場合は、次を考慮してください。

メモ: ソースとターゲット両方のプライマリサーバーをバージョン 8.1 以降にアップグレードする場合、信頼関係を更新する必要があります。次のコマンドを実行します。

```
nbseccmd -setuptrustedmaster -update
```

『NetBackup コマンドリファレンスガイド』を参照してください。

表 4-26 異なるバージョンの NetBackup での信頼の設定方法

ソースサーバーのバージョン	ターゲットサーバーのバージョン	信頼の設定方法
8.1 以降	8.1 以降	認証トークンを使用して、信頼できるプライマリサーバーを追加します。 両方のサーバーで処理を完了します。
8.1 以降	8.0 以前	ソースサーバーで、リモート (ターゲット) サーバーのクレデンシャルを使用して信頼できるプライマリサーバーとしてターゲットを追加します。

ソースサーバーのバージョン	ターゲットサーバーのバージョン	信頼の設定方法
8.0 以前	8.1 以降	ソースサーバーで、リモート (ターゲット) サーバーのクレデンシャルを使用して信頼できるプライマリサーバーとしてターゲットを追加します。

信頼できるプライマリサーバーを追加するときに使用する証明書について

ソースプライマリサーバーまたはターゲットプライマリサーバーは、NetBackup CA が署名した証明書 (ホスト ID ベースの証明書) または外部 CA が署名した証明書を使用する場合があります。

NetBackup のホスト ID ベースの証明書と外部 CA のサポートについて詳しくは、『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。

ソースプライマリサーバーとターゲットプライマリサーバー間で信頼を確立するため、NetBackup は次を確認します。

外部 CA が署名した証明書を使用してソースプライマリサーバーが信頼を確立できるかどうか。	外部 CA の構成オプション (ECA_CERT_PATH、ECA_PRIVATE_KEY_PATH、ECA_TRUST_STORE_PATH) が、ソースプライマリサーバーの NetBackup 構成ファイルで定義されている場合は、外部証明書を使用して信頼を確立できます。 Windows 証明書のトラストストアの場合、ECA_CERT_PATH オプションのみが定義されます。
ターゲットプライマリサーバーがサポートする認証局 (CA) はどれか。	ターゲットプライマリサーバーは、外部 CA、NetBackup CA、またはその両方をサポートする可能性があります。

次の表は、CA のサポートに関するシナリオ、およびソースプライマリサーバーとターゲットプライマリサーバー間で信頼を確立するために使用する証明書を示しています。この手順では、構成に NetBackup Web UI を使用することを前提としています。

表 4-27　信頼の設定に使用する証明書

プライマリサーバーが外部証明書を使用できるかどうか。	ターゲットプライマリサーバーが使用する CA はどれか。	信頼の設定に使用する証明書
はい ソースプライマリサーバーは、リモートプライマリサーバーとの通信に、NetBackup CA と外部 CA を使用できます。	外部 CA	外部 CA
	NetBackup CA	NetBackup CA
	外部 CA と NetBackup CA	NetBackup が、信頼の設定に使用する CA の選択を求めるメッセージを表示します。
いいえ ソースプライマリサーバーは、リモートプライマリサーバーとの通信に、NetBackup CA のみを使用できます。	外部 CA	信頼は確立されません。
	NetBackup CA	NetBackup CA
	外部 CA と NetBackup CA	NetBackup CA

信頼できるプライマリサーバーの追加

レプリケーション操作では、異なるドメインの NetBackup サーバー間で信頼関係が確立されている必要があります。両方が NetBackup CA または外部 CA を使用するプライマリサーバー間の信頼関係を作成できます。

始める前に、次の情報を確認してください。

- RBAC システム管理者の役割または同様の権限の役割を持っていることを確認します。または、ソフトウェアバージョン 3.1 以降のアプライアンスの場合は、NetBackup CLI ユーザーに対する権限が必要です。
- リモートの Windows プライマリサーバーの場合は、ユーザーのドメインが認証サービスのドメインと同じではない場合があります。この場合、`vssat addldapdomain` コマンドを使用して LDAP でドメインを追加する必要があります。
- NetBackup CA が署名した証明書の場合、サーバーを認証するために推奨される方法は、[信頼できるプライマリサーバーの認証トークンを指定 (Specify authentication token of the trusted primary server)]オプションです。
- [信頼できるプライマリサーバーのクレデンシャルを指定 (Specify credentials of the trusted primary server)]オプションを使用すると、その方法によってセキュリティ違反が発生する可能性があります。制限付きアクセスを提供し、両方のホスト間で安全な通信を許可できるのは、認証トークンのみです。NetBackup プライマリアプライアンス 3.1 との信頼を確立するには、NetBackup CLI クレデンシャルを使用します。

信頼できるプライマリサーバーを追加するには

1. NetBackup Web UI を開きます。
2. ソースサーバーとターゲットサーバーのそれぞれで、インストールされている NetBackup バージョンと使用されている証明書の種類を識別します。

   NetBackup Web UI では、NetBackup バージョン 8.0 以前を使用する信頼できるプライマリの追加はサポートされていません。両方のサーバーで同じ証明書の種類を使用する必要があります。
3. NetBackup CA (認証局) を使用するサーバーの場合は、リモートサーバーの認証トークンを取得します。
4. NetBackup CA (認証局) を使用するサーバーの場合は、各サーバーの指紋を取得します。
5. 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。
6. [信頼できるプライマリサーバー (Trusted primary servers)]タブを選択します。
7. [追加 (Add)]ボタンを選択します。
8. リモートプライマリサーバーの完全修飾ホスト名を入力し、[認証局の検証 (Validate Certificate Authority)]を選択します。
9. ウィザードに表示されるプロンプトに従います。
10. リモートプライマリサーバーでこの手順を繰り返します。

詳細情報

NetBackup での外部 CA の使用について詳しくは、『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。

信頼できるプライマリサーバーの削除

メモ: NetBackup バージョン 8.0 以前の信頼できるプライマリサーバーは、NetBackup 管理コンソールまたは NetBackup CLI を使用して削除する必要があります。

信頼できるプライマリサーバーを削除できます。これにより、プライマリサーバー間の信頼関係が削除されます。次の点に注意してください。

- 信頼関係を必要とするレプリケーション操作はすべて失敗します。
- 信頼関係を削除した後、リモートプライマリサーバーはどの使用状況レポートにも含まれなくなります。

信頼できるプライマリサーバーを削除するには、ソースサーバーとターゲットサーバーの両方で次の手順を実行する必要があります。

信頼できるプライマリサーバーを削除するには

1. NetBackup Web UI を開きます。
2. ターゲットプライマリサーバーへのすべてのレプリケーションジョブが完了していることを確認します。
3. 宛先として信頼できるプライマリを使用するすべてのストレージライフサイクルポリシー (SLP) を削除します。SLP を削除する前に、ストレージに SLP を使うバックアップポリシーまたは保護計画がないことを確認します。
4. 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。
5. [信頼できるプライマリサーバー (Trusted primary servers)]タブを選択します。
6. 削除するサーバーを特定します。
7. [操作 (Actions)]、[削除 (Remove)]の順に選択します。
8. [信頼を削除 (Remove trust)]を選択します。

メモ: 複数の NIC を使用する場合に、複数のホスト NIC を使用して信頼を確立し、いずれかのホスト NIC との信頼関係を削除すると、それ以外のすべてのホスト NIC との信頼関係が失われます。

NetBackup のクラスタ化されたプライマリサーバーのノード間認証の有効化

NetBackup にはクラスタ内のプライマリサーバーでのノード間の認証が必要です。認証では、クラスタのすべてのノード上で認証証明書をプロビジョニングすることが必要です。証明書は、NetBackup ホスト間で SSL 接続を確立するために利用されます。

p.147 の「信頼できるプライマリサーバーの追加」を参照してください。

ノード間認証によって、次の NetBackup 機能が可能になります。

NetBackup Web UI	プライマリサーバークラスタの NetBackup Web UI は、正常な機能を得るために NetBackup の認証証明書を必要とします。
ターゲット型 A.I.R. (自動イメージレプリケーション)	プライマリサーバーがクラスタにある自動イメージレプリケーションでは、そのクラスタ内のホストでノード間認証が必要です。NetBackup の認証証明書は適切な信頼関係を確立する手段となります。 信頼できるプライマリサーバーを追加する前に、クラスタホスト上で証明書をプロビジョニングする必要があります。この必要条件は、クラスタ化されたプライマリサーバーがレプリケーション操作のソースかターゲットかにかかわらず、適用されます。

NetBackup のクラスタ化されたプライマリサーバーのノード間認証を有効にする方法

- NetBackup プライマリサーバークラスタのアクティブノードで、次の NetBackup コマンドを実行します:
  - Windows の場合: *install_path*¥NetBackup¥bin¥admincmd¥bpnbaz -setupat
  - UNIX の場合: /usr/openv/netbackup/bin/admincmd/bpnbaz -setupat

  NetBackup によって、プライマリサーバークラスタの各ノードに証明書が作成されます。

  次に出力例を示します。

```
# bpnbaz -setupat
You will have to restart Netbackup services on this machine after

the command completes successfully.
Do you want to continue(y/n)y
Gathering configuration information.
Please be patient as we wait for 10 sec for the security services

to start their operation.
Generating identity for host 'bit1.remote.example.com'
Setting up security on target host: bit1.remote.example.com
nbatd is successfully configured on Netbackup Primary Server.
Operation completed successfully.
```

ソースとターゲットの MSDP ストレージサーバー間で安全に通信を行うための NetBackup CA と NetBackup ホスト ID ベースの証明書の構成

MSDP は、2 つの異なる NetBackup ドメインからの 2 台のメディアサーバー間での安全な通信をサポートするようになりました。安全な通信は、自動イメージレプリケーション (A.I.R) の実行時に設定されます。証明書のセキュリティチェックを行うため、2 台のメディアサーバーでは同じ CA を使用する必要があります。ソース MSDP サーバーは、ターゲット NetBackup ドメインの CA と、ターゲット NetBackup ドメインによって認可された証明書を使用します。自動イメージレプリケーションを使用する前に、CA およびソース MSDP サーバーにある証明書を手動で配備する必要があります。

メモ: NetBackup 8.1.2 以降へのアップグレード後、既存の自動イメージレプリケーションを使用するには、ソース MSDP サーバーで NetBackup CA と NetBackup ホスト ID ベースの証明書を手動で配備します。

NetBackup CA と NetBackup ホスト ID ベースの証明書を構成するには、次の手順を実行します。

1. ターゲット NetBackup プライマリサーバーで、次のコマンドを実行して NetBackup CA の指紋を表示します。
   - Windows の場合:
     install_path¥NetBackup¥bin¥nbcertcmd -displayCACertDetail
   - UNIX
     /usr/openv/netbackup/bin/nbcertcmd -displayCACertDetail
2. ソース MSDP ストレージサーバーで、次のコマンドを実行して、ターゲット NetBackup プライマリサーバーから NetBackup CA を取得します。
   - Windows の場合:
     install_path¥NetBackup¥bin¥nbcertcmd -getCACertificate -server *target_primary_server*
   - UNIX
     /usr/openv/netbackup/bin/nbcertcmd -getCACertificate -server *target_primary_server*

   CA を受け入れる際、CA の指紋が前の手順で表示されるものと同じであることを確認します。
3. ソース MSDP ストレージサーバーで、次のコマンドを実行して、ターゲット NetBackup プライマリサーバーによって生成された証明書を取得します。
   - Windows
     install_path¥NetBackup¥bin¥nbcertcmd -getCertificate -server *target_primary_server* -token *token_string*
   - UNIX
     /usr/openv/netbackup/bin/nbcertcmd -getCertificate -server *target_primary_server* -token *token_string*
4. 認証トークンを取得するには、次の 2 つの方法のいずれかを使用します。
   - NetBackup Web UI
     - NetBackup Web UI で、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
     - [追加 (Add)]をクリックし、必要な詳細を入力してトークンを作成します。
   - NetBackup コマンド
     - ターゲット NetBackup プライマリサーバーにログオンするには、bpnbat コマンドを使用します。

- 認証トークンを取得するには、nbcertcmd コマンドを使用します。

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。

ソース MSDP ストレージサーバーとターゲット MSDP ストレージサーバー間での安全な通信のための外部 CA の構成

MSDP は、2 つの異なる NetBackup ドメインからの 2 台のメディアサーバー間で、外部 CA を使用した安全な通信をサポートするようになりました。安全な通信は、自動イメージレプリケーション (A.I.R) の実行時に設定されます。2 台のメディアサーバー間で異なる外部 CA を使用している場合、自動イメージレプリケーションを使用する前に、外部証明書を交換する必要があります。

外部証明書を交換するには、次の手順を完了します。

1. ルート証明書ファイルを、ソース MSDP ストレージサーバーからターゲット MSDP ストレージサーバーにコピーします。ターゲット MSDP ストレージサーバー上の証明書ファイルを結合します。
2. ルート証明書ファイルを、ターゲット MSDP ストレージサーバーからソース MSDP ストレージサーバーにコピーします。ソース MSDP ストレージサーバー上の証明書ファイルを結合します。

ルート証明書の格納に Windows 証明書ストアを使用している場合は、ルート証明書を証明書ストアに追加します。certutil ツールを使用して root 証明書を証明書ストアに追加できます。または、root 証明書ファイルを右クリックして、[証明書のインストール (Install Certificate)] を選択します。certutil ツールを使用して root 証明書をインストールする場合、ストア名パラメータは Root にする必要があります。Windows エクスプローラを使用してルート証明書をインストールする場合、ストアの場所はローカルマシンで、ストア名は信頼できるルート認証局にする必要があります。

リモートドメインへの MSDP レプリケーションに対するターゲットの構成

元のドメインの [メディアサーバー重複排除プール (Media Server Deduplication Pool)] から別のターゲットドメインの重複排除プールへのレプリケーションのターゲットを設定するには、次の手順を実行します。NetBackup は複数の重複排除ターゲットをサポートします。

p.131 の「異なるドメインへの MSDP レプリケーションについて」を参照してください。

ターゲットストレージサーバーの構成は、MSDP レプリケーション処理内でただ 1 つの手順です。

p.132 の「異なる NetBackup ドメインへの MSDP レプリケーション設定」を参照してください。

メモ: クラスタ化されたプライマリサーバーについて: レプリケーション操作のために信頼できるプライマリサーバーを追加する場合は、クラスタ内のすべてのノードのノード間認証を有効にする必要があります。次の手順を始める前に、認証を有効にします。この必要条件は、クラスタ化されたプライマリサーバーがレプリケーション操作のソースかターゲットかにかかわらず、適用されます。

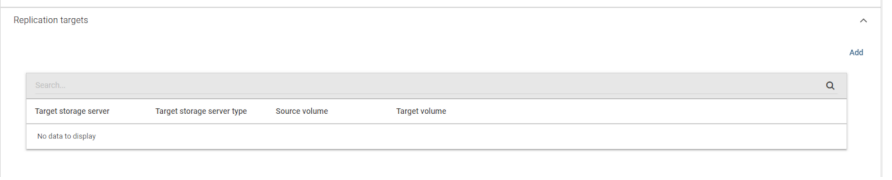
p.142 の「自動イメージレプリケーションの信頼できるプライマリサーバーについて」を参照してください。

p.149 の「 NetBackup のクラスタ化されたプライマリサーバーのノード間認証の有効化 」を参照してください。

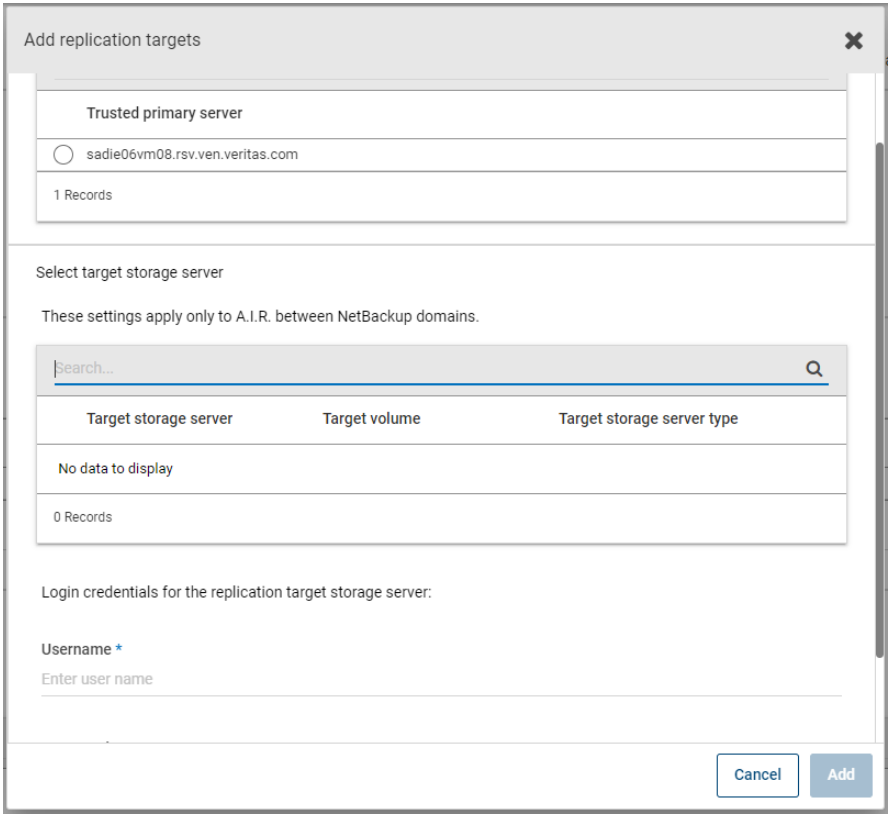
注意: ターゲットストレージサーバーは慎重に選択してください。ターゲットストレージサーバーはソースドメインのストレージサーバーにならないようにする必要があります。また、ディスクボリュームは複数の NetBackup ドメイン間で共有しないようにする必要があります。

メディアサーバー重複排除プールをレプリケーション先として構成する方法

1. Web UI を開きます。
2. 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。
3. [ディスクプール (Disk pools)]タブをクリックします。
4. ディスクプール名をクリックします。
5. [詳細 (Details)]タブで、[レプリケーションターゲット (Replication targets)]を見つけます。次に、[追加 (Add)]をクリックします。



6 信頼できるプライマリサーバーを選択します。



7 必要なターゲットストレージサーバーを選択します。

8 ユーザー名とパスワードを入力します。

9 [追加 (Add)]をクリックします。

レプリケーションターゲットを構成することで、両方のドメインにあるディスクボリュームのレプリケーションプロパティが構成されます。ただし、重複排除プールを更新して、NetBackup が新しいボリュームプロパティを読み取るようにする必要があります。

p.508 の「メディアサーバー重複排除プールのプロパティの変更」を参照してください。

MSDP レプリケーションのターゲットオプション

次の表は、NetBackup メディアサーバー重複排除プールへのレプリケーションターゲットのオプションについて説明しています。

表 4-28 MSDP レプリケーションターゲットのオプション

オプション	説明
ターゲットマスターサーバー (Target Master Server)	信頼できるすべてのプライマリサーバーがドロップダウンリストに表示されます。 バックアップのレプリケートが必要なターゲットドメインのためのプライマリサーバーを選択します。 信頼済みのプライマリとして別のドメインのプライマリサーバーを追加するには、[新規の信頼できるマスターサーバーを追加 (Add a new Trusted Master Server)]を選択します。特定のレプリケーションターゲットを選択する場合にのみ、信頼関係の構成が必要となります。
ターゲットストレージサーバーの形式 (Target storage server type)	信頼できるプライマリサーバーが構成されている場合の値は、ターゲットストレージサーバー名です。 信頼できるプライマリサーバーが構成されていない場合の値は、PureDisk です。
ターゲットストレージサーバー名 (Target storage server name)	信頼できるプライマリサーバーが設定されている場合、ターゲットストレージサーバーを選択します。信頼できるプライマリサーバーが設定されていない場合、ターゲットストレージサーバーの名前を入力します。 ドロップダウンリストには [ターゲットストレージサーバーの形式 (Target storage server type)]と一致するすべてのストレージサーバーが示されます。
ユーザー名 (User name)	レプリケーションターゲットを設定すると、NetBackup はターゲットストレージサーバーのユーザーアカウントで[ユーザー名 (User name)]フィールドを追加します。次のようになります。 ■ MSDP ターゲットの場合は、NetBackup 重複排除エンジンのユーザー名です。 セキュリティを強化するために、重複排除エンジンのユーザーに限定的な権限を付与できます。 p.156 の「自動イメージレプリケーションに限定された権限を持つ NetBackup Deduplication Engine ユーザーの構成」を参照してください。
パスワード (Password)	NetBackup 重複排除エンジンのパスワードを入力します。

p.152 の「リモートドメインへの MSDP レプリケーションに対するターゲットの構成」を参照してください。

自動イメージレプリケーションに限定された権限を持つ NetBackup Deduplication Engine ユーザーの構成

MSDP は、自動イメージレプリケーション専用のユーザーの作成をサポートします。自動イメージレプリケーションに限定された権限を持つユーザーは、管理者権限を持つユーザーよりも安全です。

自動イメージレプリケーションに限定された権限を持つ NetBackup Deduplication Engine ユーザーを構成するには、次の手順を完了します。

1. ターゲット MSDP サーバーで次のコマンドを実行して AIR のユーザーを追加します。

   Windows

   ```
   <install_path>/pdde/spauser -a -u <username> -p <password> --role
   air --owner root
   ```

   UNIX

   ```
   /usr/openv/pdde/pdcr/bin/spauser -a -u <username> -p <password>
   --role air --owner root
   ```

2. ソース NetBackup プライマリサーバーでレプリケーションターゲットとして MSDP を構成するときに、A.I.R. に限定された権限を持つユーザーのユーザー名とパスワードを入力します。

MSDP 最適化複製とレプリケーション帯域幅の構成について

各最適化複製または自動イメージレプリケーションジョブは個別のプロセスまたはストリームです。同時に実行する複製ジョブまたはレプリケーションジョブの数によって、帯域幅が競合するジョブの数が決まります。最適化複製ジョブと自動イメージレプリケーションジョブが使用するネットワーク帯域幅の量を制御できます。

2 つの構成ファイルの設定によって、次のように使われる帯域幅を制御します。

bandwidthlimit	bandwidthlimit ファイルの bandwidthlimit パラメータはグローバルな帯域幅設定です。このパラメータを使用して、すべてのレプリケーションジョブが使う帯域幅を制限できます。メディアサーバー重複排除プールがソースであるジョブに適用されます。そのため、ソースストレージサーバー上に構成します。 bandwidthlimit がゼロより大きい場合、すべてのジョブが帯域幅を共有します。つまり、各ジョブの帯域幅はジョブの数で割られた bandwidthlimit です。 bandwidthlimit=0 の場合、総帯域幅は制限されません。ただし、各ジョブが使う帯域幅を制限できます。次の OPTDUP_BANDWIDTH の説明を参照してください。 帯域幅制限を指定した場合、すべての宛先への最適化複製およびレプリケーショントラフィックが制限されます。 デフォルトでは、bandwidthlimit=0 です。 agent.cfg ファイルは、次のディレクトリに存在します。 ■ UNIX の場合: *storage_path*/etc/puredisk ■ Windows の場合: *storage_path*¥etc¥puredisk
OPTDUP_BANDWIDTH	OPTDUP_BANDWIDTH ファイルの OPTDUP_BANDWIDTH パラメータはジョブごとの帯域幅を指定します。 OPTDUP_BANDWIDTH は bandwidthlimit ファイルの bandwidthlimit パラメータがゼロのときにのみ適用されます。 OPTDUP_BANDWIDTH と bandwidthlimit が両方とも 0 の場合、レプリケーションジョブごとに帯域幅は制限されません。 デフォルトでは、OPTDUP_BANDWIDTH = 0 です。 p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。 p.175 の「MSDP pd.conf ファイルの編集」を参照してください。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

p.124 の「同じ NetBackup ドメインでの MSDP 最適化複製の構成」を参照してください。

p.132 の「異なる NetBackup ドメインへの MSDP レプリケーション設定」を参照してください。

大規模なイメージの最適化複製とレプリケーションのパフォーマンスチューニングについて

最適化複製ジョブまたは AIR ジョブを開始して大規模なイメージを移動する場合は、パフォーマンスを改善するためにソースの agent.cfg ファイルの WorkerThreadNumber と FragmentGranularity パラメータを調整します。

この agent.cfg ファイルは、MSDP ストレージサーバーの次のディレクトリにあります。

- UNIX の場合: <storage_path>/etc/puredisk
- Windows の場合: <storage_path>¥etc¥puredisk

スレッドプールは、同時性を向上させるために使用されます。WorkerThreadNumber パラメータによって、スレッドプールのスレッド数が定義されます。このパラメータには 0 から 128 の値を指定できます。デフォルトの値は 64 です。値が 0 に設定されている場合、スレッドプールは無効になります。

FragmentGranularity パラメータは、1 つのスレッドが処理するフラグメントの数を定義します。このパラメータには 1 から 1048576 の値を指定できます。デフォルト値は 8 です。

MSDP クラウドの最適化複製とレプリケーションのパフォーマンスチューニングについて

最適化複製ジョブまたは AIR ジョブを、クラウド LSU からローカル LSU または別のクラウド LSU 宛に開始するときに、高遅延ネットワークの場合はパフォーマンスを向上させるためにソース側の MaxPredownloadBatchCount パラメータをチューニングします。

agent.cfg ファイル内の MaxPredownloadBatchCount パラメータは、すべてのクラウド LSU のグローバル設定です。このパラメータをチューニングしてクラウド LSU からのダウンロードの並列実行数を制御し、パフォーマンスを向上できます。

このパラメータの範囲は 0 から 100 です。デフォルトの値は 20 です。値を 0 に設定すると、ダウンロードの並列実行は無効になります。

この agent.cfg ファイルは、MSDP ストレージサーバーの次のディレクトリにあります。

UNIX: <*storage_path*>/etc/puredisk

ストレージライフサイクルポリシーについて

メモ: SLP は NetBackup Web UI から構成できます。既存の SLP を表示したり、新しい SLP を作成したりする場合は、左側のナビゲーションペインで[ストレージ (Storage)]、[ストレージライフサイクルポリシー (Storage Lifecycle Policies)]の順にクリックします。

ストレージライフサイクルポリシー (SLP) は、一連のバックアップのストレージ計画です。SLP は、[ストレージライフサイクルポリシー (Storage Lifecycle Policies)] ユーティリティで構成します。

SLP はストレージ操作の形の手順を含み、バックアップポリシーによってバックアップされるデータに適用されます。操作はデータがどのように保存、コピー、レプリケート、保持されるかを決定する SLP に追加されます。NetBackup は必要に応じて、すべてのコピーが作成されるようにコピーを再試行します。

SLP によって、ユーザーはポリシーレベルでデータに分類を割り当てられるようになります。データの分類は、一連のバックアップ要件を表します。データの分類を使用すると、さまざまな要件でデータのバックアップを簡単に構成できるようになります。たとえば、電子メールデータと財務データなどがあります。

SLP はステージングされたバックアップ動作を行うように設定できます。SLP に含まれるすべてのバックアップイメージに所定の操作を適用することでデータ管理が簡略化されます。この処理によって、NetBackup 管理者は、ディスクを使用したバックアップの短期的な利点を活かすことができます。また、テープを使用したバックアップの長期的な利点を活かすこともできます。

NetBackup Web UI の[SLP パラメータ (SLP Parameters)]プロパティによって、管理者は SLP をどのように維持し、どのように SLP ジョブを実行するかをカスタマイズできます。

SLP についてのベストプラクティスの情報は、次に挙げるドキュメントに記載されています。

https://www.veritas.com/content/support/ja_JP/article.100009913

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

自動イメージレプリケーションに必要なストレージライフサイクルポリシーについて

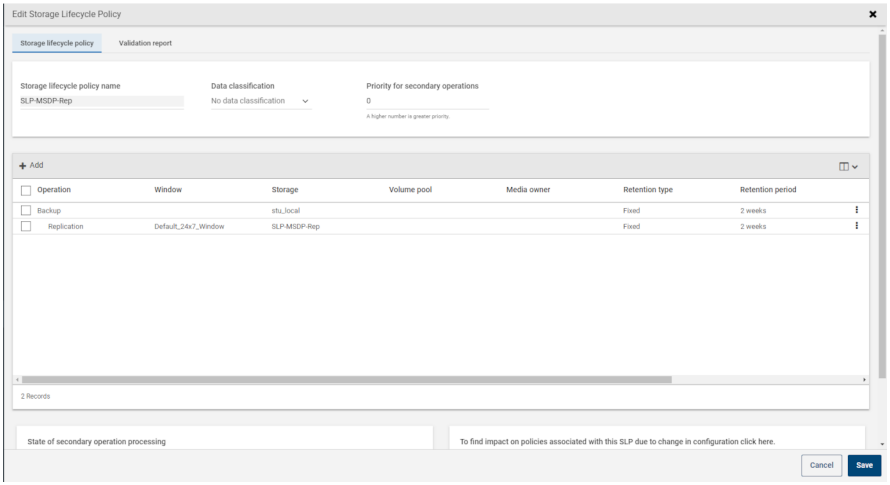
ある NetBackup ドメインから別の NetBackup ドメインにイメージを複製するには、2 つのストレージライフサイクルポリシーが必要です。次の表は、ポリシーおよび必要条件を記述したものです:

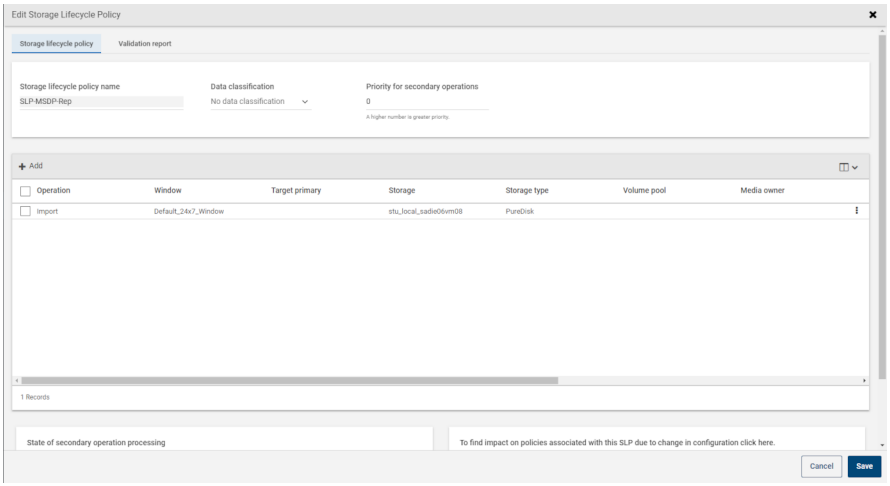
表 4-29　自動イメージレプリケーションの SLP 要件

ドメイン	ストレージライフサイクルポリシーの要件
ドメイン 1 (ソースドメイン)	ソースドメインの自動イメージレプリケーションの SLP は、次の基準を満たす必要があります: ■ 最初の操作は、メディアサーバー重複排除プール へのバックアップ操作である必要があります。ドロップダウンリストから正確なストレージユニットを指定してください。[任意 (Any Available)]は選択しません。 **メモ:** イメージをインポートするためには、ターゲットドメインに同じストレージ形式が含まれている必要があります。 ■ 少なくとも 1 つの操作は、別の NetBackup ドメインの [メディアサーバー重複排除プール (Media Server Deduplication Pool)] への[レプリケーション (Replication)]操作) である必要があります。自動イメージレプリケーションの SLP で、複数のレプリケーション操作を設定できます。[レプリケーション (Replication)]操作の設定で、バックアップがすべてのプライマリサーバードメインのすべてのレプリケーションターゲットで複製されるか、特定のレプリケーションターゲットのみに複製されるかを決定します。 ■ この SLP はドメイン 2 のインポート SLP と同じデータ分類である必要があります。
ドメイン 2 (ターゲットドメイン)	すべてのドメインのすべてのターゲットに複製する場合、各ドメインで、必要なすべての条件を満たすインポート SLP が NetBackup で自動的に作成されます。 **メモ:** 特定のターゲットに複製する場合、元のドメインで自動イメージレプリケーションの SLP を作成する前にインポート SLP を作成します。 インポート SLP は次の基準を満たす必要があります。 ■ SLP の最初の操作は[インポート (Import)]操作である必要があります。NetBackup は、ソースストレージからの複製のターゲットとして宛先ストレージをサポートしていなければなりません。ドロップダウンリストから正確なストレージユニットを指定してください。[任意 (Any Available)]は選択しません。 ■ SLP には、[ターゲットの保持 (Target retention)]が指定された操作が 1 つ以上含まれている必要があります。 ■ この SLP はドメイン 1 の SLP と同じデータ分類である必要があります。データ分類の一致により、分類に対して一貫した意味が保たれ、データ分類によるグローバルな報告が促進されます。

元のプライマリサーバードメインからのイメージがターゲットドメイン上の SLP 設定によってレプリケーションされる例を図 4-9 に示します。

図 4-9 自動イメージレプリケーションに必要なストレージライフサイクルポリシーのペア





メモ: SLP で操作をする場合には、基になるストレージへ変更を加えた後で `nbstserv` を再起動してください。

ストレージライフサイクルポリシーの作成

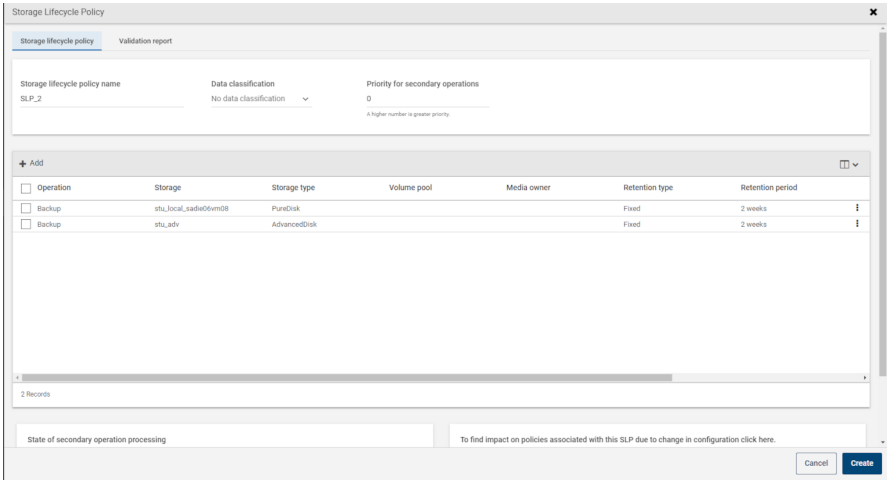
ストレージライフサイクルポリシー (SLP) は、一連のバックアップのストレージ計画です。SLP の操作はデータのバックアップ指示です。複数のストレージ操作を含んでいる SLP を作成するには、次の手順を使います。

ストレージ操作をストレージライフサイクルポリシーに追加する方法

1. NetBackup Web UI で、[ストレージ (Storage)]、[ストレージライフサイクルポリシー (SLP) (Storage lifecycle policies)]の順に選択します。
2. [追加 (Add)]をクリックします。
3. ストレージライフサイクルポリシー名を入力します。
4. SLP に 1 つ以上の操作を追加します。操作は、SLP がバックアップポリシーで従い、適用する手順です。

   これが SLP に追加される最初の操作であれば、[追加 (Add)]をクリックします。

   子操作を追加するには、操作を選択して[子の追加 (Add child)]をクリックします。



5. 操作の種類を選択します。子操作を作成している場合、SLP は選択した親操作に基づいて有効である操作だけを表示します。
6. 操作のプロパティを設定します。
7. [時間帯 (Window)]タブには、[スナップショットからのバックアップ (Backup From Snapshot)]、[複製 (Duplication)]、[インポート (Import)]、[スナップショットからのインデックス (Index From Snapshot)]および[レプリケーション (Replication)]の操作形式が表示されます。セカンダリ操作をいつ実行するかを制御したい場合は、操作の時間帯を作成します。
8. [プロパティ (Properties)]タブで、[詳細 (Advanced)]をクリックします。時間帯が終了した後に NetBackup でアクティブなイメージを処理するかどうかを選択します。
9. [作成 (Create)]をクリックして、操作を作成します。
10. 必要に応じて、追加の操作を SLP に追加します。(手順 4 を参照してください。)

11 必要に応じて、SLP の操作の階層を変更します。

12 [作成 (Create)]をクリックして、SLP を作成します。SLP は、最初に作成したときと変更するたびに NetBackup によって検証されます。

13 バックアップポリシーを設定し、ストレージライフサイクルポリシーを Policy storage として選択します。

p.166 の「バックアップポリシーの作成」を参照してください。

ストレージライフサイクルポリシーの設定

次の表に、ストレージライフサイクルポリシーの設定を示します。

図 4-10 [ストレージライフサイクルポリシー (Storage lifecycle policy)]タブ

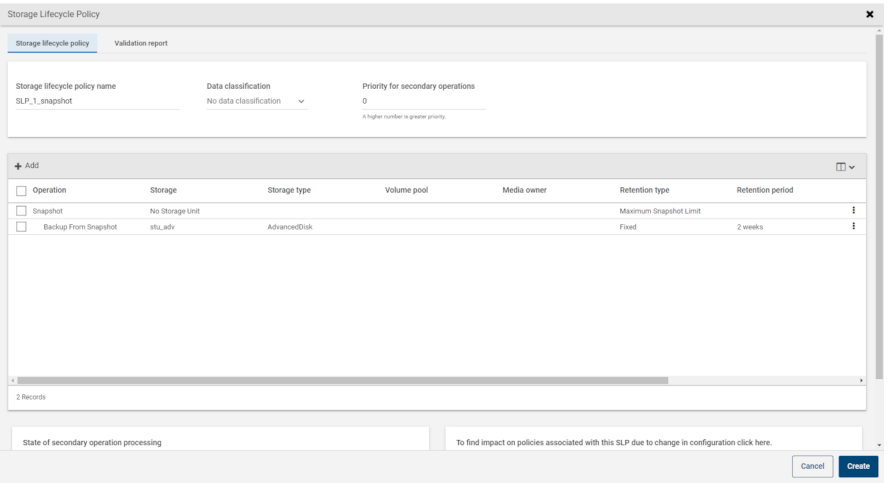


表 4-30 [ストレージライフサイクルポリシー (Storage lifecycle policy)]タブ

設定	説明
ストレージライフサイクルポリシー名 (Storage lifecycle policy name)	[ストレージライフサイクルポリシー名 (Storage lifecycle policy name)] は、SLP の説明です。SLP が作成された後は、名前は変更できません。

設定	説明
データの分類 (Data classification)	[データの分類 (Data classification)]は、SLP が処理できるデータのレベルや分類を定義します。ドロップダウンメニューには定義済みの分類がすべて表示され、そこには SLP に固有の[任意 (Any)]分類も含まれます。 [任意 (Any)]を選択すると、データの分類に関係なく、提出されるすべてのイメージを保存するよう SLP に指示します。SLP 設定のみに利用可能で、バックアップポリシーの設定には使用できません。 マスターサーバードメインが異なるバージョンの NetBackup を実行する自動イメージレプリケーション構成については、次のトピックにある特別な考慮事項を参照してください。 p.159 の「自動イメージレプリケーションに必要なストレージライフサイクルポリシーについて」を参照してください。 データ分類 は省略可能な設定です。 1 つのデータ分類は各 SLP に割り当て可能で、SLP のすべての操作に適用されます。 [任意 (Any)]以外のデータの分類を選択すると、SLP は、その分類に設定されたポリシーに含まれるイメージのみを格納します。データの分類を指定しない場合は、SLP はすべての分類のイメージおよび分類が設定されていないイメージを受け入れます。 [データの分類 (Data classification)]を使用すると、NetBackup 管理者は相対的な重要度に基づいてデータを分類できます。分類は、一連のバックアップ要件を表します。データがさまざまなバックアップ要件を満たす必要がある場合は、さまざまな分類の割り当てを検討します。 たとえば、電子メールバックアップデータをシルバーのデータの分類に割り当て、財務データのバックアップをプラチナの分類に割り当てる場合があります。 バックアップポリシーは、バックアップデータをデータ分類と関連付けます。ポリシーデータは同じデータの分類の SLP でのみ保存できます。 データが SLP でバックアップされたら、データは SLP の構成に従って管理されます。SLP によって、最初のバックアップからイメージの最後のコピーが期限切れになるまでに行われるデータへの処理が定義されます。
セカンダリ操作の優先度 (Priority for secondary operations)	[セカンダリ操作の優先度 (Priority for secondary operations)]オプションは、他のすべてのジョブに対する、セカンダリ操作からのジョブの優先度です。優先度は、バックアップ操作とスナップショット操作を除くすべての操作から派生するジョブに適用されます。範囲は、0 (デフォルト) から 99999 (最も高い優先度) です。 たとえば、データの分類にゴールドが指定されたポリシーの[セカンダリ操作の優先度 (Priority for secondary operations)]を、データの分類にシルバーが指定されたポリシーよりも高く設定できます。 バックアップジョブの優先度は、[属性 (Attributes)]タブのバックアップポリシーで設定されます。

設定	説明
操作 (Operation)	SLP の操作のリストを作成するには、[追加 (Add)]、[変更 (Change)]、および[削除 (Remove)]ボタンを使います。SLP は 1 つ以上の操作を含む必要があります。複数の操作は複数コピーが作成されることを意味します。 リストには、各操作の情報を表示する列もあります。デフォルトでは、すべての列が表示されているわけではありません。
矢印	各コピーのコピー元のインデント (または階層) は、矢印を使用して示します。1 つのコピーは他の多くのコピーのソースである場合もあります。
有効 (Active) および 延期 (Postponed)	[有効 (Active)]と[延期 (Postponed)]オプションは、[二次操作処理の状態 (State of Secondary Operation Processing)]下に表示され、SLP でのすべての複製操作の処理を対象とします。 **メモ:** [有効 (Active)]と[延期 (Postponed)]オプションは、tar 書式付きのイメージを作成する複製操作に適用されます。たとえば、bpduplicate で作成されるイメージなどです。[有効 (Active)]と[延期 (Postponed)]オプションは、OpenStorage の最適化複製や NDMP の結果として複製されたイメージには影響しません。また、1 つ以上の宛先ストレージユニットがストレージユニットグループの一部として指定されている場合も影響しません。 ■ できるだけ早くセカンダリ操作を続行するには、[有効 (Active)]を有効にします。[延期 (Postponed)]から[有効 (Active)]に変更された場合、NetBackup はセカンダリ操作が無効になったときに中断した位置から再開してイメージを処理し続けます。 ■ [延期 (Postponed)]を有効にして、SLP 全体でセカンダリ操作を延期します。[延期 (Postponed)]は複製ジョブの作成は延期しませんが、イメージの作成を延期します。複製ジョブは作成され続けますが、セカンダリ操作が再度有効になるまで実行されません。 SLP のすべてのセカンダリ操作は、管理者が[有効 (Active)]を選択するか、[終了 (Until)]オプションが選択され、有効化する日付が指定されるまで無期限に無効のままです。
[バックアップポリシー間の検証 (Validate Across Backup Policies)]ボタン	このボタンを使うと、この SLP への変更がこの SLP と関連付けられているポリシーにどのように影響するかを確認できます。ボタンを押すとレポートが生成され、[検証レポート (Validation Report)]タブに表示されます。 このボタンを nbstl コマンドと一緒に使用すると、-conflict オプションと同じ検証を実行します。

MSDP バックアップポリシーの構成について

バックアップポリシーを構成する場合、[ポリシーストレージ (Policy storage)]で、重複排除プールを使用するストレージユニットを選択します。

ストレージライフサイクルポリシーの場合、[ストレージユニット (Storage unit)]で、重複排除プールを使用するストレージユニットを選択します。

VMware バックアップの場合、VMware バックアップポリシーを構成するときに[VM バックアップからのファイルリカバリを有効にする (Enable file recovery from VM backup)]オプションを選択します。[VM バックアップからのファイルリカバリを有効にする (Enable

file recovery from VM backup)]オプションを選択すると、重複排除率が最も高くなります。

NetBackup は、重複排除ストレージユニットに送信するクライアントデータを重複排除します。

p.53 の「MSDP のストレージユニットグループについて」を参照してください。

p.52 の「MSDP の圧縮と暗号化を使う」を参照してください。

バックアップポリシーの作成

次の手順を使用してバックアップポリシーを作成します。

ポリシーを作成するには

1. NetBackup Web UI で、[保護 (Protections)]、[ポリシー (Policies)]の順に選択します。
2. [追加 (Add)]をクリックします。
3. ポリシー名を入力します。
4. 新しいポリシーの属性、スケジュール、クライアントとバックアップ対象を構成します。

[耐性ネットワーク (Resilient network)]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。サーバーまたはクライアントを選択します。必要に応じて、[接続 (Connect)]をクリックし、[プライマリサーバーの編集 (Edit primary server)]、[メディアサーバーの編集 (Edit media server)]、または[クライアントの編集 (Edit client)]をクリックします。[耐性ネットワーク (Resilient network)]をクリックします。

メディアサーバーとクライアントの場合、[耐性ネットワーク (Resilient network)] のプロパティは読み取り専用です。ジョブが実行されると、プライマリサーバーは現在のプロパティでメディアサーバーとクライアントを更新します。

[耐性ネットワーク (Resilient network)]のプロパティで、バックアップとリストアに耐性のあるネットワーク接続を使用するように NetBackup を構成できます。耐性のある接続はクライアントと NetBackup メディアサーバー間のバックアップと復元トラフィックが WAN などの高遅延、低帯域幅ネットワークで効果的に機能できるようにします。データは WAN 経由で中央のデータセンターのメディアサーバーに移動します。

NetBackup はリモートクライアントと NetBackup メディアサーバー間のソケット接続を監視します。可能であれば、NetBackup は切断された接続を再確立し、データストリームを再同期します。また、NetBackup は遅延したデータストリームを維持するために遅延の問題を解決します。耐性のある接続は 80 秒までのネットワーク割り込みを存続できます。耐性のある接続は 80 秒以上、割り込みを存続させることがあります。

NetBackup Remote Network Transport Service はコンピュータ間の接続を管理します。Remote Network Transport Service はプライマリサーバー、クライアント、そしてバックアップまたはリストアジョブを処理するメディアサーバー上で実行されます。接続が割り込まれたり、失敗したりすると、サービスは接続を再確立し、データを同期しようとします。

NetBackup は、NetBackup Remote Network Transport Service (`nbrntd`) が作成するネットワークソケット接続のみを保護します。サポートされない接続の例は次のとおりです:

- 自身のデータをバックアップするクライアント (重複排除クライアントおよび SAN クライアント)
- Exchange Server や SharePoint Server 用の個別リカバリテクノロジ（GRT）
- NetBackup `nbfsd` プロセス

NetBackup は確立された後の接続のみを保護します。ネットワークの問題のために NetBackup が接続を作成できない場合、何も保護されません。

耐性のある接続はクライアントと NetBackup メディアサーバーの間で適用され、メディアサーバーとして機能する場合は、プライマリサーバーを含みます。耐性のある接続はメディアサーバーに対してクライアントおよびバックアップデータとして機能する場合、プライマリサーバーまたはメディアサーバーには適用されません。

耐性のある接続はすべてのクライアントまたはクライアントのサブセットに適用されます。

メモ: クライアントがサーバーのサブドメインとは異なる場所にある場合、クライアントの hosts ファイルにサーバーの完全修飾ドメイン名を追加してください。たとえば、`india.veritas.org` は `china.veritas.org` とは異なるサブドメインです。

クライアントのバックアップまたはリストアジョブが開始されると、NetBackup は［耐性ネットワーク (Resilient network)］リストを上から下に検索して、クライアントを見つけます。NetBackup がクライアントを見つけると、NetBackup はクライアントとジョブを実行するメディアサーバーの耐性のあるネットワーク設定を更新します。次に NetBackup は耐性が高い接続を使用します。

表 4-31　耐性ネットワークのプロパティ

プロパティ	説明
FQDN または IP アドレス (FQDN or IP address)	ホストの完全修飾ドメイン名または IP アドレス。アドレスは IP アドレスの範囲にもできるため、一度に複数のクライアントを構成できます。IPv4 のアドレスおよび範囲を IPv6 のアドレスおよびサブネットと混在させることができます。 ホストを名前で指定する場合、ベリタスは完全修飾ドメイン名を使うことをお勧めします。 耐性のあるネットワークのリストの項目を上または下に移動するには、ペインの右側の矢印ボタンを使用します。
耐性 (Resiliency)	［耐性 (Resiliency)］は、［オン (On)］または［オフ (Off)］です。

メモ: 順序は耐性ネットワークのリストの項目にとって重要です。クライアントがリストに複数回ある場合、最初の一致で耐性のある接続の状態が判断されます。たとえば、クライアントを追加して、クライアントの IP アドレスを指定し、［耐性 (Resiliency)］に［オン (On)］を指定するとします。また、IP アドレスを［オフ (Off)］として追加し、クライアントの IP アドレスがその範囲内にあるとします。クライアントの IP アドレスがアドレス範囲の前に表示されれば、クライアントの接続には耐性があります。逆に IP アドレス範囲が最初に表示される場合、クライアントの接続には耐性がありません。

他の NetBackup のプロパティは NetBackup がネットワークアドレスを使う順序を制御します。

NetBackup の耐性のある接続は SOCKS プロトコルバージョン 5 を使います。

耐性が高い接続のトラフィックは暗号化されません。バックアップを暗号化することをお勧めします。重複排除バックアップの場合、重複排除ベースの暗号化を使用してください。他のバックアップの場合、ポリシーベースの暗号化を使用してください。

耐性のある接続はバックアップ接続に適用されます。したがって、追加のネットワークポートやファイアウォールポートを開かないでください。

メモ: 複数のバックアップストリームを同時に動作する場合、Remote Network Transport Service は多量の情報をログファイルに書き込みます。このような場合、Remote Network Transport Service のログレベルを 2 以下に設定することをお勧めします。統合ログを構成する手順は別のガイドに記載されています。

耐性が高い接続のリソース使用量

耐性が高い接続は次のとおり、通常の接続より多くのリソースを消費します。

- データストリームごとに、より多くのソケットの接続が必要になります。メディアサーバーとクライアントの両方で動作する Remote Network Transport Service に対応するには 3 ソケットの接続が必要です。耐性が高くない接続には 1 ソケットの接続しか必要ありません。
- メディアサーバーとクライアント上で開いているソケット数が増加します。3 つのソケットを開く必要があります。耐性が高くない接続では 1 つしか開く必要がありません。開いたソケットの数が増加すると、ビジー状態のメディアサーバーで問題が発生することがあります。
- メディアサーバーとクライアント上で実行されるプロセス数が増加します。通常は、複数の接続があっても、増える処理はホスト 1 台に 1 つだけです。
- 耐性が高い接続の保持に必要な処理では、パフォーマンスがわずかに減少することがあります。

クライアントへの耐性のある接続の指定

NetBackup クライアントに耐性のある接続を指定するには次の手順に従ってください。

p.166 の「［耐性ネットワーク (Resilient network)］プロパティ」を参照してください。

または、`resilient_clients` スクリプトを使用して、クライアントに耐性のある接続を指定できます。

- Windows の場合: *`install_path`*`¥NetBackup¥bin¥admincmd¥resilient_clients`
- UNIX の場合: `/usr/openv/netbackup/bin/admincmd/resilient_clients`

クライアントに耐性のある接続を指定するには

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. プライマリサーバーを選択します。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。
4. ［耐性ネットワーク (Resilient network)］をクリックします。
5. 次の操作を実行できます。

設定の追加

ホストまたは IP アドレスの設定を追加するには

1. [追加 (Add)]をクリックします。
2. クライアントのホスト名または IP アドレスを入力します。

   クライアントホストを名前で指定する場合、ベリタスは完全修飾ドメイン名を使うことをお勧めします。
3. [オン (On)]オプションが選択されていることを確認します。
4. [追加してさらに追加 (Add and add another)]をクリックします。
5. 各設定を追加するまで、この手順を繰り返します。
6. ネットワーク設定の追加を終了したら、[追加 (Add)]をクリックします。

設定の編集

ホストまたは IP アドレスの設定を編集するには

1. クライアントのホスト名または IP アドレスを見つけます。
2. [処理 (Actions)]、[編集 (Edit)]の順にクリックします。
3. 目的の[耐性 (Resiliency)]の設定を選択します。
4. [保存 (Save)]をクリックします。

設定の削除

ホストまたは IP アドレスの設定の削除

1. クライアントのホスト名または IP アドレスを見つけます。
2. [処理 (Actions)]、[削除 (Delete)]の順に選択します。

上矢印、下矢印

項目の順序を変更します

1. クライアントのホスト名または IP アドレスを選択します。
2. 上または下のボタンをクリックします。

   リストの項目の順序は重要です。

   p.166 の「[耐性ネットワーク (Resilient network)]プロパティ」を参照してください。

この設定は、通常のNetBackup ホスト間通信を介して影響を受けるホストに反映されます。この処理は、最大で15分かかる場合があります。

6. バックアップをすぐに開始する場合は、プライマリサーバーで NetBackup サービスを再起動します。

MSDP 負荷分散サーバーの追加

既存のメディアサーバーの重複排除ノードに負荷分散サーバーを追加できます。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

負荷分散サーバーを追加する方法

1. Web UI を開きます。
2. 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。
3. [ストレージサーバー (Storage servers)]タブをクリックします。
4. 重複排除ストレージサーバーをクリックします。
5. [メディアサーバー (Media servers)]で、[追加 (Add)]をクリックします。
6. 負荷分散サーバーとして使うメディアサーバーを選択して、[追加 (Add)]をクリックします。

NetBackup クライアントでの可変長の重複排除について

NetBackup の重複排除は現在、データストリームを固定長セグメント (128 KB) に分けてから重複排除処理する「固定長の重複排除」方式に従っています。固定長の重複排除には、少ない計算リソースで迅速な処理が可能という利点があります。固定長の重複排除では、ほとんどの種類のデータストリームが効率的に処理されます。ただし、固定長の重複排除で重複排除率が低くなる場合があります。

データがシフティングモードで変更された場合、つまり、一部のデータがファイルの中央に挿入された場合は、可変長の重複排除を使用したほうがデータのバックアップを作成するときに高い重複排除率を実現できます。可変長の重複排除により、バックアップストレージを縮小してバックアップのパフォーマンスを向上し、データ保護にかかるコスト全体を削減できます。

メモ: 現在の MSDP インテリジェント重複排除アルゴリズムおよび関連するストリーマーで良好な重複排除率が得られないデータについては、可変長の重複排除を使用してください。可変長の重複排除を有効にすると重複排除率を向上できますが、CPU のパフォーマンスに影響する可能性がある点を考慮してください。

可変長の重複排除では、すべてのセグメントが可変のサイズと設定可能なサイズ境界を備えています。NetBackup クライアントは、セキュアハッシュアルゴリズム (SHA-2) を検証し、データの可変長セグメントに適用します。各データセグメントには一意の ID が割り当てられ、NetBackup は同じ ID のデータセグメントがバックアップにあるかどうかを評価します。データセグメントがすでにある場合、そのセグメントのデータは保存されません。

警告: バックアップポリシーに対して圧縮を有効にすると、可変長の重複排除を設定しても機能しません。

次の表で、データバックアップでの可変長の重複排除の影響を説明します。

表 4-32　　可変長の重複排除の影響

重複排除率への影響	可変長の重複排除は、シフティングモードでデータファイルが変更された場合、つまりデータがバイナリレベルで挿入、削除、または変更された場合に有益です。このような変更されたデータを再びバックアップする際、可変長の重複排除は高い重複排除率を実現します。そのため、次回以降のバックアップでは、より高い重複排除率を得られます。
CPU への影響	可変長の重複排除は、高い重複排除率を実現するため、固定長の重複排除より多いリソースを消費する場合があります。可変長の重複排除では、セグメント境界を計算するため、より多くの CPU サイクルが必要となります。バックアップにかかる時間も固定長の重複排除方式より長くなる場合があります。
データのリストアへの影響	可変長の重複排除は、データのリストア処理には影響しません。

可変長の重複排除の設定

NetBackup クライアントでは、可変長の重複排除はデフォルトで無効になっています。NetBackup 10.2 以降では、cacontrol コマンドラインユーティリティを使用して可変長の重複排除を有効にできます。以前のバージョンの NetBackup では、`pd.conf` ファイルにパラメータを追加することによって有効にできます。すべての NetBackup クライアントまたはポリシーで同じ設定を有効にするには、`pd.conf` ファイルですべてのクライアントまたはポリシーを指定する必要があります。

NetBackup 10.2 以降、可変長の重複排除のデフォルトバージョンは VLD v2 です。`pd.conf` ファイルで可変長の重複排除を有効にしており、イメージバックアップがストレージに存在しない場合、VLD v2 がデフォルトで使用されます。イメージバックアップがストレージにすでに存在する場合、NetBackup は引き続き VLD v1 を使用します。

重複排除の負荷分散のシナリオでは、メディアサーバーを NetBackup 8.1.1 以降にアップグレードし、すべてのメディアサーバーで `pd.conf` ファイルを変更する必要があります。バックアップジョブで、負荷分散プール用に古いメディアサーバー (NetBackup 8.1.1 より前) が選択された場合は、可変長の重複排除ではなく固定長の重複排除が使用されます。負荷分散のシナリオでは、NetBackup バージョンが異なるメディアサーバーは構成しないでください。可変長の重複排除で生成されたデータセグメントは、固定長の重複排除で生成されたデータセグメントとは異なります。そのため、NetBackup バージョンが異なる負荷分散メディアサーバーを使用すると、重複排除率が低下します。

p.173 の「cacontrol コマンドラインユーティリティを使用した可変長の重複排除の管理」を参照してください。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.175 の「MSDP pd.conf ファイルの編集」を参照してください。

p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

cacontrol コマンドラインユーティリティを使用した可変長の重複排除の管理

cacontrol コマンドラインユーティリティを使用して可変長の重複排除を設定できます。--vld フラグを使用して、構成ファイルにクライアントまたはポリシーのマーカーエントリを作成して可変長の重複排除を設定します。

cacontrol コマンドラインユーティリティは次の場所にあります。

- Windows の場合: `install_path¥Veritas¥pdde¥cacontrol`
- UNIX の場合: `/usr/openv/pdde/pdcr/bin/cacontrol`

NetBackup 10.2 以降では、次のオプションを使用して可変長の重複排除を構成できます。

表 4-33 cacontrol の VLD のコマンドオプション

オプション	説明
`client`	特定のクライアントに対して可変長の重複排除を有効にします。
`policy`	特定のポリシーに対して可変長の重複排除を有効にします。
`vldtype`	■ `VLD` 可変長の重複排除アルゴリズムのバージョン 1。 ■ `VLD_2` 可変長の重複排除アルゴリズムのバージョン 2。このバージョンをデフォルトとして使用することをお勧めします。 ■ `VLD_3` 可変長の重複排除アルゴリズムの別のバージョン。
`minsegsize`	可変長の重複排除セグメンテーション (KB) のセグメンテーション範囲の最小セグメントサイズ (KB)。推奨値は 16、32、64 です。サイズは 4 の倍数で、4 から 16384 の範囲である必要があります。
`maxsegSize`	可変長の重複排除セグメンテーション (KB) のセグメンテーション範囲の最大セグメントサイズ (KB)。この値は、`sw_min` を超える必要があります。推奨値は 32、64、128 です。最大セグメントサイズは、最小サイズより大きくする必要があります。

警告: 可変長の重複排除バージョンを変更すると、新しいイメージが 1 回または 2 回バックアップされるまで、イメージバックアップの重複排除率が低下します。したがって、新しい可変長の重複排除は慎重に選択してください。

cacontrol コマンドラインユーティリティを使用して MSDP の可変長の重複排除を管理するには

1. クライアントとポリシーの有効な設定を問い合わせます。

   ```
   cacontrol --vld queryactive <CLIENT> <POLICY>
   ```

2. クライアントとポリシーを構成します。

   ```
   cacontrol --vld update <CLIENT> <POLICY> <VLDTYPE>
   <MINSEGMENTSIZE> <MAXSEGMENTSIZE>
   ```

3. クライアントとポリシーの設定を削除します。

   ```
   cacontrol --vld delete <CLIENT> <POLICY>
   ```

4. クライアントとポリシーの設定を問い合わせます。

   ```
   cacontrol --vld get <CLIENT> <POLICY>
   ```

5. ポリシーの構成を行います。

   ```
   cacontrol --vld updatebypolicy <POLICY> <VLDTYPE> <MINSEGMENTSIZE>
   <MAXSEGMENTSIZE>
   ```

6. クライアントの設定を削除します。

   ```
   cacontrol --vld deletebypolicy <POLICY>
   ```

7. ポリシーの設定を問い合わせます。

   ```
   cacontrol --vld getbypolicy <POLICY>
   ```

8. クライアントの構成を行います。

   ```
   cacontrol --vld updatebyclient <CLIENT> <VLDTYPE> <MINSEGMENTSIZE>
   <MAXSEGMENTSIZE>
   ```

9 クライアントの設定を削除します。

```
cacontrol --vld deletebyclient <CLIENT>
```

10 クライアントの設定を問い合わせます。

```
cacontrol --vld getbyclient <CLIENT>
```

クライアントおよびポリシーのパラメータを設定する場合、アスタリスク (*) を使用して、すべてのクライアントまたはポリシーを示すことができます。

次に例を示します。

```
cacontrol --vld updatebypolicy "*" VLD_V2 32 64
```

MSDP pd.conf 構成ファイルについて

データを重複排除する NetBackup ホストごとに、pd.conf ファイルはホストの重複排除操作を制御する各種の設定を含んでいます。デフォルトでは、重複排除のストレージサーバーの pd.conf ファイル設定は、それ自体のデータを重複排除するすべてのクライアントとすべての負荷分散サーバー適用されます。

このファイルを編集して、そのホストの詳細設定を構成できます。構成設定が pd.conf ファイルにない場合は、設定を追加できます。ホストの pd.conf ファイルを変更すると、そのホストのみの設定が変更されます。データを重複排除するすべてのホストで同じ設定にするには、すべてのホストの pd.conf ファイルを変更する必要があります。

pd.conf ファイル設定は、リリースによって変更されることがあります。アップグレード中に、NetBackup は必須の設定のみを pd.conf ファイルに追加します。

pd.conf ファイルは、次のディレクトリに存在します。

- (UNIX) /usr/openv/lib/ost-plugins/
- (Windows) *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins

p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

p.175 の「MSDP pd.conf ファイルの編集」を参照してください。

MSDP pd.conf ファイルの編集

ホストの pd.conf ファイルを変更すると、そのホストのみの設定が変更されます。データを重複排除するすべてのホストで同じ設定にするには、すべてのホストの pd.conf ファイルを変更する必要があります。

メモ: Cohesity ベリタス社では、編集前にファイルのバックアップコピーを取ることをお勧めします。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

pd.conf ファイルを編集する方法

1. テキストエディタを使用して pd.conf ファイルを開きます。

   pd.conf ファイルは、次のディレクトリに存在します。

   - (UNIX) /usr/openv/lib/ost-plugins/
   - (Windows) *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins

2. 設定を有効にするには、編集する各行から列 1 のシャープ記号 (#) を削除します。
3. 設定を変更するには、新しい値を指定します。

   メモ: ファイルの等号 (=) の左右にあるスペースは重要です。ファイルを編集した後、ファイルに空白文字があることを確認してください。

4. ファイルを保存して閉じます。
5. ホストで NetBackup Remote Manager and Monitor Service (nbrmms) を再起動します。

MSDP pd.conf ファイルのパラメータ

表 4-34 に、NetBackup メディアサーバー重複排除プール環境で構成できる重複排除パラメータについて説明します。

この表のパラメータはアルファベット順です。pd.conf ファイルのパラメータはアルファベット順でないことがあります。

ご使用のリリースでのファイルのパラメータは、このトピックに記述されているパラメータとは異なることがあります。

このファイルを編集して、そのホストの詳細設定を構成できます。パラメータが pd.conf ファイルにない場合は、パラメータを追加できます。アップグレード中に、NetBackup は必須のパラメータのみを pd.conf ファイルに追加します。

pd.conf ファイルは、次のディレクトリに存在します。

- (Windows) *install_path*¥Veritas¥NetBackup¥bin¥ost-plugins
- (UNIX) /usr/openv/lib/ost-plugins/

表 4-34 pd.conf ファイルのパラメータ

パラメータ	説明
BACKUPRESTORERANGE	クライアントで、バックアップとリストア用に、ローカルネットワークインターフェースカード (NIC) の IP アドレスまたはアドレス範囲を指定します。 次のように、2 つの方法のいずれかで値を指定します。 ■ Classless Inter-Domain Routing (CIDR) 形式。たとえば、次の表記法はトラフィックのために 192.168.10.0 と 192.168.10.1 を指定します。 BACKUPRESTORERANGE = 192.168.10.1/31 ■ IP アドレスのカンマ区切りリスト。たとえば、次の表記法はトラフィックのために 192.168.10.1 と 192.168.10.2 を指定します。 BACKUPRESTORERANGE = 192.168.10.1, 192.168.10.2 デフォルト値: BACKUPRESTORERANGE= (デフォルト値なし) 指定可能な値: Classless Inter-Domain Routing 形式か IP アドレスのカンマ区切りのリスト
BANDWIDTH_LIMIT	重複排除ホストと重複排除プール間のデータをバックアップまたはリストアするときに許可する最大帯域幅を指定します。値は、KB/秒で指定されます。デフォルトは、制限なしです。 デフォルト値: BANDWIDTH_LIMIT = 0 指定可能な値: 0(限度なし) - 実際のシステムの限度 (KB/秒)
COMPRESSION	バックアップ時にデータを圧縮するかどうか指定します。 デフォルトでは、データは圧縮されます。 デフォルト値: COMPRESSION = 1 指定可能な値: 0 (オフ) または 1 (オン) p.104 の「MSDP の圧縮について」を参照してください。

パラメータ	説明
CR_STATS_TIMER	ストレージサーバーホストから統計を取り込む時間間隔を秒単位で指定します。デフォルト値の 0 はキャッシュへの保存を無効にし、オンデマンドで統計を取り込みます。 この設定を変更する前に次の情報を考慮してください。 ■ 無効 (0) に設定すると、NetBackup が要求するたびに、最新のストレージ容量の情報の要求が行われます。 ■ 値を指定した場合は、前回の要求から指定された秒数が経過してから、要求が実行されます。値を指定しないと、前の要求からのキャッシュされた値が使用されます。 ■ この設定を有効にすると、ストレージサーバーへの問い合わせが減少する場合があります。欠点は、NetBackup によって報告される容量の情報が最新のものではなくなることです。したがって、ストレージ容量が限界に近い場合、Cohesity はこのオプションを有効にしないことをお勧めします。 ■ 高負荷のシステムでは、負荷によって容量の情報のレポートが遅れることがあります。その場合、NetBackup はストレージユニットに停止としてマークすることがあります。 デフォルト値: CR_STATS_TIMER = 0 指定可能な値: 0 以上の値 (秒単位) **メモ:** 環境内で msdpcloud が構成されている場合は、pd.conf ファイルで CR_STATS_TIMER パラメータを構成しないようにしてください。
DEBUGLOG	NetBackup ファイルが重複排除プラグインのログ情報を書き込むファイルを指定します。NetBackup は毎日のログファイルの先頭に日付印を追加します。 Windows では、ファイル名の前にパーティション識別子とスラッシュがある必要があります。UNIX では、ファイル名の前にスラッシュがある必要があります。 **メモ:** このパラメータは NetApp アプライアンスからの NDMP バックアップには適用されません。 デフォルト値: ■ UNIX の場合: DEBUGLOG = /var/log/puredisk/pdplugin.log ■ Windows の場合: DEBUGLOG = C:¥pdplugin.log 指定可能な値: 任意のパス

パラメータ	説明
DISABLE_BACKLEVEL_TLS	クライアントとサーバー間のセキュア通信が確立されるとき、このパラメータで古い TLS バージョンを無効にするかどうかを指定します。NetBackup バージョン 8.0 以前では、SSLV2、SSLV3、TLS 1.0、TLS 1.1 などの古い TLS バージョンを使用しています。 TLS 1.2 を有効にするには、DISABLE_BACKLEVEL_TLS パラメータの値を 1 に変更して、NetBackup 重複排除エンジン (spoold) と NetBackup 重複排除マネージャ (spad) を再起動します。 デフォルト値: DISABLE_BACKLEVEL_TLS = 0 指定可能な値: 0 (オフ) または 1 (オン) **メモ:** TLS 1.2 を有効にするには、NetBackup バージョンが 8.1 以降であることが必要です。マシン (クライアントまたはメディアサーバーまたは負荷分散サーバーの可能性があります) で TLS 1.2 を有効にすると (DISABLE_BACKLEVEL_TLS = 1)、通信を確立するには、接続されているすべてのマシンでも TLS 1.2 を有効にする必要があります。 標準バックアップの場合、NetBackup クライアントバージョン 8.0 以前では、TLS 1.2 が有効になっている NetBackup サーバー (メディアサーバーまたは負荷分散サーバー) バージョン 8.1 と通信できます。 ただし、最適化複製とレプリケーション、負荷分散、および Client Direct 複製の場合、NetBackup クライアントバージョン 8.0 以前では TLS 1.2 が有効になっている NetBackup サーバー (メディアサーバーまたは負荷分散サーバー) バージョン 8.1 と通信できません。
DONT_SEGMENT_TYPES	重複排除しないファイルのファイル名拡張子のカンマ区切りリスト。指定された拡張子を持つバックアップストリームのファイルは、16 MB より小さい場合に単一のセグメントが割り当てられます。それより大きいファイルは、最大 16 MB のセグメントサイズを使用して重複排除されます。 例: DONT_SEGMENT_TYPES = mp3,avi。 この設定は、NetBackup でグローバルに重複排除されないファイル形式内のセグメントが分析および管理されないようにします。注意: このパラメータは、NetApp ストリームハンドラを使う NDMP バックアップには適用されません。 デフォルト値: DONT_SEGMENT_TYPES = (デフォルト値なし) 指定可能な値: カンマ区切りのファイル拡張子

パラメータ	説明
ENCRYPTION	バックアップ時にデータを暗号化するかどうか指定します。デフォルトでは、ファイルは暗号化されません。 すべてのホストでこのパラメータを 1 に設定すると、データは転送中とストレージ上で暗号化されます。 デフォルト値: ENCRYPTION = 0 指定可能な値: 0 (暗号化なし) または 1 (暗号化) p.106 の「MSDP の暗号化について」を参照してください。 MSDP サーバーのすべてのデータを暗号化するには、サーバーオプションを使用することをお勧めします。ENCRYPTION パラメータは、pd.conf ファイルがあるホストを使用するバックアップまたはレプリケーションにのみ有効です。
FIBRECHANNEL	NetBackup シリーズアプライアンスに出入するバックアップとリストアのトラフィックについてファイバーチャネルを有効にします。 デフォルト値: FIBRECHANNEL = 0 指定可能な値: 0 (オフ) または 1 (オン)
FILE_KEEP_ALIVE_INTERVAL	アイドル状態のソケットに keepalive を実行する間隔 (秒単位)。 以下の項目は、このパラメータの構成に基づく動作について説明しています。 ■ コメントアウトされ (デフォルト)、耐性のあるネットワーク接続が有効: 値が 75 秒未満の場合、keep alive の間隔は 60 秒です。値が 1800 秒 (30 分) より大きい場合、keep alive の間隔は 1440 秒 (30 分の 80%) です。値が 75 から 1,800 セクションまでの間にある場合、keep-alive の間隔はパラメータ値の 80% です。 p.166 の「[耐性ネットワーク (Resilient network)]プロパティ」を参照してください。 ■ コメントアウトされ (デフォルト)、耐性の高いネットワーク接続が有効でない: keep-alive の間隔は 1,440 秒 (30 分の 80%) です。 ■ 0 以下、無効: keepalive は送信されません。 ■ 0 より大きい: keep-alive の間隔は指定した秒単位の値です。ただし、60 秒未満または 7200 秒 (2 時間) より大きい場合、keep-alive の間隔は 1440 秒 (30 分の 80%) です。 デフォルト値: FILE_KEEP_ALIVE_INTERVAL = 1440 指定可能な値: 0 (無効) または 60 から 7200 秒まで NetBackup が使用する keep alive 間隔を決定するため、以下と同様のメッセージの重複排除プラグインログファイルを検査します。 Using keepalive interval of *xxxx* seconds 重複排除プラグインのログファイルについての詳細は、この表の DEBUGLOG および LOGLEVEL を参照してください。

パラメータ	説明
FP_CACHE_CLIENT_POLICY	**メモ:** Cohesity 自身のデータをバックアップする個々のクライアントでこの設定を使うことを推奨します (クライアント側の重複排除)。ストレージサーバーまたは負荷分散サーバーでこの設定を使用すると、すべてのバックアップジョブに影響します。 クライアント、バックアップポリシーおよびクライアントの最初のバックアップの指紋キャッシュを取得する日付を指定します。 デフォルトでは、以前のバックアップからの指紋がロードされます。このパラメータによって、別の類似したバックアップから指紋キャッシュをロードできます。これにより、クライアントの最初のバックアップに必要な時間を減らすことができます。このパラメータは、特に、WAN 上でデータが長距離を移動する、リモートオフィスから中央のデータセンターへのバックアップに役立ちます。 次の形式で設定を指定します。 clienthostmachine,backuppolicy,date *date* は指定したクライアントからの指紋キャッシュを使う最後の日付 (mm/dd/yyyy 形式) です。 デフォルト値: FP_CACHE_CLIENT_POLICY = (デフォルト値なし) p.77 の「クライアントでの MSDP フィンガープリントキャッシュのシードの構成」を参照してください。
FP_CACHE_INCREMENTAL	増分バックアップに指紋キャッシュを使用するかどうかを指定します。 増分バックアップでは、前回のバックアップ以降、変更されたものだけがバックアップされるので、キャッシュのロードは増分バックアップのパフォーマンスにほとんど影響しません。 デフォルト値: FP_CACHE_INCREMENTAL = 0 指定可能な値: 0 (オフ) または 1 (オン) **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。
FP_CACHE_LOCAL	ストレージサーバーで重複排除するバックアップジョブについて指紋キャッシュを使用するかどうかを指定します。このパラメータは、負荷分散サーバーまたは自身のデータを重複排除するクライアントには適用されません。 重複排除ジョブが NetBackup 重複排除エンジンと同じホストにある場合、指紋キャッシュを無効にするとパフォーマンスが向上します。 デフォルト値: FP_CACHE_LOCAL = 1 指定可能な値: 0 (オフ) または 1 (オン)

パラメータ	説明
FP_CACHE_MAX_COUNT	指紋キャッシュにロードするイメージの最大数を指定します。 デフォルト値: FP_CACHE_MAX_COUNT = 1024 指定可能な値: 0 - 4096 **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。
FP_CACHE_MAX_MBSIZE	指紋キャッシュに使用するメモリの容量を MB 単位で指定します。 デフォルト値: FP_CACHE_MAX_MBSIZE = 20 指定可能な値: 0 からコンピュータの制限値まで **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。
FP_CACHE_PERIOD_REBASING_THRESHOLD	バックアップ中の定期的なリベースのしきい値 (MB) を指定します。次の両方に該当する場合、コンテナのリベースが検討されます。 ■ コンテナが過去 3 カ月間リベースされていません。 ■ そのバックアップの場合、コンテナ内のデータセグメントが消費する領域は FP_CACHE_PERIOD_REBASING_THRESHOLD 値より少なくなります。 デフォルト値: FP_CACHE_PERIOD_REBASING_THRESHOLD = 16 指定可能な値: 0 (無効) ～ 256 p.525 の「MSDP ストレージのリベースについて」を参照してください。
FP_CACHE_REBASING_THRESHOLD	バックアップ中の標準リベースのしきい値 (MB) を指定します。次の両方に該当する場合、コンテナのリベースが検討されます。 ■ コンテナが過去 3 カ月間にリベースされました。 ■ そのバックアップの場合、コンテナ内のデータセグメントが消費する領域は FP_CACHE_REBASING_THRESHOLD 値より少なくなります。 デフォルト値: FP_CACHE_REBASING_THRESHOLD = 4 指定可能な値: 0 (無効) ～ 200 この値を変更する場合は、新しい値を慎重に検討してください。大きすぎる値を設定する場合、すべてのコンテナがリベースの対象になります。重複排除率は、リベースを実行するバックアップジョブより低くなります。 p.525 の「MSDP ストレージのリベースについて」を参照してください。

パラメータ	説明
LOCAL_SETTINGS	ローカルホストの pd.conf 設定を使うか、サーバーでローカル設定を上書きできるようにするかどうか指定します。次にローカル設定の優先度を示します。 ■ ローカルホスト ■ 負荷分散サーバー ■ ストレージサーバー ローカル設定を使用するには、この値を 1 に設定します。 デフォルト値: LOCAL_SETTINGS = 0 指定可能な値: 0 (上書きを許可) または 1 (常にローカル設定を使用)
LOGLEVEL	ログファイルに書き込まれる情報量を指定します。範囲は 0 から 10 で、10 を指定すると情報量が最も多くなります。 デフォルト値: LOGLEVEL = 0 指定可能な値: 0 以上 10 以下の整数 **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。
MAX_IMG_MBSIZE	バックアップイメージフラグメントの最大サイズ (MB 単位)。 デフォルト値: MAX_IMG_MBSIZE = 51200 指定可能な値: 0 - 51,200 (MB 単位) **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。
MAX_LOG_MBSIZE	ログファイルの最大サイズ (MB 単位)。NetBackup はログファイルがこの限度に達するとき新しいログファイルを作成します。NetBackup は各ログファイル名の先頭に、日付と 0 から始まる序数を追加します (120131_0_pdplugin.log、120131_1_pdplugin.log など)。 デフォルト値: MAX_LOG_MBSIZE = 100 指定可能な値: 0 - 50,000 (MB 単位)
META_SEGKSIZE	メタデータストリームのセグメントサイズ。 デフォルト値: META_SEGKSIZE = 16384 指定可能な値: 32-16384、32 の倍数 **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。

パラメータ	説明
MTSTRM_BACKUP_CLIENTS	設定する場合、指定されたクライアントのバックアップに対するマルチスレッドエージェントの使用が制限されます。指定されていないクライアントは単一スレッドを使います。 この設定では、指定されたクライアントがマルチスレッドエージェントを使うことは保証されません。mtstrm.conf ファイルの MaxConcurrentSessions パラメータは、マルチスレッドエージェントが同時に処理するバックアップの数を制御します。MaxConcurrentSessions 値より多くのクライアントを指定した場合、クライアントの一部は単一スレッドプロセスを使う可能性があります。 p.67 の「MSDP mtstrm.conf ファイルパラメータ」を参照してください。 形式は、大文字と小文字を区別しない、クライアントのカンマ区切りリストです (例: MTSTRM_BACKUP_CLIENTS = client1,client2,client3)。 デフォルト値: MTSTRM_BACKUP_CLIENTS = (デフォルト値なし) 指定可能な値: カンマ区切りのクライアント名 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。

パラメータ	説明
MTSTRM_BACKUP_ENABLED	重複排除プラグインと NetBackup 重複排除エンジン間のバックアップストリームにマルチスレッドエージェントを使います。 デフォルト値: MTSTRM_BACKUP_ENABLED = (デフォルト値なし) 指定可能な値: 1 (オン) または 0 (オフ) このパラメータの値は、インストール中またはアップグレード中に構成されます。ホストの同時ハードウェア値が同時ハードウェアしきい値より大きい場合、MTSTRM_BACKUP_ENABLED は NetBackup によって 1 に設定されます(このパラメータにおいて、同時ハードウェアは、CPU またはコアまたはハイパースレッディングユニットの数です)。 以下の項目では、決定アルゴリズムに使われる値について説明します。 ■ 同時ハードウェア値は次のいずれかです。 ■ メディアサーバーの場合、ホストの同時ハードウェアの半分がアルゴリズムの同時ハードウェア値に使われます。 ■ クライアントの場合、ホストの同時ハードウェアのすべてがアルゴリズムの同時ハードウェア値に使われます。 ■ マルチスレッドを有効にする同時ハードウェアのしきい値は次のいずれかです。 ■ Windows と Linux の場合: しきい値は 2 です。 ■ Solaris の場合: しきい値は 4 です。 次の例が参考になります。 ■ コアごとに 2 つのハイパースレッディングユニットを含む 8 つの CPU コアがある Linux メディアサーバーの同時ハードウェアは 16 です。したがって、アルゴリズムの同時ハードウェア値は 8 (メディアサーバーではシステムの同時ハードウェアの半分) です。8 は 2 より大きいため (Windows と Linux のしきい値)、マルチスレッドは有効になります (MTSTRM_BACKUP_ENABLED = 1)。 ■ ハイパースレッディングのない 2 つの CPU コアがある Solaris クライアントの同時ハードウェアは 2 です。アルゴリズムの同時ハードウェア値は 2 (クライアントではシステムの同時ハードウェアのすべて) です。2 は 4 より大きくないため (Solaris のしきい値)、マルチスレッドは有効になりません (MTSTRM_BACKUP_ENABLED = 0)。 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。

パラメータ	説明
MTSTRM_BACKUP_POLICIES	設定する場合、指定されたポリシーのバックアップに対するマルチスレッドエージェントの使用が制限されます。指定されていないポリシーのクライアントは、クライアントが MTSTRM_BACKUP_CLIENTS パラメータで指定されていないかぎり、単一スレッドを使います。 この設定では、指定されたポリシーのクライアントのすべてがマルチスレッドエージェントを使うことは保証されません。mtstrm.conf ファイルの MaxConcurrentSessions パラメータは、マルチスレッドエージェントが同時に処理するバックアップの数を制御します。MaxConcurrentSessions 値より多くのクライアントがポリシーに含まれる場合、クライアントの一部は単一スレッドプロセスを使う可能性があります。 p.67 の「MSDP mtstrm.conf ファイルパラメータ」を参照してください。 形式は、大文字と小文字を区別する、ポリシーのカンマ区切りリストです (例: MTSTRM_BACKUP_POLICIES = policy1,policy2,policy3)。 デフォルト値: MTSTRM_BACKUP_POLICIES = (デフォルト値なし) 指定可能な値: カンマ区切りのバックアップポリシー名 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。
MTSTRM_IPC_TIMEOUT	重複排除プラグインがエラーによりタイムアウトするまでにマルチスレッドエージェントからの応答を待機する秒数。 デフォルト値: MTSTRM_IPC_TIMEOUT = 1200 指定可能な値: 1 以上 86400 以下 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。
OPTDUP_BANDWIDTH	重複排除サーバーの各々の最適化複製と自動イメージレプリケーションのストリームに割り当てられる帯域幅を指定します。OPTDUP_BANDWIDTH はクライアントには適用されません。値は、KB/秒で指定されます。 デフォルト値: OPTDUP_BANDWIDTH= 0 指定可能な値: 0(限度なし) - 実際のシステムの限度 (KB/秒) グローバルな帯域幅パラメータは、OPTDUP_BANDWIDTH が適用されるかどうかに影響します。 p.156 の「MSDP 最適化複製とレプリケーション帯域幅の構成について」を参照してください。

パラメータ	説明
OPTDUP_COMPRESSION	最適化複製および自動イメージレプリケーション時にデータを圧縮するかどうか指定します。デフォルトでは、ファイルは圧縮されます。圧縮を無効にするには、値を 0 に変更します。このパラメータはクライアントには適用されません。 デフォルト値: OPTDUP_COMPRESSION = 1 指定可能な値: 0 (オフ) または 1 (オン) p.104 の「MSDP の圧縮について」を参照してください。
OPTDUP_ENCRYPTION	最適化複製およびレプリケーション時にデータを暗号化するかどうか指定します。デフォルトでは、ファイルは暗号化されません。暗号化が必要な場合は、MSDP ストレージサーバーと MSDP の負荷分散サーバーで値を 1 に変更します。このパラメータはクライアントには適用されません。 すべてのホストでこのパラメータを 1 に設定すると、データは転送時に暗号化されます。 デフォルト値: OPTDUP_ENCRYPTION = 0 指定可能な値: 0 (オフ) または 1 (オン) p.106 の「MSDP の暗号化について」を参照してください。
OPTDUP_TIMEOUT	最適化複製がタイムアウトするまでの時間 (分) を指定します。 デフォルト値: OPTDUP_TIMEOUT = 720 指定可能な値: 分単位で表される値
PREFERRED_EXT_SEGKSIZE	特定のファイルの種類について、ファイル拡張子と優先セグメントサイズ (KB 単位) を指定します。ファイル拡張子では大文字と小文字が区別されます。デフォルト値は次のとおりです。edb は Exchange Server ファイル、mdf は SQL Server マスターデータベースファイル、ndf は SQL Server セカンダリデータファイル、segsize64k は Microsoft SQL ストリームです。 デフォルト値: PREFERRED_EXT_SEGKSIZE = edb:32,mdf:64,ndf:64,segsize64k:64 指定可能な値: カンマで区切った *file_extension*:*segment_size_in_KBs* のペア。 SEGKSIZE も参照してください。
PREFETCH_SIZE	リストア操作のデータバッファに使用するバイト単位のサイズ。 デフォルト値: PREFETCH_SIZE = 33554432 指定可能な値: 0 からコンピュータのメモリの制限値まで **メモ:** Cohesity の担当者によって指示された場合のみこの値を変更します。

パラメータ	説明
PREDOWNLOAD_FACTOR	クラウド LSU からデータをリストアするときに使用する事前ダウンロードの係数を指定します。 デフォルト値: PREDOWNLOAD_FACTOR=40 指定可能な値: 0 - 100 **メモ:** 事前ダウンロードのバッチサイズのパラメータは、PREDOWNLOAD_FACTOR * PREFETCH_SIZE です。
RESTORE_DECRYPT_LOCAL	リストア操作の間にデータをどのホストで復号し、解凍するかを指定します。 環境によって、クライアントで復号と解凍を行うことによってパフォーマンスが向上することがあります。 デフォルト値: RESTORE_DECRYPT_LOCAL = 1 指定可能な値: 0 はメディアサーバーでの復号と解凍を有効にします。1 はクライアントでの復号と解凍を有効にします。
SEGKSIZE	デフォルトのファイルセグメントサイズ (KB 単位)。 デフォルト値: SEGKSIZE = 128 指定可能な値: 32 to 16384 (KB 単位、追加は 32 KB 単位のみ) **警告:** この値を変更すると、容量が少なくなり、パフォーマンスが低下する場合があります。Cohesity の担当者によって指示された場合のみこの値を変更します。 また特定のファイルの種類のセグメントサイズを指定できます。PREFERRED_EXT_SEGKSIZE を参照してください。

パラメータ	説明
VLD_CLIENT_NAME	可変長の重複排除を有効にするNetBackupクライアントの名前を指定します。デフォルトでは、VLD_CLIENT_NAME パラメータは pd.conf 構成ファイルに存在しません。 このパラメータを使用して、さまざまな NetBackup クライアントに対し、セグメントサイズに異なる最大値や最小値を指定することもできます。セグメントサイズを指定しない場合は、デフォルト値が考慮されます。 これらの値では、大文字と小文字が区別されます。 次の形式のいずれかを使用します。 ■ VLD_CLIENT_NAME = * すべての NetBackup クライアントに対して可変長の重複排除を有効にし、デフォルトの VLD_MIN_SEGKSIZE 値と VLD_MAX_SEGKSIZE 値を使用します。 ■ VLD_CLIENT_NAME = *clientname* NetBackup クライアント *clientname* に対して可変長の重複排除を有効にし、デフォルトの VLD_MIN_SEGKSIZE 値と VLD_MAX_SEGKSIZE 値を使用します。 ■ VLD_CLIENT_NAME = *clientname (64, 256)* NetBackup クライアント *clientname* に対して可変長の重複排除を有効にし、VLD_MIN_SEGKSIZE 値に 64 KB、VLD_MAX_SEGKSIZE 値に 256 KB を使用します。 **メモ:** pd.conf ファイルには最大で 50 のクライアントを追加できます。
VLD_MIN_SEGKSIZE	可変長の重複排除の最小データセグメントサイズ (KB 単位)。セグメントサイズは、4 KB から 16384 KB までの範囲の 4 の倍数にする必要があります。デフォルト値は 64 KB です。 値は、VLD_MAX_SEGKSIZE より小さくなければなりません。NetBackup クライアントごとに、異なるセグメントサイズを指定できます。 値を大きくすると、CPU 使用量が減りますが、重複排除率が低下します。値を小さくすると、CPU 使用量が増えますが、重複排除率が上昇します。 **メモ:** VLD_MIN_SEGKSIZE と VLD_MAX_SEGKSIZE の値が近いと、固定長の重複排除と似たパフォーマンスになります。

パラメータ	説明
VLD_MAX_SEGKSIZE	可変長の重複排除の最大データセグメントサイズ (KB 単位)。 VLD_MAX_SEGKSIZE は、データセグメントの境界を設定するために使用されます。セグメントサイズは、4 KB から 16384 KB までの範囲の 4 の倍数にする必要があります。デフォルト値は 128 KB です。 値は、VLD_MIN_SEGKSIZE より大きくなければなりません。NetBackup クライアントごとに、異なるセグメントサイズを指定できます。 **メモ:** VLD_MIN_SEGKSIZE と VLD_MAX_SEGKSIZE の値が近いと、固定長の重複排除と似たパフォーマンスになります。
VLD_POLICY_NAME	可変長の重複排除を有効にするバックアップポリシーの名前を指定します。デフォルトでは、VLD_POLICY_NAME パラメータは pd.conf 構成ファイルに存在しません。 このパラメータを使用して、さまざまな NetBackup ポリシーに対し、セグメントサイズに異なる最大値や最小値を指定することもできます。セグメントサイズを指定しない場合は、デフォルト値が考慮されます。 これらの値では、大文字と小文字が区別されます。 次の形式のいずれかを使用します。 ■ VLD_POLICY_NAME = * すべての NetBackup ポリシーに対して可変長の重複排除を有効にし、デフォルトの VLD_MIN_SEGKSIZE 値と VLD_MAX_SEGKSIZE 値を使用します。 ■ VLD_POLICY_NAME = *policyname* NetBackup ポリシー *policyname* に対して可変長の重複排除を有効にし、デフォルトの VLD_MIN_SEGKSIZE 値と VLD_MAX_SEGKSIZE 値を使用します。 ■ VLD_POLICY_NAME = *policyname (64, 256)* NetBackup ポリシー *policyname* に対して可変長の重複排除を有効にし、VLD_MIN_SEGKSIZE 値に 64 KB、VLD_MAX_SEGKSIZE 値に 256 KB を使用します。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.175 の「MSDP pd.conf ファイルの編集」を参照してください。

MSDP contentrouter.cfg ファイルについて

contentrouter.cfg ファイルには、重複排除環境の一部の操作を制御する各種の構成設定が含まれます。

通常、ファイルの設定を変更する必要はありません。ただし、場合によっては、Cohesity のサポート担当者によって、設定を変更するように指示されることがあります。

NetBackup マニュアルでは、一部の contentrouter.cfg ファイルパラメータのみを記述しています。それらのパラメータは、構成設定を変更するタスクや処理を説明するトピックで示されています。

メモ: NetBackup のマニュアルまたは Cohesity の担当者によって、そうするように指示された場合のみ、contentrouter.cfg の値を変更してください。

contentrouter.cfg ファイルは、次のディレクトリに存在します。

- (UNIX) *storage_path*/etc/puredisk
- (Windows) *storage_path*¥etc¥puredisk

p.526 の「MSDP サーバー側リベースのパラメータ」を参照してください。

p.175 の「MSDP pd.conf ファイルの編集」を参照してください。

MSDP ストレージサーバーの構成の保存について

ストレージサーバーの設定をテキストファイルに保存できます。保存されたストレージサーバーの構成ファイルはストレージサーバーの構成設定を含んでいます。ストレージについての状態情報も含んでいます。保存された構成ファイルはストレージサーバーのリカバリに役立つ場合があります。そのため、Cohesity では、ストレージサーバーの構成を取得し、ファイルに保存することをお勧めします。このファイルは作成しないかぎり存在しません。

作成された構成ファイルの例は次のとおりです。

```
V7.0 "storagepath" "D:¥DedupeStorage" string
V7.0 "spalogpath" "D:¥DedupeStorage¥log" string
V7.0 "dbpath" "D:¥DedupeStorage" string
V7.0 "required_interface" "HOSTNAME" string
V7.0 "spalogretention" "7" int
V7.0 "verboselevel" "3" int
V7.0 "replication_target(s)" "none" string
V7.0 "Storage Pool Size" "698.4GB" string
V7.0 "Storage Pool Used Space" "132.4GB" string
V7.0 "Storage Pool Available Space" "566.0GB" string
V7.0 "Catalog Logical Size" "287.3GB" string
V7.0 "Catalog files Count" "1288" string
V7.0 "Space Used Within Containers" "142.3GB" string
```

V7.0 は、NetBackup のリリースレベルではなく、入出力形式のバージョンを表します。このバージョンはシステムによって異なる場合があります。

ストレージサーバーが構成されていないか、停止または利用不能なときにストレージサーバー構成を取得すると、NetBackup はテンプレートファイルを作成します。テンプレート構成ファイルの例は次のとおりです。

```
V7.0 "storagepath" " " string
V7.0 "spalogin" " " string
V7.0 "spapasswd" " " string
V7.0 "spalogretention" "7" int
V7.0 "verboselevel" "3" int
V7.0 "dbpath" " " string
V7.0 "required_interface" " " string
```

ストレージサーバーの構成ファイルをリカバリに使用するには、リカバリに必要な情報のみを含むように構成ファイルを編集する必要があります。

p.192 の「MSDP ストレージサーバーの構成の保存」を参照してください。

p.193 の「MSDP ストレージサーバーの構成ファイルの編集」を参照してください。

p.194 の「MSDP ストレージサーバーの構成の設定」を参照してください。

MSDP ストレージサーバーの構成の保存

Cohesity ベリタスでは、ストレージサーバーの構成をファイルに保存することをお勧めします。ストレージサーバーの構成ファイルはリカバリで役に立ちます。

p.191 の「MSDP ストレージサーバーの構成の保存について」を参照してください。

p.54 の「MSDP ストレージサーバーの構成を保存する」を参照してください。

p.539 の「MSDP ストレージサーバーのディスクエラーからのリカバリ」を参照してください。

p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。

ストレージサーバーの構成を保存する方法

- プライマリサーバーで、次のコマンドを入力します。

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -getconfig -storage_server` *`sshostname`* `-stype PureDisk -configlist` *`file.txt`*

Windows の場合: *`install_path`*`¥NetBackup¥bin¥admincmd¥nbdevconfig -getconfig -storage_server` *`sshostname`* `-stype PureDisk -configlist` *`file.txt`*

sshostname には、ストレージサーバーの名前を使用します。*file.txt* では、その目的を示すファイル名を使用します。

ストレージサーバーが構成されていないか、停止または利用不能なときにファイルを取得すると、NetBackup はテンプレートファイルを作成します。

MSDP ストレージサーバーの構成ファイルの編集

ストレージサーバーの構成ファイルをリカバリに使用するには、リカバリに必要な情報のみが構成ファイルに含まれている必要があります。特定時点の状態情報をすべて削除する必要があります。(状態情報はアクティブなストレージサーバーに保存された構成ファイルにのみ存在します)。また、保存された構成ファイルまたはテンプレートの構成ファイルに含まれていない複数の構成設定を追加する必要があります。

表 4-35 に、必要になる構成の行を示します。

表 4-35　　リカバリファイルの必須の行

構成設定	説明
`V7.0 "storagepath" " " string`	この値は、ストレージサーバーを構成したときに使用した値と同じにする必要があります。
`V7.0 "spalogpath" " " string`	`spalogpath` には `storagepath` 値を使い、パスに `log` を付加します。たとえば `storagepath` が `D:¥DedupeStorage` の場合、`D:¥DedupeStorage¥log` を入力します。
`V7.0 "dbpath" " " string`	データベースパスが `storagepath` 値と同じである場合は、その同じ値を `dbpath` に入力します。それ以外の場合は、データベースへのパスを入力します。
`V7.0 "required_interface" " " string`	`required_interface` の値は、インターフェースを最初に構成する場合にのみ必要であり、特定のインターフェースが必要ない場合は空白にしておきます。保存された構成ファイルでは、必須インターフェースはデフォルトでコンピュータのホスト名に設定されます。
`V7.0 "spalogretention" "7" int`	この値を変更しないでください。
`V7.0 "verboselevel" "3" int`	この値を変更しないでください。
`V7.0 "replication_target(s)" "none" string`	`replication_target(s)` の値は、最適化された複製を構成した場合にのみ必要となります。それ以外の場合は、この行を編集しないでください。
`V7.0 "spalogin" "`*`username`*`" string`	NetBackup Deduplication Engine のユーザー ID で *username* を置換します。
`V7.0 "spapasswd" "`*`password`*`" string`	NetBackup Deduplication Engine のユーザー ID のパスワードで *password* を置換します。
`V7.0 "encryption" " " int`	この値は、ストレージサーバーを構成したときに使用した値と同じにする必要があります。

構成設定	説明
V7.0 "kmsenabled" " " int	値は、MSDP KMS 設定を有効または無効にするために使用されます。この値は、ストレージサーバーを構成したときに使用した値と同じにする必要があります。
V7.0 "kmsservertype" " " int	値は、KMS サーバーの種類です。この値は 0 である必要があります。
V7.0 "kmsservername" " " string	値は、NBU キー管理サーバーです。この値は、ストレージサーバーを構成したときに使用した値と同じにする必要があります。 KMS サーバーとして外部 KMS を使用する場合、値は NetBackup プライマリサーバー名である必要があります。『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup での外部 KMS のサポート」を参照してください。
V7.0 "keygroupname" " " string	この値は、ストレージサーバーを構成したときに使用した値と同じにする必要があります。

p.191 の「MSDP ストレージサーバーの構成の保存について」を参照してください。

p.539 の「MSDP ストレージサーバーのディスクエラーからのリカバリ」を参照してください。

p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。

ストレージサーバーの構成を編集する方法

1. ストレージサーバーの構成ファイルを保存していない場合は、ストレージサーバーの構成ファイルを取得します。

   p.192 の「MSDP ストレージサーバーの構成の保存」を参照してください。

2. テキストエディタを使用して値の入力、変更または削除を行います。

   必須の行 (表 4-35 を参照) のみが構成ファイルに含まれるようになるまで、ファイルから行を削除したり、ファイルに行を追加したりします。各行の 2 つ目の引用符セットの間の値を入力または変更します。テンプレート構成ファイルには、2 つ目の引用符セットの間に空白文字 (" ") があります。

MSDP ストレージサーバーの構成の設定

ファイルから構成をインポートすることによって、ストレージサーバーの構成を設定 (つまり、ストレージサーバーを構成) できます。構成を設定すると、環境のリカバリに役立つ場合があります。

p.539 の「MSDP ストレージサーバーのディスクエラーからのリカバリ」を参照してください。

p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。

構成を設定するには、編集されたストレージサーバー構成ファイルが必要となります。

p.191 の「MSDP ストレージサーバーの構成の保存について」を参照してください。

p.192 の「MSDP ストレージサーバーの構成の保存」を参照してください。

p.193 の「MSDP ストレージサーバーの構成ファイルの編集」を参照してください。

メモ: `-setconfig` オプションを指定して `nbdevconfig` コマンドを使う必要があるのは、ホストかホストディスクをリカバリするときだけです。

ストレージサーバーの構成を設定する方法

- 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: `nbdevconfig -setconfig -storage_server <storage server host name> -stype PureDisk -configlist <configuration file name>`
  - Windows の場合: `nbdevconfig -setconfig -storage_server <storage server host name> -stype PureDisk -configlist <configuration file name>`

MSDP ホストの構成ファイルについて

重複排除に使われる NetBackup の各ホストには構成ファイルがあり、そのファイル名は次のとおり、ストレージサーバーの名前と一致します。

storage_server_name`.cfg`

storage_server_name は、ストレージサーバーの構成に使われた場合には完全修飾ドメイン名です。たとえば、ストレージサーバー名が `DedupeServer.` **の場合には、構成ファイル名は** `DedupeServer.example.comexample.com.cfg` です。

ファイルの場所は次のとおりです。

Windows の場合: *install_path*`¥Veritas¥NetBackup¥bin¥ost-plugins`

UNIX の場合: `/usr/openv/lib/ost-plugins`

p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

MSDP ホストの構成ファイルの削除

重複排除ホストから構成ファイルを削除する必要がある場合もあります。たとえば、重複排除の環境を再構成したり、ディザスタリカバリで、構成ファイルが存在するサーバーでそのファイルを削除することが必要な場合があります。

p.195 の「MSDP ホストの構成ファイルについて」を参照してください。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

p.539 の「MSDP ストレージサーバーのディスクエラーからのリカバリ」を参照してください。

ホスト構成ファイルを削除する方法

- 重複排除ホストのファイルを削除します。その場所は、次のようにオペレーティングシステムの形式によって異なります。

  UNIX の場合: `/usr/openv/lib/ost-plugins`

  Windows の場合: *`install_path`*`¥Veritas¥NetBackup¥bin¥ost-plugins`

  次は完全修飾ドメイン名があるサーバーのホスト構成ファイル名の例です。

  ```
  DedupeServer.example.com.cfg
  ```

MSDP レジストリのリセット

重複排除環境を再構成する場合は、手順の 1 つとして重複排除レジストリをリセットします。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

警告: 次の手順に従うのは、ストレージサーバーとストレージパスを再構成する場合のみです。

手順は UNIX と Windows で異なります。

UNIX と Linux 上で MSDP レジストリファイルをリセットする方法

- 重複排除レジストリファイルをリセットするためにストレージサーバーで次のコマンドを入力します。

  ```
  rm /etc/pdregistry.cfg
  cp -f /usr/openv/pdde/pdconfigure/cfg/userconfigs/pdregistry.cfg

   /etc/pdregistry.cfg
  ```

Windows 上で MSDP レジストリをリセットする方法

- Windows レジストリで次のキーの内容を削除します。
  - HKLM¥SOFTWARE¥Symantec¥PureDisk¥Agent¥ConfigFilePath
  - HKLM¥SOFTWARE¥Symantec¥PureDisk¥Agent¥EtcPath

警告: Windows レジストリを編集すると、予期しない結果になる場合があります。

MSDP カタログの保護について

可用性を高めるために、NetBackup では次のように 2 つの方法で MSDP カタログを保護します。

日単位のシャドーコピー	NetBackup は自動的に MSDP カタログの複製を作成します。 p.197 の「MSDP シャドーカタログについて」を参照してください。
カタログバックアップポリシー	Cohesity では、MSDP カタログのバックアップを作成する NetBackup ポリシーの設定に使うことができるユーティリティが用意されています。 p.198 の「MSDP カタログバックアップポリシーについて」を参照してください。

p.536 の「MSDP カタログのリカバリについて」を参照してください。

p.675 の「外部 MSDP カタログバックアップについて」を参照してください。

MSDP シャドーカタログについて

NetBackup Deduplication Manager ではカタログの シャドーコピー が毎日自動的に作成されます。Deduplication Manager によってシャドーコピーごとにトランザクションログも作成されます。NetBackup が MSDP カタログで破損を検出した場合には、Deduplication Manager がカタログを最新のシャドーコピーから自動的にリストアします。このリストア処理はリカバリされた MSDP カタログが最新になるようにトランザクションログも使います。

デフォルトで、NetBackup Deduplication Manager はシャドーコピーをカタログ自体と同じボリュームで保存します。Cohesity では、シャドーコピーを異なるボリュームで保存することを推奨します。

警告: 初回の MSDP 構成時にのみパスを変更できます。MSDP バックアップの後にパスを変更すると、データが失われることがあります。

p.200 の「MSDP シャドーカタログパスの変更」を参照してください。

NetBackup Deduplication Manager ではシャドーコピーが毎日 0340 時間、ホスト時間に作成されます。スケジュールを変更するには、スケジューラー定義ファイルを変更する必要があります。

p.201 の「MSDP シャドーカタログスケジュールの変更」を参照してください。

デフォルトで、NetBackup Deduplication Manager ではカタログの 5 つのシャドーコピーが保持されます。コピー数は変更できます。

p.202 の「MSDP カタログのシャドーコピー数の変更」を参照してください。

MSDP カタログバックアップポリシーについて

Cohesity では、MSDP カタログをバックアップして保護することを推奨します。NetBackup のカタログバックアップに MSDP カタログは含まれていません。NetBackup 重複排除カタログポリシー管理およびカタログディザスタリカバリユーティリティ (`drcontrol` ユーティリティ) では、MSDP カタログに対しバックアップポリシーが構成されます。ポリシーには、他の重要な MSDP 構成情報も含まれています。

MSDP カタログバックアップはカタログの保護に対して二次保護を提供します。カタログバックアップはシャドウコピーが利用不可または破損している場合に限り、利用可能です。

次に、`drcontrol` ユーティリティで作成されるカタログバックアップポリシーの属性を示します。

スケジュール	週単位の[完全バックアップ (Full backup)]と日単位の[差分増分バックアップ (Differential Incremental Backup)]。
バックアップ処理時間帯 (Backup Window)	午前 6:00 から午後 6:00 まで
保持 (Retention)	2 週間

バックアップ対象　デフォルトのカタログパスは次のとおりです。

UNIX の場合:

```
/database_path/databases/catalogshadow
/storage_path/etc
/database_path/databases/spa
/storage_path/var
/usr/openv/lib/ost-plugins/pd.conf
/usr/openv/lib/ost-plugins/mtstrm.conf
/database_path/databases/datacheck
```

Windows の場合:

```
database_path¥databases¥catalogshadow
storage_path¥etc
storage_path¥var
install_path¥Veritas¥NetBackup¥bin¥ost-plugins¥pd.conf
install_path¥Veritas¥NetBackup¥bin¥ost-plugins¥mtstrm.conf
database_path¥databases¥spa
database_path¥databases¥datacheck
```

デフォルトで、NetBackup ではストレージとカタログに同じパスが使用されます。 *database_path* と *storage_path* は同じです。重複排除データベースに対し別のパスを構成する場合、パスは異なります。それにもかかわらず、drcontrol ユーティリティはカタログバックアップ対象の正しいパスをキャプチャします。

MSDP カタログバックアップを構成する前に、次の項目を考慮する必要があります。

- メディアサーバー重複排除プールをカタログバックアップの宛先として使わないでください。メディアサーバー重複排除プールから MSDP カタログのリカバリは行えません。
- MSDP ストレージサーバー以外の NetBackup ホストに接続されるストレージユニットを使用します。
- MSDP ストレージサーバーごとに別の MSDP カタログバックアップポリシーを使用します。
  drcontrol ユーティリティはバックアップ対象が複数のストレージサーバーに対し同じであること検証しません。バックアップポリシーに複数の MSDP ストレージサーバーが含まれている場合、バックアップ対象はホストごとのバックアップ対象を組み合わせたものになります。
- 1 つのポリシーを UNIX ホストと Windows ホスト両方の MSDP ストレージサーバーの保護には使えません。
  UNIX MSDP のストレージサーバーには標準バックアップポリシーが必要です。
  Windows MSDP ストレージサーバーには MS-Windows ポリシーが必要です。

p.203 の「MSDP カタログバックアップの設定」を参照してください。

p.207 の「MSDP カタログバックアップポリシーの更新」を参照してください。

MSDP シャドーカタログパスの変更

カタログのシャドーコピーの場所を変更できます。*storage_path* および *database_path* と異なるボリュームにコピーを格納することをお勧めしますおよび と異なるボリュームにコピーを格納することをお勧めします（重複排除データベース用に別のパスを構成した場合、パスは異なります）。

NetBackup は MSDP カタログのシャドーコピーを次の場所に格納します。

UNIX の場合: `/database_path/databases/catalogshadow`

Windows の場合: `database_path¥databases¥catalogshadow`

警告: シャドーカタログパスを変更できるのは、MSDP の初回構成の間のみです。MSDP バックアップの後にパスを変更すると、データが失われることがあります。

---

p.197 の「MSDP カタログの保護について」を参照してください。

MSDP カタログのシャドーパスを変更する方法

1. テキストエディタで次のファイルを開きます。

   UNIX の場合: *storage_path*`/etc/puredisk/spa.cfg`

   Windows の場合: *storage_path*`¥etc¥puredisk¥spa.cfg`

2. `CatalogShadowPath` パラメータを検索し、値を目的のパスに変更します。

   ボリュームはマウントされていて、使用可能である必要があります。

3. 変更後に、ファイルを保存します。

4. 手順 1 で指定したカタログのシャドーパスに `.catalog_shadow_identity` ファイルを作成します。

   メモ: ファイル名の先頭には、隠しファイルを示すピリオド (`.`) があります。

   ---

5. NetBackup Deduplication Manager (`spad`) を再起動します。

6 MSDP ストレージサーバーで次のコマンドを呼び出して、シャドーカタログのディレクトリを作成します。

UNIX の場合: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog backup all`

Windows の場合: *install_path*`¥Veritas¥pdde¥cacontrol --catalog backup all`

7 MSDP カタログのバックアップポリシーが存在する場合は、新しいシャドーカタログのディレクトリを使ってポリシーを更新します。これを行うには、MSDP ストレージサーバーで次のコマンドを呼び出します。

UNIX の場合: `/usr/openv/pdde/pdcr/bin/drcontrol --update_policy --policy` *policy_name*

Windows の場合: *install_path*`¥Veritas¥pdde¥drcontrol --update_policy --policy` *policy_name*

MSDP シャドーカタログスケジュールの変更

NetBackup は、MSDP カタログのコピーを毎日 0340 (ホストタイム) に自動的に作成します。デフォルトのスケジュールを変更できます。

p.197 の「MSDP カタログの保護について」を参照してください。

MSDP シャドーカタログスケジュールを変更する方法

1 テキストエディタで次のファイルを開きます。

UNIX の場合: */database_path*/databases/spa/database/scheduler/5

Windows の場合: *database_path*¥databases¥spa¥database¥scheduler¥5

デフォルトで、NetBackup ではストレージとカタログに同じパスが使用されます。*database_path* と *storage_path* は同じです。重複排除データベースに対し別のパスを構成する場合、パスは異なります。

ファイルの内容は次の行のようになります。行の 2 つ目のセクション (`40 3 * * *`) はスケジュールを構成します。

```
CatalogBackup|40 3 * * *|21600|32400|
```

2 ファイルの 2 つ目のセクション (`40 3 * * *`) を編集します。スケジュールセクションは、次のように UNIX `crontab` ファイルの命名規則に準拠します。

```
40 3 * * *
┬  ┬ ┬ ┬ ┬
│  │ │ │ │
│  │ │ │ │
│  │ │ │ └──── Day of week (0 - 7, Sunday is both 0 and 7, or
use
│  │ │ │       sun, mon, tue, wed, thu, fri, sat; asterisk (*)
is
│  │ │ │       every day)
│  │ │ └─────────── Month (1 - 12; asterisk (*) is every month)
│  │ └──────────────── Day of month (1 - 31; asterisk (*) is every
│  │                   day of the month)
│  └────────────────────── Hour (0 - 23; asterisk (*) is every hour)
└──────────────────────────── Minute (0 - 59; asterisk (*) is every

                              minute of the hour)
```

3 変更後に、ファイルを保存します。

4 NetBackup 重複排除マネージャ (`spad`) を再起動します。

MSDP カタログのシャドーコピー数の変更

NetBackup は MSDP カタログのシャドーコピーを 5 つ保持します。コピー数は変更できます。

p.197 の「MSDP カタログの保護について」を参照してください。

MSDP カタログのシャドーコピー数を変更するには

1. テキストエディタで次のファイルを開きます。

   UNIX の場合: *storage_path*/etc/puredisk/spa.cfg

   Windows の場合: *storage_path*¥etc¥puredisk¥spa.cfg

2. CatalogBackupVersions パラメータを検索し、値を目的のシャドーコピー数に変更します。有効値は 1 ～ 256 です。
3. 変更後に、ファイルを保存します。
4. NetBackup 重複排除マネージャ (spad) を再起動します。

MSDP カタログバックアップの設定

次の手順で NetBackup MSDP カタログのバックアップポリシーを設定します。

p.53 の「MSDP データの保護について」を参照してください。

p.739 の「MSDP カタログバックアップのトラブルシューティング」を参照してください。

MSDP カタログバックアップを設定する方法

1 MSDP ストレージサーバーホスト (つまり、メディアサーバー) が NetBackup プライマリサーバーの追加サーバーであることを確認します。Web UI で、メディアサーバーのホストプロパティを開きます。次に、[サーバー (Servers)]をクリックし、[追加サーバー (Additional servers)]タブをクリックします。

ストレージサーバーが[追加サーバー (Additional servers)]のリストにない場合は、このリストに MSDP ストレージサーバーホストを追加します。ホストは[追加サーバー (Additional servers)]のリストに入れる必要があります。[メディアサーバー (Media servers)]のリストに入れることはできません。

2 MSDP ストレージサーバーで `drcontrol` ユーティリティを呼び出し、必要に応じて適切なオプションを使います。次に、ユーティリティの構文を示します。

Windows の場合: *`install_path`*`¥Veritas¥pdde¥drcontrol--new_policy --residence residence [--policy policy_name] [--client host_name] [--hardware machine_type] [--OS operating_system] [--dsid data_selection_ID] [--NB_install_dir install_directory]`

UNIX の場合: `/usr/openv/pdde/pdcr/bin/drcontrol--new_policy --residence residence [--policy policy_name] [--disk_pool disk_pool_name] [--client host_name] [--hardware machine_type] [--OS operating_system] [--dsid data_selection_ID]`

オプションについては別の項で説明します。注意: NetBackup によるポリシーのアクティブ化を確実に実行するには、`--residence residence` オプションを指定する必要があります。

p.204 の「MSDP の drcontrol オプション」を参照してください。

ユーティリティはログファイルを作成し、コマンド出力のパスを表示します。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

MSDP の drcontrol オプション

`drcontrol` ユーティリティはホストの種類によって次のディレクトリに存在します。

- UNIX の場合: `/usr/openv/pdde/pdcr/bin`
- Windows の場合: *`install_path`*`¥Veritas¥pdde`

`drcontrol` ユーティリティはログファイルを作成します。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

表 4-36 は MSDP カタログバックアップポリシー作成と更新用のオプションを記述します。

表 4-36 カタログバックアップとリカバリの MSDP drcontrol オプション

オプション	説明
--auto_recover_DR	最新のバックアップイメージから MSDP カタログをリカバリします。このオプションは自動的にカタログをリカバリし、MSDP に完全な機能を戻すために必要な処理すべてを実行します。 このオプションには --policy *policy_name* オプションが必要です。 最新ではないバックアップからカタログをリカバリする場合は、Cohesity のサポート担当者にお問い合わせください。
--client *host_name*	バックアップするクライアント (すなわち、MSDP ストレージサーバーのホスト名)。 デフォルト: bpgetconfig CLIENT_NAME が返す値。
--cleanup	カタログリカバリ処理中にすべての古い MSDP カタログのディレクトリを削除します。それらのディレクトリはリカバリ中に名前が変更されます。
--disk_pool	このオプションは、ホスト名からディスクプール名を指定できないときに、auto_recover_DR で必要となります。
--dsid	データ選択 ID は、いずれかの NetBackup ドメインのカタログディレクトリです。 複数ドメインのシナリオでは、別のドメインからカタログをリカバリするときに、他の NetBackup ドメインの dsid が使用されます。他の NetBackup ドメインの dsid を取得するには、spauser コマンドを実行して dsid を表示します。 デフォルト値は 2 です。
--hardware *machine_type*	ホストのハードウェアの種類またはコンピュータの種類。 スペースは使用できません。文字列に特殊文字が含まれる場合は二重引用符 (") で囲みます。 デフォルト: 不明。
--initialize_DR	MSDP カタログリカバリを準備するために次の処理を実行します。 ■ 最新のカタログバックアップが有効であることを確認する。 ■ 重複排除サービスを停止する。 ■ 既存のカタログファイルを移動してリカバリ用にカタログファイルを空にする。
--list_files	最新の MSDP カタログバックアップのファイルを表示します。 このオプションには --policy *policy_name* オプションが必要です。

オプション	説明
--log_file *pathname*	drcontrol ユーティリティが作成するログファイルのパス名。デフォルトでは、ユーティリティは /*storage_path*/log/drcontrol/ にログファイルを書き込みます。
--NB_install_dir *install_directory*	Windows のみ。NetBackup をデフォルト (C:¥Program Files¥Veritas) 以外の場所にインストールした場合の必須オプション。 文字列にスペースや特殊文字が含まれる場合は二重引用符 (") で囲みます。*install_directory* 文字列の末尾にバックスラッシュを使わないでください。
--new_policy	このホストの重複排除カタログを保護する新しいポリシーを作成します。指定した名前のポリシーがすでに存在する場合にはコマンドは失敗します。 **メモ:** NetBackup によるポリシーのアクティブ化を確実に実行するには、--residence *residence* オプションを指定する必要があります。
--OS *operating_system*	ホストのオペレーティングシステム。 スペースは使用できません。文字列に特殊文字が含まれる場合は二重引用符 (") で囲みます。 デフォルト: UNIX/Linux または MS-Windows。
--policy *policy_name*	バックアップポリシーの名前。 --auto_recover_DR と --update_policy で必須。--new_policy では省略可能。 デフォルト: Dedupe_Catalog_*shorthostname*
--print_space_required	MSDP カタログのリカバリに必要なファイルシステム容量の推定パーセントを表示します。
--recover_last_image	バックアップイメージ (つまり、最後の完全バックアップとすべての後続の増分バックアップ) の最後のセットから MSDP カタログをリストアします。drcontrol ユーティリティは NetBackup bprestore コマンドをリストア操作のために呼び出します。
--refresh_shadow_catalog	すべての既存のシャドウカタログコピーを削除して新しいカタログシャドウコピーを作成します。

オプション	説明
`--residence residence`	MSDP カタログバックアップを格納するストレージユニットの名前。 メディアサーバー重複排除プールをカタログバックアップの宛先として使わないでください。メディアサーバー重複排除プールから MSDP カタログのリカバリは行えません。 MSDP ストレージサーバーではなく Cohesity ホストに接続するストレージユニットを使うことを NetBackup が推奨します。
`--update_policy`	ポリシーを次のように更新します。 ■ (このメディアサーバーの) クライアント名がポリシーのクライアントリストに入っていない場合は、ポリシーのクライアントリストにクライアント名を追加する。 ■ `--os` オプションまたは `--hardware` オプションを指定して、ポリシーの現在の値を新しい値に置き換える。 ■ MSDP ストレージディレクトリと設定ファイルの場所に基づいてバックアップ対象を更新する。したがって、次のいずれかを修正する場合はこのオプションを使用してカタログバックアップポリシーを更新する必要がある。 ■ `spa.cfg` ファイル (`section:variable` ペア) の次のいずれかの値 ■ `StorageDatabase:CatalogShadowPath` ■ `StorageDatabase:Path` ■ `Paths:Var` ■ `pdregistry.cfg` ファイルの `spa.cfg` または `contentrouter.cfg` の場所。 このオプションは、指定したポリシー名を使うポリシーが存在しない場合は失敗します。既存のポリシーの種類がコマンドを実行するホストのオペレーティングシステムと適合しない場合も失敗します。 このオプションには `--policy policy_name` オプションが必要です。
`--verbose`	stdout に対してすべての `drcontrol` ログ文をエコーします。

p.203 の「MSDP カタログバックアップの設定」を参照してください。

MSDP カタログバックアップポリシーの更新

任意の NetBackup 方式を使って、MSDP カタログバックアップポリシーを手動で更新できます。ただし、次の状況で NetBackup 重複排除カタログポリシーの管理とカタログのディザスタリカバリ (`drcontrol`) を使う必要があります。

- ストレージサーバーのクライアント名をポリシーのクライアントリストに追加するため。
- `--os` 値を更新するため。

- --hardware 値を更新するため。
- 次の構成値のいずれかを変更した場合にバックアップ対象を更新するため。
  - spa.cfg ファイル (section:variable ペア) の次のいずれかの値
    - StorageDatabase:CatalogShadowPath
    - StorageDatabase:Path
    - Paths:Var
  - pdregistry.cfg ファイルの spa.cfg または contentrouter.cfg の場所。

p.53 の「MSDP データの保護について」を参照してください。

p.739 の「MSDP カタログバックアップのトラブルシューティング」を参照してください。

MSDP カタログバックアップを更新する方法

◆ MSDP ストレージサーバーで drcontrol ユーティリティを呼び出し、必要に応じて適切なオプションを使います。更新操作の構文を次に示します。

UNIX の場合: `/usr/openv/pdde/pdcr/bin/drcontrol--update_policy --policy policy_name [--client host_name] [--hardware machine_type] [--OS operating_system]`

Windows の場合: `install_path¥Veritas¥pdde¥drcontrol--update_policy --policy policy_name [--client host_name] [--hardware machine_type] [--OS operating_system] [--OS operating_system] [--NB_install_dir install_directory]`

オプションについては別の項で説明します。

p.204 の「MSDP の drcontrol オプション」を参照してください。

ユーティリティはログファイルを作成し、コマンド出力のパスを表示します。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

MSDP の FIPS 準拠について

FIPS (連邦情報処理標準) には米国連邦政府とカナダ政府のコンピュータシステムに対するセキュリティと相互運用性の必要条件が定義されています。FIPS 140-2 標準には暗号化モジュールのセキュリティ必要条件が明記されています。対称キー暗号化と非対称キー暗号化、メッセージ認証、ハッシュの承認済みセキュリティ機能について説明しています。

FIPS 140-2 標準とその検証プログラムについて詳しくは、https://csrc.nist.gov/projects/cryptographic-module-validation-program で、米国標

準技術研究所 (NIST) とカナダの通信セキュリティ機構 (CSEC) の暗号化モジュール検証プログラム Web サイトを参照してください。

NetBackup MSDP は FIPS 検証済みとなり、FIPS モードで操作できるようになりました。

メモ: NetBackup 8.1.1 の新規インストールでは FIPS モードを実行する必要があります。NetBackup 10.0 以降のバージョンでは OCSD FIPS のみ有効にできます。

MSDP の FIPS モードの有効化

MSDP の FIPS モードを有効にする前に、ストレージサーバーを構成します。

注意: MSDP の FIPS を有効にすると、Solaris オペレーティングシステムのサーバーでの NetBackup のパフォーマンスに影響する場合があります。

MSDP の FIPS モードは、次のコマンドを実行して有効にします。

- UNIX の場合:
  `/usr/openv/pdde/pdag/scripts/set_fips_mode.sh 1`
  Windows の場合:
  `<install_path>¥Veritas¥pdde¥set_fips_mode.bat 1`
- サーバーとクライアントで NetBackup サービスを再起動します。
  - UNIX の場合:
    - `/usr/openv/netbackup/bin/bp.kill_all`
    - `/usr/openv/netbackup/bin/bp.start_all`
  - Windows の場合:
    - `<install_path>¥NetBackup¥bin¥bpdown`
    - `<install_path>¥NetBackup¥bin¥bpup`

次の手順を実行して、MSDP または OpenCloudStorageDaemon (OCSD) の FIPS モードを有効にします。

- 既存のツールを使用して OCSD FIPS を有効または無効にします。この方法を使用すると、MSDP の FIPS 構成全体が変更されます。
  - Windows の場合:
    `<install_path>¥Veritas¥pdde¥set_fips_mode.bat 1`
  - UNIX の場合:
    `/usr/openv/pdde/pdag/scripts/set_fips_mode.sh 1`

- NetBackup では、OCSD FIPS はデフォルトで無効になっています。
  OpenCloudStorageDaemon/FIPS を変更して OCSD FIPS を有効または無効にします。
  /etc/pdregistry.cfg

サーバーとクライアントで NetBackup サービスを再起動して、これらの変更を有効にします。

- Windows の場合:
  - *<install_path>*¥NetBackup¥bin¥bpdown
  - *<install_path>*¥NetBackup¥bin¥bpup
- UNIX の場合:
  - /usr/openv/netbackup/bin/bp.kill_all
  - /usr/openv/netbackup/bin/bp.start_all

警告: セキュリティ上の理由により、MSDP の FIPS モードを一度有効にしたら、無効にしないことをお勧めします。

MSDP の FIPS モードの状態の取得

MSDP の FIPS モードの状態を取得するには、次のコマンドを入力します。

UNIX の場合:

```
/usr/openv/pdde/pdcr/bin/crcontrol --getmode
```

Windows の場合:

```
<install_path>¥Veritas¥pdde¥crcontrol.exe --getmode
```

他にも、以下の点に注意してください。

- 接続を確立するには、すべての NetBackup コンポーネントで FIPS を有効にする必要があります。FIPS モードが有効でない場合、以前のサポートされているバージョンの NetBackup クライアントと NetBackup サーバー間で通信が発生することがあります。

MSDP の複数のインターフェースをサポートするための NetBackup クライアント側の重複排除の構成

NetBackup クライアントで VLAN やサブネットなどのネットワーク構成を使用している場合、複数のネットワークインターフェースが MSDP サーバーに存在します。これらのインターフェースは、異なるスイッチまたは VLAN に接続されています。MSDP ではストレージサーバーが 1 つしかないため、NetBackup クライアントはストレージサーバー名を使

用して MSDP サーバーにアクセスできず、クライアント上で重複排除が失敗する可能性があります。

最大 30 個のインターフェースのサポートを追加できます。

次の手順を実行して cacontrol コマンドオプション (場所: /usr/openv/pdde/pdcr/bin/) を使用し、MSDP を構成して、NetBackup クライアントが使用できるネットワークインターフェースを指定します。

1 MSDP サーバーにログオンします。

2 次のコマンドを使用して、代替のインターフェースを追加します。

```
cacontrol --interface add msdp-a.server.com
```

次のコマンドを使用して、追加したインターフェースを削除できます。

```
cacontrol --interface remove msdp-a.server.com
```

3 インターフェースの構成を検証するには、次のいずれかのオプションを使用します。

- cacontrol --interface list
- bpstsinfo -si -storage_server *msdp-a.server.com* -stype PureDisk
  bpstsinfo コマンドの場所: /usr/openv/netbackup/bin/admincmd/

4 NetBackup クライアント側の重複排除バックアップポリシーを構成し、バックアップ操作を実行します。

MSDP のマルチドメインのサポートについて

MSDP ストレージサーバーは、NetBackup メディアサーバーで構成されます。NetBackup ドメインの NetBackup メディアサーバーとクライアントはこのストレージサーバーを使用します。デフォルトでは、NetBackup メディアサーバーとクライアントは他の NetBackup ドメインから MSDP ストレージサーバーを直接使用できません。たとえば、他の NetBackup ドメインの NetBackup メディアサーバーまたはクライアントは、MSDP ストレージサーバーにデータをバックアップできません。

他の NetBackup ドメインから MSDP ストレージサーバーを使用するには、MSDP ストレージサーバーに複数の MSDP ユーザーが必要です。これにより、NetBackup メディアサーバーまたはクライアントが、他の NetBackup ドメインから異なる MSDP ユーザーを使用して MSDP ストレージサーバーにアクセスできます。複数の NetBackup ドメインが同じ MSDP ストレージサーバーを使用できますが、各 NetBackup ドメインは異なる MSDP ユーザーを使用して MSDP ストレージサーバーにアクセスする必要があります。

MSDP ストレージサーバーに MSDP ユーザーを追加するには、次のコマンドを実行します。

- Windows

```
<install_path>¥pdde¥spauser -a -u <username> -p <password> --role
admin
```

- UNIX

```
/usr/openv/pdde/pdcr/bin/spauser -a -u <username> -p <password>
--role admin
```

ストレージサーバーが NetBackup WORM ストレージサーバーまたは NetBackup Flex Scale ストレージサーバーの場合は、次の NetBackup 重複排除シェルコマンドを実行します。

```
setting MSDP-user add-MSDP-user username=<username> [role=<role-name>]
```

ここで、role は任意で、admin または app にできます。役割が指定されていない場合は、デフォルトの役割 admin が使用されます。

すべての MSDP ユーザーを一覧表示するには、MSDP ストレージサーバーで次のコマンドを実行します。

- Windows

```
<install_path>¥pdde¥spauser -l
```

- UNIX

```
/usr/openv/pdde/pdcr/bin/spauser -l
```

ストレージサーバーが NetBackup WORM ストレージサーバーまたは NetBackup Flex Scale ストレージサーバーの場合は、次の NetBackup 重複排除シェルコマンドを実行します。

```
setting MSDP-user list
```

メモ: マルチドメインをサポートするために作成する MSDP ユーザーの合計数が 128 ユーザーを超えないようにすることをお勧めします。

他の NetBackup ドメインから MSDP ストレージサーバーを使用するには、他の NetBackup ドメインから NetBackup 証明書を取得する必要があります。

他のドメインから MSDP ストレージサーバーを使用する各 NetBackup メディアサーバーまたはクライアントで、次のコマンドを実行します。

- Windows

```
install_path¥NetBackup¥bin¥nbcertcmd -getCACertificate -server
another_primary_server
install_path¥NetBackup¥bin¥nbcertcmd -getCertificate -server
another_primary_server -token token_string
```

- UNIX

```
/usr/openv/netbackup/bin/nbcertcmd -getCACertificate -server
another_primary_server
/usr/openv/netbackup/bin/nbcertcmd -getCertificate -server
another_primary_server -token token_string
```

ストレージサーバーが NetBackup WORM ストレージサーバーまたは NetBackup Flex Scale ストレージサーバーの場合は、次の NetBackup 重複排除シェルコマンドを実行します。

```
setting certificate get-CA-certificate
primary_server=another_primary_server
```

```
setting certificate get-certificate
primary_server=another_primary_server token=token_string
```

認証トークンを取得するには、次の 2 つの方法のいずれかを使用します。

- NetBackup Web UI
  - 左側で、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
  - [追加 (Add)]をクリックしてトークンを作成します。
- NetBackup コマンド
  - ターゲット NetBackup プライマリサーバーにログオンするには、bpnbat コマンドを使用します。
  - 認証トークンを取得するには、nbcertcmd コマンドを使用します。
    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。

他の NetBackup ドメインから MSDP ストレージサーバーを使用する例

次の表は、この例で使用される階層について説明します。

NetBackup ドメイン A	NetBackup ドメイン B
primaryA	primaryB
mediaA1	mediaB
mediaA2	
clientA	

primaryA は NetBackup ドメイン A のプライマリサーバーのホスト名で、ドメインには 2 台のメディアサーバー (mediaA1 と mediaA2) と 1 台のクライアント (clientA) が含まれます。primaryB は NetBackup ドメイン B のプライマリサーバーのホスト名で、ドメインには 1 台のメディアサーバー (mediaB) が含まれます。

次のサンプルの手順を使用して、ドメイン B に MSDP ストレージサーバーを作成し、ドメイン A が MSDP ストレージサーバーを使用できるようにします。

1. NetBackup ドメイン B のメディアサーバー mediaB に MSDP ストレージサーバーを作成します。
   - Web UI を開きます。
   - 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。
   - [ストレージサーバー (Storage servers)]タブで[追加 (Add)]をクリックして、[ローカルまたはクラウドストレージへのメディアサーバー重複排除プール (Media Server Deduplication Pool to local or cloud storage)]を選択します。
2. mediaB で次のコマンドを実行し、新しい MSDP ユーザー testuser1 をパスワード testuser1pass で作成します。

   ```
   spauser -a -u "testuser1" -p "testuser1pass" --role admin
   ```
3. mediaA1 で次のコマンドを実行し、primaryB から CA 証明書とホスト証明書を取得します。

   ```
   nbcertcmd -GetCACertificate -server primaryB

   nbcertcmd -GetCertificate -server primaryB -token <token_string>
   ```
4. NetBackup ドメイン A の mediaA1 に MSDP OpenStorage サーバーを作成します。
   - Web UI を開きます。
   - 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。
   - [ストレージサーバー (Storage servers)]タブで[追加 (Add)]をクリックし、[OpenStorage Technology]を選択します。

   そうすると、OpenStorage サーバー形式は PureDisk、ストレージサーバー名は mediaB、ユーザー名は testuser1、パスワードは testuser1pass になります。

   サーバー形式には PureDisk と入力する必要があります。

   これで、NetBackup ドメインの mediaA1 は MSDP ストレージサーバー mediaB を使用できます。mediaA2 を MSDP ストレージサーバーの負荷分散サーバーとして使用するには、mediaA2 で次の証明書コマンドを実行します。
   - nbcertcmd -GetCACertificate -server primaryB
   - nbcertcmd -GetCertificate -server primaryB -token <token_string>

clientA から MSDP ストレージサーバー mediaB にクライアントからの直接バックアップを実行するには、clientA で次の証明書コマンドを実行します。

- nbcertcmd -GetCACertificate -server primaryB
- nbcertcmd -GetCertificate -server primaryB -token <*token_string*>

5. MSDP OpenStorage サーバーを作成した後、関連する NetBackup ディスクプールとストレージユニットを作成します。関連するすべての NetBackup ジョブを実行するには、ストレージユニットを使用します。

最適化複製または A.I.R. とマルチドメインを併用すると、2 つの異なる NetBackup ドメインの MSDP ストレージサーバー間で通信が行われます。他のドメインの MSDP ストレージサーバーには、ローカルの NetBackup ドメインのプライマリサーバーによって生成された証明書が存在する必要があります。ソース側の MSDP ストレージサーバーで nbcertcmd コマンドを実行して、ターゲット MSDP ストレージサーバーの NetBackup プライマリサーバーから証明書を要求します。

クライアントとマルチドメインでバックアップジョブとリストアジョブを併用すると、2 つの異なる NetBackup ドメインの NetBackup クライアントと MSDP ストレージサーバー間で通信が行われます。NetBackup クライアントで nbcertcmd コマンドを実行して、MSDP ストレージサーバーの NetBackup プライマリサーバーから証明書を要求します。

ある NetBackup ドメインが別の NetBackup ドメインの MSDP ストレージサーバーを使用している場合、その NetBackup ドメインの MSDP ストレージサーバーを A.I.R ターゲットにすることはできません。

NetBackup 設定で外部 CA が使用されている場合、nbcertcmd -GetCACertificate コマンドと nbcertcmd -GetCertificate コマンドを実行する必要はありません。NetBackup ドメイン A と B が同じ外部 CA を使用していない場合は、MSDP 通信のため、2 つの NetBackup ドメイン間で外部ルート CA を同期します。

外部 CA 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。

1 つの NetBackup ドメインが、複数のネットワークインターフェースと関連するホスト名がある MSDP ストレージサーバーを使用している場合、他の NetBackup ドメインは任意のホスト名を使用して OpenStorage サーバーを構成できます。複数のホスト名がある MSDP ストレージサーバーで外部 CA を使用している場合、外部証明書のサブジェクトの別名フィールドには、OpenStorage サーバーの構成に使用されるすべてのホスト名が含まれている必要があります。

他の NetBackup ドメインで使用できるのは、1 つの MSDP ストレージのローカルストレージのみです。1 台の MSDP ストレージサーバーのクラウド LSU は、他の NetBackup ドメインでは使用できません。異なる NetBackup ドメインが同じ MSDP ユーザーを使用して MSDP ストレージサーバーにアクセスしないようにしてください。そうしないと、数分後

にストレージサーバーが停止します。この問題を解決するには、p.744 の「複数ドメインの問題のトラブルシューティング」を参照してください。

MSDP ストレージサーバーにデータ破損がある場合、MSDP ストレージサーバーの最初のドメインのみがデータ破損の通知を受信します。マルチドメインでは、複数の NetBackup ドメインが 1 つのストレージサーバーを使用し、各ドメインからこのストレージサーバーの使用領域を確認できます。ストレージサーバーの使用領域は、すべてのドメインのデータの合計です。

メモ: ターゲットドメインへのユニバーサル共有バックアップは、マルチドメイン設定ではサポートされません。

MSDP アプリケーションのユーザーサポートについて

Oracle 用 NetBackup 直接重複排除を使用することを目的とした MSDP アプリケーションユーザーを作成できます。Oracle 用 NetBackup 直接重複排除は、RMAN バックアップからのデータを MSDP ストレージに直接格納するために使用できる軽量のプラグインです。

Oracle 用 NetBackup 直接重複排除について詳しくは、『NetBackup for Oracle 管理者ガイド』を参照してください。

MSDP アプリケーションユーザーを管理するには、MSDP サーバーの spauser コマンドラインツールを使用します。

MSDP アプリケーションユーザーを管理する方法

1. MSDP サーバーにログオンします。
2. アプリケーションユーザーを作成します。

   ```
   /usr/openv/pdde/pdcr/bin/spauser -a -u <username> -p <password>
   --role app
   ```

3. アプリケーションユーザーを削除します。

   ```
   /usr/openv/pdde/pdcr/bin/spauser -d -u username [-p password]
   ```

4. アプリケーションユーザーのパスワードを変更します。

   ```
   /usr/openv/pdde/pdcr/bin/spauser -c -u username [-p oldpassword
   -q newpassword]
   ```

5. すべてのユーザーを一覧表示します。

   ```
   /usr/openv/pdde/pdcr/bin/spauser -l
   ```

MSDP マルチドメイン VLAN のサポートについて

MSDP は、マルチドメインの NetBackup 設定をサポートします。マルチドメイン設定では、他のドメインのプライマリサーバーが、MSDP サーバーを含む NetBackup ドメインの MSDP ストレージサーバーとプライマリサーバーに接続できることが重要です。マルチドメイン設定では、プライマリサーバーとメディアサーバーに複数のネットワークインターフェースとホスト名が必要です。

MSDP VLAN を構成するとき、ローカルの NetBackup ドメインとその他の NetBackup ドメインには NetBackup バージョン 8.2 以降が必要です。

MSDP VLAN の使用例

次の表は、この例で使用される階層について説明します。

NetBackup ドメイン A	NetBackup ドメイン B
`primaryA - (10.XX.30.1/24)`	`primaryB - (10.XX.40.3/24)`
`primaryA2 - (10.XX.40.1/24)`	`mediaB - (10.XX.40.4/24)`
`mediaA - (10.XX.30.2/24)`	
`mediaA2 - (10.XX.40.2/24)`	

`primaryA` はドメイン A のプライマリサーバーで、2 つのホスト名と IP アドレスがあります。`mediaA` はドメイン A のメディアサーバーで、2 つのホスト名と IP アドレスがあります。MSDP ストレージサーバーは、メディアサーバー `mediaA` で作成されます。

ドメイン B からドメイン A の `mediaA` にある MSDP ストレージサーバーへのアクセスを許可するには、次の手順を実行します。

1. NetBackup ドメイン A のメディアサーバー `mediaA` に MSDP ストレージサーバーを作成します。

   NetBackup Web UI を開きます。[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。[ストレージサーバー (Storage servers)]タブをクリックします。[追加 (Add)]をクリックし、[ローカルまたはクラウドストレージへのメディアサーバー重複排除プール (Media Server Deduplication Pool to local or cloud storage)]を選択します。

2. `mediaA` で次のコマンドを実行し、新しい MSDP ユーザー `testuser1` をパスワード `testuser1pass` で作成します。

   ```
   spauser -a -u "testuser1" -p "testuser1pass" --role admin
   ```

3. ドメイン B のサーバーがアクセスできるのは 10.XX.40.* などの IP のみなので、`primaryA2` がドメイン A のプライマリサーバーのホスト名として使用されます。

mediaB で次のコマンドを実行し、primaryA から CA 証明書とホスト証明書を取得します。

```
nbcertcmd -GetCACertificate -server primaryA2

nbcertcmd -GetCertificate -server primaryA2 -token <token_string>
```

nbcertcmd -GetCACertificate で「サーバー名がサーバーの証明書に表示されているどのホスト名とも一致しません (The server name does not match any of the host names listed in the server's certificate)」というエラーが表示された場合は、次の記事を参照して、プライマリサーバーにホスト名を追加してください。

https://www.veritas.com/support/en_US/article.100034092

4. NetBackup ドメイン B の mediaB に MSDP OpenStorage サーバーを作成します。

   NetBackup Web UI を開きます。[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。[ストレージサーバー (Storage server)]タブをクリックします。[追加 (Add)]をクリックし、[OpenStorage Technology (OST)]を選択します。

   OpenStorage サーバー名 mediaA2 が、IP アドレス 10.XX.40.* のホスト名として使用されます。

   OpenStorage サーバー形式は PureDisk、ユーザー名は testuser1、パスワードは testuser1pass です。サーバー形式には PureDisk と入力する必要があります。

これで、NetBackup ドメイン B の mediaB は MSDP ストレージサーバー mediaA2 とネットワーク IP アドレス 10.XX.40.* を使用できます。

マルチドメイン NetBackup 構成では、ドメイン B のメディアサーバーがドメイン A のメディアサーバーのサーバー証明書を認識する必要がある場合があります。たとえば、VMware イメージリカバリをドメイン A からドメイン B に実行する場合は、この設定が必要です。

mediaA2 のサーバー証明書の primaryB への移動は 2 段階のプロセスで、次の手順を実行するには特権ユーザーである必要があります。

1. ファイル /etc/nginx/conf.d/nginx_spws.conf を読み、ssl_certificate フィールドを確認します。

   mediaA2 から primaryB に ssl_certificate フィールド (たとえば /msdp/data/dp1/pdvol/spws/var/keys/cluster_spws_cert.pem) をコピーします。

   サンプルファイル:

   ```
   engine : cat /etc/nginx/conf.d/nginx_spws.conf
   server {
   listen 443 default ssl;
   listen [::]:443 default ssl;
   ```

```
server_name _;
ssl_session_cache shared:SSL:1m;
ssl_session_timeout 5m;
ssl_certificate
/msdp/data/dp1/pdvol/spws/var/keys/cluster_spws_cert.pem;
ssl_certificate_key
/msdp/data/dp1/pdvol/spws/var/keys/cluster_spws_key.pem;
ssl_verify_client off;
ssl_protocols TLSv1.2;
ssl_ciphers
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-G
CM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES
128-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256;
ssl_prefer_server_ciphers on;
include /etc/nginx/locations/nginx_loc_spws.conf;
}
```

2. primaryB で次のコマンドを実行し、その証明書を primaryB の信頼できるキーストアにインポートします。

メモ: storepass と keypass の値は、primaryB の /usr/openv/var/global/jkskey にあります。

```
/usr/openv/java/jre/bin/keytool
-keystore
/usr/openv/var/global/wsl/credentials/truststoreMSDP.bcfks
-storetype BCFKS
-providername CCJ
-providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
-providerpath /usr/openv/wmc/webserver/lib/ccj.jar
-storepass
4d2b912d38dff8d2406b2aba2d023740aafa520a16cd3bb8b1b39b10b58a4ce5
-keypass
4d2b912d38dff8d2406b2aba2d023740aafa520a16cd3bb8b1b39b10b58a4ce5
-alias primaryB -importcert -file cluster_spws_cert.pem
```

メモ: ご使用の bc-fips-X.X.X.X.jar ファイルのバージョンが前述の例とは異なる場合があります。NetBackup インストールに適したバージョンを見つけるには、そのディレクトリで bc-fips* を検索します。

---

3. primaryB で -list コマンドを実行すると、次の例のようなメッセージが表示されます。

```
/usr/openv/java/jre/bin/keytool -list
-keystore
/usr/openv/var/global/wsl/credentials/truststoreMSDP.bcfks
-storetype BCFKS
-providername CCJ
-providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
-providerpath /usr/openv/wmc/webserver/lib/ccj.jar
-storepass
4d2b912d38dff8d2406b2aba2d023740aafa520a16cd3bb8b1b39b10b58a4ce5

Keystore type: BCFKS
Keystore provider: BCFIPS
Your keystore contains 2 entries
ca1, Jan 11, 2023, trustedCertEntry,
Certificate fingerprint (SHA-256):
4A:52:C8:9E:B1:1F:A9:21:99:3B:AA:5A:0C:B5:C3:2F:51:(string
continues)
primaryB, Jan 16, 2023, trustedCertEntry,
Certificate fingerprint (SHA-256):
AE:34:D1:63:B1:94:33:8C:07:5D:9A:D6:2B:CF:5B:52:D7:(string
continues)
```

表示されている 2 番目の証明書は mediaA2 の証明書です。

NetBackup 設定で外部 CA が使用されている場合、nbcertcmd -GetCACertificate コマンドと nbcertcmd -GetCertificate コマンドを実行する必要はありません。NetBackup ドメイン A と NetBackup ドメイン B が同じ外部 CA を使用していない場合は、MSDP 通信のため、2 つの NetBackup ドメイン間で外部ルート CA を同期する必要があります。サーバーに複数のホスト名がある場合、外部証明書の[サブジェクトの別名 (Subject Alternative Name)]フィールドにはすべてのホスト名を含める必要があります。

変更不可および削除不可のデータの NetBackup WORM ストレージサポートについて

NetBackup WORM ストレージサーバーは、変更不可および削除不可のデータストレージをサポートします。

詳しくは、『NetBackup 管理者ガイド Vol. 1』の「NetBackup でのデータの変更不可と削除不可の設定」の章を参照してください。

NetBackup WORM ストレージと保持期間

保持期間を使用すると、バックアップイメージを保護する時間を定義できます。保持期間を定義すると、保持期間が満了するタイミングを示すため、MSDP にイメージメタデータとタイムスタンプが格納されます。保持期間が満了すると、イメージデータを削除できます。

保持期間には次のパラメータを設定できます。

- ロックの最小期間 (Lock Minimum Duration)
- ロックの最大期間 (Lock Maximum Duration)

詳しくは、『NetBackup 管理者ガイド Vol. 1』の「変更不可データと削除不可データを構成するためのワークフロー」のトピックを参照してください。

WORM ストレージでは、次の保持期間モードがサポートされます。

- compliance モード
  どのタイプのユーザーも、定義された保持期間にコンプライアンスモードを使用して保護されているデータを上書きまたは削除できません。データストレージの保持期間を設定すると、期間は短縮できません。延長のみ可能です。
- enterprise モード
  保持ロックを無効にしてイメージを削除するには、ユーザーに特別な権限が必要です。MSDP セキュリティ管理者ユーザーのみが、必要に応じて保持ロックを無効にしてイメージを削除できます。compliance モードの保持期間を作成する前に、enterprise モードを使用して保持期間の動作をテストできます。

p.221 の「変更不可および削除不可のデータを構成するための NetBackup コマンドラインオプションについて」を参照してください。

p.664 の「NetBackup 重複排除シェルについて」を参照してください。

変更不可および削除不可のデータを構成するための NetBackup コマンドラインオプションについて

セキュリティ管理者として、次の `catdbutil` および `spadb` のコマンドラインオプションを使用して、変更不可および削除不可のデータまたは WORM ストレージを構成できます。

p.220 の「変更不可および削除不可のデータの NetBackup WORM ストレージサポートについて 」を参照してください。

`catdbutil` コマンドを使用すると、カタログデータベースに対する問い合わせや修正を実行できます。コマンドは、次の場所で利用できます。

```
/usr/openv/pdde/pdcr/bin/
```

次の表で、catdbutil コマンドの WORM 固有のオプションおよび引数を説明します。

表 4-37 catdbutil コマンドのオプションおよび引数は次のとおりです。

コマンドとその説明	オプション	説明
catdbutil カタログデータベースに対する問い合わせや修正を実行します。	worm list 使用方法: --worm list [--pattern PATTERN]	WORM 対応イメージのバックアップ ID とその他の情報を表示します。 次の情報が表示されます。 backupid、retention lock date、time left、worm flags
	worm disable 使用方法: --worm disable --backupid	バックアップ ID を使用してイメージの保持ロックを無効にします。
	worm audit 使用方法: --worm audit [--sdate *yyyy-MM-ddThh:mm:ss* | --edate *yyyy-MM-ddThh:mm:ss*]	指定した日付と時間間隔の WORM 監査情報を表示します。

NetBackup Deduplication Manager (spad) を使用して LSU の WORM を設定し、イメージを変更不可および削除不可にする WORM モードと間隔を定義する spadb コマンドラインユーティリティ。

Deduplication Manager は、/etc/lockdown-mode.conf ファイルから WORM モードを読み取ります。

コマンドは、次の場所で利用できます。

/usr/openv/pdde/pdcr/bin/

次の表で、spadb コマンドの WORM 固有のオプションおよび引数を説明します。

表 4-38 spadb コマンドのオプションおよび引数は次のとおりです。

コマンドとその説明	オプション	説明
spadb NetBackup Deduplication Manager (spad) を使用できるコマンドラインユーティリティ。	spadb update WORM set ${FIELD1_NAME}=xxx, ${FIELD2_NAME}=xxxx where id=${*DSID*} # field names: ■ indeliable_minimum_interval ■ indeliable_maximum_interval	データ選択 ID を使用して、次の WORM プロパティを構成します。 ■ indelible_minimum_interval および indelible_maximum_interval イメージを削除不可にするための最小間隔と最大間隔を日数で設定します。 次に例を示します。 spadb -c "update WORM set indelible_minimum_interval=1 where dsid=2" spadb -c "update WORM set indelible_maximum_interval=1000000 where dsid=2"

root 以外のユーザーによる MSDP サービスの実行

root 以外のユーザーとしてアプリケーションを実行することで、セキュリティリスクを低減できます。

NetBackup 10.3 以降、NetBackup BYO (Red Hat Enterprise Linux and SUSE)、NetBackup Appliance、Flex Appliance の NetBackup メディアサーバーで root 以外のユーザーを使用して MSDP デーモンを実行できます。

root 以外のユーザーは、MSDP サービスユーザーが変更された後、MSDP 構成ファイル /etc/pdregistry.cfg で自動的に構成される MSDP サービスユーザーです。root 以外のユーザーを MSDP サービスユーザーとして使用することをお勧めします。

インストールまたはアップグレード後のサービスユーザーの変更

NetBackup のインストール後に、MSDP ストレージサーバーを作成します。MSDP ストレージサーバーが作成される前に、root 以外のサービスユーザーで実行するように NetBackup が構成されている場合、MSDP はこのサービスユーザーを使用して自動的に実行されるようにもできます。

MSDP サービスがこのサービスユーザーとして実行されていない場合は、msdpserviceusercmd コマンドを使用してサービスユーザーを手動で変更できます。

root 以外のサービスユーザーで MSDP を実行するための前提条件を次に示します。

- root 以外のユーザーが NetBackup サービスを実行できるかどうかを確認します。
  root 以外のユーザーが NetBackup サービスを実行できない場合は、NetBackup

サービスユーザーアカウントを変更します。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 BYO で次のコマンドを実行して、サービスユーザーが開くことができるファイルの最大数を確認します。

  ulimit -Hn

  /etc/security/limits.conf ファイルで制限を 1048576 に設定します。

NetBackup BYO で MSDP サービスユーザーを変更する方法

1. 次のサービスを停止します。

   systemctl stop crond.service

   /usr/openv/netbackup/bin/bp.kill_all

   /opt/VRTSpbx/bin/vxpbx_exchanged stop

2. 次のコマンドを実行して、MSDP サービスユーザーを変更します。

   /usr/openv/pdde/pdconfigure/scripts/support/msdpserviceusercmd

3. 次のサービスを開始します。

   /opt/VRTSpbx/bin/vxpbx_exchanged start

   /usr/openv/netbackup/bin/bp.start_all

   systemctl start crond.service

Flex Appliance でメディアサーバーの MSDP サービスユーザーを変更する方法

1. 次のサービスを停止します。

   /opt/veritas/vxapp-manage/health disable

   systemctl stop crond.service

   /opt/veritas/vxapp-manage/stop

2. 次のコマンドを実行して、MSDP サービスユーザーを変更します。

   /usr/openv/pdde/pdconfigure/scripts/support/msdpserviceusercmd

3. 次のサービスを開始します。

   /opt/veritas/vxapp-manage/start

   systemctl start crond.service

   /opt/veritas/vxapp-manage/health enable

NetBackup Appliance で MSDP サービスユーザーを変更する方法

1. NetBackup Appliance シェルメニューから crond サービスを停止します。

   ```
   Main_Menu > Support > Service Stop crond
   ```

   NetBackup Appliance シェルメニューの使用方法については、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

2. NetBackup Appliance シェルメニューから NetBackup プロセスを停止します。

   ```
   Main_Menu > Support > Processes > NetBackup Stop
   ```

3. NetBackup CLI から次のコマンドを実行して、MSDP サービスユーザーを変更します。

   ```
   nbucliuser-!> msdpserviceusercmd
   ```

   NetBackup CLI の使用方法について詳しくは、『NetBackup Appliance セキュリティガイド』の「NetBackupCLI ユーザーロールについて」のトピックを参照してください。

4. NetBackup Appliance シェルメニューから NetBackup プロセスを開始します。

   ```
   Main_Menu > Support > Processes > NetBackup Start
   ```

5. NetBackup Appliance シェルメニューから crond サービスを開始します。

   ```
   Main_Menu > Support > Service Restart crond
   ```

メモ: MSDP サービスユーザーは NetBackup サービスユーザーと同じです。

---

msdpserviceusercmd は、MSDP ストレージのデータサイズによっては時間がかかる場合があります。コマンドが中断された (ノートパソコンをオフにするなど) と考えられる場合は、Linux コマンド nohup を使用して、バックグラウンドで msdpserviceusercmd コマンドを実行します。

msdpserviceusercmd が中断された場合、MSDP サービスの開始が失敗します。その場合は、コマンドを再度実行して、サービスユーザーを変更するプロセスを再び開始します。

コマンド crcontrol --dsaddpartition [volume path] を使用して MSDP ストレージボリュームを追加する場合は、MSDP サービスユーザーに新しいストレージボリュームパスに対する読み取りおよび書き込み権限があることを確認します。

サービス spad、spoold、ocsd、s3srv は、サービスユーザーで実行される MSDP サービスです。MSDP Web サービス spws は、常に spws ユーザーで実行されます。

root 以外のユーザーによる MSDP コマンドの実行

root ユーザーで MSDP コマンドを実行している場合、サービスユーザーに自動的に切り替わります。ただし、root 以外のユーザーが MSDP コマンドを実行する必要がある場合は、msdpcmdrun ラッパーコマンドを使用できます。このツールは NetBackup BYO、Flex Appliance のメディアサーバー、NetBackup Cloud Scale、NetBackup Appliance でサポートされます。

nbcmdrun が構成されて有効になっている場合は、次のように msdpcmdrun を使用できます。

```
/usr/openv/netbackup/bin/nbcmdrun msdpcmdrun <msdp commands>
```

nbcmdrun について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』で、nbcmdrun ラッパーコマンドを使用した NetBackup コマンドの実行に関するトピックを参照してください。

メモ: nbcmdrun コマンドでは、環境変数またはユーザー入力を MSDP コマンドに渡すことはサポートされていません。

または、次のように、nbcmdrun を指定せずに msdpcmdrun を直接実行できます。

```
/usr/openv/pdde/pdcr/bin/msdpcmdrun <msdp_commands>
```

p.747 の「msdpcmdrun の問題のトラブルシューティング」を参照してください。

msdpcmdrun を使用して MSDP コマンドを実行するための root 以外のユーザーの構成

MSDP ストレージサーバーが構成されているサーバーでは、root 以外のユーザーは、msdpcmdrun というラッパーを介して MSDP コマンドを実行することもできます。

msdpcmdrun を介して実行されるすべてのコマンドが監査されます。監査レポートは、NetBackup Web UI の［セキュリティ (Security)］、［セキュリティイベント (Security events)］、［監査イベント (Audit events)］に表示されます。

前提条件:

- 重複排除管理者グループ pdadmin のユーザーのみが、msdpcmdrun を介して MSDP コマンドを実行できます。
- 管理者ユーザーは、重複排除管理者グループ pdadmin が存在しない場合は作成し、必要なユーザーをユーザーグループに追加する必要があります。
- pdadmin グループを作成する前に MSDP ストレージサーバーがすでに構成されていた場合、管理者ユーザーは PDPAS (PureDisk 権限アクセスサービス) サービスを手動で開始する必要があります。

root 以外のユーザーに対して msdpcmdrun を構成して有効にするには

1 pdadmin グループがまだ存在しない場合は作成します。

```
groupadd pdadmin
```

2 pdadmin グループにユーザーを追加します。新しいユーザーを作成するか、既存のユーザーを pdadmin グループに追加します。

```
useradd test -G pdadmin
```

3 PDPAS サービスが実行されていることを確認します。

- PDPAS サービスがアクティブかどうかを確認します。
  ```
  /usr/openv/pdde/pdconfigure/pdde ps | grep pdpas
  ```
- 実行中でない場合は、サービスを起動します。
  ```
  /usr/openv/pdde/pdconfigure/pdde pdpas start
  ```

4 `msdpcmdrun` を root 以外のユーザーとして実行します。

例: `/usr/openv/pdde/pdcr/bin/msdpcmdrun crstats`

p.747 の「msdpcmdrun の問題のトラブルシューティング」を参照してください。

PDPAS ログについて

PDPAS ログは `/<MSDP storage>/logs/pdpas.log` ファイルにあります。デフォルトでは、ログレベルは 1 に設定されています。このレベルでは、情報メッセージ、警告メッセージおよびエラーメッセージがログに書き込まれます。

目的のログレベルを設定するには、`/etc/pdregistry.cfg` ファイルの PDPAS セクションで `loglevel` パラメータを変更します。値の範囲は 1 から 4 です。

例:

```
[PDPAS]
loglevel=1
logpath=/<storage-server-dir>/log
```

表 4-39 PDPAS ログレベル

ログレベル	説明
1	情報メッセージ、警告メッセージおよびエラーメッセージをログに記録します。
2	警告メッセージおよびエラーメッセージをログに記録します。
3	エラーメッセージのみをログに記録します。
4	情報メッセージ、警告メッセージ、エラーメッセージ、デバッグ/トレースメッセージをログに記録します。これはログ記録の最高レベルです。

msdpcmdrun コマンドの例

サポートされている MSDP コマンドを一覧表示するには、次のコマンドを実行します。

```
/usr/openv/pdde/pdcr/bin/msdpcmdrun -l
```

表 4-40 msdpcmdrun コマンドの例

タスク	コマンド
MSDP LSU データ統計を取得します。	`/usr/openv/pdde/pdcr/bin/msdpcmdrun crstats`
すべてのユーザーを一覧表示します。	`/usr/openv/pdde/pdcr/bin/msdpcmdrun spauser -l`

変更不可クラウドボリュームと構成を一覧表示します。環境変数を設定する必要があります。	`export MSDPC_ACCESS_KEY=AccessKeyID`
	`export MSDPC_SECRET_KEY=SecretAccessKey`
	`export MSDPC_REGION=us-east-1`
	`export MSDPC_PROVIDER=amazon`
	`/usr/openv/pdde/pdcr/bin/msdpcmdrun msdpcldutil list`

ファイルアクセスに関する考慮事項

MSDP コマンドをサービスユーザーとして実行するときに、コマンドでファイルパスが必要な場合は、サービスユーザーがそのファイルにアクセスできることを確認します。

例: `msdpcldutil list --credfile /tmp/env.txt`

この場合、`/tmp/env.txt` ファイルを MSDP サービスユーザーが読み取れるようにする必要があります。このファイルは、`MSDP_SERVICE_USER` 構成の `/etc/pdregistry.cfg` ファイルにあります。

NetBackup Appliance での MSDP コマンドの実行

NetBackup Appliance で、NetBackup CLI ユーザーを使用してアプライアンスシェルメニューにログインします。そこから、シェルで `msdpcmdrun` コマンドを直接実行できます。

```
nbcliuser-!> msdpcmdrun catdbutil --count
```

NetBackup CLI の使用方法について詳しくは、『NetBackup Appliance セキュリティガイド』の NetBackup CLI ユーザーロールに関するトピックを参照してください。

5

MVG (MSDP ボリュームグループ)

この章では以下の項目について説明しています。

MSDP ボリュームグループについて

通常大規模な NetBackup システムには、複数の MSDP サーバーがあります。管理を簡素化するために、それらを 1 つのプールとして一緒に処理することもできます。

MVG (MSDP ボリュームグループ) は、個々の MSDP ストレージサーバーの上にストレージ層のボリュームグループを構築する MSDP 機能です。1 つのボリュームグループが NetBackup に仮想ボリュームとして示され、この仮想ボリュームが MVG ボリュームと呼ばれます。これは、ディスクプールまたはストレージユニット構成の通常のボリュームと同様に、NetBackup で使用できます。MVG 機能を備え、MVG ボリュームを管理する

MSDP サーバーは、MVG サーバーと呼ばれます。これは軽量な MSDP サーバーです。

MSDP ボリュームグループの利点の一部を次に示します。

- MSDP ボリュームの管理を容易にするために、1 つの大規模なストレージプールとしてグループ化します。
- ノードエラー時のシステム回復性が向上します。
- 作業負荷の割り当てと分散を管理します。
  - 初期設定時の多数のクライアントを持つシステムに対する割り当て
  - 通常の操作中に新しく追加されたクライアントに対する割り当て
  - 容量拡張のためのストレージサーバーの追加による再調整
  - ストレージエラーへの耐障害性のための再割り当て
- ストレージユニットグループの次の制限事項に対処します。
  - AIR (自動イメージレプリケーション)
  - 最適化複製ターゲットのサポート
- 既存のほぼすべての MSDP 機能をサポートします。
  p.249 の「MSDP ボリュームグループの制限事項」を参照してください。
- 新しい MSDP サーバーまたは既存の MSDP サーバーと連携して動作します。
- NetBackup Appliance、Flex、BYO の単一エクスペリエンスにより、総所有コストを削減します。

p.232 の「MSDP ボリュームグループの構成」を参照してください。
p.245 の「MSDP ボリュームグループのディザスタリカバリ」を参照してください。
p.248 の「MSDP サーバーのメンテナンス」を参照してください。
p.249 の「MSDP ボリュームグループの制限事項」を参照してください。
p.250 の「ノードのエラー管理について」を参照してください。
p.251 の「MSDP ボリュームグループのベストプラクティス」を参照してください。

MSDP ボリュームグループコンポーネント

MSDP ボリュームグループには、次の 2 つのコンポーネントがあります。

- MVG サーバー
  MVG サーバーは、MVG 機能を備えた軽量の MSDP サーバーです。1 つの NetBackup ドメインに複数の MVG サーバーを構成できます。

NetBackup 10.5 では、Linux Red Hat プラットフォーム上の任意の NetBackup メディアサーバーで実行できます。Flex マルチノードアプライアンス上で、または NetBackup プライマリサーバーと一緒に実行することをお勧めします。
p.231 の「MVG 耐性について」を参照してください。

- MVG ボリューム
  MVG ボリュームは仮想ボリュームです。これは、個々の MSDP サーバーからの通常のボリュームのグループの抽象化です。1 台の MVG サーバーで複数の MVG ボリュームを管理できます。
  これは、NetBackup が、ディスクプールまたはストレージユニット構成の通常のボリュームと同様に使うことができます。

MVG 耐性について

MVG 耐性は、システムの安定性を維持し、バックアップ処理の中断を防ぐために不可欠です。MVG 耐性で考慮すべき主な事項を次に示します。

- MVG サーバーの耐性
  MVG サーバーの耐性は、システム全体の信頼性にとって重要です。最適な耐性を確保するための主な配備戦略は次のとおりです。
  - BYO システムの場合は、NetBackup プライマリサーバーとともに MVG サーバーを配備します。NetBackup プライマリサーバーがクラスタ化されているかどうかに関係なく、MVG サーバーと NetBackup プライマリサーバー両方の耐性は同じです。
  - Flex の場合は、NetBackup プライマリサーバーインスタンスと同じ Flex ホストに MVG サーバーを配備します。この場合も、Flex マルチノードアプライアンスであるかどうかに関係なく、両方のサーバーの耐性レベルは同じになります。
- MVG ノードの耐性
  ノードレベルの耐性は、Flex マルチノードアプライアンスなど、ノードレベルで耐障害性を提供するシステムによって管理されます。
- MVG データの耐性
  また、RAID6 ディスクアレイなどの技術により、データ損失に対する冗長性と保護が提供され、格納されたデータの整合性を確保することでも、データの耐性が提供されます。
- バックアップジョブの耐性
  ノードレベルの耐性がないノード障害が発生した場合、MVG サーバーは特定の条件下で別のノードにバックアップジョブをリダイレクトできるため、バックアップ操作への影響を最小限に抑えることができます。

これらの戦略により、MVG サーバーは耐性を確保し、中断を最小限に抑え、バックアップタスクの高可用性を維持できます。

MSDP ボリュームグループの構成

MSDP ボリュームグループを構成して使用するために、次のタスクを実行できます。

表 5-1 MSDP ボリュームグループの構成

タスク	説明
MSDP ボリュームグループの要件が満たされていることを確認します。	p.233 の「MSDP ボリュームグループの要件」を参照してください。
MVG サーバーを構成します。	p.234 の「Web UI を使用した MVG サーバーの構成」を参照してください。
MVG ボリュームを構成します。	p.235 の「Web UI を使用した MVG ボリュームの作成」を参照してください。
コマンドラインを使用した MVG サーバーの構成	p.236 の「コマンドラインを使用した MVG サーバーの構成」を参照してください。
コマンドラインを使用した MVG ボリュームの作成	p.238 の「コマンドラインを使用した MVG ボリュームの作成」を参照してください。
コマンドラインを使用した MVG ボリュームの更新	p.239 の「コマンドラインを使用した MVG ボリュームの更新」を参照してください。
MVG ボリュームを持つターゲット型 AIR を構成します。	p.239 の「MVG ボリュームを持つターゲット型 AIR の構成 」を参照してください。
MVG ボリュームを更新します。	p.240 の「Web UI を使用した MVG ボリュームの更新」を参照してください。
MVG ボリュームを一覧表示します。	p.240 の「MVG ボリュームの一覧表示」を参照してください。
MVG ボリュームを削除します。	p.240 の「MVG ボリュームの削除」を参照してください。
クレデンシャルが異なる場合の MVG サーバーが使用する MSDP サーバーの構成	p.241 の「クレデンシャルが異なる場合の MVG サーバーが使用する MSDP サーバーの構成」を参照してください。
MSDP ボリュームグループを使用するために、バックアップポリシーを移行します。	p.243 の「通常の MSDP ディスクボリュームから MVG ボリュームへのバックアップポリシーの移行」を参照してください。
MVG から通常の MSDP ディスクボリュームにバックアップポリシーを移行します。	p.243 の「MVG ボリュームから通常の MSDP ディスクボリュームへのバックアップポリシーの移行」を参照してください。

タスク	説明
別の MSDP サーバーにクライアントポリシーの組み合わせを割り当てます。	p.244 の「別の MSDP サーバーへのクライアントポリシーの組み合わせの割り当て」を参照してください。
MVG サーバーの構成を削除します。	p.244 の「MVG サーバーの構成の削除」を参照してください。

MSDP ボリュームグループの要件

MVG サーバーの要件は次のとおりです。

- MVG サーバーは、Red Hat Enterprise Linux プラットフォーム上の任意の NetBackup メディアサーバーで実行できます。
  - これは、Flex メディアサーバーコンテナ、BYO メディアサーバー、プライマリサーバーのいずれかにできます。
  - MVG サーバーは Flex マルチノードアプライアンス上、または NetBackup プライマリサーバーと一緒に実行することをお勧めします。
    p.231 の「MVG 耐性について」を参照してください。
  - これは、Flex WORM、Access Appliance、NetBackup Flex Scale、または Cloud Scale のような MSDP コンテナではありません。
  - MVG サーバーと MSDP サーバーは、軽量の MSDP サーバーである MVG サーバーと同じメディアサーバー上に共存させることはできません。
- MVG サーバーは新しいため、通常の MSDP サーバーからアップグレードまたは移行できません。
- デフォルトでは、1 台の MVG サーバーに最大 64 個の MVG ボリュームを設定でき、各 MVG ボリュームに最大 8 個のディスクボリュームを含めることができます。
- ディスクボリューム PureDiskVolume またはクラウドボリュームは、MVG サーバー上には構成できません。
- MVG サーバーは大規模な環境で数百 GB のディスクストレージを必要とします。
- 1 つの NetBackup ドメインに複数の MVG サーバーを構成できます。

MVG ボリュームのディスクボリュームの要件は次のとおりです。

- ディスクボリュームの MSDP サーバーは、NetBackup 10.5 以降で実行する必要があります。
- MVG サーバーは、デフォルトのクレデンシャルを使用してディスクボリュームの MSDP サーバーにアクセスできます。

- ディスクボリュームは、すべて PureDiskVolumes またはすべてクラウドボリュームである必要があります。
- 複数のディスクボリュームは、異なる MSDP サーバーからのものである必要があります。
- ディスクボリュームの KMS、暗号化、WORM の設定は同じである必要があります。
- クラウドボリュームの場合は、比較ストレージクラスまたは階層で構成されている必要があります。
- WORM ディスクボリュームには、保持ロック用に重複した範囲が必要です。MVG WORM ボリューム内では、WORM ボリュームの最短の最大ロック期間は、WORM ボリュームの最長の最小ロック期間より長くする必要があります。
- 1 つのディスクボリュームを複数の MVG ボリュームに割り当てることはできません。

Web UI を使用した MVG サーバーの構成

MVG サーバーは、NetBackup Web UI を使用して MSDP ボリュームグループを使用するように構成できます。

MVG サーバーを構成するには

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。[ストレージサーバー (Storage servers)]タブをクリックし、[追加 (Add)]をクリックします。
2. [ストレージ形式 (Storage type)]リストで、[ディスクストレージサーバー (Disk storage servers)]を選択します。
3. [カテゴリ (Category)]オプションから、[メディアサーバー重複排除プール (MSDP, MSDP Cloud, MVG) (Media Server Deduplication Pool (MSDP, MSDP Cloud, MVG))]を選択します。

   [開始 (Start)]をクリックします。
4. [基本プロパティ (Basic properties)]で必要なすべての情報を入力します。

   メディアサーバーを選択するには、検索アイコンをクリックします。使用するメディアサーバーが表示されない場合は、[検索 (Search)]フィールドを使用して検索できます。

   [次へ (Next)]をクリックします。

5 [ストレージサーバー (Storage server)]オプションで、必要なすべての情報を入力し、[MSDP ボリュームグループ (MVG) サービスの有効化 (Enable MSDP volume group (MVG) service)]を選択します。

このオプションは、MSDP サーバーを MSDP ボリュームグループ (MVG) サーバーとして構成します。これにより、他の MSDP サーバーのボリュームをグループ化して MVG ボリュームを作成できます。有効にすると、MVG サーバーは MVG ボリュームのみをホストでき、独自のローカルボリュームまたはクラウドボリュームをホストできません。

KMS (キーマネージメントサービス) を使用する場合、[KMS]オプションを選択するには、まず KMS を構成する必要があります。

[次へ (Next)]をクリックします。

6 (オプション) [メディアサーバー (Media servers)]で、[追加 (Add)]をクリックして、使用する追加のメディアサーバーを追加します。

[次へ (Next)]をクリックします。

7 [確認 (Review)]ページで、すべてのオプションが正しいことを確認し、[保存 (Save)]をクリックします。

Web UI を使用した MVG ボリュームの作成

MVG ボリュームは、NetBackup Web UI を使用して構成できます。

MVG ボリュームを構成するには

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 [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。[ディスクプール (Disk pools)]タブをクリックし、[追加 (Add)]をクリックします。

3 [ディスクプールオプション (Disk pool options)]で、[変更 (Change)]をクリックして MVG が有効なストレージサーバーを選択します。

4 必要な情報をすべて入力します。[次へ (Next)]をクリックします。

5 [ボリューム (Volume)]で、[ボリューム (Volume)]ドロップダウンから[MVG ボリュームの追加 (Add MVG volume)]を選択します。

6 MVG ボリューム名を入力し、目的のボリュームをフィルタする属性を選択します。

7 MVG ボリュームの複数のボリュームを選択します。[次へ (Next)]をクリックします。

8 [確認 (Review)]ページで、すべての設定と情報が正しいことを確認します。[完了 (Finish)]をクリックします。

9 MVG ボリュームが追加されると、[ディスクプール (Disk pools)]タブの下に[MVG]列が表示されます。

以前と同じ方法で MVG ボリュームのディスクプールを使用して、ストレージユニットとレプリケーションターゲットを構成します。

コマンドラインを使用した MVG サーバーの構成

コマンドラインを使用して、Red Hat Linux メディアサーバーで MVG サーバーを構成できます。

p.252 の「MVG メンテナンス用の MSDP コマンド」を参照してください。

コマンドラインを使用して MSDP ボリュームグループサーバーを構成するには

1 NetBackup にストレージサーバーレコードを作成します。

```
nbdevconfig -creatests -storage_server <media-server-fqdn> -stype
PureDisk -media_server <media-server-fqdn> -st 9
```

2 NetBackup に MSDP クレデンシャルを追加します。

```
/usr/openv/volmgr/bin/tpconfig -add -storage_server
<media-server-fqdn> -stype PureDisk -sts_user_id <msdp-username>
-password <msdp-password>
```

3 MSDP 構成ファイルテンプレートを取得します。返されるテンプレートには、構成項目 `mvgenabled 0` があるはずです。

```
nbdevconfig -getconfig -storage_server <media-server-fqdn> -stype
PureDisk -configlist ./cfg.msdp.template
```

4 MSDP 構成ファイルを次の形式で作成します。

構成ファイルテンプレート `./cfg.msdp.template` を使用して、構成ファイル `./cfg.msdp` を作成します。

`mvgenabled: 0` を `mvgenabled: 1` に変更します。

構成ファイルの MSDP クレデンシャルは、前の手順で NetBackup に追加したクレデンシャルである必要があります。

例:

```
# cat ./cfg.msdp
V7.5 "storagepath" "/sample-msdp-path" string
V7.5 "spalogin" "sample-username" string
V7.5 "spapasswd" "sample-password" string
V7.5 "spalogretention" "7" int
V7.5 "verboselevel" "3" int
V7.5 "dbpath" "/sample-msdp-path" string
V7.5 "required_interface" "" string
V7.5 "encryption" "1" string
V7.5 "mvgenabled" "1" string
```

`storagepath` と `dbpath` で、MSDP ストレージとカタログに同じパスを指定することをお勧めします。

5 MSDP サーバーを初期化します。

```
nbdevconfig -setconfig -storage_server <media-server-fqdn> -stype
PureDisk -configlist ./cfg.msdp
```

成功すると、他の MSDP サービスとともに `mvg-controller` と `mvg-mds` が初期化され、開始されます。

コマンドラインを使用した MVG ボリュームの作成

コマンドラインを使用して MVG ボリュームを構成するには

1 MVG ボリュームの構成ファイルを次の形式で作成します。

```
V7.5 "operation" "add-virtual-volume" string
V7.5 "virtualVolume" "<mvg-volume>" string
V7.5 "diskVolume" "<msdp-server1>:<msdp-volume1>:Y" string
V7.5 "diskVolume" "<msdp-server2>:<msdp-volume2>:Y" string
V7.5 "diskVolume" "<msdp-server...>:<msdp-volume...>:Y" string
```

例:

```
# cat sample-mvg-local.cfg
V7.5 "operation" "add-virtual-volume" string
V7.5 "virtualVolume" "sample-mvg-local" string
V7.5 "diskVolume" "sample-msdp-server1:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server2:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server3:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server4:PureDiskVolume:Y" string

# cat sample-mvg-cloud.cfg
V7.5 "operation" "add-virtual-volume" string
V7.5 "virtualVolume" "sample-mvg-cloud" string
V7.5 "diskVolume" "sample-msdp-server1:cloud-volume1:Y" string
V7.5 "diskVolume" "sample-msdp-server2:cloud-volume2:Y" string
V7.5 "diskVolume" "sample-msdp-server3:cloud-volume3:Y" string
V7.5 "diskVolume" "sample-msdp-server4:cloud-volume4:Y" string
```

2 MVG サーバーの MVG ボリュームを作成します。

```
nbdevconfig -setconfig -storage_server <mvg-server> -stype
PureDisk -configlist <configuration-file>
```

3 NetBackup に MVG ボリュームを含むディスクプールを作成します。

```
nbdevconfig -previewdv -storage_server <mvg-server> -stype
PureDisk | grep <mvg-volume> > <mvg-volume-cfg-file>
```

```
nbdevconfig -createdp -dp <disk-pool-name> -storage_server
<mvg-server> -stype PureDisk -dvlist <mvg-volume-cfg-file>
```

コマンドラインを使用した MVG ボリュームの更新

コマンドラインを使用して既存の MVG ボリュームを更新するには

1 MVG ボリュームを更新するための構成ファイルを次の形式で作成します。

```
V7.5 "operation" "update-virtual-volume" string
V7.5 "virtualVolume" "<mvg-volume>" string
V7.5 "diskVolume" "<msdp-server1>:<msdp-volume1>:Y" string
V7.5 "diskVolume" "<msdp-server2>:<msdp-volume2>:Y" string
V7.5 "diskVolume" "<msdp-server...>:<msdp-volume...>:Y" string
V7.5 "diskVolume" "<new-msdp-server1>:<new-msdp-volume1>:Y" string
V7.5 "diskVolume" "<new-msdp-server...>:<new-msdp-volume...>:Y"
string
```

例:

```
# cat sample-mvg-local.cfg
V7.5 "operation" "update-virtual-volume" string
V7.5 "virtualVolume" "sample-mvg-local" string
V7.5 "diskVolume" "sample-msdp-server1:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server2:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server3:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server4:PureDiskVolume:Y" string
V7.5 "diskVolume" "sample-msdp-server-new1:PureDiskVolume:Y"
string
V7.5 "diskVolume" "sample-msdp-server-new2:PureDiskVolume:Y"
string
```

2 仮想ボリュームに構成変更を適用します。

```
nbdevconfig -setconfig -storage_server <mvg-server> -stype
PureDisk -configlist <configuration-file>
```

MVG ボリュームを持つターゲット型 AIR の構成

MSDP ボリュームグループは、ターゲット型 AIR のみをサポートします。レガシーのターゲット型でない AIR はサポートされません。

MVG ボリュームが使用する MSDP サーバーで安全な通信を設定する必要があります。これらの MSDP サーバーは、データレプリケーションのターゲット MVG ボリュームまたは MSDP サーバーに接続します。

NetBackup Web UI でレプリケーションターゲットを構成する前に、それらの MSDP サーバーと MVG サーバーで次のコマンドを実行します。

```
nbcertcmd -getCACertificate -server <target-primary-server>
```

```
nbcertcmd -getCertificate -server <target-primary-server> -token
<auth-token>
```

MSDP ボリュームグループを使用したレプリケーションターゲットの構成は、通常の MSDP と同じです。

p.134 の「NetBackup 自動イメージレプリケーションについて」を参照してください。

Web UI を使用した MVG ボリュームの更新

MVG ボリュームは、追加のみの更新をサポートします。ディスクボリュームの挿入、削除、ディスクボリュームリストの順序の変更はサポートされていません。

MVG ボリューム内のディスクボリュームのモードを更新できます。

ディスクボリュームリストを変更する必要がある場合は、MVG ボリュームを削除して再作成できます。

メモ: ディスクボリュームに障害が発生し、リカバリできない場合は、MVG ボリューム内でそのディスクボリュームを読み取り専用モードに変更できます。または、ディスクボリュームのリストから MVG ボリュームを削除し、再作成できます。

MVG ボリュームの一覧表示

MVG ボリュームを一覧表示するには

- MVG サーバーで次のコマンドを実行し、MVG ボリュームの構成情報をダンプします。

  ```
  cacontrol --mvg listvvols [<dsid-of-mvg-volume>]
  ```

MVG ボリュームの削除

MVG ボリュームは、NetBackup Web UI 上の対応するディスクプールが削除されたときに、MVG サーバーから削除されません。

MVG ボリュームを削除するには

1. (オプション) MSDP ボリュームグループ構成のバックアップを作成します。MVG サーバーで次のコマンドを実行し、MVG ボリュームの構成情報をファイルにダンプします。

   ```
   cacontrol --mvg listvvols [<dsid-of-mvg-volume>]
   ```

2. MVG ボリューム削除の構成ファイルを次の形式で作成します。

   ```
   V7.5 "operation" "delete-virtual-volume" string
   V7.5 "virtualVolume" "<mvg-vol>" string
   ```

3. MVG サーバーの MVG ボリュームを削除します。

   ```
   nbdevconfig -setconfig -storage_server <mvg-server> -stype
   PureDisk -configlist <configuration-file>
   ```

   このコマンドは、ディスクボリュームの MSDP サーバーから MVG ボリュームの関連付け情報を削除し、MVG サーバーから MVG ボリューム情報を削除します。このコマンドを実行するときは、MSDP サーバーにアクセスできることを確認します。

   何らかの理由で MSDP サーバーが停止している場合、コマンドは失敗しません。MSDP サーバーが停止している場合、MVG ボリューム関連情報はその MSDP サーバーから削除されないため、このコマンドを使用しないでください。

   MSDP サーバーが戻ったときに、次のコマンドを実行して、そのサーバーから手動で情報を削除します。

   ```
   cacontrol --dataselection removefromvvol <dsid-of-disk-volume>
   <disk-volume> <msdp-server> <mvg-server> <mvg-volume>
   ```

   ```
   cacontrol --dataselection refresh-disk-volume <msdp-server>
   <disk-volume >
   ```

クレデンシャルが異なる場合の MVG サーバーが使用する MSDP サーバーの構成

MSDP サーバーのディスクボリュームを MVG ボリュームに追加するには、その MVG サーバーは、デフォルトのクレデンシャルを使用して MSDP サーバーと通信できる必要があります。

MSDP サーバーが新しい場合は、MSDP サーバーで追加の構成の変更が必要ないように、MVG サーバーと同じクレデンシャルで MSDP サーバーを構成します。

多くの場合、特に MSDP サーバーがすでに存在する場合は、クレデンシャルは異なる可能性があります。MSDP サーバーで既存のクレデンシャルを変更するか、新しいクレデンシャルを追加する必要があります。

パスワードが異なる場合に MVG サーバーが使用する MSDP サーバーを構成するには

- MSDP の既存の指示に従って、パスワードを変更します。

  MSDP ディスクプールで NetBackup 認証パスワードをリセットする方法。

ユーザー名が異なる場合に MVG サーバーが使用する MSDP サーバーを構成するには

1. MSDP のデフォルトユーザーのエイリアスを追加します。エイリアスユーザーのユーザー名とパスワードは、MVG サーバーのクレデンシャルと同じです。

   Windows の場合: `<install_path>¥pdde¥spauser --a -u username [-p password] --owner admin -alias`

   UNIX の場合: `/usr/openv/pdde/pdcr/bin/spauser -a -u username [-p password] --owner admin -alias`

   メモ: エイリアスユーザーの追加は、NetBackup 10.5 以降でサポートされています。以前のバージョンの MSDP サーバーでは、このコマンドを実行しないでください。

2. エイリアスユーザーを追加した後、エイリアスユーザーのデータ選択 ID が管理者ユーザーと同じであることを確認します。次のコマンドを実行します。

   ```
   spauser -l
   ```

   例:

   ```
   root@host ~ # spauser -l
   user 1 : msdp, data selection: 2, role: admin
   root@host ~ # spauser -a -u mvg-user --owner msdp --alias

   Password:
   Reenter Password:
   Please input password of super user [msdp]:

   Add user mvg-user successful !

   One MSDP user can only be used by one NBU domain! Do not use one
    same user in two or more NBU domains!
   root@host ~ # spauser -l
   user 1 : msdp, data selection: 2, role: admin
   user 2 : mvg-user, data selection: 2, role: admin
   ```

p.667 の「重複排除シェルからの MSDP 管理エイリアスユーザーの追加」を参照してください。

通常の MSDP ディスクボリュームから MVG ボリュームへのバックアップポリシーの移行

移行の前に、そのポリシーが使用するMVGボリュームに、そのポリシーが使用するMSDPディスクボリュームを割り当てることをお勧めします。この手順は、アクセラレータバックアップポリシーで特に重要です。MVG サーバーは、以前のディスクボリュームと以前のアクセラレータのトラックログを新しいバックアップジョブのために引き続き使用します。重複排除率とバックアップパフォーマンスが、最小限の影響を受けます。

バックアップポリシーが複数のMSDPディスクボリュームを使用しており、それらのMSDPサーバーにバックアップイメージがまだ存在する場合は、少なくとも最近使用されたディスクボリュームを MVG ボリュームに割り当てます。すべての MSDP ディスクボリュームを MVG ボリュームに割り当てることもできます。

次の MSDP コマンドを実行して、最近使用されたボリュームをプライマリボリュームとして指定します。

```
cacontrol --cluster set-cp-assignment <dsid-of-mvg-volume> <client>
<policy> <msdp-server>
```

バックアップポリシーを通常作業時間外に徐々に移行して、潜在的な影響を軽減します。

MVG ボリュームから通常の MSDP ディスクボリュームへのバックアップポリシーの移行

ポリシーの MVG ボリュームが最近使用した MSDP ディスクボリュームに変更することをお勧めします。この情報は、NetBackup Web UI の通知 Web ページで見つけることができます。MSDP コマンドラインを使用して情報を検索するには、次のコマンドを実行します。

```
cacontrol --cluster get-cp-assignment <dsid-of-mvg-volume> <client>
<policy>
```

また、この情報は、最近のバックアップジョブのジョブ詳細でも見つけることができます。

バックアップポリシーを通常作業時間外に徐々に移行して、潜在的な影響を軽減します。

別の MSDP サーバーへのクライアントポリシーの組み合わせの割り当て

別の MSDP サーバーにクライアントポリシーの組み合わせを割り当てるには

1. 次の MSDP コマンドを実行して、クライアントポリシーの組み合わせの現在の割り当て先の MSDP サーバーを確認します。

   ```
   cacontrol --cluster get-cp-assignment <dsid-of-mvg-volume>
   <client> <policy>
   ```

2. 次の MSDP コマンドを実行して、割り当てを変更します。

   ```
   cacontrol --cluster set-cp-assignment <dsid-of-mvg-volume>
   <client> <policy> <msdp-server>
   ```

MVG サーバーの構成の削除

MVG サーバーの構成を削除するには、次の手順を実行します。

MVG サーバーの構成を削除するには

1. NetBackup で、MVG サーバーを備えた対応するストレージユニット、ディスクプール、ストレージサーバーのすべての構成を削除します。
2. MVG ボリュームを MVG サーバーから削除します。

   メモ: MVG データを保持する場合、または既存のデータを再利用して MVG サーバーを再構成する場合は、MVG ボリュームを削除しないでください。

3. ホストで NetBackup サービスを停止します。

   ```
   bp.kill_all
   ```

4. ディスク上のストレージサーバーデータを削除します。
   - 次のスクリプトを実行します。
     ```
     /usr/openv/pdde/pdconfigure/scripts/installers/PDDE_deleteConfig.sh
     ```
     y と入力して、Enter キーを押します。
     構成ファイルは元の状態にリストアされます。
   - MSDP ストレージパスとデータベースパスのデータを削除します。

メモ: MVG データを保持する場合、または既存のデータを再利用して MVG サーバーを再構成する場合は、この手順を実行しないでください。

5 ホスト側で NetBackup サービスを再起動します。

```
bp.start_all
```

MSDP ボリュームグループのディザスタリカバリ

MVG サーバーの MSDP カタログは、通常の MSDP サーバーとして保護できます。MSDP カタログバックアップポリシーを使用できます。

シナリオ 1: MSDP カタログをリカバリできる

MSDP カタログをリカバリできる場合は、同じ手順に従って、リカバリされたカタログを使用して MSDP サーバーを再構成できます。

MVG サーバーの MSDP カタログは、通常の MSDP サーバーとして保護することをお勧めします。1 つの方法は、MSDP カタログバックアップポリシーを使用することです。

シナリオ 2: MSDP カタログを MVG サーバーカタログバックアップからリカバリできない

バックアップがない、またはバックアップデータを使用できないため、何らかの理由で MSDP カタログをリカバリできません。MSDP ボリュームグループの構成データを再構築し、MVG サーバーを再構成できます。

表 5-2

いいえ	手順	説明

1	MSDP ボリュームグループの構成を再構築します。	MVG サーバーが持っていた MVG ボリュームと、各 MVG ボリュームが使用していた物理ボリュームを調べます。
		この情報を見つけるには、次のいずれかの方法を使用します。
		■ `GET /storage/storage-servers/{storageServerId}/disk-volumes` API の使用
		物理ボリュームが MVG ボリュームによって使用されている場合、その物理ボリュームには、返されたデータに `usedByVLsu=<mvg-server>:<mvg-volume>` 属性が含まれます。それが MVG ボリュームの場合、`diskVolumeCapabilities` リストには、返されたデータの属性に `PUREDISK_VIRTUAL` キーワードが含まれます。
		■ 次の NetBackup コマンドを実行します。
		`nbdevquery -liststs -stype PureDisk`
		`bpstsinfo -li`
		■ 各 MSDP サーバーで、次の MSDP コマンドを実行します。
		`/usr/openv/pdde/pdcr/bin/cacontrol --dataselection list`

2	MVG サーバーを再構成します。	MSDP サーバーと同様に MVG オプションが選択された MSDP サーバーを構成できます。以前のホスト名を使用することをお勧めしますが、必須ではありません。 NetBackup で MVG サーバーのストレージサーバーの構成が失われた場合は、NetBackup Web UI を使用して構成します。 NetBackup にまだ MVG サーバーのストレージサーバーの構成がある場合は、`nbdevconfig -setconfig` コマンドを使用します。 次を追加して MVG を有効にする必要がある場合を除き、構成リストファイルと通常の MSDP サーバーの構成リストファイルに違いはありません。 `V7.5 "mvgenabled" "1" string` 詳しくは、p.236 の「コマンドラインを使用した MVG サーバーの構成」を参照してください。

いいえ	手順	説明
3	MVG ボリュームを 1 つずつ追加し戻します。	NetBackup にまだ MVG ボリュームで構成されたディスクプールがある場合は、`add-virtual-volume` オプションを指定して NetBackup コマンド `nbdevconfig -setconfig` を実行し、手順 1 で収集した情報を使用して MVG ボリュームを 1 つずつ追加します。 p.238 の「コマンドラインを使用した MVG ボリュームの作成」を参照してください。 MVG ボリュームでのディスクプール構成が失われた場合は、NetBackup Web UI を使用して、手順 1 で収集した情報で対応するディスクプールと MVG ボリュームを再作成します。 この場合、NetBackup カタログでも、MVG ボリュームに関連付けられたバックアップイメージレコードが高い可能性で失われます。したがって、NetBackup イメージの 2 フェーズインポートも、物理ボリュームに対する通常の MSDP サーバーのリカバリの場合と同様に、MVG サーバーと MVG ボリュームの再構成後に必要です。

4	(オプション) クライアントとポリシーの割り当てテーブルを調整します。	クライアントとポリシーの割り当てテーブルは、手順 3 で再構築されます。障害の発生前に、クライアントとポリシーの組み合わせが複数の MSDP サーバーによって取得されていた場合、情報は再構築できますが、プライマリサーバーは障害前のサーバーと異なる場合があります。
		
		必要に応じて、次の MSDP コマンドを実行して、クライアントとポリシーの組み合わせのプライマリ MSDP サーバーを確認して調整します。
		
		`cacontrol --cluster get-cp-assignment <dsid-of-mvg-volume> [<client> [<policy>]]`
		
		`cacontrol --cluster set-cp-assignment <dsid-of-mvg-volume> <client> <policy> <msdp-server>`
		
		通常、クライアントとポリシーのデータが多い MSDP サーバーがプライマリサーバーとして設定されます。

MSDP サーバーのメンテナンス

アップグレード、EEB インストール、OS のパッチ適用、システム再起動などの定期的なノードメンテナンスでは、重複排除率またはジョブエラーへの影響を軽減するために、手動で介入することをお勧めします。

MVG サーバーの MSDP コマンドラインまたは NetBackup Web UI を使用して、定期的なメンテナンスの前にノードをメンテナンスモードに設定し、メンテナンス後にリセットします。MVG サーバーは、メンテナンス中のノードから別のノードにクライアントポリシーの割り当てを移動しません。ノードが安定していない、またはメンテナンス中に機能していない場合、新しいバックアップジョブは一時的に失敗することがあります。

MVG サーバーで、次の MSDP コマンドを実行します。

```
cacontrol --mvg set-mvg-maintenance <msdp-server>

cacontrol --mvg unset-mvg-maintenance <msdp-server>

cacontrol --mvg get-mvg-maintenance
```

例:

```
PATH=$PATH:/usr/openv/pdde/pdcr/bin
cacontrol --mvg set-maintenance-mode vramvg037340.rsv.ven.veritas.com
Updated virtual volumes: mvg-local
cacontrol --mvg get-maintenance-mode
MSDP servers in maintenance mode: vramvg037340.rsv.ven.veritas.com
Virtual volumes which have the MSDP servers in maintenance mode:
mvg-local
cacontrol --mvg unset-maintenance-mode
vramvg037340.rsv.ven.veritas.com
Updated virtual volumes: mvg-local
cacontrol --mvg get-maintenance-mode
No MSDP servers found in maintenance mode.
```

NetBackup Web UI で、MVG ボリュームの[ディスクプール (Disk Pool)] Web ページに移動し、MVG ボリュームのディスクボリュームを選択して編集し、モードを[メンテナンス (Maintenance)]と[通常 (Normal)]の間で切り替えます。

または、ノードのメンテナンス中、対応するバックアップポリシーを一時的に無効にできます。

また、メンテナンス周期が短い場合は、MVG サーバーで MVG 再調整凍結時間を使うかチューニングして、MVG サーバーが MVG 再調整凍結時間内にノードを安定に戻せる場合に、MVG サーバーがクライアントポリシーの割り当てを移動しないようにすることもできます。デフォルトの値は 0.5 時間です。MVG コントローラ API によって調整できます。

```
curl -K /uss/config/certificates/controller/.curl_config
https://localhost:10100/v1/agent/mvg/loadbalance/config -d
'{"asmt_rb_freezing_timeout": 3600 }' -X PATCH
```

調整パラメータは、次のように確認します。

```
curl -K /uss/config/certificates/controller/.curl_config
https://localhost:10100/v1/agent/mvg/loadbalance/config
```

MSDP ボリュームグループの制限事項

MSDP ボリュームグループは次をサポートしません。

- 次の構成で IRE (分離リカバリ環境) をサポートします。
  - MSDP サーバーのクロックの時間とタイムゾーンは MVG サーバーと一致している必要があり、両方とも Linux プラットフォームで実行する必要があります。
  - 1 台の MSDP サーバーを複数の MVG サーバーで使用しないでください。
- ユニバーサル共有はサポートされません。ユニバーサル共有には、そのまま個々の MSDP サーバーを使用できます。
- 通常の MSDP サーバーでのイメージ共有をサポートします。MVG ボリュームを介して作成されたバックアップイメージの場合は、通常の MSDP サーバーをイメージ共有用として使用できます。
- ノード間の重複排除はありません。
- ノード間のデータ分散が制限されます。
  - 重複排除率への影響を減らすには、制限されたノード数に基づく 1 つのクライアントポリシーの再割り当てを制限します。1 つのクライアントポリシーの割り当ての手動による変更がサポートされます。MSDP コマンドを使用して、制限されたノード数に基づいてこれを変更できます。
  - 単一の大きいバックアップを複数のノードに分散することはできません。
    ローカルボリューム (PureDiskVolumes) の MVG ボリュームの場合、MVG ボリュームには領域がありますが、どの単一のノードにもバックアップデータを格納するのに十分な領域がないために、問題と見なされる場合があります。
    この問題が発生した場合は、代わりに、クラウドボリュームの MVG ボリュームにその大きいバックアップポリシーを移動するか、「MSDPLB+」ポリシーを使用して複数ストリームバックアップを有効にできます。
  - 複数ストリームバックアップポリシーのバックアップジョブは、「MSDPLB+」ポリシーでない限り、同じノードに移動します。MSDPLB+ ポリシーは、MSDP ノード間でデータ重複排除が行われないため、必要でないかぎり使用しないでください。

メモ: 「MSDPLB+」ポリシーは、名前が「MSDPLB+」で始まるバックアップポリシーを意味します。NetBackup 11.0 以降では、ポリシー属性[複数の MSDP ノードを有効にする (Enable Multiple MSDP nodes)]が有効になっているバックアップポリシーであることも意味します。

ノードのエラー管理について

次の表に、ノードエラーのシナリオとその管理方法を示します。

表 5-3

ノードエラー	説明

計画されたノードエラー	定期的なノードメンテナンスでは、重複排除率またはジョブエラーへの影響を軽減することをお勧めします。
	
	MVG サーバーでノードをメンテナンスモードに設定します。ノードがメンテナンスモードの場合、ノードでのクライアントポリシーの割り当ては、自動的には変更されません。
	
	次の MSDP コマンドを実行して、それらを手動で変更します。
	
	`cacontrol --mvg set-mvg-maintenance <msdp-server>`
	`cacontrol --mvg unset-mvg-maintenance <msdp-server>`
	`cacontrol --mvg get-mvg-maintenance`
	
	NetBackup Web UI で、MVG ボリュームの[ディスクプール (Disk Pool)] Web ページに移動し、MVG ボリュームのディスクボリュームを選択して編集し、モードを[メンテナンス (Maintenance)]と[通常 (Normal)]の間で切り替えます。

計画外のノードエラー	MVG サーバーには、タイムアウトを凍結する再調整があります。クライアントポリシーは、現在のノードが次回バックアップの開始時に再調整の凍結時間よりも長く到達不能なままになるまでは、別のノードに移動されません。 この値は、キーワード `asmt_rb_freezing_timeout` を使用して MVG チューニング API で構成できます。デフォルトでは、これは 0.5 時間です。
障害発生後にノードが再び稼働中になる	ノードが長時間停止したままの場合、クライアントポリシーの割り当ては、バックアップポリシーを使用して NetBackup がバックアップジョブを実行するときに、そのノードから移動されます。 ノードが復帰すると、元のクライアントポリシーの組み合わせのほとんどは、システムのバランスを再び維持するために戻されます。

ノードエラー	説明
ノードに空きがない	ディスクボリュームに空きがない場合、クライアントポリシーは別のノードに移動されます。 新しいノードが非アクティブまたは空きがなく、元のノードに再び利用可能な領域がない場合を除き、元のノードには戻されません。

MSDP ボリュームグループのベストプラクティス

MSDP ボリュームグループのベストプラクティスのいくつかを次に示します。

- MVG サーバーを、物理ボリュームが MVG サーバーによってグループ化される通常の MSDP サーバーに近付けます。
  MVG サーバーと MVG サーバーの負荷分散メディアサーバーは、低遅延かつ良好なスループットで MSDP サーバーに効率的にアクセスできます。
- MVG サーバーの負荷分散メディアサーバーリストに通常の MSDP サーバーのメディアサーバーを追加します。メディアサーバーが存在する場合は、リストにさらにメディアサーバーを追加することを検討します。
- MVG サーバーを信頼性の高い場所に配置します。この場所は、通常の MSDP サーバーと物理的に分離されていることが望まれます。
  たとえば、MVG サーバーが唯一の MVG サーバーである場合は NetBackup プライマリサーバー上に構成し、HA 対応 Flex Appliance または BYO 環境に構成できます。
- 1 つの MVG ボリュームの物理ボリュームにも同様の設定があります。
  これらは類似のボリュームサイズと類似のサーバー CPU やメモリを持ち、ディスクまたはネットワークのパフォーマンスが類似しています。これにより、物理ボリュームと MSDP サーバー間の負荷がより分散されます。
  同じ暗号化、KMS、WORM、その他のセキュリティ構成が適用されます。設定が一致しない場合、MVG ボリュームの作成は失敗します。
- 新しい MVG サーバーは、コストを削減し、パフォーマンスが損なわれないようにする必要があるときにのみ、追加します。
  既存の MVG サーバーが要件を満たすことができない場合にのみ、新しい MVG サーバーを追加します。たとえば、MVG サーバーと MVG ボリューム間の物理的な分離が必要です。既存の MVG サーバーは小さすぎて多くの MVG ボリュームを管理できません。MVG サーバーが持つ MVG ボリュームが多すぎます。
- 複数の MVG サーバーを使用して同じ MSDP サーバーの物理ボリュームを管理しないでください。
  複数の MVG ボリュームに割り当てられた物理ボリュームがない場合、MVG ボリュームが同じ MVG サーバーによって管理されているか、異なる MVG サーバーによって管理されているかは関係ありません。

MSDP サーバーに複数のボリュームがある場合は、異なる MVG サーバーの異なる MVG ボリュームに割り当てることができます。ただし、この方法は推奨されません。

- MVG ボリュームに割り当てられた物理ボリュームは、NetBackup ジョブに使用しないでください。
  物理ボリュームが引き続き使用されている場合、何もブロックされません。既存のバックアップイメージのリストアには引き続き使用できます。物理ボリュームで現在機能している構成は、引き続き機能し続けることができます。負荷をより分散するには、MVG ボリュームに割り当てられているときに、バックアップポリシーの構成から削除します。
- MVG サーバー上のメディアサーバーが小さい場合は、非アクティブ化します。
  MVG サーバーが小さい場合は、MVG サーバーに追加の負荷分散メディアサーバーがあるときに、MVG サーバー上のメディアサーバーを非アクティブ化して、NetBackup がそこでジョブをスケジュールしないようにします。そのサーバーが、MVG サーバーの唯一の負荷分散メディアサーバーである場合は、非アクティブ化しないでください。
  NetBackup Web UI の[ストレージ (Storage)]、[メディアサーバー (Media server)]の順に移動し、MVG サーバーを選択し、[無効化 (Deactivate)]をクリックします。
  次の NetBackup コマンドを実行することもできます。

  ```
  /usr/openv/netbackup/bin/admincmd/nbemmcmd -updatehost -machinename
  <mvg-server> -machinestateop set_admin_pause -machinetype media
  -masterserver <primary-server>
  ```
- メディアサーバーと MSDP エンジンの親和性を作成します。
  p.534 の「MSDP クラスタでのメディアサーバーと MSDP エンジンの親和性の有効化」を参照してください。

MVG メンテナンス用の MSDP コマンド

次の表に、MVG 構成の管理に使用できる MSDP コマンドを示します。

表 5-4 MVG の MSDP コマンド

タスク	コマンド
MSDP サーバーのデータ選択項目を一覧表示します。	MSDP または MVG サーバーで、次のコマンドを実行します。 `cacontrol --dataselection list`
MSDP ディスクボリュームの構成を取得します。	MSDP または MVG サーバーで、次のコマンドを実行します。 `cacontrol --dataselection getlsuconfig`

タスク	コマンド
既存の NetBackup ディスクプールの MSDP ディスクボリュームを更新します。	MSDP サーバーで、次のコマンドを実行します。 `cacontrol --dataselection refresh-disk-volume <msdp_server> <volume-name>`
MSDP ディスクボリュームに MVG ボリュームの関連付けの状態を追加します。	MSDP サーバーで、次のコマンドを実行します。 `cacontrol --dataselection assigntovvol <dsid-of-disk-volume> <disk-volume> <msdp-server> <mvg-server> <mvg-vol>` MVG コントローラは、MVG ボリュームが作成または更新されたときに、各 MSDP サーバーと各物理ボリュームに対してコマンドを呼び出します。このコマンドは、デバッグおよびトラブルシューティングの目的でのみ使用します。
MSDP ディスクボリュームの MVG ボリュームの関連付けの状態を削除します。	MSDP サーバーで、次のコマンドを実行します。 `cacontrol --dataselection removefromvvol <dsid-of-disk-volume> <disk-volume> <msdp-server> <mvg-server> <mvg-vol>` MVG コントローラは、MVG ボリュームが削除されたか、MVG ボリュームの作成または更新がキャンセルされたときに、各 MSDP サーバーと各物理ボリュームに対してコマンドを呼び出します。 このコマンドは、デバッグおよびトラブルシューティングの目的でのみ使用します。
クライアントとポリシーの組み合わせが割り当てられる MSDP サーバーを取得します。	MVG サーバーで、次のコマンドを実行します。 `cacontrol --cluster get-cp-assignment <dsid-of-mvg-volume> [<client> [<policy>]]`
MSDP サーバーにクライアントとポリシーの組み合わせを割り当てます。	MVG サーバーで、次のコマンドを実行します。 `cacontrol --cluster set-cp-assignment <dsid-of-mvg-volume> <client> <policy> <msdp-server>`

タスク	コマンド

MSDP カタログを検索します。	MSDP サーバーで、次のコマンドを実行します。
	`cacontrol --catalog find <dsid-of-disk-volume> <dirname> <basename> [ --listtype ALL|DV_ONLY|VV_ONLY ]`
	`VV_ONLY`: MVG を介して作成されたパスオブジェクトをフィルタ処理します。
	`DV_ONLY`: MVG を介さずに作成されたパスオブジェクトをフィルタ処理します。
	例:
	`/usr/openv/pdde/pdcr/bin/cacontrol --catalog find 2 / "*" --listtype VV_ONLY`

MVG サーバーの MVG ボリュームを一覧表示します。	MVG サーバーで、次のコマンドを実行します。 `cacontrol --mvg listvvols`
MSDP サーバーを保守モードに設定します。	MVG サーバーで、次のコマンドを実行します。 `cacontrol --mvg get-maintenance-mode | set-maintenance-mode <msdp_server> | unset-maintenance-mode <msdp_server>`
MVG サーバーで通常の MSDP サーバーの MSDP カタログをリモートで見つけます。	MVG サーバーで、次のコマンドを実行します。 `cacontrol --mvg catalog-find <dsid-of-mvg-volume> <dirname> <basename> [ --listtype VV_ONLY|DV_ONLY|ALL ] [ --hostname <msdp_server> ]`
MSDP サーバーのクレデンシャルを検証します。	MSDP または MVG サーバーで、次のコマンドを実行します。 `/usr/openv/pdde/pdcr/bin/spauser -v -stdin` プロンプトが表示されたら、`-u <username> -p <password> --role admin` と入力します。

MVG のエラーのトラブルシューティング

次の表に、MVG のエラーメッセージとそのトラブルシューティング方法を示します。

表 5-5 MVG のエラーメッセージ

エラーメッセージ	説明
名前の検証に失敗しました: <detailed info>。(Failed to validate the name: <detailed info>.)	指定したボリューム名が MSDP の要件を満たしていません。 p.24 の「NetBackup 命名規則」を参照してください。
データ選択項目の一覧表示に失敗しました。(Listing the data selections failed.) または 仮想ボリュームの認識の確認に失敗しました。(Checking virtual volume awareness failed.)	このエラーは、MVG サーバーがデフォルトのクレデンシャルを使用して MVG ボリュームの MSDP ディスクボリュームの一部の MSDP サーバーと通信できない場合に発生します。 MSDP サーバーのクレデンシャルを変更する必要があります。 p.241 の「クレデンシャルが異なる場合の MVG サーバーが使用する MSDP サーバーの構成」を参照してください。 このエラーは、MVG サーバーが MSDP サーバーに接続できない場合にも発生する可能性があります。接続が確立され、MSDP サーバーが機能していることを確認します。 このエラーは、MSDP サーバーが古いバージョンの NetBackup を使用して実行されている場合にも発生する可能性があります。MSDP サーバーが NetBackup 10.5 以降で実行されていることを確認します。
<description> の構成で競合が発生しました。(Conflict in the configuration on <description>.) **メモ:** <description> は、「暗号化」、「KMS」、「WORM」、「ウォーム化が必要 (コールドクラウドストレージ用)」などです。	MVG ボリュームのディスクボリュームがクラウドボリュームの場合、WORM、暗号化、KMS、ストレージクラスタイプに互換性のある設定がありません。
ボリューム <msdp-server>:<volume-name> (dsid:<dsid>) が非アクティブです。(Volume <msdp-server>:<volume-name> (dsid:<dsid>) is inactive.)	1 つのディスクボリュームの MSDP サーバーにアクセスできないか、非アクティブなクラウドボリュームです。

エラーメッセージ	説明
メンバー <msdp-server>:<volume-name1> および <msdp-server>:<volume-name2> のサーバー名が同じです。(Members <msdp-server>:<volume-name1> and <msdp-server>:<volume-name2> have the same server name.)	同じ MSDP サーバーの複数のディスクボリュームが、1 つの MVG ボリュームに割り当てられるように選択されています。
仮想ボリュームはすでに存在します。(Virtual volume already exists.)	重複する MVG ボリューム名が指定されています。
仮想ボリュームにクラウド LSU とローカル LSU の両方を含めることは想定されません。(Including both cloud LSU and local LSU in a virtual volume is not expected.)	PureDiskVolumes を使用して MVG ボリュームにクラウドボリュームを追加するか、クラウドボリュームを使用して MVG ボリュームに PureDiskVolume を追加します。
MVG ボリュームのメンバー数 (<#>) が最大許容数 (<#>) を超えています。(Member number (<#>) of the MVG volume exceeds the maximum allowed number (<#>).)	このエラーは、MVG ボリュームに割り当てようとするディスクボリュームの数が多すぎる場合に発生します。 デフォルトでは、MVG ボリュームには最大 8 つのディスクボリュームを含めることができます。数値は構成可能ですが、推奨されません。
許容される最大 MVG ボリューム数 (<#>) に達しました。(Maximum allowed MVG volume number (<#>) is reached.)	このエラーは、MVG サーバーに作成しようとした MVG ボリュームが多すぎる場合に発生します。 デフォルトでは、MVG サーバーには最大で 64 個の MVG ボリュームを含めることができます。数値は構成可能ですが、推奨されません。
仮想ボリューム <volume-name> のメンバー数を <#> から <#> に減らすことは許可されません。(It's not allowed to reduce the member number from <#> to <#> for virtual volume <volume-name>.)	このエラーは、MVG ボリュームからいくつかのディスクボリュームを削除しようとすると発生します。
仮想ボリューム %s のディスクボリューム <msdp-server1>:<volume-name1> を <msdp-server2>:<volume-name2> に変更することはできません。(It's not allowed to change disk volume <msdp-server1>:<volume-name1> to <msdp-server2>:<volume-name2> for virtual volume %s.)	このエラーは、ディスクボリュームを挿入しようとしたり、MVG ボリュームのディスクボリュームリストの順序を変更しようとした場合に発生します。

エラーメッセージ	説明
メンバー <msdp-server>:<volume-name> が仮想ボリュームを認識しません。(Member <msdp-server>:<volume-name> is not aware of virtual volume.)	このエラーは、古い MSDP サーバーのディスクボリュームを MVG ボリュームに割り当てようとすると発生します。
メンバー <msdp-server>:<volume-name> の dsid が見つかりません。(Cannot find dsid for member <msdp-server>:<volume-name>.)	不適切なディスクボリューム名が指定されています。
仮想ボリュームの割り当ての変更に失敗しました: ディスクボリュームのディスクプールが見つかりませんでした。(Changing virtual volume assignment failed: No disk pool was found for the disk volume.)	MVG ボリュームに割り当てられているディスクボリュームに、NetBackup で構成されている対応するディスクプールがありません。
仮想ボリュームの割り当ての変更に失敗しました: ディスクプール名 <dp-name> の検出に失敗しました。(Changing virtual volume assignment failed: failed to find the disk pool name <dp-name>.)	NetBackup Web サービスが正常に動作していません。 エラーが発生したら、MVG ボリューム構成を再試行するか、NetBackup Web サービスが正しく動作していることを確認します。

6

MSDP クラウドのサポート

この章では以下の項目について説明しています。

MSDP クラウドのサポートについて

今回のリリースでは、NetBackup MSDP クラウドのサポートが強化され、柔軟性と拡張性に優れ、高性能で簡単に設定できるソリューションを提供します。これにより、クラウドストレージをより効率的に活用できます。

この機能の概要は次のとおりです。

- 1 つのローカルストレージターゲットと 0 (ゼロ) 以上のクラウドストレージターゲットを含む、複数のストレージターゲットをサポートするように 1 つの MSDP ストレージサーバーを構成できます。ローカルと複数のクラウドターゲットに同時にデータを移動できます。
- クラウドターゲットとして、同一または異なるプロバイダに存在する、パブリックまたはプライベートのクラウドを指定できます。たとえば、AWS、Azure、HCP などに対応しています。
- クラウドターゲットは、MSDP サーバーを構成して有効にした後、必要に応じて追加できます。
- 1 つのクラウドバケットか、1 つまたは異なるクラウドプロバイダに分散している複数のバケットで、複数のクラウドターゲットを共存させることができます。

- ローカルストレージおよび複数のクラウドターゲットのデータとメタデータは、マルチテナントの使用をサポートするために分離されています。
- 最適化された重複排除は 1 つの MSDP サーバーのスコープ内でサポートされるため、データをまずローカルストレージに格納してから、同じメディアサーバーのクラウドターゲットに複製できます。
- クラウドターゲットからのディザスタリカバリが強化され、より簡単になりました。
- 機能が MSDP クラスタソリューションと適切に統合されました。
- クラウド LSU でユニバーサル共有またはインスタントアクセスを使用するには、NetBackup 重複排除エンジン (spoold) はフィンガープリントインデックスファイルを保存するために MSDP ストレージ容量の 0.2% 以上を必要とします。クラウド LSU でユニバーサル共有またはインスタントアクセスを構成する場合は、フィンガープリントインデックスファイルを保存するのに十分な領域がローカルドライブにあることを確認します。

OpenStorage Technology (OST) に基づき、新しいアーキテクチャでは複数の論理ストレージユニット (LSU) を使用してデータを管理および移動します。これらの LSU は個別にカスタマイズして、さまざまな顧客の要件を満たすことができます。たとえば、純粋なローカルターゲット (NetBackup 8.2 以前の MSDP と同じ) として、またはローカルターゲットと 1 つ以上のクラウドターゲットとして使用できます。

NetBackup 8.3 以降では、NetBackup Web UI から MSDP を構成できます。詳しくは、NetBackup Web UI のマニュアルを参照してください。

この章では、コマンドラインインターフェースを使用して MSDP を構成する方法について説明します。

メモ: OCSD ログ情報または MSDP クラウドを有効にするには、メディアサーバーの `/etc/pdregistry.cfg` に含まれるセクション `[Symantec/PureDisk/OpenCloudStorageDaemon]` に `loglevel=3` を追加して、サービスを再起動します。

`/<MSDP Storage>/log/ocsd_storage/` のログを確認します。

構成のオペレーティングシステム要件

クラウド LSU は、Red Hat Linux Enterprise Linux、SUSE Linux Enterprise、または CentOS プラットフォームで実行されているストレージサーバーで構成できます。クライアントおよび負荷分散サーバーには、プラットフォームの制限事項はありません。

制限事項

- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU ではインスタントアクセスはサポートされていません。

- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU ではユニバーサル共有はサポートされていません。
- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU ではアクセラレータはサポートされていません。
- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU は、ターゲット型または従来型のいずれのタイプの AIR でもソースとして使用できません。
- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU は最適化複製のターゲットとして使用できますが、ソースとしては使用できません。
- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU では合成バックアップはサポートされていません。
- AWS Glacier、AWS Deep Archive、Microsoft Azure Archive のクラウド LSU ではバックアップのイメージ検証はサポートされていません。
- Microsoft Azure Archive のクラウド LSU 向けの SAP HANA はサポートされていません。
- 8.3 より前のバージョンの NetBackup を実行する NetBackup クライアントによって Client Direct バックアップが使用されている場合は、マルチスレッドエージェントを無効にする必要があります。
- 8.3 より前のバージョンの NetBackup が含まれる負荷分散メディアサーバーを選択した場合、クラウド LSU は一覧表示されません。8.3 より前のバージョンの NetBackup を含むメディアサーバーでクラウド LSU を選択した場合でも、バックアップは失敗することがあります。
- マルウェアスキャンは、AWS Glacier、AWS Deep Archive、Microsoft Azure Archive ではサポートされません。
- SUSE Linux Enterprise では、インスタントアクセス機能とユニバーサル共有機能はサポートされません。

NetBackup Web UI でのメディアサーバー重複排除プールストレージサーバーの作成

この手順を使用して、NetBackup Web UI でメディアサーバー重複排除プールストレージサーバーを作成します。ストレージサーバーを作成した後で、ディスクプール (ローカルストレージまたはクラウドストレージ) とストレージユニットを作成するオプションがあります。NetBackup にディスクプールとストレージユニットが存在しない場合は、作成することを推奨します。

MSDP ストレージサーバーを追加するには

1. NetBackup Web UI にサインインします。
2. 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。[ストレージサーバー (Storage servers)]タブを選択し、[追加 (Add)]をクリックします。
3. [ストレージ形式 (Storage type)]リストで、[ディスクストレージサーバー (Disk storage servers)]を選択します。
4. [カテゴリ (Category)]オプションから、[メディアサーバー重複排除プール (MSDP, MSDP Cloud, MVG) (Media Server Deduplication Pool (MSDP, MSDP Cloud, MVG))]を選択します。

   [開始 (Start)]をクリックします。
5. [基本プロパティ (Basic properties)]で必要なすべての情報を入力します。

   メディアサーバーを選択するには、検索アイコンをクリックします。使用するメディアサーバーが表示されない場合は、[検索 (Search)]フィールドを使用して検索できます。

   [次へ (Next)]をクリックします。
6. [ストレージサーバーのオプション (Storage server options)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

   KMS (キーマネージメントサービス) を使用する場合、[KMS]オプションを選択するには、まず KMS を構成する必要があります。
7. (オプション) [メディアサーバー (Media servers)]で、[追加 (Add)]をクリックして、使用する追加のメディアサーバーを追加します。

   [次へ (Next)]をクリックします。
8. [確認 (Review)]ページで、すべてのオプションが正しいことを確認し、[保存 (Save)]をクリックします。

   MSDP ストレージサーバーの作成に失敗した場合は、画面に表示されるメッセージに従って問題を修正します。

   クラウドストレージを使用するように MSDP を構成するには、次の手順 ([ボリューム (Volumes)]のドロップダウンを使用する手順) で、既存のディスクプールボリュームを選択するか、新しいボリュームを作成します。

9 (オプション) 上部の[ディスクプールの作成 (Create disk pool)]をクリックします。

10 (オプション)レプリケーションを使用してクラウド論理ストレージユニットとディスクプールを作成するには、[ディスクプールを作成 (Create disk pool)]をクリックします。

ディスクプールの作成に必要な情報を入力します。

次のタブで、必要なクラウドボリュームを選択し、追加します。クラウドストレージプロバイダを選択し、ストレージプロバイダの必要な詳細情報を指定します。クレデンシャルを入力して、クラウドストレージプロバイダにアクセスし、詳細設定を定義します。

クラウド論理ストレージユニットの場合、[編集 (Edit)]をクリックして、対応するディスクプールのプロパティページの[クラウドキャッシュのプロパティ (Cloud cache properties)]設定を更新します。更新された設定を機能させるには、pdde サービスを再起動する必要があります。

追加情報

以下の追加情報を確認してください。

- 現在、AWS S3 と Azure ストレージの API 形式がサポートされています。
  NetBackup でサポートされるストレージ API 形式について詳しくは、『NetBackup クラウド管理者ガイド』にある「NetBackup のクラウドストレージベンダーについて」のトピックを参照してください。
- サーバー側の暗号化を有効にした場合は、AWS のカスタマ管理キーを構成できます。これらのキーは、一度 NetBackup で使用されたら削除できません。各オブジェクトはアップロード中にキーで暗号化されます。AWS からキーを削除すると、NetBackup でリストアのエラーが発生します。
- Veritas Alta Recovery Vault for NetBackup の環境と配備について詳しくは、次の記事を参照してください。
  https://www.veritas.com/support/ja_JP/article.100051821
  Veritas Alta Recovery Vault の Azure と Azure Government のオプションを有効にする前に、『NetBackup 重複排除ガイド』の Veritas Alta Recovery Vault の Azure と Azure Government 構成に関するセクションの手順を確認してください。
  Veritas Alta Recovery Vault は、複数のオプションをサポートしています。Web UI の Azure と Azure Government の Veritas Alta Recovery Vault のオプションについて、クレデンシャルが必要な場合や、質問がある場合は、Cohesity NetBackup のアカウントマネージャにお問い合わせください。
  p.326 の「Cohesity Alta Recovery Vault Azure と Amazon について」を参照してください。

MSDP-C のクレデンシャルの管理

[クレデンシャルの管理 (Credential management)]機能を使用して、NetBackup がシステムまたは作業負荷への接続に使用する MSDP-C のクレデンシャルを追加および編集できます。

MSDP-C のクレデンシャルを追加するには:

1. 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
2. [指定したクレデンシャル (Named credentials)]タブで[追加 (Add)]をクリックします。[クレデンシャルを追加 (Add credentials)]ダイアログの[クレデンシャルストア (Credential store)]で[NetBackup]を選択し、[開始 (Start)]をクリックします。
3. [基本プロパティ (Basic properties)]で[クレデンシャル名 (Credential name)]を指定します。オプションで、[タグ (Tag)]と[説明 (Description)]を入力します。[次へ (Next)]をクリックします。
4. [カテゴリ (Category)]ドロップダウンから[MSDP-C]を選択します。

   AWS の場合は、次の操作を実行します。

   - [AWS S3 互換 (AWS S3 compatible)]を選択します。
   - 認証形式として[アクセスキー (Access key)]を選択した場合は、[アクセスキー ID (Access key ID)]と[シークレットアクセスキー (Secret access key)]を指定します。これら 2 つのパラメータは、NetBackup に AWS API へのアクセスを許可します。
   - [IAM Role Anywhere]を選択した場合は、次の手順を実行します。
     - [トラストアンカー ARN (Trust Anchor ARN)]を次の形式で指定します: *arn:aws:rolesanywhere:region:account:trust-anchor/TA_ID*。
     - [プロファイル ARN (Profile ARN)]を次の形式で指定します: *arn:aws:rolesanywhere:region:account:profile/PROFILE_ID*。
     - [役割 ARN (Role ARN)]を次の形式で指定します: *arn:aws::account:role/role-name-with-path*。
     - [CA 証明書 (CA Certificate)]を入力します。証明書は *-----BEGIN CERTIFICATE-----* で始め、*-----END CERTIFICATE-----* で終わる必要があります。
     - [秘密鍵 (Private Key)]を入力します。秘密鍵は、BEGIN RSA PRIVATE KEY----- で始め、-----END RSA PRIVATE KEY----- で終わる必要があります。または、-----BEGIN EC PARAMETERS----- で始め、-----END EC PRIVATE KEY----- で終わることもできます。

   Azure の場合は、次の手順を実行します。

- 認証形式として[アクセスキー (Access key)]を選択した場合は、[ストレージアカウント (Storage account)]と[アクセスキー (Access key)]を指定します。
- 認証形式として［サービスプリンシパル (Service principal)]を選択した場合は、［ストレージアカウント (Storage account)]、[クライアント ID (Client ID)]、[テナント ID (Tenant ID)]、および［シークレットキー (Secret key)]を指定します。

5 ［次へ (Next)]をクリックします。

6 クレデンシャルへのアクセス権を付与する役割を追加します。

- ［追加 (Add)]をクリックします。
- 役割を選択します。
- 役割に付与するクレデンシャル権限を選択します。

7 ［次へ (Next)]をクリックし、プロンプトに従ってクレデンシャルを作成します。

クラウドストレージユニットの作成

NetBackup Web UI またはコマンドラインを使用して、クラウドストレージユニットを作成します。

次の手順では、コマンドラインを使用してクラウドストレージユニットを作成する方法について説明します。

1 MSDP ストレージサーバーを作成します。

p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

2 クラウドインスタンスエイリアスを作成します。

例:

例 1: Amazon S3 クラウドインスタンスエイリアスの作成

```
# /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in
amazon.com -sts <storage server> -lsu_name <lsu name>
```

例 2: Amazon Glacier クラウドインスタンスエイリアスの作成

```
# /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in
amazon.com -sts <storage server> -lsu_name <lsu name>
-storage_class GLACIER
```

例 3: Microsoft Azure Archive クラウドインスタンスエイリアスの作成

```
# /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in
my -azure -sts <storage server> -lsu_name <lsu name> -storage_tier
ARCHIVE -post_rehydration_period 3
```

クラウドエイリアス名は *<storage server>_<lsu name>* で、バケットを作成するために使用されます。

3 新しいバケットを作成します (省略可能)。

例:

```
# /usr/openv/netbackup/bin/nbcldutil -createbucket -storage_server
<storage server>_<lsu name> -username <cloud user> -bucket_name
<bucket name>
```

4 構成ファイルを作成して、nbdevconfig コマンドを実行します。

新しいクラウド LSU を追加するための構成ファイルの内容:

構成設定	説明
V7.5 "operation" "add-lsu-cloud" string	新しいクラウド LSU を追加するための値 "add-lsu-cloud" を指定します。
V7.5 "lsuName" " " string	LSU 名を指定します。
V7.5 "cmsCredName" " " string	クレデンシャル名を指定します。
V7.5 "lsuCloudBucketName" " " string	クラウドバケット名を指定します。
V7.5 "lsuCloudBucketSubName" " " string	複数のクラウド LSU で同じクラウドバケットを使用できます。この値によって、異なるクラウド LSU が区別されます。
V7.5 "lsuEncryption" " " string	省略可能な値。デフォルトは NO です。 現在の LSU の暗号化プロパティを設定します。
V7.5 "lsuKmsEnable" " " string	省略可能な値。デフォルトは NO です。 現在の LSU の KMS を有効にします。
V7.5 "lsuKmsKeyGroupName" " " string	省略可能な値。 キーグループ名はすべての LSU 間で共有されます。 キーグループ名には、次の有効な文字を使用する必要があります: A-z、a-z、0-9、_ (アンダースコア)、- (ハイフン)、: (コロン)、. (ピリオド) および空白。
V7.5 "lsuKmsServerName" " " string	省略可能な値。 KMS サーバー名はすべての LSU 間で共有されます。
V7.5 "lsuKmsServerType" " " string	省略可能な値。
V7.5 "requestCloudCacheCapacity" "" string	省略可能な値。 ディスクキャッシュサイズを指定します。入力がない場合は、デフォルトの 1017 GB が使用されます。

例 1: 暗号化が無効になっている構成ファイル

```
V7.5 "operation" "add-lsu-cloud" string
V7.5 "lsuName" "s3amazon1" string
V7.5 "cmsCredName" "cpcp" string
V7.5 "lsuCloudBucketName" "bucket1" string
V7.5 "lsuCloudBucketSubName" "sub1" string
```

例 2: 暗号化が有効になっている構成ファイル

```
V7.5 "operation" "add-lsu-cloud" string
V7.5 "lsuName" "s3amazon2" string
V7.5 "cmsCredName" "cpcp" string
V7.5 "lsuCloudBucketName" "bucket1" string
V7.5 "lsuCloudBucketSubName" "sub2" string
V7.5 "lsuEncryption" "YES" string
V7.5 "lsuKmsEnable" "YES" string
V7.5 "lsuKmsKeyGroupName" "test" string
V7.5 "lsuKmsServerName" "test" string
```

メモ: 1 つのストレージサーバーに存在するすべての暗号化された LSU は、同じ keygroupname と kmsservername を使用する必要があります。nbdevconfig コマンドを使用して、新しい暗号化されたクラウド LSU (論理ストレージユニット) を追加するとき、暗号化された LSU がこの MSDP に存在する場合、keygroupname が暗号化済みの LSU の keygroupname と同じである必要があります。

p.111 の「NetBackup Key Management Server サービスを使用した MSDP 暗号化について」を参照してください。

構成ファイルを作成して、次の nbdevconfig コマンドを実行します。

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

メモ: パラメータ *<storage server>* は、手順 2 のパラメータ *<storage server>* と同じである必要があります。

---

5 nbdevconfig コマンドを使用して、ディスクプールを作成します。

例:

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv
-storage_servers <storage server name> -stype PureDisk | grep
<LSU name> > /tmp/dvlist

# /usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp
<disk pool name> -stype PureDisk -dvlist /tmp/dvlist
-storage_servers <storage server name>
```

メモ: NetBackup Web UI からディスクプールを作成することもできます。

6 bpstuadd コマンドを使用して、ストレージユニットを作成します。

例:

```
# /usr/openv/netbackup/bin/admincmd/bpstuadd -label <storage unit
name> -odo 0 -dt 6 -dp <disk pool name> -nodevhost
```

メモ: NetBackup Web UI からストレージユニットを作成することもできます。

クラウド LSU のクラウドクレデンシャルの更新

クラウド LSU のクラウドクレデンシャルを更新するには、構成ファイルを作成してから nbdevconfig コマンドを実行します。

クラウドクレデンシャルを更新するための構成ファイルの内容は次のとおりです。

構成設定	説明
V7.5 "operation" "update-lsu-cloud" string	一部のクラウド LSU パラメータを更新するには、値「update-lsu-cloud」を使用します。
V7.5 "lsuName" " " string	LSU 名を指定します。
V7.5 "cmsCredName" " " string	クレデンシャル名を指定します。

例:

```
V7.5 "operation" "update-lsu-cloud" string
V7.5 "lsuName" "s3amazon1" string
```

```
V7.5 "cmsCredName" "changedCmsCredName" string
After creating the configuration file, run the following command:

# /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

メモ: 元のストレージアカウントを使用して、Azure Recovery Vault または Veritas Alta Recovery Vault CMS のクレデンシャルを更新します。

クラウド LSU の暗号化構成の更新

クラウド LSU の KMS 暗号化構成を有効にするには、構成ファイルを作成してから nbdevconfig コマンドを実行します。

暗号化構成を更新するための構成ファイルの内容は次のとおりです。

構成設定	説明
V7.5 "operation" "update-lsu-cloud" string	KMS の状態は無効から有効にのみ更新できます。
V7.5 "lsuName" " " string	LSU 名を指定します。
V7.5 "lsuKmsEnable" "YES" string	クラウド LSU の KMS の状態を指定します。
V7.5 "lsuKmsServerName" "" string	省略可能な値。 すべての LSU 間で共有される KMS サーバー名。
V7.5 "lsuKmsKeyGroupName" "" string	省略可能な値。 すべての LSU 間で共有されるキーグループ名。 キーグループ名には、次の有効な文字を使用する必要があります: A-z、a-z、0-9、_ (アンダースコア)、- (ハイフン)、: (コロン)、. (ピリオド) および空白。

次の例では、クラウド LSU「s3amazon」の KMS の状態を無効から有効に変更します。

```
V7.5 "operation" "update-lsu-cloud" string
V7.5 "lsuName" "s3amazon" string

V7.5 "lsuKmsEnable" "YES" string
V7.5 "lsuKmsServerName" "XXX" string
V7.5 "lsuKmsKeyGroupName" "XXX" string
```

メモ: 1 つのストレージサーバーに存在するすべての暗号化された LSU は、同じ keygroupname と kmsservername を使用する必要があります。nbdevconfig コマンドを使用して、新しい暗号化されたクラウド LSU (論理ストレージユニット) を追加するとき、暗号化された LSU がこの MSDP に存在する場合、keygroupname が暗号化済みの LSU の keygroupname と同じである必要があります。

詳しくは、p.111 の「NetBackup Key Management Server サービスを使用した MSDP 暗号化について」を参照してください。

構成ファイルを作成して、次のコマンドを実行します。

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

クラウド LSU の削除

MSDP クラウド LSU を削除するには、次の手順を慎重に実行します。

クラウド LSU が MVG ボリュームに関連付けられている場合は、まず MVG ボリュームを削除してからクラウド LSU を削除します。cacontrol --dataselection list コマンドを実行して、クラウド LSU が MVG ボリュームに関連付けられているかどうかを確認します。関連付けがある場合、コマンド出力にはクラウド LSU の説明が UsedByVLSU=<mvg-server>:<mvg-volume> として表示されます。たとえば、次の出力では、クラウドボリューム demohost-cloud は MVG サーバー mvgdemo-host1.mvgdemo.com の MVG ボリューム mvg-cloud と関連付けられます。

```
cacontrol --dataselection list

[
…
    {
        "dsid": 3,
        "type": 9,
        "name": "demohost-cloud",
        "description":
"UsedByVLSU=mvgdemo-host1.mvgdemo.com:mvg-cloud;"
    }
]
```

p.240 の「MVG ボリュームの削除」を参照してください。

クラウド LSU を削除する方法

1. NetBackup のクラウド LSU のすべてのイメージを期限切れにします。
2. この MSDP クラウド LSU のストレージユニットとディスクプールを削除します。
3. MSDP S3 が構成されている場合は、クラウド LSU のすべての S3 バケットを削除します。
4. クラウド LSU を削除するには、storageId と CachePath が必要です。

   次のコマンドを実行して、1 つのクラウド LSU の情報を取得します。

   ```
   /usr/openv/pdde/pdcr/bin/pddecfg -a listcloudlsu
   dsid, lsuname, storageId, CachePath
   3, S3Volume, server1_ S3Volume/cloud-bucket1/sub1, /msdp/data/ds_3
   4, S3Volume2, server1_ S3Volume2/cloud-bucket1/sub2,
   /msdp/data/ds_4
   ```

   ここで、クラウド LSU の storageId とは、「server1_ S3Volume/cloud-bucket1/sub1」で、クラウド LSU の CachePath とは「/msdp/data/ds_3」です。
5. CRQP を実行して、tlog エントリが *<msdp_storage_path>*/spool フォルダと *<msdp_storage_path>*/queue フォルダに存在しないことを確認します。
6. nbdevconfig コマンドを使用して、spad の LSU 構成を削除します。

   MSDP クラウド LSU 構成を削除するための構成ファイルの内容は、次のとおりです。

構成設定	説明
V7.5 "operation" "delete-lsu-cloud" string	spad の MSDP クラウド LSU 構成を削除するための値「delete-lsu-cloud」。
V7.5 "lsuName" " " string	LSU 名を指定します。

例:

```
V7.5 "operation" "delete-lsu-cloud" string
V7.5 "lsuName" "s3amazon1" string
```

構成ファイルを作成して、次のコマンドを実行します。

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

7 MSDP サービスとその監視サービスを停止します。

```
# /usr/openv/netbackup/bin/nbsvcmon -terminate

# /usr/openv/pdde/pdconfigure/pdde stop
```

8 次のコマンドを使用して、spoold の LSU 構成を削除します。

```
# /usr/openv/pdde/pdcr/bin/spoold --removepartition <storageId>
```

9 次のコマンドを使用して、キャッシュフォルダやその他のバックエンドのフォルダを削除します (省略可能)。

```
# rm -r <CachePath>

# rm -r <msdp_storage_path>/spool/ds_<dsid>

# rm -r <msdp_storage_path>/queue/ds_<dsid>

# rm -r <msdp_storage_path>/processed/ds_<dsid>

# rm -r <msdp_storage_path>/databases/refdb/ds_<dsid>

# rm -r <msdp_storage_path>/databases/datacheck/ds_<dsid>
```

10 クラウドのサブバケットフォルダ全体を削除します(省略可能)。

11 MSDP サービスとその監視サービスを開始します。

```
# /usr/openv/pdde/pdconfigure/pdde start

# /usr/openv/netbackup/bin/nbsvcmon
```

12 クラウドインスタンスのエイリアスを削除します。

```
# /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -rs -in
<instance_name> -sts <storage_server_name>_<lsu_name>
```

クラウド LSU を使用したクラウドへのデータのバックアップ

クラウド LSU にデータをバックアップするには、次の手順を実行します。

- クラウド LSU、関連するディスクプール、ストレージユニット (クラウドストレージユニット) を作成します。
- バックアップポリシーを作成し、クラウドストレージユニットをポリシーストレージとして使用します。
- バックアップを実行し、データをクラウドストレージに書き込みます。

同じストレージサーバーに複数のクラウド LSU を作成してバックアップできます。

クラウド LSU を使用したデータクラウドの複製

次の手順を実行して、ローカル MSDP からクラウド LSU にバックアップイメージを複製します。

- MSDP ストレージサーバーを構成し、「PureDiskVolume」を使用してディスクプールを作成してから、ストレージユニット (ローカルストレージユニット) を作成します。
- クラウド LSU、関連するディスクプール、ストレージユニット (クラウドストレージユニット) を作成します。
- ストレージライフサイクルポリシーを作成し、「バックアップ」と「複製」の値を追加します。データはローカルストレージユニットにバックアップされた後、クラウドストレージユニットに複製されます。
- バックアップポリシーを作成し、ストレージライフサイクルポリシーをポリシーストレージとして使用します。
- バックアップを実行し、データはクラウドストレージに書き込まれた後、クラウドストレージに複製されます。

クラウド LSU からローカル MSDP、および 2 つのクラウド LSU 間で複製を実行することもできます。

クラウド LSU を使用するための AIR の構成

次の手順では、ある LSU から、異なる NetBackup ドメインの別の LSU にバックアップイメージを複製するために必要なタスクについて説明します。

- p.132 の「異なる NetBackup ドメインへの MSDP レプリケーション設定」を参照してください。
- ターゲット NetBackup ドメインと信頼関係を構成する
  p.142 の「自動イメージレプリケーションの信頼できるプライマリサーバーについて」を参照してください。
- リモートストレージサーバーにレプリケーションターゲットとして LSU を追加します。
  別の NetBackup ドメインにレプリケーションターゲットを追加するには、NetBackup Web UI を使用するか、コマンドラインインターフェースを使用します。

1 レプリケーションターゲットを追加するための構成ファイルを作成します。

レプリケーションターゲットを追加するための構成ファイルの内容は次のとおりです。

構成設定	説明
V7.5 "operation" " " string	新しいレプリケーションターゲットを追加するには、この値を「set-replication」にする必要があります。
V7.5 " rephostname" " " string	レプリケーションターゲットのホスト名を指定します。
V7.5 "replogin" " " string	レプリケーションターゲットのストレージサーバーのユーザー名を指定します。
V7.5 "reppasswd" " " string	レプリケーションターゲットのストレージサーバーのパスワードを指定します。
V7.5 "repsourcevolume" " " string	レプリケーションソースのボリューム名を指定します。
V7.5 "reptargetvolume" " " string	レプリケーションターゲットのボリューム名を指定します。

例:

```
[root@sourceserver~]# cat add-replication-local2cloud.txt
V7.5 "operation" "set-replication" string
V7.5 "rephostname" "targetserver1.example.com" string
V7.5 "replogin" "root" string
V7.5 "reppasswd" "root" string
V7.5 "repsourcevolume" "PureDiskVolume" string
V7.5 "reptargetvolume" "s3amamzon1" string
```

構成ファイルを作成して、nbdevconfig コマンドを実行します。

例:

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

2 nbdevconfig を実行し、ディスクボリュームを更新します。

例:

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -updatedv -stype
PureDisk -dp diskpool1 -media_server sourceserver.example.com
```

- ストレージライフサイクルポリシーを構成します。
ソースドメインで SLP を構成する前に、ターゲットドメインでインポート SLP を作成する必要があります。
p.159 の「ストレージライフサイクルポリシーについて」を参照してください。

p.159 の「自動イメージレプリケーションに必要なストレージライフサイクルポリシーについて」を参照してください。
p.161 の「ストレージライフサイクルポリシーの作成」を参照してください。

レプリケーションターゲットの削除

レプリケーションターゲットを削除するには、次の手順を実行します。

1. レプリケーションターゲットを削除するための構成ファイルを作成します。

   レプリケーションターゲットを削除するための構成ファイルの内容は次のとおりです。

構成設定	説明
V7.5 "operation" " " string	新しいレプリケーションターゲットを削除するには、この値を「delete-replication」にする必要があります。
V7.5 " rephostname" " " string	レプリケーションターゲットのホスト名を指定します。
V7.5 "repsourcevolume" " " string	レプリケーションソースのボリューム名を指定します。
V7.5 "reptargetvolume" " " string	レプリケーションターゲットのボリューム名を指定します。

   例:

```
[root@sourceserver~]# cat delete-replication-local2cloud.txt
V7.5 "operation" "delete-replication" string
V7.5 "rephostname" "targetserver1.example.com" string
V7.5 "repsourcevolume" "PureDiskVolume" string
V7.5 "reptargetvolume" "s3amamzon1" string
```

   構成ファイルを作成して、nbdevconfig コマンドを実行します。

   例:

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

2. nbdevconfig を実行し、ディスクボリュームを更新します。

   例:

```
# /usr/openv/netbackup/bin/admincmd/nbdevconfig -updatedv -stype
PureDisk -dp diskpool1 -media_server sourceserver.example.com
```

下位互換性のサポートについて

以前のバージョン (NetBackup 8.2 以前) の MSDP サーバーからターゲット MSDP サーバーのクラウド LSU にイメージをレプリケートするには、A.I.R. ターゲットを追加するときにユーザー名とクラウド LSU 名が必要です。A.I.R. ターゲットを追加するには、Web UI を使用します。ユーザー名とターゲットクラウド LSU の形式は次のとおりです。

```
<username>?LSU=<target cloud LSU>
```

たとえば、ターゲットストレージサーバーが存在し、そのサーバーのユーザー名が `userA` で、ターゲットストレージサーバーにクラウド LSU `s3cloud1` が存在するとします。古いストレージサーバーからターゲットサーバーのクラウド LSU にイメージをレプリケートするには、A.I.R. ターゲットを追加するときに、次のユーザー名を使用できます。

```
userA?LSU=s3cloud1
```

また、ターゲットプライマリサーバーにあるターゲットストレージサーバーのローカルボリューム用にインポート SLP を作成する必要があります。次に、ソース側でターゲット A.I.R. SLP を作成するときに、インポートされた SLP を選択します。A.I.R. を実行すると、ターゲット側のインポートジョブは、アクティビティモニターに SLP_No_Target_SLP としてポリシー名を表示しますが、データはクラウドに送信されます。

NetBackup クライアントのバージョンが 8.2 以前の場合、その古いクライアントからストレージサーバーのクラウド LSU へのクライアントの直接バックアップが失敗することがあります。バックアップ中にクライアント側で `mtstrmd` が使用されると、ジョブはメディア書き込みエラーで失敗します。クライアント側で `mtstrmd` を無効にするには、クライアント上の構成ファイル `pd.conf` を開いて次を変更します。

`MTSTRM_BACKUP_ENABLED = 1` を `MTSTRM_BACKUP_ENABLED = 0` にします。

`pd.conf` ファイルは次のディレクトリにあります。

- UNIX の場合
  `/usr/openv/lib/ost-plugins/`
- Windows の場合
  `install_path``¥Veritas¥NetBackup¥bin¥ost-plugins`

クラウド LSU と古いクライアントを使用してクライアントの直接バックアップを実行する場合、クライアントはクライアント側の重複排除のみを実行します。

クラウド LSU を使用するには、ストレージサーバーの負荷分散サーバーが以前のバージョン (NetBackup 8.2 以前) ではないことが必要です。新しい負荷分散サーバーと古い負荷分散サーバーがある場合は、ジョブを正常に実行できるように、新しい負荷分散サーバーが自動的に選択されます。クラウド LSU でバックアップイメージをリストアし、メディアサーバーを明示的に選択する場合、選択するメディアサーバーが NetBackup の古いバージョンではないことが必要です。

cloud.json、contentrouter.cfg、spa.cfg 内の構成項目について

cloud.json ファイルは、<*STORAGE*>/etc/puredisk/cloud.json にあります。

このファイルには次のパラメータがあります。

パラメータ	詳細	デフォルト値
UseMemForUpload	true に設定すると、アップロードキャッシュディレクトリが tmpfs としてメモリにマウントされます。これは特に、ディスク速度がボトルネックになっている高速クラウドで役立ちます。また、ローカル LSU とのディスクの競合を減らすこともできます。システムメモリが十分である場合、値は true に設定されます。 利用可能なメモリが十分にある場合、デフォルト値は true です。	true
CachePath	キャッシュのパス。MSDP ボリュームの領域使用状況に応じて、MSDP ボリュームに作成されます。ローカル LSU が書き込むことができない領域を予約します。通常、一部のボリュームが他のボリュームよりも大幅に少ない場合を除き、このパスを変更する必要はありません。複数のクラウド LSU を同じディスクボリュームに分散させることができます。パフォーマンスを考慮して、別のボリュームに分散させるためにこのオプションの変更が必要になる場合があります。このパスは、MSDP 以外のボリュームに格納するように変更できます。	なし
UploadCacheGB	アップロードキャッシュの最大領域使用量です。アップロードキャッシュは、CachePath の下の「upload」という名前のサブディレクトリです。パフォーマンスを考慮して、次より大きい値に設定する必要があります。 (最大並列書き込みストリーム数) * MaxFileSizeMB * 2。 したがって、100 の並列実行ストリームの場合、約 13 GB で十分です。 **メモ:** cloud.json ファイルの UploadCacheGB の初期値は、contentrouter.cfg ファイルの CloudUploadCacheSize の値です。 新しいクラウド LSU を追加すると、UploadCacheGB の値は CloudUploadCacheSize と等しくなります。後で、cloud. json ファイルでこの値を変更できます。	12

パラメータ	詳細	デフォルト値
DownloadDataCacheGB	これは、データファイル (主に SO BIN ファイル) の最大領域使用量です。このキャッシュを大きくするほど、より多くのデータファイルをキャッシュに格納できます。そうすれば、リストアの実行時にクラウドからこれらのファイルをダウンロードする必要はありません。 **メモ:** cloud.json ファイルの DownloadDataCacheGB の初期値は、contentrouter.cfg ファイルの CloudDataCacheSize の値です。 新しいクラウド LSU を追加すると、DownloadDataCacheGB の値は CloudDataCacheSize と等しくなります。後で、cloud. jsonファイルでこの値を変更できます。	500
DownloadMetaCacheGB	これは、データファイル (主に DO ファイルおよび SO BHD ファイル) の最大領域使用量です。このキャッシュを大きくするほど、より多くのメタファイルをキャッシュに格納できます。そうすれば、リストアの実行時にクラウドからこれらのファイルをダウンロードする必要はありません。 **メモ:** cloud.json ファイルの DownloadMetaCacheGB の初期値は、contentrouter.cfg ファイルの CloudMetaCacheSize の値です。 新しいクラウド LSU を追加すると、DownloadMetaCacheGB の値は CloudMetaCacheSize と等しくなります。後で、cloud. jsonファイルでこの値を変更できます。	500
MapCacheGB	これは、MD5 形式の指紋の互換性のために使用される map ファイルの最大領域使用量です。このキャッシュを大きくするほど、より多くの map ファイルをキャッシュに格納できます。 **メモ:** cloud.json ファイルの MapCacheGB の初期値は、contentrouter.cfg ファイルの CloudMapCacheSize の値です。 新しいクラウド LSU を追加すると、MapCacheGB の値は CloudMapCacheSize と等しくなります。後で、cloud. jsonファイルでこの値を変更できます。	5
UploadConnNum	アップロードする際のクラウドプロバイダへの最大同時接続数。この値を大きくすると、特に高遅延ネットワークに役立ちます。	60
DataDownloadConnNum	データをダウンロードする際のクラウドプロバイダへの最大同時接続数。この値を大きくすると、特に高遅延ネットワークに役立ちます。	40
MetaDownloadConnNum	メタデータをダウンロードする際のクラウドプロバイダへの最大同時接続数。この値を大きくすると、特に高遅延ネットワークに役立ちます。	40
MapConnNum	マップをダウンロードする際のクラウドプロバイダへの最大同時接続数。	40

パラメータ	詳細	デフォルト値
DeleteConnNum	削除する際のクラウドプロバイダへの最大同時接続数。この値を大きくすると、特に高遅延ネットワークに役立ちます。	100
KeepData	データキャッシュにアップロードされたデータを保持します。UseMem が true の場合、この値は常に false になります。	false
KeepMeta	アップロードされたメタをメタキャッシュに保持します。UseMem が true の場合、この値は常に false になります。	false
ReadOnly	LSU は読み取り専用で、この LSU に対する書き込みと削除はできません。	false
MaxFileSizeMB	bin ファイルの最大サイズ (MB 単位)。	64
WriteThreadNum	データをデータコンテナに並列で書き込むためのスレッドの数。これにより、IO のパフォーマンスを向上させることができます。	2
RebaseThresholdMB	リベースしきい値 (MB)。コンテナのイメージデータがしきい値より少ない場合、このコンテナ内のすべてのイメージデータは、適切な局所性を実現するために重複排除には使用されません。指定可能な値: 0 から MaxFileSizeMB の半分まで、0 = 無効	4
AgingCheckContainerIntervalDay	このクラウド LSU のコンテナをチェックする間隔 (日数)。 **メモ:** アップグレードされたシステムでは、クラウド LSU の値を変更する場合は、これを手動で追加する必要があります。	180

contentrouter.cfg ファイルは、<*STORAGE*>/etc/puredisk/contentrouter.cfg にあります。

このファイルには次のパラメータがあります。

パラメータ	詳細	デフォルト値
CloudDataCacheSize	クラウド LSU を追加するときのデフォルトのデータキャッシュサイズ。 十分な空き領域が利用できない場合は、この値を小さくします。	500 GiB
CloudMapCacheSize	クラウド LSU を追加するときのデフォルトのマップキャッシュサイズ。 十分な空き領域が利用できない場合は、この値を小さくします。	5 GiB
CloudMetaCacheSize	クラウド LSU を追加するときのデフォルトのメタキャッシュサイズ。 十分な空き領域が利用できない場合は、この値を小さくします。	500 GiB

パラメータ	詳細	デフォルト値
CloudUploadCacheSize	クラウド LSU を追加するときのデフォルトのアップロードキャッシュサイズ。 最小値は 12 GiB です。	12 GiB
MaxPredictiveCacheSize	予測キャッシュの最大サイズを指定します。これは、システムメモリの合計に基づき、スワップ領域は除外されます。	20
CloudBits	クラウドキャッシュの最上位エントリの数。この数は (2^CloudBits) です。この値を増やすと、キャッシュのパフォーマンスを向上させることができますが、余分にメモリを消費します。最小値 = 16、最大値 = 48。	MaxCloudCacheSize に基づく自動サイズ
DCSCANDownloadTmpPath	dcscan を使用してクラウド LSU を調べる際に、データがこのフォルダにダウンロードされます。詳しくは、クラウドサポートセクションの dcscan ツールを参照してください。	disabled
UsableMemoryLimit	利用可能な最大メモリサイズをパーセントで指定します。 MaxCacheSize + MaxPredictiveCacheSize + MaxSamplingCacheSize + Cloud in-memory upload cache size は UsableMemoryLimit の値以下である必要があります。	85%
MaxSamplingCacheSize	ここではすべての LSU の最大サンプリングキャッシュサイズをパーセントで指定します。 クラウド LSU の最大サンプリングキャッシュサイズを制限する場合は、cloud.json で LSUSamplingCachePercent を構成します。このパラメータのデフォルト値は -1.0% です。これは制限がないことを意味します。 サンプリングキャッシュは、MSDP AKS と MSDP FlexScale クラスタのグローバル重複排除の実装にも使用されます。	5%
ClusterHookEngineCount	グローバル重複排除は履歴データを使用してサンプリングキャッシュのフックアップ処理を最適化します。履歴データが有効な場合は、ノード間のオーバーヘッドを減らすために、リモート S キャッシュルックアップ要求のみが ClusterHookEngineCount ノードの数に送信されます。この機能を無効にするには、ClusterHookEngineCount を 0 に設定します。	3
ClusterHookMinHistoryAgeInSecond	履歴データが有効になる最小経過時間 (秒単位)。最小経過時間より新しいデータは使用されません。	604800
ClusterHookMaxHistoryAgeInSecond	履歴データが有効になる最大経過時間 (秒単位)。最大経過時間より古いデータは削除されます。	2592000

パーティションに、次よりも多い空き領域がない場合、新しいクラウド LSU の追加は失敗します。

```
CloudDataCacheSize + CloudMapCacheSize + CloudMetaCacheSize +
CloudUploadCacheSize + WarningSpaceThreshold * partition size
```

`crcontrol --dsstat 2` コマンドを使用して、各パーティションの領域を確認します。

メモ: 各クラウド LSU にはキャッシュディレクトリがあります。すべての MSDP ボリュームのディスク容量の使用状況に応じて、選択した MSDP ボリュームにディレクトリが作成されます。クラウド LSU はそのボリュームからキャッシュ用にディスク容量を予約し、ローカル LSU はより多くのディスク領域を使用できません。

各クラウド LSU の初期予約ディスク容量は、`<STORAGE>/etc/puredisk/cloud.json` ファイルの `UploadCacheGB`, `DownloadDataCacheGB`, `DownloadMetaCacheGB`, と `MapCacheGB` の値の合計です。キャッシュを使用すると、ディスク容量が減少します。

`crcontrol --dsstat 2` の出力には `Cache` オプションがあります。

```
# crcontrol --dsstat 2

=============== Mount point 2 ===============

Path = /msdp/data/dp1/1pdvol

Data storage

Raw Size Used Avail Cache Use%

48.8T 46.8T 861.4G 46.0T 143.5G 2%

Number of containers : 3609

Average container size : 252685915 bytes (240.98MB)

Space allocated for containers : 911943468161 bytes (849.31GB)

Reserved space : 2156777086976 bytes (1.96TB)

Reserved space percentage : 4.0%
```

`Cache` オプションは、このボリュームのクラウドによって現在予約されているディスク容量です。ディスク容量は、このボリュームにキャッシュディレクトリがあるすべてのクラウド LSU の予約済み領域の合計です。このボリューム上でローカル LSU に対して実際に利用可能な領域は `Avail - Cache` です。

`spa.cfg` ファイルは、*<STORAGE>*`/etc/puredisk/spa.cfg` にあります。

このファイルには次のパラメータがあります。

パラメータ	詳細	デフォルト値
CloudLSUCheckInterval	クラウド LSU の状態を確認する間隔 (秒単位)。	1800
EnablePOIDListCache	POID (パスオブジェクト ID) リストのキャッシュの状態 (有効または無効)。パスオブジェクトには、そのイメージに関連付けられたメタデータが含まれています。	true

クラウド領域の再利用

MSDP はデータコンテナにデータセグメントを格納し、データコンテナはクラウドストレージに送信され、オブジェクトとして格納されます。1 つのコンテナ内のセグメントは、異なるバックアップイメージに属する場合があります。バックアップイメージが期限切れになると、そのセグメントはガーベジになります。1 つのコンテナ内のすべてのセグメントがガーベジである場合、コンテナ全体を再利用できます。すべてがガーベジでない場合、そのコンテナには有用なデータとガーベジの両方が含まれているため、そのコンテナを再利用できません。1 つのコンテナ内のセグメントの数が少ないと、それらのセグメントが多くのバックアップイメージによって参照されている場合、そのコンテナが長期間再利用されない場合があります。

MSDP では、コンテナの有効期間とクラウド圧縮を使用して、これらのコンテナの領域を再利用します。

コンテナのエージングの設定

コンテナのエージングは、セグメントの数が少ないが長時間存続しているコンテナを識別し、新しいバックアップイメージによって参照されないようにしようとします。

contentrouter.cfg ファイルには、次のエージングチェック関連のパラメータがあります。

パラメータ	説明	デフォルト値
EnableAgingCheck	クラウド LSU コンテナのエージングチェックを有効または無効にします。	true
AgingCheckAllContainers	このパラメータはすべてのコンテナをチェックするかどうかを決定します。「false」に設定すると、一部の最新のイメージのコンテナのみがチェックされます。	false
AgingCheckSleepSeconds	この時間間隔 (秒数) でエージングチェックスレッドが定期的に開始されます。	20
AgingCheckBatchNum	エージングチェックで一度にチェックするコンテナの数。	400

パラメータ	説明	デフォルト値
AgingCheckContainerInterval	クラウド LSU を追加するときにコンテナをチェックするデフォルトの間隔の値 (日数)。	180
AgingCheckSizeLowBound	このしきい値は、サイズがこの値より小さいコンテナをエージングチェック時にフィルタ処理するために使用されます。	8 Mib
AgingCheckLowThreshold	このしきい値は、ガーベジの割合がこの値 (パーセント) より小さいコンテナをフィルタ処理するために使用されます。	10%

エージングチェック関連のパラメータを更新した後は、MSDP サービスを再起動する必要があります。crcontrol コマンドラインを使用すると、MSDP サービスを再起動せずにこれらのパラメータを更新できます。

crcontrol コマンドラインを使用してエージングパラメータを更新するには

1. すべてのクラウド LSU のクラウドエージングチェックを有効にします。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingcheckon
   ```

2. 指定したクラウド LSU のクラウドエージングチェックを有効にします。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingcheckon <dsid>
   ```

3. すべてのクラウド LSU のクラウドエージングチェックを無効にします。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingcheckoff
   ```

4. 指定したクラウド LSU のクラウドエージングチェックを無効にします。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingcheckoff <dsid>
   ```

5. すべてのクラウド LSU のクラウドエージングチェック状態を表示します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingcheckstate
   ```

6. 指定したクラウド LSU のクラウドエージングチェック状態を表示します。

   /usr/o```penv/pdde/pdcr/bin/crcontrol --cloudagingcheckstate <dsid>```

7. すべてのクラウド LSU のクラウドエージングチェックを高速モードに変更します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingfastcheck
   ```

8. 指定したクラウド LSU のクラウドエージングチェックを高速モードに変更します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --cloudagingfastcheck <dsid>
   ```

クラウド圧縮の構成

クラウド圧縮により、既存のコンテナはガーベジを含まない新しい小さなコンテナに置き換えられます。ローカルストレージの圧縮に似ています。圧縮プロセスでは、条件を満たすコンテナがオブジェクトクラウドストレージからローカルコピーにダウンロードされます。

圧縮によって、ローカルコピー内のガーベジが削除され、アップロードされてクラウド内の古いオブジェクトが上書きされます。このプロセスでは、クラウドストレージとの間でデータが転送され、追加コストが発生する場合があります。圧縮を効率的に動作させるために適切な帯域幅も必要です。そのため、クラウド圧縮はデフォルトでは無効になっています。コストと帯域幅に問題がない配備で有効にできます。たとえば、プライベートクラウドで有効にするか、MSDP がオブジェクトストレージと同じクラウドに配備されている場合に有効にすることをお勧めします。

制限事項:

- WORM クラウド LSU はサポートされません。
- バージョン管理が有効なバケットはサポートされません。
- CloudCatalyst 移行システムはサポートされません。
- MSDP クラスタ配備 (AKS、EKS、NBFS) はサポートされません。

cloud.json の次のオプションを使用して、クラウド圧縮を構成できます。

パラメータ	説明	デフォルト値
CompactEnable	クラウド圧縮の有効と無効を切り替えます。	false
CompactBatchNum	毎回のクラウド圧縮のコンテナ数。	400
EnableCompactCandidateCheck	クラウド圧縮チェックの有効と無効を切り替えます。この値は CompactEnable が true の場合に利用可能です。	true
CompactLboundMB	クラウド圧縮のために、この値より小さいガーベジサイズのコンテナをフィルタ処理します。	16
CompactSizeLboundMB	クラウド圧縮にのために、この値より小さいサイズのコンテナをフィルタ処理します。	32
CompactMaxPo	クラウド圧縮のために、このパスオブジェクトの数より多く参照されているコンテナをフィルタ処理します。	100

crcontrol コマンドラインを使用してクラウド圧縮パラメータを更新するには

1 1 つのクラウド LSU に対してクラウド圧縮を有効にします。

```
/usr/openv/pdde/pdcr/bin/crcontrol --cloudcompacton <dsid>
```

このコマンドは一時的に圧縮を有効にします。圧縮を永続的に有効にするには、cloud.json で CompactEnable の値を手動で更新します。

コンテナの経過時間は、クラウド圧縮が有効になると自動的に無効になります。

2 1 つのクラウド LSU に対してクラウド圧縮を無効にします。

```
/usr/openv/pdde/pdcr/bin/crcontrol --cloudcompactoff <dsid>
```

圧縮を永続的に無効にするには、cloud.json で CompactEnable を手動で更新し、spoold を再起動します。

3 すべてのクラウド LSU のクラウド圧縮状態を表示します。

```
/usr/openv/pdde/pdcr/bin/crcontrol --cloudcompactstate
```

クラウドサポートのツールの更新について

DCSCAN:

Dcscan は、クラウドからデータコンテナをダウンロードします。デフォルトのダウンロードパスは <STORAGE>/tmp/DSID_#dsid です。ここで、#dsid はクラウド LSU の DSID 値に依存します。クラウドストレージプロバイダごとに、異なる DSID 値があります。DSID を知る必要はありません。dcscan が自動的に DSID 値を取得します。DCSCANDownloadTmpPath フィールドを使用して、contentrouter.cfg ファイル内のデフォルトのダウンロードパスを変更できます。

dcscan ツールを使用してクラウドデータを参照している間、すべてのデータコンテナがクラウドからダウンロードされるため、-a オプションは無効になります。dcscan はクラウドからデータコンテナのみをダウンロードするため、-fixdo オプションも無効になります。その他の操作は、ローカル LSU と同じです。

dcscan はデータコンテナを自身のキャッシュにダウンロードします。一部の LSU で圧縮が有効になっている場合は、この LSU で dcscan を実行する前に、これらの古いコンテナを dcscan キャッシュディレクトリから削除します。

SEEDUTIL:

Seedutil をバックアップのシード処理に使用すると、重複排除率を向上させることができます。名前に <backup ID> が含まれているパス <client name>/<policy name> で見つかったすべてのバックアップファイルへのリンクが、<destination client name> ディレクトリに作成されます。ユーザーは、クラウド LSU が使用した DSID 値を知る必要があります。この DSID 値を seedutil に指定し、クライアントをシード処理するクラウド

LSU を seedutil が特定できるようにする必要があります。ローカル LSU に対してシード処理を実行する場合、デフォルトの DSID は 2 です。DSID 値を指定する必要はありません。Seedutil は、異なる DSIDs にまたがってシード処理することはできません。

たとえば、/usr/openv/pdde/pdag/bin/seedutil -seed -sclient <*source_client_name*> -spolicy <*source_policy_name*> -dclient <*destination_client_name*> -dsid <*dsid_value*> です。

CRCONTROL

crcontrol -clouddsstat オプションを使用して、クラウド LSU データストアの使用状況を表示します。DSID 値を指定する必要があります。クラウドストレージには無制限の領域があるため、サイズは 8 PB にハードコードされます。

例:

```
# /user/openv/pdde/pdcr/bin/crcontrol --clouddsstat <dsid_value>
************ Data Store statistics ************
Data storage      Raw    Size   Used   Avail  Use%
8.0P   8.0P  80.9G  8.0P   0%
Number of containers             : 3275
Average container size           : 26524635 bytes (25.30MB)
Space allocated for containers   : 86868179808 bytes (80.90GB)
Reserved space                   : 0 bytes (0.00B)
Reserved space percentage        : 0.0%
```

CRSTATS:

crstats -cloud -dsid オプションを使用して、クラウド LSU の統計情報を表示します。DSID 値を指定する必要があります。クラウドストレージには無制限の領域があるため、サイズは 8 PB にハードコードされます。

例:

```
#/usr/openv/pdde/pdcr/bin/crstats --cloud-dsid <dsid_value>
Storage Pool Raw Size=9007199254740992Bytes
Storage Pool Reserved Space=0Bytes
Storage Pool Required Space=0Bytes
Storage Pool Size=9007199254740992Bytes
Storage Pool Used Space=86868179808Bytes
Storage Pool Available Space=9007112386561184Bytes
Catalog Logical Size=402826059439Bytes
Catalog files Count=3726
Space Allocated For Containers=86868179808Bytes
Deduplication Ratio=4.6
```

PDDECFG:

pddecfg を使用して、すべてのクラウド LSU を一覧表示します。

例:

```
/usr/openv/pdde/pdcr/bin/pddecfg -a listcloudlsu
dsid, lsuname, storageId, CachePath
3, S3Volume, amazon_1/cloud-bucket1/sub1, /msdp/data/ds_3
4, S3Volume2, amazon_1/cloud-bucket1/sub2, /msdp/data/ds_4
```

クラウド LSU のディザスタリカバリについて

NetBackup ソフトウェアが存在するディスクまたは重複排除データが存在するディスクで障害が発生した場合、次の手順を使用して、さまざまなシナリオに応じてシステムとデータをリカバリできます。

リカバリ後、NetBackup の重複排除環境は正常に機能します。そのクラウド LSU ストレージ上にある有効なバックアップイメージは、リストアに利用できます。

ディザスタリカバリを開始する前に、次のことを確認します。

- MSDP サービスが存在するメディアサーバーが引き続き機能する。メディアサーバーが機能しない場合は、メディアサーバーを再インストールする必要があります。メディアサーバーソフトウェアの再インストールについては、『NetBackup インストールガイド』を参照してください。
- KMS 暗号化がクラウド LSU によって使用されている場合、KMS サーバーの準備ができている。

クラウド LSU のディザスタリカバリの後、次の場合にバックアップイメージのインポートが必要です。

- プライマリサーバーの MSDP ストレージにイメージのカタログがない。たとえば、プライマリサーバーが再インストールされて、プライマリサーバーのカタログが失われた場合です。カタログはバックアップイメージをインポートするために必要です。詳しくは、『NetBackup 管理者ガイド Vol. 1』の「バックアップイメージのインポートについて」セクションを参照してください。
- プライマリサーバーに MSDP ストレージに関する不正なカタログレコードがある。ディザスタリカバリ後にストレージサーバーが新しいメディアサーバーに移動されるため、プライマリサーバーのカタログが正しくなくなりました。プライマリサーバーのカタログを修正するには、bpimage コマンドを実行します。ここでの新しいメディアサーバーは、新しく追加されたメディアサーバー、または他の既存のメディアサーバーを意味します。
- プライマリの MSDP ストレージにイメージのカタログが存在し、同じメディアサーバーがディザスタリカバリに使用されている場合、バックアップイメージのインポートは不要。

- Amazon S3 Glacier、Deep Archive、Microsoft Azure Archive クラウドの LSU に保存されたバックアップが以前に Cloud Catalyst から移行されている場合、それらのバックアップではインポートはサポートされません。

次の 3 つの手順を使用して、クラウド LSU のディザスタリカバリを実行できます。

1. ローカルストレージで MSDP ストレージサーバーを設定します。
2. クラウド LSU を追加して、既存のクラウドデータを再利用します。
3. プライマリサーバーでカタログを利用できない場合は、バックアップイメージのインポートを実行します。

シナリオ 1: MSDP サーバー名が変更されておらず、ローカルストレージが失われていて、NetBackup カタログがある

手順	タスク	手順詳細
1	空のローカル LSU を作成します。	「「MSDP ローカルストレージの構成または再構成」」を参照
2	クラウド LSU を再利用します。	「「クラウド LSU の再利用」」を参照

シナリオ 2: MSDP サーバー名が変更されておらず、ローカルストレージが失われていて、NetBackup カタログがない

手順	タスク	手順詳細
1	古いストレージサーバー関連の構成を削除します。	「MSDP ストレージサーバーのエラーからのリカバリ」のトピックにある、次の手順を実行します。p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。 ■ ディスクプールを使用するストレージユニットを削除します。 ■ ディスクプールを削除します。 ■ 重複排除ストレージサーバーを削除します。 ■ 重複排除ホストの構成ファイルを削除します。 ■ 重複排除サーバー上のクレデンシャルを削除します。
2	新しいストレージサーバーを構成します。	プライマリサーバーで次のコマンドを実行します。 `/usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests -storage_server “storage server” -stype PureDisk -media_server “media server” -st 9` **メモ:** NetBackup Web UI からストレージサーバーを作成することもできます。
3	空のローカル LSU を作成します。	「「MSDP ローカルストレージの構成または再構成」」を参照
4	クラウド LSU を再利用します。	「「クラウド LSU の再利用」」を参照

手順	タスク	手順詳細

5	クラウド LSU のディスクプールを作成します。	プライマリサーバーで次のコマンドを実行します。
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk | grep <LSU name> > /tmp/dvlist`
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name>`
		メモ: NetBackup Web UI からディスクプールを作成することもできます。

6	遅延の大きいストレージのインポート用にイメージを準備します。	ソースバージョンが 11.0 以降の場合、MSDP はイメージをバックグラウンドでインポートするための準備を自動的に行います。イメージのインポート準備ができるのを待ちます。次のコマンドを実行して状態を調べます。
		`tiermover --status --lsu <LSU name> [--client <client>] [--policy <policy>] [--backupid <backup ID>] [--sobins] [--active] [--lsulist] [--debug] [--verbose]`
		ソースバージョンが 11.0 より前であるか、ソースサーバーが停止してインポート前の操作が完了しなかった場合は、次のコマンドを実行してイメージのインポートを準備します。
		`tiermover --start --lsu <LSU name> --client <client> --policy <policy> [--backupid <backup ID>] [--retrieval Bulk|Standard|Expedited] [--verbose] [--debug]`
		メモ: イメージをインポートする準備が整っていない場合、インポートは失敗します。

7	イメージをインポートして戻します。	2 段階のインポートを実行します。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 ソースが 11.0 以降で高遅延ストレージの場合: 高遅延ストレージのインポートジョブが失敗した場合は、ソースストレージが災害発生前にインポート用のイメージの準備を完了しなかった可能性があります。その場合は、手順 6 を再度実行して、イメージのインポートを準備します。

シナリオ 3: MSDP サーバー名が変更されていて、ローカルストレージが失われておらず、NetBackup カタログがある

手順	タスク	手順詳細
1	古い MSDP サーバーから新しい MSDP サーバーにリカバリする場合は、古い MSDP サーバーが停止していることを確認します。	古い MSDP サーバーで、次のコマンドを実行します。 `/usr/openv/netbackup/bin/bp.kill_all`
2	新しいストレージサーバーを構成します。	プライマリサーバーで次のコマンドを実行します。 `/usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests -storage_server "storage server" -stype PureDisk -media_server "media server" -st 9` **メモ:** NetBackup Web UI からストレージサーバーを作成することもできます。
3	既存のローカルストレージパスを再利用します。	「「MSDP ローカルストレージの構成または再構成」」を参照

4	ストレージサーバーを再起動します。	プライマリサーバーで次のコマンドを実行します。
		`/usr/openv/netbackup/bin/bp.kill_all`
		`/usr/openv/netbackup/bin/bp.start_all`

5	クラウド LSU のディスクプールを作成します。	プライマリサーバーで次のコマンドを実行します。
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk | grep <LSU name> > /tmp/dvlist`
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name>`
		メモ: NetBackup Web UI からディスクプールを作成することもできます。

6	カタログイメージを更新します。	プライマリサーバーで次のコマンドを実行します。 `bpimage -newserver "new storage server" -oldserver "old storage server" -newdiskpool "new disk pool name" -olddiskpool "old disk pool name"`

手順	タスク	手順詳細
7	古いストレージサーバー関連の構成を削除します。	古い MSDP サーバーで、次のコマンドを実行します。 `/usr/openv/netbackup/bin/bp.start_all` 「MSDP ストレージサーバーのエラーからのリカバリ」のトピックにある、次の手順を実行します。p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。 ■ ディスクプールを使用するストレージユニットを削除します。 ■ ディスクプールを削除します。 ■ 重複排除ストレージサーバーを削除します。 ■ 重複排除ホストの構成ファイルを削除します。 ■ 重複排除サーバー上のクレデンシャルを削除します。

シナリオ 4: MSDP サーバー名が変更されていて、ローカルストレージが失われておらず、NetBackup カタログがない

手順	タスク	手順詳細
1	古いストレージサーバー関連の構成を削除します。	「MSDP ストレージサーバーのエラーからのリカバリ」のトピックにある、次の手順を実行します。p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。 ■ ディスクプールを使用するストレージユニットを削除します。 ■ ディスクプールを削除します。 ■ 重複排除ストレージサーバーを削除します。 ■ 重複排除ホストの構成ファイルを削除します。 ■ 重複排除サーバー上のクレデンシャルを削除します。
2	新しいストレージサーバーを構成します。	プライマリサーバーで次のコマンドを実行します。 `/usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests -storage_server "storage server" -stype PureDisk -media_server "media server" -st 9` **メモ:** NetBackup Web UI からストレージサーバーを作成することもできます。
3	既存のローカルストレージパスを再利用します。	「「MSDP ローカルストレージの構成または再構成」」を参照

4	ストレージサーバーを再起動します。	新しい MSDP サーバーで、次のコマンドを実行します。
		`/usr/openv/netbackup/bin/bp.kill_all`
		`/usr/openv/netbackup/bin/bp.start_all`

手順	タスク	手順詳細

5	クラウド LSU のディスクプールを作成します。	プライマリサーバーで次のコマンドを実行します。
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk | grep <LSU name> > /tmp/dvlist`
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name>`
		メモ: NetBackup Web UI からディスクプールを作成することもできます。

6	遅延の大きいストレージのインポート用にイメージを準備します。	ソースバージョンが 11.0 以降の場合、MSDP はイメージをバックグラウンドでインポートするための準備を自動的に行います。イメージのインポート準備ができるのを待ちます。次のコマンドを実行して状態を調べます。
		`tiermover --status --lsu <LSU name> [--client <client>] [--policy <policy>] [--backupid <backup ID>] [--sobins] [--active] [--lsulist] [--debug] [--verbose]`
		ソースバージョンが 11.0 より前であるか、ソースサーバーが停止してインポート前の操作が完了しなかった場合は、次のコマンドを実行してイメージのインポートを準備します。
		`tiermover --start --lsu <LSU name> --client <client> --policy <policy> [--backupid <backup ID>] [--retrieval Bulk|Standard|Expedited] [--verbose] [--debug]`
		メモ: イメージをインポートする準備が整っていない場合、インポートは失敗します。

7	イメージをインポートして戻します。	2 段階のインポートを実行します。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 ソースが 11.0 以降で高遅延ストレージの場合: 高遅延ストレージのインポートジョブが失敗した場合は、ソースストレージが災害発生前にインポート用のイメージの準備を完了しなかった可能性があります。その場合は、手順 6 を再度実行して、イメージのインポートを準備します。

シナリオ 5: MSDP サーバー名が変更されていて、ローカルストレージが失われており、NetBackup カタログがある

手順	タスク	手順詳細
1	新しいストレージサーバーを構成します。	プライマリサーバーで次のコマンドを実行します。 `/usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests -storage_server "storage server" -stype PureDisk -media_server "media server" -st 9` **メモ:** NetBackup Web UI からストレージサーバーを作成することもできます。
2	空のローカル LSU を作成します。	「「MSDP ローカルストレージの構成または再構成」」を参照
3	クラウド LSU を再利用します。	「「クラウド LSU の再利用」」を参照

4	クラウド LSU のディスクプールを作成します。	プライマリサーバーで次のコマンドを実行します。
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk | grep <LSU name> > /tmp/dvlist`
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name>`
		メモ: NetBackup Web UI からディスクプールを作成することもできます。

5	カタログイメージを更新します。	プライマリサーバーで次のコマンドを実行します。 `bpimage -newserver "new storage server" -oldserver "old storage server" -newdiskpool "new disk pool name" -olddiskpool "old disk pool name"`
6	古いストレージサーバー関連の構成を削除します。	古い MSDP サーバーで、次のコマンドを実行します。 `/usr/openv/netbackup/bin/bp.start_all` 「MSDP ストレージサーバーのエラーからのリカバリ」のトピックにある、次の手順を実行します。p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。 ■ ディスクプールを使用するストレージユニットを削除します。 ■ ディスクプールを削除します。 ■ 重複排除ストレージサーバーを削除します。 ■ 重複排除ホストの構成ファイルを削除します。 ■ 重複排除サーバー上のクレデンシャルを削除します。

シナリオ 6: MSDP サーバー名が変更されていて、ローカルストレージが失われており、NetBackup カタログがない

手順	タスク	手順詳細
1	古いストレージサーバー関連の構成を削除します。	「MSDP ストレージサーバーのエラーからのリカバリ」のトピックにある、次の手順を実行します。p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。 ■ ディスクプールを使用するストレージユニットを削除します。 ■ ディスクプールを削除します。 ■ 重複排除ストレージサーバーを削除します。 ■ 重複排除ホストの構成ファイルを削除します。 ■ 重複排除サーバー上のクレデンシャルを削除します。
2	新しいストレージサーバーを構成します。	プライマリサーバーで次のコマンドを実行します。 `/usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests -storage_server "storage server" -stype PureDisk -media_server "media server" -st 9` **メモ:** NetBackup Web UI からストレージサーバーを作成することもできます。
3	空のローカル LSU を作成します。	「「MSDP ローカルストレージの構成または再構成」」を参照
4	クラウド LSU を再利用します。	「「クラウド LSU の再利用」」を参照

5	クラウド LSU のディスクプールを作成します。	プライマリサーバーで次のコマンドを実行します。
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk | grep <LSU name> > /tmp/dvlist`
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name>`
		メモ: NetBackup Web UI からディスクプールを作成することもできます。

手順	タスク	手順詳細

6	遅延の大きいストレージのインポート用にイメージを準備します。	ソースバージョンが 11.0 以降の場合、MSDP はイメージをバックグラウンドでインポートするための準備を自動的に行います。イメージのインポート準備ができるのを待ちます。次のコマンドを実行して状態を調べます。
		`tiermover --status --lsu <LSU name> [--client <client>] [--policy <policy>] [--backupid <backup ID>] [--sobins] [--active] [--lsulist] [--debug] [--verbose]`
		ソースバージョンが 11.0 より前であるか、ソースサーバーが停止してインポート前の操作が完了しなかった場合は、次のコマンドを実行してイメージのインポートを準備します。
		`tiermover --start --lsu <LSU name> --client <client> --policy <policy> [--backupid <backup ID>] [--retrieval Bulk|Standard|Expedited] [--verbose] [--debug]`
		メモ: イメージをインポートする準備が整っていない場合、インポートは失敗します。

7	イメージをインポートして戻します。	2 段階のインポートを実行します。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 ソースが 11.0 以降で高遅延ストレージの場合: 高遅延ストレージのインポートジョブが失敗した場合は、ソースストレージが災害発生前にインポート用のイメージの準備を完了しなかった可能性があります。その場合は、手順 6 を再度実行して、イメージのインポートを準備します。

一般的なディザスタリカバリ手順

一般的なディザスタリカバリ手順を次に示します。

- 「MSDP ローカルストレージの構成または再構成」
- 「クラウド LSU の再利用」

MSDP ローカルストレージの構成または再構成

手順	タスク	手順詳細
1	重複排除の構成を削除します。	`/usr/openv/pdde/pdconfigure/scripts/installers/PDDE_deleteConfig.sh`

手順	タスク	手順詳細

2	負荷分散サーバー上の NetBackup 重複排除エンジンのクレデンシャルを削除します。	`/usr/openv/volmgr/bin/tpconfig -delete -storage_server <sts_hostname> -stype PureDisk -sts_user_id <user_id> -all_hosts`
		
		`/usr/openv/volmgr/bin/tpconfig -add -storage_server <sts_hostname> -stype PureDisk -sts_user_id <user_id> -password <your_passwd>`

3	コマンド出力をファイルにリダイレクトして、構成テンプレートを準備します。	`/usr/openv/netbackup/bin/admincmd/nbdevconfig -getconfig -storage_server <sts_hostname> -stype PureDisk >/root/local-lsu.txt`
		
		local-lsu.txt ファイルの内容
		
		`V7.5 "storagepath" " " string`
		`V7.5 "spalogin" " " string`
		`V7.5 "spapasswd" " " string`
		`....`
		`V7.5 "kmsservername" " " string`
		`V7.5 "keygroupname" " " string`
		`V7.5 "extendedcapabilities" " " string`
		`V7.5 "imagesharingincloud" "false" string`

4	構成テンプレートを生成します。	テンプレートファイル `local-lsu.txt` を変更し、不要な他のエントリをすべての削除します。
		
		パラメータ:
		
		`/root/local-lsu.txt`
		`V7.5 "storagepath" "/Storage" string`
		`V7.5 "spalogin" "my-user-name" string`
		`V7.5 "spapasswd" "my-password" string`
		`V7.5 "spalogretention" "90" int`
		`V7.5 "verboselevel" "3" int`
		
		パラメータについて詳しくは、p.193 の「MSDP ストレージサーバーの構成ファイルの編集」を参照してください。

5	ストレージパスを再利用または作成します。	`/usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig -storage_server sts_hostname -stype PureDisk -configlist /root/local-lsu.txt`

クラウド LSU の再利用

手順	タスク	手順詳細

1	クラウド LSU 構成を再利用する前に、LSU 名を取得します。	次のコマンドのいずれかを実行して、この MSDP サーバーで LSU (ディスクボリューム) を取得します。
		`/usr/openv/netbackup/bin/admincmd/nbdevquery -listdp -stype PureDisk -U`
		`/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype PureDisk -U`
		次に出力例を示します。
		`Disk Pool Name : my-aws-pool`
		`Disk Type : PureDisk`
		`Disk Volume Name : my-aws-lsu`
		ディスクボリューム名は LSU 名です。この例では、LSU 名は `my-aws-lsu` です。

2	テンプレートファイルを準備して保存します。	構成テンプレートの例 1:
		`V7.5 "operation" "reuse-lsu-cloud" string`
		`V7.5 "cmsCredName" "your-cms-cred-name" string`
		`V7.5 "lsuCloudAlias" "<storageserver_lsuname>" string`
		`V7.5 "lsuCloudBucketName" "bucket-name" string`
		`V7.5 "lsuCloudBucketSubName" "lsuname" string`
		`V7.5 "requestCloudCacheCapacity" "1017" string`
		暗号化が有効になっている構成テンプレートの例 2:
		`V7.5 "operation" "reuse-lsu-cloud" string`
		`V7.5 "cmsCredName" "your-cms-cred-name" string`
		`V7.5 "lsuCloudAlias" "<storageserver_lsuname>" string`
		`V7.5 "lsuCloudBucketName" "bucket-name" string`
		`V7.5 "lsuCloudBucketSubName" "lsuname" string`
		`V7.5 "lsuKmsServerName" "FQDN-KMS-server-host" string`
		`V7.5 "requestCloudCacheCapacity" "1017" string`

手順	タスク	手順詳細
3	lsuCloudAlias があるかどうかを確認します。	次のコマンドを実行してインスタンスを一覧表示し、lsuCloudAlias があるかどうかを確認します。 /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -i | grep <lsuname> エイリアスがない場合は、次のコマンドを実行してエイリアスを追加します。 /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in <cloud_privder_name> -sts <storageserver> -lsu_name <lsuname> [-storage_class <storage class or tier>] **メモ:** ストレージクラスは、ソースストレージサーバーでの LSU の初期構成時に選択されたストレージクラスと一致する必要があります。誤ったストレージクラスを指定すると、ジョブが失敗する場合があります。 次のコマンドを実行して、cloud_privder_name を見つけます。 /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -l
4	クラウド LSU の構成を再利用します。	各 LSU に対して次のコマンドを実行し、クラウド LSU を構成します。 /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig -storage_server <storageserver> -stype PureDisk -configlist /root/dr-lsu.txt
5	クラウドから spad/spoold メタデータをリカバリします。	各クラウド LSU で前の 4 つの手順を実行し、次のコマンドを実行します。 /usr/openv/pdde/pdcr/bin/cacontrol --catalog clouddr <lsuname> **メモ:** このコマンドを実行する時間はコンテナのサイズによって変わります。 次のコマンドを実行して、カタログのリカバリ状態を取得します。 /usr/openv/pdde/pdcr/bin/cacontrol --catalog clouddrstatus <lsuname>
6	ストレージサーバーを再起動します。	/usr/openv/netbackup/bin/bp.kill_all /usr/openv/netbackup/bin/bp.start_all

手順	タスク	手順詳細

7	MSDP のオンラインチェックを開始して refdb を再作成します。	`/usr/openv/pdde/pdcr/bin/pddecfg -a enabledataintegritycheck -d <dsid>`
		`/usr/openv/pdde/pdcr/bin/pddecfg -a startdatafullcheck -d <dsid>`
		`/usr/openv/pdde/pdcr/bin/crcontrol --processqueue --dsid <dsid>`
		メモ: -d オプションと --dsid オプションは省略可能なパラメータであり、クラウド LSU にのみ適用可能です。クラウド LSU の dsid 値を取得するには /usr/openv/pdde/pdcr/bin/pddecfg -a listcloudlsu を使用します。dsid 値が「0」に指定されている場合、ローカル LSU が処理されます。

p.477 の「クラウド LSU からの MSDP S3 IAM 構成のリカバリ」を参照してください。

Flex Scale でのクラウド LSU のディザスタリカバリ

NetBackup Flex Scale がサイトベースの災害からリカバリする際には、クラウド LSU のディザスタリカバリによってクラウド LSU のバックアップデータをリカバリできます。

クラウド LSU のディザスタリカバリ前の考慮事項:

- セカンダリ NetBackup Flex Scale の準備が完了していること。
  詳しくは、『NetBackup Flex Scale 管理者ガイド』にあるサイトベースのディザスタリカバリに関するセクションを参照してください。
- MSDP ストレージサーバーの準備が完了し、同じ構成になっていること。
- このクラウド LSU で MSDP KMS 暗号化が有効になっている場合は、KMS サーバーの準備が完了し、KMS サーバーのキーグループの準備が完了していること。

クラウド LSU のディザスタリカバリを実行するには

1. クラウドインスタンスエイリアスが存在しない場合は、次のコマンドを実行してエイリアスを追加します。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in <cloud_privder_name> -sts <storageserver> -lsu_name <lsuname>
   ```

2. NetBackup プライマリサーバーで、次のコマンドを実行してクラウド LSU を再利用します。ディザスタリカバリの前に使用したのと同じクレデンシャル、バケット名、サブバケットを使用します。

   ```
   /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig -storage_server <storageserver> -stype PureDisk -configlist <configuration file>
   ```

サンプル構成ファイル:

- このクラウド LSU で MSDP KMS 暗号化が有効になっている場合:

```
V7.5 "operation" "reuse-lsu-cloud" string
V7.5 "cmsCredName" "your-cms-cred-name" string
V7.5 "lsuCloudAlias" "<storageserver_lsuname>" string
V7.5 "lsuCloudBucketName" "bucket-name" string
V7.5 "lsuCloudBucketSubName" "lsuname" string
V7.5 "lsuKmsServerName" "FQDN-KMS-server-host" string
```

- このクラウド LSU で MSDP KMS 暗号化が無効になっている場合:

```
V7.5 "operation" "reuse-lsu-cloud" string
V7.5 "cmsCredName" "your-cms-cred-name" string
V7.5 "lsuCloudAlias" "<storageserver_lsuname>" string
V7.5 "lsuCloudBucketName" "bucket-name" string
V7.5 "lsuCloudBucketSubName" "lsuname" string
```

3 NetBackup プライマリサーバーで、ストレージサーバー名を取得します。ストレージサーバー名を持つエンジンコンテナで、次のコマンドを実行してクラウドからカタログを取得します。

```
/usr/openv/pdde/pdcr/bin/cacontrol --catalog clouddr <lsuname>
```

断続的なネットワークの問題によって失敗した場合は、このコマンドを再試行します。

4 クラスタを再起動します。

5 クラウド LSU のディスクプールを作成します。

6 2 段階のインポートを実行します。

p.288 の「クラウド LSU のディザスタリカバリについて」を参照してください。

Cohesity Alta Recovery Vault Azure ディザスタリカバリの追加手順

NetBackup 10.2 以降に対してディザスタリカバリを実行した後、Cohesity Alta Recovery Vault クレデンシャルの更新トークンが無効になる場合があります。これにより、Cohesity Alta Recovery Vault ボリュームを使用するジョブでエラーが発生する可能性があります。NetBackup Web UI のディスクプールの詳細ページ ([ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ディスクプール (Disk pools)]) に、[関連付けられたクレデンシャルを取得できません。(Unable to retrieve associated credentials.)]というエラーメッセージが表示されます。

この問題を解決するには、サポートに問い合わせて、ディスクボリュームに関連付けられている Cohesity Alta Recovery Vault クレデンシャルの新しい更新トークンを取得します。次に、NetBackup Web UI でクレデンシャルを置き換えます。

NetBackup Web UI でクレデンシャルを置き換えるには

1. 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
2. [指定したクレデンシャル (Named credential)]タブで、クレデンシャル名の右側にある[処理 (Actions)]メニューをクリックし、[編集 (Edit)]をクリックします。
3. [基本プロパティ (Basic properties)]ページで必要なすべての情報を入力し、[次へ (Next)]をクリックします。
4. [カテゴリ (Category)]ページで、ストレージアカウント名と、サポートが提供した新しい更新トークンを入力します。
5. [次へ (Next)]をクリックします。
6. [確認 (Review)]ページで、変更内容を確認して[完了 (Finish)]をクリックします。

MSDP クラウドを使用したイメージ共有について

オンプレミスの NetBackup サーバーから別の NetBackup サーバーにイメージを共有するには、イメージ共有を使用します。イメージ共有用に構成されている NetBackup サーバーは、CRS (クラウドリカバリサーバー) と呼ばれます。特定のシナリオでは、イメージ共有を使用して、バックアップされた VM を AWS インスタンスまたは Azure VHD として変換することもできます。

イメージ共有を備えた MSDP は、自己記述型のストレージサーバーです。イメージ共有を構成する際、NetBackup は、イメージのリカバリに必要なすべてのデータとメタデータをクラウドに格納します。

メモ: クラウドリカバリサーバーのバージョンは、オンプレミス NetBackup のバージョンと同じかそれ以降である必要があります。

次の表に、イメージ共有機能のワークフローを示します。

表 6-1 イメージ共有のワークフロー

作業	説明
クラウドリカバリサーバーを準備します。	クラウド環境に仮想マシンがあり、NetBackup がインストールされている必要があります。仮想マシンは、次のいずれかの方法を使用して配備できます。 ■ AWS Marketplace または Azure Marketplace を使用して仮想マシンを配備します。 ■ AWS Marketplace: 『Deploying NetBackup 10.0 from the AWS marketplace』を参照 ■ Azure Marketplace: 『Deploying NetBackup 10.0 from the Azure marketplace 』を参照 ■ オンデマンドで仮想マシンを配備します。 ■ 仮想マシンを作成します。 ■ NetBackup をインストールします 『NetBackup インストールガイド』を参照してください。 「イメージ共有を使用する前の考慮事項」
NetBackup KMS サーバーを構成します。	KMS 暗号化が有効になっている場合は、次のタスクを実行します。 ■ 「NetBackup KMS の場合のイメージ共有での KMS キーの手動転送」 ■ 「外部 KMS の場合にイメージ共有で行う手動の手順」
クラウドリカバリサーバーでイメージ共有を構成します。	イメージ共有用に構成された、クラウド上の NetBackup 仮想マシンは、クラウドリカバリサーバーと呼ばれます。イメージ共有を構成するには、次の手順を実行します。 ■ 「NetBackup Web UI による MSDP クラウドを使用したイメージ共有の構成」 ■ 「ims_system_config.py スクリプトによる MSDP クラウドを使用したイメージ共有の構成」
遅延の大きいストレージのインポート用にイメージを準備します。	この手順は、Amazon Glacier、Amazon Glacier Deep Archive、Azure Archive ストレージなどの遅延の大きいストレージにのみ適用されます。 「遅延の大きいストレージへのインポート用イメージの準備」

作業	説明
イメージ共有を使用します。	イメージ共有用にこの NetBackup 仮想マシンを構成した後は、オンプレミス環境からクラウドにイメージをインポートし、必要に応じてリカバリできます。また、VM を Azure の VHD や AWS の AMI に変換できます。 ■ 「NetBackup Web UI でのイメージ共有の使用」 ■ 「nbimageshare コマンドでのイメージ共有の使用」 ■ 「イメージ共有を使用して VM イメージを Azure の VHD に変換する前の考慮事項」 ■ 「Azure での VM イメージの VHD への変換」
イメージ共有についての追加情報を確認します。	「イメージ共有についての追加情報」

イメージ共有の重要な機能

- MSDP クラウドが重複排除されたデータのバックアップをクラウドに作成し、NetBackup カタログがオンプレミス NetBackup サーバーで利用できるとします。
  クラウドでのイメージ共有は、バックアップイメージとともに NetBackup カタログをアップロードするため、オンプレミス NetBackup サーバーなしでクラウドからデータをリストアできます。
- クラウドリカバリサーバーと呼ばれる NetBackup をオンデマンドで起動し、クラウドからバックアップイメージをリカバリできます。
- イメージ共有は、REST API、コマンドライン、Web UI のいずれかを使用してクラウドストレージに格納されたバックアップイメージを検出し、NetBackup カタログをリカバリしてイメージをリストアします。
- REST API としての機能を持つ、コマンドラインオプションまたは NetBackup Web UI を使用できます。
- インポートされた標準、MS Windows、ユニバーサル共有のバックアップイメージの場合、エクスポートされた共有は読み取り専用モードであるため、NetBackup インスタントアクセス API を使用してすぐにアクセスできます。インポートされた VMware イメージの場合は、エクスポートされた共有が読み取り専用モードであるため、VMware マルウェアスキャン API を使用して即座にスキャンできます。
  p.369 の「オブジェクトストレージのインスタントアクセスについて 」を参照してください。
- Veritas Alta Recovery Vault の場合、VM 変換手順では、一時バケットまたは Blob コンテナが自動的に作成されます。バケットの領域とセキュリティオプションは、イメージ共有サーバーの Veritas Alta Recovery Vault アカウントと同じです。
  一時バケットまたは Blob コンテナ名の形式は、*vrtsonvert-<timestamp>/VRTSConvert-<timestamp>*です。

- Veritas Alta Recovery Vault Amazon の場合、VM 変換の前に、IAM と EC2 関連の権限を持つ AWS アカウントで MSDP-C クレデンシャルを作成する必要があります。Veritas Alta Recovery Vault Azure の場合、VM 変換の前に、Azure の汎用ストレージアカウントで MSDP-C クレデンシャルを作成する必要があります。
- Veritas Alta Recovery Vault の場合、イメージのインポート機能のみが Veritas Alta Recovery Vault のクレデンシャルを使用します。VM イメージ変換を実行する前に、Azure/AWS アカウントのアクセスクレデンシャルを使用して MSDP-C クレデンシャルを作成していることを確認します。Recovery Vault ストレージは AMI または VHD の作成をサポートしていないため、VM イメージ変換には Azure/AWS アカウントのアクセスクレデンシャルが必要です。さらに、Azure サービスプリンシパルと AWS IAM Roles Anywhere の MSDP-C クレデンシャルは、Veritas Alta Recovery Vault を使用した VM 変換ではサポートされません。

イメージ共有を使用する前の考慮事項

- NetBackup をインストールする前に、SUSE Linux Enterprise または RHEL 7.3 以降をベースにしたインスタンスを作成します。また、SUSE Linux Enterprise または RHEL 7.3 以降をベースにしたコンピュータを設定することもできます。インスタンスには 64 GB を超えるメモリ、8 個を超える CPU を備えることをお勧めします。
- HTTPS ポート 443 を有効にします。
- ホスト名をサーバーの FQDN に変更します。
  Azure 仮想マシンでは、自動的に作成される内部ホスト名を変更する必要があります。IP アドレスから内部ホスト名を取得することはできません。
- 次の項目を `/etc/hosts` ファイルに追加します。
  "外部 IP" "サーバーの FQDN"
  "内部 IP" "サーバーの FQDN"
  コンピュータの場合、次の項目を `/etc/hosts` ファイルに追加します。
  "IP アドレス" "サーバーの FQDN"
- (省略可能) インスタンスでは、内部ドメインの前に外部ドメインを検索するように、`/etc/resolv.conf` ファイルでドメインの検索順序を変更します。
- 新しいイメージ共有サーバーの場合、NGINX がインストールされ、実行されていることを確認します。
  Red Hat Software Collections から NGINX をインストールします。手順については、https://www.softwarecollections.org/en/scls/rhscl/rh-nginx114/ を参照してください。
  パッケージ名は NGINX のバージョンによって異なります。`yum search rh-nginx` を実行して、最新バージョンが利用可能かどうかを確認します(NetBackup 8.3 では、NGINX を Red Hat Software Collections からインストールする場合は EEB が必要です)。

NGINXをインストールして有効にする前にイメージ共有用のストレージサーバーを構成する場合は、NGINXをインストールして有効にした後、ストレージサーバーで次のコマンドを実行します。

```
/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo
```

NetBackup Web UI による MSDP クラウドを使用したイメージ共有の構成

NetBackup Web UI にアクセスして、イメージ共有を使用できます。詳しくは、『NetBackup Web UI 管理者ガイド』で、イメージ共有のためのメディアサーバー重複排除プール (MSDP) ストレージサーバーの作成に関するトピックを参照してください。

ims_system_config.py スクリプトによる MSDP クラウドを使用したイメージ共有の構成

NetBackup をインストールした後に、ims_system_config.py スクリプトを実行してイメージ共有を構成できます。

コマンドにアクセスするためのパスは /usr/openv/pdde/pdag/scripts/ です。

アマゾンウェブサービスクラウドプロバイダ:

```
ims_system_config.py -t PureDisk -k <AWS_access_key> -s
<AWS_secret_access_key> -b <name_S3_bucket> -bs <bucket_sub_name>
[-r <bucket_region>] [-p <mount_point>] [-sc <storage class>]
```

EC2 インスタンスで IAM ロールを構成している場合は、次のコマンドを使用します。

```
ims_system_config.py  -t PureDisk -k dummy -s dummy <bucket_name>
-bs <bucket_sub_name> [-r <bucket_region>] [-p <mount_point>]
```

Microsoft Azure クラウドプロバイダ:

```
ims_system_config.py -cp 2 -k <key_id> -s <secret_key> -b
<container_name> -bs <bucket_sub_name> [-p <_mount_point_>] [-sc
<storage tier>]
```

その他の S3 対応クラウドプロバイダ (Hitachi HCP など):

NetBackup にクラウドインスタンスが存在している場合は、次のコマンドを使用:

```
ims_system_config.py -cp 3 -t PureDisk -k <key_id> -s <secret_key>
-b <bucket_name> -bs <bucket_sub_name> -c <Cloud_instance_name> [-p
 <mount_point>]
```

または、次のコマンドを使用:

```
ims_system_config.py -cp 3 -t PureDisk -k <key_id> -s <secret_key>
-b <bucket_name> -pt <cloud_provider_type> -sh <s3_hostname> -sp
```

<*s3_http_port*> -sps <*s3_https_port*> -ssl <*ssl_usage*> [-p <*mount_point*>]

HCP プロバイダの例:

```
ims_system_config.py -cp 3 -t PureDisk -k xxx -s xxx -b emma -bs
subtest -pt hitachicp  -sh yyy.veritas.com -sp 80 -sps 443 -ssl 0
```

説明: (HCP クラウドを使用するには、次のオプションを指定します)

-cp 3: 使用するサードパーティの S3 クラウドプロバイダを指定します。

-pt hitachicp: クラウドプロバイダ形式を hitachicp (HCP LAN) と指定します。

-t PureDisk: ストレージサーバーの種類として PureDisk を指定します。

-sh <s3_hostname>: HCP ストレージサーバーのホスト名を指定します。

-sp <s3_http_port>: HCP ストレージサーバーの HTTP ポートを指定します (デフォルトは 80 です)。

-sps <s3_https_port>: HCP ストレージサーバーの HTTP ポートを指定します (デフォルトは 443 です)。

-ssl <ssl_usage>: SSL を使用するかどうかを指定します (0: SSL を無効にします。1: SSL を有効にします。デフォルトは 1 です) SSL を無効にすると、<s3_http_port> を使用して <s3_hostname> に接続します。それ以外の場合は、<s3_https_port> を使用します。

メモ: ims_system_config.py スクリプトによる MSDP クラウドを使用したイメージ共有の構成は、SUSE Linux Enterprise ではサポートされません。SUSE Linux Enterprise の MSDP クラウドを使用してイメージ共有を構成するには、NetBackup Web UI を使用します。

遅延の大きいストレージへのインポート用イメージの準備

Amazon Glacier、Amazon Glacier Deep Archive、Azure Archive ストレージなどの遅延の大きいストレージにイメージ共有を使用している場合は、クラウドストレージにインポートする前にイメージを準備する必要があります。ソースバージョンが 11.0 以降の場合、MSDP はイメージをバックグラウンドでインポートするための準備を自動的に行います。

遅延の大きいストレージへのインポート用イメージを準備する方法

1. ソースバージョンが 11.0 より前であるか、ソースサーバーが停止してインポート前の操作が完了しなかった場合は、次のコマンドを実行してイメージのインポートを準備します。

   ```
   tiermover --start --lsu <LSU name> --client <client> --policy
   <policy> [--backupid <backup ID>] [--retrieval
   Bulk|Standard|Expedited] [--verbose] [--debug]
   ```

2. ソースバージョンが 11.0 以降の場合、MSDP はイメージをバックグラウンドでインポートするための準備を自動的に行います。イメージのインポート準備ができるのを待ちます。次のコマンドを実行して状態を調べます。

   ```
   tiermover --status --lsu <LSU name> [--client <client>] [--policy
   <policy>] [--backupid <backup ID>] [--sobins] [--active]
   [--lsulist] [--debug] [--verbose]
   ```

メモ: イメージをインポートする準備が整っていない場合、インポートは失敗します。

NetBackup Web UI でのイメージ共有の使用

NetBackup Web UI にアクセスして、イメージ共有を使用できます。詳しくは、『NetBackup Web UI 管理者ガイド』の「オンプレミスの場所からクラウドへのイメージの共有」のトピックを参照してください。

`nbimageshare` コマンドでのイメージ共有の使用

`nbimageshare` コマンドを使用して、イメージ共有を設定できます。

仮想マシンと標準イメージを一覧表示してインポートし、仮想マシンをリカバリするには、`nbimageshare` コマンドを実行します。

コマンドにアクセスするパスは `/usr/openv/netbackup/bin/admincmd/` です。

`nbimageshare` 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。

次の表は、イメージ共有の手順とコマンドオプションの一覧です。

表 6-2　　イメージ共有の手順とコマンドオプション

手順	コマンド

NetBackup にログオンします。	`nbimageshare --login <username> <password>`
	
	`nbimageshare --login -interact`

手順	コマンド
クラウドにあるすべてのバックアップイメージを一覧表示します。	`nbimageshare --listimage <LSU name> <MSDP image sharing server>` **メモ:** イメージの一覧では、増分スケジュール形式が差分増分バックアップまたは累積増分バックアップと表示される場合があります。

バックアップイメージを NetBackup にインポートします。	1 つのイメージのインポート:
	
	`nbimageshare --singleimport <client> <policy> <backupID> <LSU name> <MSDP image sharing server>`
	
	複数のイメージのインポート:
	
	`--batch-import <image list file path> <LSU name> <MSDP image sharing server>`
	
	メモ: `image_list_file_path` の形式は、「イメージの一覧表示」の出力と同じです。
	
	複数のイメージをインポートできます。100 個のイメージごとに新しいインポートジョブが作成されます。
	
	すでにインポートされたイメージをインポートできます。この処理は NetBackup イメージカタログには影響しません。

手順	コマンド

VM を AWS EC2 AMI または Azure の VHD としてリカバリします。	`nbimageshare --recovervm <LSU name> <MSDP image sharing server>`
	
	■ VM イメージのみがサポートされます。
	■ このコマンドは、Veritas Alta Recovery Vault をサポートしていません。
	■ Azure の場合、アカウントは Azure 汎用ストレージアカウントである必要があります。
	■ AWS の場合、AWS アカウントには S3 に対する次の読み取り権限と書き込み権限が必要です。
	
	`"ec2:CreateTags"`
	`"ec2:DescribeImportImageTasks"`
	`"ec2:ImportImage"`
	`"ec2:DescribeImages"`
	`"iam:ListRolePolicies"`
	`"iam:ListRoles"`
	`"iam:GetRole"`
	`"iam:GetRolePolicy"`
	`"iam:CreateRole"`
	`"iam:PutRolePolicy"`

NetBackup KMS の場合のイメージ共有での KMS キーの手動転送

KMS 暗号化が有効になっている場合は、KMS キーを手動で転送して、クラウドストレージ内のイメージをクラウドリカバリサーバーに共有できます。

オンプレミス側:

1. ストレージサーバー: 指定されたストレージサーバーのキーグループ名を検索します。

   場所 `/etc/pdregistry.cfg` で `contentrouter.cfg` を検索します。

   キーグループ名の検索場所は `[KMSOptions]` の下の `contentrouter.cfg` です。

   (例 `KMSKeyGroupName=amazon.com:test1`)

2. NetBackup プライマリサーバー: パスフレーズを含むキーグループをファイルにエクスポートします。

   ```
   /usr/openv/netbackup/bin/admincmd/nbkmsutil -export -key_groups
   <key-group-name> -path <key file path>
   ```

クラウドリカバリサーバー (クラウド側):

1. クラウドリカバリサーバーに、エクスポートされたキーをコピーします。

2. KMS サーバーを構成します。

```
/usr/openv/netbackup/bin/nbkms -createemptydb
/usr/openv/netbackup/bin/nbkms
/usr/openv/netbackup/bin/nbkmscmd -discovernbkms -autodiscover
```

3. KMS サービスにキーをインポートします。

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -import -path <key
file path> -preserve_kgname
```

4. NetBackup Web UI または `ims_system_config.py` を使用してクラウドリカバリサーバーを構成します。

オンプレミス KMS キーの変更:

クラウドリカバリサーバーを設定した後に、オンプレミスストレージサーバーの特定のグループの KMS キーを変更した場合は、オンプレミス KMS サーバーからキーファイルをエクスポートして、そのキーファイルをクラウドリカバリサーバーにインポートする必要があります。

1. オンプレミス NetBackup プライマリサーバー:

   パスフレーズを含むキーグループをファイルにエクスポートします。

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -export -key_groups
<key-group-name> -path <key file path>
```

2. クラウドリカバリサーバー:

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -deletekg -kgname
<key-group-name> -force
```

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -import -path <key
file path> -preserve_kgname
```

外部 KMS の場合にイメージ共有で行う手動の手順

外部 KMS サーバーのキーを使用するようにオンプレミスストレージサーバーが構成されている場合は、`ims_system_config.py` を実行する前に、クラウドリカバリサーバーで同じ KMS サーバーが設定されていることを確認します。NetBackup での外部 KMS サーバー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。

特定のポートのクラウドリカバリサーバーから外部 KMS サーバーに接続できることを確認してください。

イメージ共有についての追加情報

- オンデマンドでクラウドリカバリサーバーを起動し、アップグレードはしないことをお勧めします。
- nbdevconfig を使用してイメージ共有サーバーでクラウド LSU を変更したり、新しいクラウド LSU を追加したりしないでください。イメージ共有サーバー (クラウドリカバリサーバー) で問題が発生する可能性があります。イメージ共有サーバーを構成した後にオンプレミス側で KMS 暗号化を有効にすると、暗号化されたイメージはこのイメージ共有サーバーではインポートできません。
- クラウド LSU に空きディスク容量が必要です。ims_system_config.py script スクリプトを使用してイメージ共有を設定する場合、デフォルトのマウントポイントやストレージに十分なディスク容量があることを確認してください。または、ims_system_config.py の -p パラメータを使用して、空きディスク容量の要件を満たす別のマウントポイントを指定できます。
- イメージがイメージ共有サーバーにインポートされると、イメージ共有サーバーにイメージカタログが格納されます。オンプレミス NetBackup ドメインでイメージが期限切れになると、イメージ共有サーバーにイメージカタログが存在しても、イメージ共有へのイメージのリストアは失敗します。
- インポートされたイメージの有効期限は、インポートされたイメージカタログがイメージ共有サーバーに存在する時間です。イメージ共有サーバーでイメージが期限切れになると、イメージ共有サーバーにあるイメージカタログは削除されますが、クラウドストレージ内のイメージデータは削除されません。
- イメージ共有サーバーにインポートした任意のイメージをリストアできます。AWS と Azure の VM イメージは、AWS で EC2 インスタンスに、または Azure で VHD に変換できるため、これらの VM イメージのみリカバリできます。他のクラウドストレージの VM イメージは変換できず、リストアのみ可能です。完全バックアップイメージまたはアクセラレータが有効な増分バックアップイメージの VM イメージのみ、リカバリできます。
- イメージ共有は、さまざまなポリシー形式をサポートしています。
  サポートされているポリシー形式の最新情報については、NetBackup の互換性リストを参照してください。
- イメージ共有を構成した後、ストレージサーバーは読み取り専用になります。一部の MSDP コマンドはサポートされません。
- AWS における VM のリカバリの制限事項について詳しくは、AWS のヘルプで AWS VM のインポート情報を参照してください。
- イメージをクラウドストレージにインポートするときに、実行中のジョブの最大数を設定できます。
  ファイルパス /usr/openv/var/global/wsl/config/web.conf を変更し、imageshare.maxActiveJobLimit として構成項目を追加します。

たとえば、imageshare.maxActiveJobLimit=16 を追加します。
デフォルト値は 16 で、設定可能な範囲は 1 から 100 です。
インポート要求が行われ、実行中のジョブ数が構成された制限を超えると、次のメッセージが表示されます。
「現在実行中のジョブ数が実行中ジョブ数の上限を超えています。(Current active job count exceeded active job count limitation.)」

- クラウドストレージのイメージを共有できます。Amazon Glacier、Deep Archive、Azure Archive が有効になっている場合、11.0 より前のバージョンを実行しているストレージサーバーでイメージ共有は使用できません。
- Amazon Glacier、Deep Archive、または Azure Archive が有効になっていて、LSU が Cloud Catalyst から以前に移行された場合、イメージ共有は使用できません。
- AWS でのロールポリシーのサイズの制限事項に関するエラーについて:
  ロールポリシーのサイズが最大サイズを超えた場合に発生するエラーは、AWS の制限事項です。失敗したリストアジョブでは、次のエラーを確認できます。

  ```
  "error occurred (LimitExceeded) when calling the PutRolePolicy
  operation:
  Maximum policy size of 10240 bytes exceeded for role vmimport"
  ```

  回避方法:

  - vmimport ロールのポリシーの最大サイズ制限を変更できます。
  - 次のコマンドを使用して、既存のポリシーを一覧表示して削除できます。

    ```
    aws iam list-role-policies --role-name vmimport
    aws iam delete-role-policy --role-name vmimport --policy-name
    <bucketname> -vmimport
    ```

- AWS プロバイダとのリカバリ操作には AWS のインポート処理が含まれています。したがって、同時に 2 つのリストアジョブでは vmdk イメージをリカバリできません。
- AWS のイメージ共有機能では、アマゾンウェブサービスの VM のインポートに関する前提条件を満たしている仮想マシンをリカバリできます。
  前提条件について詳しくは、次の記事を参照してください。
  https://docs.aws.amazon.com/vm-import/latest/userguide/vmie_prereqs.html
- Windows OS が搭載された AWS EC2 インスタンスを使用するための管理者パスワードを取得できない場合、次のエラーが表示されます。

  ```
  Password is not available. This instance was launched from a custom
  AMI, or the default password has changed. A password cannot be
  retrieved for this instance. If you have forgotten your password,
  you can reset it using the Amazon EC2 configuration service. For
  more information, see Passwords for a Windows Server Instance.
  ```

このエラーは、イメージ共有を使用して変換した AMI からインスタンスを起動した後に発生します。

詳しくは、次の記事を参照してください。

- Amazon Elastic Compute Cloud の一般的なメッセージ
- ADMT を使用して AWS の管理対象 Microsoft AD にオンプレミスドメインを移行する方法

- クラウドリカバリサーバーのインポートジョブは取り消せません。
- オンプレミスイメージでデータ最適化が行われている場合、クラウドリカバリサーバーにインポートしたイメージをリストアできない場合があります。イメージを期限切れにして、イメージ共有サーバーに再度インポートしてから、イメージをリストアできます。
- バックアップジョブ、複製ジョブ、または AIR インポートジョブが完了した後、クラウドリカバリサーバーにイメージをインポートできます。ユーザーアーカイブジョブによって作成されるイメージはインポートできません。
- AIR はイメージ共有サーバーではサポートされません。
- VM イメージを再び変換する場合は、Azure Blob から VHD を削除する必要があります。

イメージ共有を使用して VM イメージを Azure の VHD に変換する前の考慮事項

Azure プロバイダとのイメージ共有では、VMware 仮想マシンから Azure VHD への変換がサポートされています。この Azure VHD は、Azure ストレージ Blob にアップロードされます。Azure Web ポータルを使用して、VHD に基づいて VM を作成できます。イメージ共有では VM 変換に関する追加の制限事項はありませんが、Azure にはソース VM に関して次の前提条件があります。

- ソース仮想マシンの OS の種類
  ソース仮想マシンでは、次のゲストオペレーティングシステムがサポートされます。
  - Windows 10 シリーズ
  - Windows 2012 R2 シリーズ
  - Windows 2016 シリーズ
  - Windows 2019 シリーズ
  - Windows 2022 シリーズ
  - RHEL 7.6、7.7、7.9、8.6
  - Ubuntu 18.04
  - SUSE 12SP4、15SP4

その他のオペレーティングシステムについては、「サポートされているプラットフォーム」を参照してください。
動作保証外のディストリビューションについては、VM を変換する前に、ソース VM が動作保証外のディストリビューションの要件を満たしていることを確認してください。この確認が重要であるのは、Microsoft Azure の動作保証済みディストリビューションに基づく Linux VM は Azure 上で実行するための前提条件を備えているのに対し、他の Hypervisor で作成された VM はそうでない可能性があるためです。詳しくは、「動作保証外のディストリビューションに関する情報」を参照してください。

- ソース仮想マシンの Hyper-V ドライバ
  Linux の場合、ソース VM には次の Hyper-V ドライバが必要です。
  - hv_netvsc.ko
  - hv_storvsc.ko
  - hv_vmbus.ko

  必要なカーネルモジュールが初期 ramdisk で利用可能になるように、initrd の再作成が必要な場合があります。initrd または initramfs イメージを再作成するためのメカニズムは、ディストリビューションによって異なる場合があります。多くのディストリビューションでは、これらの組み込みドライバはすでに利用可能です。Red Hat または CentOS では、組み込みドライバが機能しない場合に最新の Hyper-V ドライバ (LIS) が必要になる場合があります。詳しくは、「Linux カーネルの要件」を参照してください。
  たとえば、CentOS または Red Hat を実行する Linux ソース VM のバックアップを実行する前に、必要な Hyper-V ドライバがソース VM にインストールされていることを確認します。これらのドライバは、変換後に VM を起動するためにソース VM バックアップ上に存在する必要があります。
  - ソース VM のスナップショットを作成します。
  - 次のコマンドを実行して、ブートイメージを変更します。
    ```
    sudo dracut -f -v -N
    ```
  - 次のコマンドを実行して、Hyper-V ドライバがブートイメージ内に存在することを確認します。
    ```
    lsinitrd | grep hv
    ```
  - 次の行が含まれている dracut conf ファイル (たとえば `/usr/lib/dracut/dracut.conf.d/01-dist.conf`) がないことを確認します。
    ```
    hostonly="yes"
    ```
  - 変換に使用する新しいバックアップを実行します。
- ディスク

- ソース VM の OS は、ソース VM の最初のディスクにインストールされます。オペレーティングシステムディスクにスワップパーティションを構成しないようにしてください。「動作保証外のディストリビューションに関する情報」を参照してください。
- 変換された VHD によって作成された新しい VM に接続された複数のデータディスクは、Windows ではオフライン状態になり、Linux ではマウント解除されます。これらのデータディスクは変換後に手動でオンラインにしてマウントする必要があります。
- 変換された VHD で VM を作成した後、VM のサイズによってサイズが決まる追加の一時ストレージディスクが 1 つ、Azure によって Linux と Windows の両方のシステムに追加される場合があります。詳しくは、「Azure VM の一時ディスク」を参照してください。

- ネットワーク
  ソース VM に複数のネットワークインターフェースがある場合、変換された VHD によって作成される新しい VM で利用可能になるインターフェースは 1 つだけです。
  Linux: 動作保証済みの Linux ディストリビューションでは、ソース VM のプライマリネットワークインターフェースの名前を eth0 にする必要があります。名前が eth0 にされていない場合、変換された VHD によって作成される新しい VM に接続できず、変換された VHD でいくつかの手順を手動で実行する必要があります。詳しくは、「ネットワーク経由で Azure Linux VM に接続できない」を参照してください。
  Windows: ソース VM でリモートデスクトッププロトコル (RDP) を有効にします。一部の Windows システムではソース VM のファイアウォールを無効にする必要があります。そうしないと、リモートで接続できません。
- Azure アカウント
  VMDK を VHD に変換する場合、MSDP クラウドを使用するイメージ共有の Azure アカウントは、Azure 汎用ストレージアカウントである必要があります。「ストレージアカウントの概要」を参照してください。

メモ: VM の変換では、イメージ共有ボリュームが Veritas Alta Recovery Vault の場合、アクセスクレデンシャルのみがサポートされ、Azure サービスプリンシパルまたは AWS IAM Anywhere のクレデンシャルはサポートされません。

Azure での VM イメージの VHD への変換

イメージ共有を使用して、Azure で次の VM イメージを VHD に変換できます。

表 6-3 VM イメージの VHD への変換

VM イメージのオペレーティングシステム	説明
Windows VM	p.317 の「Windows VM イメージの VHD への変換 」を参照してください。

VM イメージのオペレーティングシステム	説明
RHEL 7.6 VM	p.317 の「RHEL 7.6 VM イメージの VHD への変換 」を参照してください。
SUSE 12 SP4 VM	p.320 の「SUSE 12 SP4 VM イメージの VHD への変換」を参照してください。
RHEL 8.6 VM	p.322 の「RHEL 8.6 VM イメージの VHD への変換 」を参照してください。
SLES 15 SP4 VM	p.324 の「SLES 15 SP4 VM イメージの VHD への変換 」を参照してください。

Windows VM イメージの VHD への変換

Windows VM イメージを VHD に変換するには

1. バックアップ前に対象のソース VM でリモートデスクトップ接続を有効にしてください。
2. ソース VM の新しい完全バックアップを実行します。
3. イメージ共有サーバーを準備し、Azure アカウントでイメージ共有機能を構成します。
4. バックアップイメージをインポートし、変換を実行します。
5. 変換された vhd ファイルを確認します。

   Azure Web ポータルで、以下を実行します。

   - 変換された .vhd ファイルを使ってディスクを作成します。
   - 以前のディスクを使用して VM を作成します。
     [ディスク]>[作成されたディスク (Created disk)]>[VM の作成]の順に移動します。デフォルトのネットワーク設定、ディスク設定、管理設定で、ブート診断を有効にします。
   - 変換された VM に RDP 経由でログインします。

RHEL 7.6 VM イメージの VHD への変換

前提条件:

- ソース VM OS ボリュームでは、GPT ではなく MBR パーティション分割を使用する必要があります。
- `fstab` 構成では永続的な命名規則 (ファイルシステムラベルまたは UUID) を使用します。

ほとんどのディストリビューションでは、`fstab nofail` パラメータまたは `nobootwait` パラメータが提供されます。これらのパラメータにより、起動時にディスクのマウントが失敗した場合にシステムがブートできます。

- オペレーティングシステムがソース VM の最初のディスクにインストールされていることを確認します。オペレーティングシステムディスクにスワップパーティションを構成しないようにしてください。「動作保証外のディストリビューションに関する情報」を参照してください。
- ソース VM のネットワークインターフェースで DHCP を使用し、ブート時に有効にすることをお勧めします。Azure ネットワークインターフェースの IP アドレスの追加、変更、削除を参照してください。
- Azure 用の Red Hat ベースの仮想マシンの準備を参照してください。

RHEL 7.6 VM イメージを VHD に変換するには

1 最新の LIS 4.3.5 をインストールします。

```
tar -xzf lis-rpms-4.3.5.x86_64.tar.gz

cd LISISO

./install

reboot
```

2 initramfs イメージファイルを再作成します。

```
cd /boot

cp initramfs-`uname -r`.img initramfs-`uname -r`.img.bak
```

次のコマンドを実行して dracut.conf ファイルを開きます。

```
vi /etc/dracut.conf
```

#add_drivers+="" の行のコメントアウトを解除します。

この行に、各モジュールをスペースで区切って次のドライバを追加します。

```
hv_netvsc hv_storvsc hv_vmbus
```

例:

```
# additional kernel modules to the default.
add_drivers+="hv_netvsc hv_storvsc hv_vmbus"
```

新しいモジュールを含む、新しい初期 ramdisk イメージを作成します。

```
dracut -f -v -N
```

次のコマンドのいずれかを実行して、新しい初期 ramdisk イメージに新しいモジュールが存在するかどうかを確認します。

```
lsinitrd | grep -i hv

lsinitrd -f /boot/initramfs-`uname -r`.img | grep -i hv

modinfo hv_netvsc hv_storvsc hv_vmbus
```

3 ネットワークインターフェースの名前を eth0 に変更し、ブート時に有効にします。

ネットワークインターフェースの構成ファイルで、ONBOOT=yes を構成します。

次に例を示します。

```
mv /etc/sysconfig/network-scripts/ifcfg-ens192
/etc/sysconfig/network-scripts/ifcfg-eth0
```

```
sed -i 's/ens192/eth0/g' /etc/sysconfig/network-scripts/ifcfg-eth0
```

/etc/default/grub ファイルで、行 GRUB_CMDLINE_LINUX="xxxxxxx" を GRUB_CMDLINE_LINUX="xxxxxxx net.ifnames=0 biosdevname=0" に変更します。

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

4 ソース VM の新しい完全バックアップを実行します。

5 イメージ共有サーバーを準備し、Azure アカウントでイメージ共有機能を構成します。

6 バックアップイメージをインポートし、変換を実行します。

7 変換された vhd ファイルを確認します。

Azure Web ポータルで、以下を実行します。

- 変換された .vhd ファイルを使ってディスクを作成します。
- 以前のディスクを使用して VM を作成します。
  [ディスク]>[作成されたディスク (Created disk)]>[VM の作成]の順に移動します。デフォルトのネットワーク設定、ディスク設定、管理設定で、ブート診断を有効にします。
- 変換された VM に RDP 経由でログインします。

SUSE 12 SP4 VM イメージの VHD への変換

前提条件:

- ソース VM OS ボリュームでは、GPT ではなく MBR パーティション分割を使用する必要があります。
- fstab 構成では永続的な命名規則 (ファイルシステムラベルまたは UUID) を使用します。
  ほとんどのディストリビューションでは、fstab nofail パラメータまたは nobootwait パラメータが提供されます。これらのパラメータにより、起動時にディスクのマウントが失敗した場合にシステムが起動できます。
- オペレーティングシステムがソース VM の最初のディスクにインストールされていることを確認します。オペレーティングシステムディスクにスワップパーティションを構成し

ないようにしてください。「動作保証外のディストリビューションに関する情報」を参照してください。

- ソース VM のネットワークインターフェースで DHCP を使用し、ブート時に有効にすることをお勧めします。Azure ネットワークインターフェースの IP アドレスの追加、変更、削除を参照してください。

SUSE 12 SP4 VM イメージを VHD に変換するには

1. 必要なモジュールがインストールされていることを確認します。
   - `lsinitrd -f /boot/initramfs-`uname -r`.img | grep -i hv`
     または
     `modinfo hv_vmbus hv_storvsc hv_netvsc`
     `reboot`
   - `initrd` を再作成します。
     `cd /boot/`
     `cp initrd-$(uname -r) initrd-$(uname -r).backup`
     `mkinitrd -v -m "hv_vmbus hv_netvsc hv_storvsc" -f`
     `/boot/initrd-$(uname -r) $(uname -r)`
2. ネットワークインターフェースの名前が eth0 で、ブート時に有効であることを確認します。
   /etc/sysconfig/network/ifcfg-eth0 にはレコードが含まれています。
   `STARTMODE='auto'`
3. ソース VM の新しい完全バックアップを実行します。
4. イメージ共有サーバーを準備し、Azure アカウントでイメージ共有機能を構成します。
5. バックアップイメージをインポートし、変換を実行します。
6. 変換された vhd ファイルを確認します。
   Azure Web ポータルで、以下を実行します。
   - 変換された .vhd ファイルを使ってディスクを作成します。
   - 以前のディスクを使用して VM を作成します。
     [ディスク]>[作成されたディスク (Created disk)]>[VM の作成]の順に移動します。デフォルトのネットワーク設定、ディスク設定、管理設定で、ブート診断を有効にします。
   - 変換された VM に RDP 経由でログインします。

RHEL 8.6 VM イメージの VHD への変換

前提条件:

- ソース VM のブートオプションは BIOS または UEFI です。多くのインストールのデフォルトである LVM (論理ボリュームマネージャ) ではなく、標準パーティションを使用します。
- `fstab` 構成では永続的な命名規則 (ファイルシステムラベルまたは UUID) を使用します。
- オペレーティングシステムがソース VM の最初のディスクにインストールされていることを確認します。オペレーティングシステムディスクにスワップパーティションを構成しないようにしてください。
- ソース VM のネットワークインターフェースで DHCP を使用し、起動時に有効にすることをお勧めします。

「Azure 用の Red Hat ベースの仮想マシンの準備」を参照してください

RHEL 8.6 VM イメージを VHD に変換するには

1 Hyper-V デバイスドライバをインストールし、`initramfs` イメージファイルを再構築します。

Hyper-V ドライバ (hv_netvsc、hv_storvsc、hv_vmbus) がインストールされているかどうかを確認します。

```
lsinitrd | grep hv
```

インストールされていない場合は、次の手順を実行します。

- 以前の `initramfs` イメージファイルをバックアップします。

```
cd /boot
cp initramfs-`uname -r`.img initramfs-`uname -r`.img.bak
```

- `/etc/dracut.conf.d` ディレクトリの下に `hv.conf` ファイルを作成します。`hv.conf` ファイルに次のドライバパラメータを追加します。

```
add_drivers+=" hv_vmbus "
add_drivers+=" hv_netvsc "
add_drivers+=" hv_storvsc "
add_drivers+=" nvme "
```

メモ: 引用符とドライバ名の間にスペースを追加します。

- 新しいモジュールを含む、新しい初期 ramdisk イメージを作成します。

```
dracut -f -v -N -regenerate-all
```

新しい初期 ramdisk イメージに新しいモジュールが存在するかどうかを確認します。

```
lsinitrd | grep -i hv
```

2 ネットワークインターフェースの名前を eth0 に変更し、ブート時に NIC を有効にします。

Azure Linux VM はデフォルトで従来の NIC 名を使用します。

ネットワークインターフェースの構成ファイルで、ONBOOT=yes を構成します。

次に例を示します。

```
mv /etc/sysconfig/network-scripts/ifcfg-ens192
/etc/sysconfig/network-scripts/ifcfg-eth0 sed -i 's/ens192/eth0/g'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

3 カーネルブートオプションの grub.cfg を再生成します。

- /etc/default/grub ファイルで従来の NIC 名を使用するには、行 GRUB_CMDLINE_LINUX="xxxxxxx" を GRUB_CMDLINE_LINUX="xxxxxxx net.ifnames=0" に変更します。
  次のパラメータが存在する場合は削除します。rhgb quiet crashkernel=auto
- grub.cfg ファイルを再生成します。
  BIOS ベースのコンピュータの場合: grub2-mkconfig -o /boot/grub2/grub.cfg
  UEFI ベースのコンピュータの場合: grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg

4 ソース VM の新しい完全バックアップを実行します。

5 イメージ共有サーバーを準備し、Azure アカウントでイメージ共有機能を構成します。

6 バックアップイメージをインポートし、変換を実行します。

7 変換された VHD ファイルを確認します。

Azure Web ポータルで、以下を実行します。

- 変換された .vhd ファイルを使ってディスクを作成します。
- 以前のディスクを使用して VM を作成します。
  [ディスク]、[作成されたディスク]、[VM の作成]の順に移動します。デフォルトのネットワーク設定、ディスク設定、管理設定で、ブート診断を有効にします。
- 変換された VM に SSH 経由でログインします。

SLES 15 SP4 VM イメージの VHD への変換

前提条件:

- ソース VM のブートオプションは BIOS または UEFI です。多くのインストールのデフォルトである LVM (論理ボリュームマネージャ) ではなく、標準パーティションを使用します。
- `fstab` 構成では永続的な命名規則 (ファイルシステムラベルまたは UUID) を使用します。
- オペレーティングシステムがソース VM の最初のディスクにインストールされていることを確認します。オペレーティングシステムディスクにスワップパーティションを構成しないようにしてください。
- ソース VM のネットワークインターフェースで DHCP を使用し、起動時に有効にすることをお勧めします。

RHEL 8.6 VM イメージを VHD に変換するには

1 Hyper-V デバイスドライバをインストールし、`initramfs` イメージファイルを再構築します。

Hyper-V ドライバ (hv_netvsc、hv_storvsc、hv_vmbus) がインストールされているかどうかを確認します。

```
lsinitrd | grep hv
```

インストールされていない場合は、次の手順を実行します。

- 以前の `initramfs` イメージファイルをバックアップします。

```
cd /boot
cp initramfs-`uname -r`.img initramfs-`uname -r`.img.bak
```

- `/etc/dracut.conf.d` ディレクトリの下に `hv.conf` ファイルを作成します。`hv.conf` ファイルに次のドライバパラメータを追加します。

```
add_drivers+=" hv_vmbus "
add_drivers+=" hv_netvsc "
add_drivers+=" hv_storvsc "
add_drivers+=" nvme "
```

メモ: 引用符とドライバ名の間にスペースを追加します。

- 新しいモジュールを含む、新しい初期 ramdisk イメージを作成します。

```
dracut -f -v -N -regenerate-all
```

新しい初期 ramdisk イメージに新しいモジュールが存在するかどうかを確認します。

```
lsinitrd | grep -i hv
```

2 ネットワークインターフェース名が eth0 であることを確認します。ネットワークインターフェースが DHCP を使用しており、ブート時に有効になっていることを確認します。

/etc/sysconfig/network/ifcfg-eth0 には次のものが含まれています。

```
BOOTPROTO='dhcp'
STARTMODE='auto'
```

3 grub.cfg を再生成し、コンソールログがシリアルポートに送信されるようにします。

- /etc/default/grub ファイルで従来の NIC 名を使用するには、行 GRUB_CMDLINE_LINUX="xxxxxxx" を GRUB_CMDLINE_LINUX="xxxxxxx net.ifnames=0" に変更します。
  次のパラメータが存在する場合は削除します。rhgb quiet crashkernel=auto
- grub.cfg ファイルを再生成します。
  BIOS ベースのコンピュータの場合: grub2-mkconfig -o /boot/grub2/grub.cfg
  UEFI ベースのコンピュータの場合: grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg

4 ソース VM の新しい完全バックアップを実行します。

5 イメージ共有サーバーを準備し、Azure アカウントでイメージ共有機能を構成します。

6 バックアップイメージをインポートし、変換を実行します。

7 変換された VHD ファイルを確認します。

Azure Web ポータルで、以下を実行します。

- 変換された .vhd ファイルを使ってディスクを作成します。
- 以前のディスクを使用して VM を作成します。
  [ディスク]>[作成されたディスク (Created disk)]>[VM の作成]の順に移動します。デフォルトのネットワーク設定、ディスク設定、管理設定で、ブート診断を有効にします。
- 変換された VM に SSH 経由でログインします。

Microsoft Azure Archive 内のバックアップからのリストアについて

リストアを開始した後、Microsoft Azure Archive のリハイドレート処理には時間がかかります。詳しくは Microsoft Azure のマニュアルを参照してください。リハイドレート処理は、データがホット層に移行されると完了します。LSU を構成するときに指定した日数によって、データがホット層に維持される時間が計測されます。その後、データはアーカイブ層に移行されます。

データをホット層に維持する日数はクラウドプロバイダのコストに影響します。

`csconfig CLI. -post_rehydration_period` コマンドを使用して、リハイドレート期間の値を変更できます。

Cohesity Alta Recovery Vault Azure と Amazon について

Cohesity Alta Recovery Vault は、シームレスなセカンダリストレージオプションを提供するクラウドベースのサービスとしてのストレージ (SaaS) を提供します。この機能は、オンプレミスからパブリッククラウドにわたる作業負荷を保存する、単一の柔軟なリポジトリとして機能します。Recovery Vault は Web UI で利用できるため、クラウドストレージリソースと保持ポリシーのプロビジョニング、管理、監視を簡素化できます。

Recovery Vault ストレージの正確な表示は、Cohesity Alta View の Recovery Vault ストレージの使用状況の概要ページに表示されます。構成したクラウドサービスプロバイダのストレージの詳細と使用状況の詳細を表示できます。クラウドサービスプロバイダによって提供される定期的なデータ更新サイクルにより、ストレージの詳細は通常 24 時間から 48 時間遅延します。

Cohesity Alta Recovery Vault について詳しくは、次のリンクを参照してください。

Cohesity Alta Recovery Vault Deployment Guide

Recovery Vault の詳細

Veritas Alta Recovery Vault Azure および Azure Government の構成

次の手順を使用して、Azure と Azure Government 用の Veritas Alta Recovery Vault を構成します。

メモ: Veritas Alta Recovery Vault は、複数のオプションをサポートしています。Web UI の Azure と Azure Government の Veritas Alta Recovery Vault のオプションについて、クレデンシャルが必要な場合や、質問がある場合は、Cohesity NetBackup のアカウントマネージャにお問い合わせください。

表 6-4 Azure と Azure Government 用の Alta Recovery Vault の構成手順

手順	作業	手順の詳細
手順 1	クレデンシャルを取得します。	Cohesity NetBackup のアカウントマネージャから Alta Recovery Vault のクレデンシャルを取得します。
手順 2	(オプション) MSDP ストレージサーバーが存在しない場合は作成します。	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

手順	作業	手順の詳細
手順 3	ディスクプールを追加します。	NetBackup Web UI で、ディスクプールを作成します。『NetBackup Web UI 管理者ガイド』の「ディスクプールの作成」の手順に従います。 ■ ［ボリューム (Volumes)］手順で、次の手順を実行します。 ■ ［クラウドストレージプロバイダ (Cloud storage provider)］ドロップダウンから、Veritas Alta Recovery Vault Azure または Veritas Alta Recovery Vault Azure Government のオプションを選択します。 ■ 適切な地域を選択します。 ■ ［クレデンシャルの関連付け (Associate credential)］セクションで、［新しいクレデンシャルの追加 (Add a new credential)］を選択し、プロビジョニングチームが提供するストレージアカウントと更新トークンを入力します。または、Azure のクレデンシャルが存在する場合は、［既存のクレデンシャルの選択 (Select existing credentials)］を使用できます。 ［クレデンシャル名 (Credential name)］には、ハイフンまたはアンダースコアを含む英数字を使用する必要があり、空白や不正な文字を含めることはできません。 Veritas Alta Recovery Vault Azure は、次の 2 つのストレージクラスを提供します。 ■ Alta Recovery Vault Standard - AZURE ■ Alta Recovery Vault Archive - AZURE ストレージの配備に応じて適切なストレージ階層を選択します。実際のストレージ階層は、構成中に NetBackup によって決まります。 **メモ:** NetBackup が使用するために作成された、`alta-recovery-vault-azure-29cb2539-39ce-427e-8e72-48bf62177bc3` という名前のコンテナが表示される場合があります。同じ名前のバケットを作成しないでください。同じ名前のバケットを作成すると、ディスクプールの構成が失敗します。
手順 4	ストレージユニットを追加します。	NetBackup Web UI で、ストレージユニットを作成します。『NetBackup Web UI 管理者ガイド』の「ストレージユニットの作成」の手順に従います。 ストレージユニットを作成するときに、［メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP))］オプションを選択します。［ディスクプール (Disk pool)］の手順で、手順 3 で作成したディスクプールを選択します。

メモ: 既存のストレージアカウントの更新トークンの更新が必要な場合は、ストレージアカウントに関連付けられているクレデンシャルを編集する必要があります。Web UI を使用し、[クレデンシャル管理 (Credential management)]内で更新トークンを更新します。

同じストレージアカウントに複数のクレデンシャルを設定することはできません。クレデンシャルはストレージアカウントに一意である必要があります。一意のクレデンシャルがない場合、ディスクボリュームの停止や、そのディスクボリュームへのバックアップとリストアの失敗などの問題が発生する可能性があります。

メモ: 元のストレージアカウントを使用して、Veritas Alta Recovery Vault CMS クレデンシャルを更新します。

CLI を使用した Veritas Alta Recovery Vault Azure および Azure Government の構成

次の手順を使用して、CLI で Azure と Azure Government 用の Veritas Alta Recovery Vault を構成します。

表 6-5 CLI を使用した Azure と Azure Government 用の Alta Recovery Vault の構成手順

手順	作業	手順の詳細
手順 1	クレデンシャルを取得します。	Cohesity NetBackup のアカウントマネージャから Veritas Alta Recovery Vault のクレデンシャルを取得します。

手順	作業	手順の詳細
手順 2	[クレデンシャルの管理 (Credential management)]オプションを使用して、クレデンシャルを追加します。	NetBackup Web UI にログインし、次を実行します。 **1** 左側の[クレデンシャルの管理 (Credential management)]をクリックします。 **2** [指定したクレデンシャル (Named credentials)]タブで[追加 (Add)]をクリックし、次のプロパティを指定します。 ■ クレデンシャル名 (Credential name) [クレデンシャル名 (Credential name)]には、ハイフンまたはアンダースコアを含む英数字を使用する必要があり、空白や不正な文字を含めることはできません。 ■ タグ (Tag) ■ 説明 (Description) **3** [次へ (Next)]をクリックします。 **4** ドロップダウンで、[Cohesity Alta Recovery Vault]を選択します。 **5** [Veritas Alta Recovery Vault Azure]をクリックします。 **6** ストレージアカウントと更新トークンを追加します。 **7** このクレデンシャルにアクセスできる役割を選択または追加します。 **8** 情報を確認して[完了 (Finish)]をクリックします。
手順 3	MSDP ストレージサーバーを作成します。	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

手順	作業	手順の詳細

手順 4	クラウドインスタンスエイリアスを作成します。	環境に応じて、次の例を使用します。
		■ Veritas Alta Recovery Vault Azure クラウドインスタンスエイリアスの作成:
		`/usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in Veritas-Alta-Recovery-Vault-Azure -sts <storage server> -lsu_name <lsu name>`
		■ Veritas Alta Recovery Vault Azure Archive クラウドインスタンスエイリアスの作成:
		`/usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in Veritas-Alta-Recovery-Vault-Azure -sts <storage server> -lsu_name <lsu name> -storage_tier Alta-Recovery-Vault-Archive-AZURE -post_rehydration_period 3`
		クラウドエイリアス名は <storage server>_<lsu name> で、バケットを作成するために使用されます。

手順 5	(省略可能) 新しいバケットを作成します。	必要に応じて、新しいバケットを作成します。 `/usr/openv/netbackup/bin/nbcldutil -createbucket -storage_server <storage server>_<lsu name> -username <cloud user> -bucket_name <bucket name>`

手順	作業	手順の詳細
手順 6	構成ファイルを作成して、nbdevconfig コマンドを実行します。	

手順	作業	手順の詳細

		新しいクラウド LSU を追加するための構成ファイルの内容 (構成設定と説明):
		■ V7.5 "operation" "add-lsu-cloud" 文字列 - 新しいクラウド LSU を追加するための値 "add-lsu-cloud" を指定します。
		■ V7.5 "lsuName" " " 文字列 - LSU 名を指定します。
		■ V7.5 "cmsCredName" " " 文字列 - クレデンシャル管理を使用して作成されたクレデンシャル名を指定します。
		■ V7.5 "lsuCloudBucketName" " " 文字列 - クラウドバケット名を指定します。
		■ V7.5 "lsuCloudBucketSubName" " " 文字列 - 複数のクラウド LSU が同じクラウドバケットを使用できます。この値は、異なるクラウド LSU を識別します。
		■ V7.5 "lsuEncryption" " " 文字列 - オプションの値で、デフォルトは NO です。現在の LSU の暗号化プロパティを設定します。
		■ V7.5 "lsuKmsEnable" " " 文字列 - オプションの値で、デフォルトは NO です。現在の LSU の KMS を有効にします。
		■ V7.5 "lsuKmsKeyGroupName" " " 文字列 - 省略可能な値。キーグループ名はすべての LSU 間で共有されます。キーグループ名には、次の有効な文字を使用する必要があります: A-z、a-z、0-9、_ (アンダースコア)、- (ハイフン)、: (コロン)、. (ピリオド) および空白。
		■ V7.5 "lsuKmsServerName" " " 文字列 - 省略可能な値。KMS サーバー名はすべての LSU 間で共有されます。
		■ V7.5 "lsuKmsServerType" " " 文字列 - 省略可能な値。
		暗号化が無効になっている構成ファイルの例:
		`V7.5 "operation" "add-lsu-cloud" string`
		`V7.5 "lsuName" "nbrvltazure1" string`
		`V7.5 "cmsCredName" "RVLT-creds" string`
		`V7.5 "lsuCloudBucketName" "bucket1" string`
		`V7.5 "lsuCloudBucketSubName" "sub1" string`
		暗号化が有効になっている構成ファイルの例:
		`V7.5 "operation" "add-lsu-cloud" string`
		`V7.5 "lsuName" "nbrvltazure2" string`
		`V7.5 "cmsCredName" "RVLT-creds" string`
		`V7.5 "lsuCloudBucketName" "bucket1" string`
		`V7.5 "lsuCloudBucketSubName" "sub2" string`

手順	作業	手順の詳細
		V7.5 "lsuEncryption" "YES" string V7.5 "lsuKmsEnable" "YES" string V7.5 "lsuKmsKeyGroupName" "test" string V7.5 "lsuKmsServerName" "test" string **メモ:** 1 台のストレージサーバーに存在するすべての暗号化された LSU は、同じ keygroupname と kmsservername を使用する必要があります。nbdevconfig コマンドを使用して、新しい暗号化されたクラウド LSU を追加するときに、この MSDP にすでに 1 つが存在する場合、keygroupname が前の暗号化済みの LSU の keygroupname と同じである必要があります。 構成ファイルを作成したら、nbdevconfig コマンドを実行します。 /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig -storage_server <storage server> -stype PureDisk -configlist <configuration file path> **メモ:** パラメータ <storage server> は、手順 4 のパラメータ <storage server> と同じである必要があります。

手順	作業	手順の詳細
手順 7	ディスクプールを作成します。	nbdevconfig コマンドを実行して、ディスクプールを作成します。次に、nbdevconfig コマンドの使用例を示します。 例 1: /usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk | grep <LSU name> > /tmp/dvlist 例 2: /usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name> **メモ:** また、NetBackup Web UI または NetBackup 管理コンソールからディスクプールを作成することもできます。
手順 8	ストレージユニットを作成します。	bpstuaddコマンドを使用して、ストレージユニットを作成します。次に、bpstuadd コマンドの使用例を示します。 /usr/openv/netbackup/bin/admincmd/bpstuadd -label <storage unit name> -odo 0 -dt 6 -dp <disk pool name> -nodevhost **メモ:** また、NetBackup Web UI または NetBackup 管理コンソールからストレージサーバーを作成することもできます。

メモ: 既存のストレージアカウントの更新トークンの更新が必要な場合は、ストレージアカウントに関連付けられているクレデンシャルを編集する必要があります。Web UI を使用し、[クレデンシャル管理 (Credential management)]内で更新トークンを更新します。

同じストレージアカウントに複数のクレデンシャルを設定することはできません。クレデンシャルはストレージアカウントに一意である必要があります。一意のクレデンシャルがない場合、ディスクボリュームの停止や、そのディスクボリュームへのバックアップとリストアの失敗などの問題が発生する可能性があります。

Azure と Azure Government 用の Cohesity Alta Recovery Vault の `csconfig cldinstance` の変更について

`csconfig cldinstance` コマンドはエイリアス情報を取得する[**トークンの更新が必要** `(Need Token Renew)`] フラグを表示します (はい/いいえ)。[**はい** `(Yes)`]の場合、Recovery Vault はストレージアカウントとアクセスキーではなく、ストレージアカウントとトークンの更新クレデンシャルを想定します。

クラウドインスタンスには、[トークンの更新が必要 (Need Token Renew)] (-ntr) オプションを無効 (0) または有効 (1) にするオプションがあります。この `Veritas-Alta-Recovery-Vault-Azure` と `Veritas-Alta-Recovery-Vault-Azure-Gov` のデフォルト値は[はい (Yes)](1) です。

`csconfig cldinstance` と `-ntr` の使用例:

```
csconfig cldinstance -us -in <instance name> -sts <alias name> -ntr
 <0,1>
```

メモ: CLI を使用して旧バージョンのメディアサーバーにクラウド LSU を追加する場合は、`-ntr` オプションを `No` (0) に設定する必要があります。古いバージョンのメディアサーバーではトークンベースのクレデンシャルがサポートされていないため、このオプションを[いいえ (No)]に設定する必要があります。バージョン 10.2 以降の NetBackup ストレージサーバーを使用する場合、クラウドエイリアスインスタンスの `-ntr` オプションは `Yes` に設定されている必要があります。設定を `No` に設定することはできません。

Azure と Azure Government 用の Veritas Alta Recovery Vault の `nbcldutil` の変更について

`nbcldutil` コマンドで、Azure と Azure Government 用の Veritas Alta Recovery Vault を構成する際の `-createbucket` および `-validatecreds` オプションに新しい入力が追加されました。

使用例:

```
nbcldutil -createbucket storage_server storage-server-name_lsu-name

-username rvlt-creds -bucket_name sl-bucket-cli
```

`-username` のストレージアカウント名を入れる代わりに、クレデンシャル管理を使用して作成されたクレデンシャルの名前を使用します。また、パスワードの入力を求められたら、パスワードは必要ないため仮で入力します。

Azure と Azure Government 用の Cohesity Alta Recovery Vault の msdpcldutil の変更について

このユーティリティを使用するには、NetBackup Web UI を使用してクレデンシャル名を作成し、csconfig コマンドを次の例のように使用してクラウドエイリアスを作成する必要があります。

```
/usr/openv/netbackup/bin/admincmd/csconfig cldinstance
-as -in Veritas-Alta-Recovery-Vault-Azure -sts <storage_server_name>

-stype PureDisk -lsu_name test1

Successfully added storage server(s): <storage_server_name>_test1
```

Cohesity Alta Recovery Vault Azure に使用する --enable_sas オプションが追加されました。さらに、--enable _sas オプションを使用する場合は、次の環境変数をエクスポートする必要があります。

- MSDPC_MASTER_SERVER - このオプションは NetBackup プライマリサーバーの名前です。
- MSDPC_ALIAS - このオプションは、csconfig を使用して作成されたクラウドエイリアスです。
- MSDPC_ACCESS_KEY - クレデンシャル名。MSDPC_SECRET_KEY はダミーの文字列です。

出力例は次のとおりです。

```
export MSDPC_PROVIDER=vazure
export MSDPC_REGION="East US"
export
MSDPC_ENDPOINT="https://<storage-account>.blob.core.windows.net/"
export MSDPC_ACCESS_KEY=<credential name>
export MSDPC_SECRET_KEY="dummy<any non-null string>
export MSDPC_MASTER_SERVER=<primary server>
export MSDPC_ALIAS=<storage_server_name>_test1

/usr/openv/pdde/pdcr/bin/msdpcldutil create -b rv-worm1
-v dv-worm --mode ENTERPRISE --min 1D --max 3D --enable_sas
```

または、Cohesity から受信したアクセストークンを指定して WORM バケットまたはボリュームを作成することもできます。メディアサーバーが Recovery Vault Web サーバーに接続し、Cohesity が Recovery Vault Web サーバー URI を指定する必要があるため、このオプションは推奨されません。

- MSDPC_RVLT_API_URI - Cohesity が別のエンドポイントを提供する場合に使用する新しい環境パラメータ。
- MSDPC_ACCESS_TOKEN - Cohesity が提供するクレデンシャルの一部であるアクセストークン。
- MSDPC_CMS_CRED_NAME - クレデンシャルを格納するためのクレデンシャル名。
  出力例

```
export MSDPC_CMS_CRED_NAME=your_cms_credential_name
export MSDPC_ALIAS=your_alias_name
export MSDPC_REGION=your_region
export MSDPC_PROVIDER=vazure
export
MSDPC_ENDPOINT="https://your_storage_account.blob.core.windows.net/"
export MSDPC_MASTER_SERVER=<primary server>
```

Amazon および Amazon Government 用の Veritas Alta Recovery Vault の構成

次の手順を使用して、Amazon および Amazon Government 用の Cohesity Alta Recovery Vault を構成します。

メモ: Cohesity Alta Recovery Vault は、複数のオプションをサポートしています。Web UI の Amazon と Amazon Government の Cohesity Alta Recovery Vault のオプションについて、クレデンシャルが必要な場合や、質問がある場合は、Cohesity NetBackup のアカウントマネージャにお問い合わせください。

表 6-6

手順	作業	手順の詳細
手順 1	クレデンシャルを取得します。	Cohesity NetBackup のアカウントマネージャから Veritas Alta Recovery Vault のクレデンシャルを取得します。
手順 2	(オプション) MSDP ストレージサーバーが存在しない場合は作成します。	詳しくは、『NetBackup 重複排除ガイド』の「MSDP サーバー側の重複排除の構成」を参照してください。

手順	作業	手順の詳細
手順 3	ディスクプールを追加します。	NetBackup Web UI で、ディスクプールを作成します。『NetBackup Web UI 管理者ガイド』の「ディスクプールの作成」の手順に従います。 ■ ［ボリューム (Volumes)］手順で、次の手順を実行します。 ■ ［クラウドストレージプロバイダ (Cloud storage provider)］ドロップダウンから、Veritas Alta Recovery Vault Amazon または Veritas Alta Recovery Vault Amazon Government のオプションを選択します。 ■ 適切な地域を選択します。 ■ ［クレデンシャルの関連付け (Associate credential)］セクションで、［新しいクレデンシャルの追加 (Add a new credential)］を選択し、プロビジョニングチームが提供する更新トークンを入力します。または、Amazon のクレデンシャルが存在する場合は、［既存のクレデンシャルの選択 (Select existing credentials)］を使用できます。 ［クレデンシャル名 (Credential name)］には、ハイフンまたはアンダースコアを含む英数字を使用する必要があり、空白や不正な文字を含めることはできません。 ■ クレデンシャルを指定したクラウドバケット名を入力します。
手順 4	ストレージユニットを追加します。	NetBackup Web UI で、ストレージユニットを作成します。『NetBackup Web UI 管理者ガイド』の「ストレージユニットの作成」の手順に従います。 ストレージユニットを作成するときに、［メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP))］オプションを選択します。［ディスクプール (Disk pool)］の手順で、手順 3 で作成したディスクプールを選択します。

メモ: Web UI を使用し、［クレデンシャル管理 (Credential management)］内で更新トークンを更新します。

CLI を使用した Amazon および Amazon Government 用の Cohesity Alta Recovery Vault の構成

次の手順を使用して、Amazon および Amazon Government 用の Cohesity Alta Recovery Vault を CLI を使用して構成します。

表 6-7 CLI を使用した Amazon および Amazon Government 用の Alta Recovery Vault の構成手順

手順	作業	手順の詳細
手順 1	クレデンシャルを取得します。	Cohesity NetBackup のアカウントマネージャから Veritas Alta Recovery Vault のクレデンシャルを取得します。
手順 2	[クレデンシャルの管理 (Credential management)] オプションを使用して、クレデンシャルを追加します。	NetBackup Web UI にログインし、次を実行します。 **1** 左側の[クレデンシャルの管理 (Credential management)]をクリックします。 **2** [指定したクレデンシャル (Named credentials)]タブで[追加 (Add)]をクリックし、次のプロパティを指定します。 ■ クレデンシャル名 (Credential name) [クレデンシャル名 (Credential name)]には、ハイフンまたはアンダースコアを含む英数字を使用する必要があり、空白や不正な文字を含めることはできません。 ■ タグ (Tag) ■ 説明 (Description) **3** [次へ (Next)]をクリックします。 **4** ドロップダウンで、[Cohesity Alta Recovery Vault]を選択します。 **5** [Veritas Alta Recovery Vault Amazon]をクリックします。 **6** 更新トークンを追加します。 **7** このクレデンシャルにアクセスできる役割を選択または追加します。 **8** 情報を確認して[完了 (Finish)]をクリックします。
手順 3	MSDP ストレージサーバーを作成します。	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。
手順 4	クラウドインスタンスエイリアスを作成します。	環境に応じて、次の例を使用します。 ■ Veritas Alta Recovery Vault Amazon クラウドインスタンスエイリアスの作成: `/usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in Veritas-Alta-Recovery-Vault-Amazon -sts <storage server> -lsu_name <lsu name>` クラウドエイリアス名は <storage server>_<lsu name> で、バケットを作成するために使用されます。

手順	作業	手順の詳細
手順 6	構成ファイルを作成して、nbdevconfig コマンドを実行します。	

手順	作業	手順の詳細

		新しいクラウド LSU を追加するための構成ファイルの内容 (構成設定と説明):
		■ V7.5 "operation" "add-lsu-cloud" 文字列 - 新しいクラウド LSU を追加するための値 "add-lsu-cloud" を指定します。
		■ V7.5 "lsuName" " " 文字列 - LSU 名を指定します。
		■ V7.5 "cmsCredName" " " 文字列 - クレデンシャル管理を使用して作成されたクレデンシャル名を指定します。
		■ V7.5 "lsuCloudBucketName" " " 文字列 - クラウドバケット名を指定します。
		■ V7.5 "lsuCloudBucketSubName" " " 文字列 - 複数のクラウド LSU が同じクラウドバケットを使用できます。この値は、異なるクラウド LSU を識別します。
		■ V7.5 "lsuEncryption" " " 文字列 - オプションの値で、デフォルトは NO です。現在の LSU の暗号化プロパティを設定します。
		■ V7.5 "lsuKmsEnable" " " 文字列 - オプションの値で、デフォルトは NO です。現在の LSU の KMS を有効にします。
		■ V7.5 "lsuKmsKeyGroupName" " " 文字列 - 省略可能な値。キーグループ名はすべての LSU 間で共有されます。キーグループ名には、次の有効な文字を使用する必要があります: A-z、a-z、0-9、_ (アンダースコア)、- (ハイフン)、: (コロン)、. (ピリオド) および空白。
		■ V7.5 "lsuKmsServerName" " " 文字列 - 省略可能な値。KMS サーバー名はすべての LSU 間で共有されます。
		■ V7.5 "lsuKmsServerType" " " 文字列 - 省略可能な値。
		
		暗号化が無効になっている構成ファイルの例については、Azure のセクションを参照してください。
		
		p.329 の「CLI を使用した Veritas Alta Recovery Vault Azure および Azure Government の構成」を参照してください。
		
		メモ: 1 台のストレージサーバーに存在するすべての暗号化された LSU は、同じ keygroupname と kmsservername を使用する必要があります。nbdevconfig コマンドを使用して、新しい暗号化されたクラウド LSU を追加するときに、この MSDP にすでに 1 つが存在する場合、keygroupname が前の暗号化済みの LSU の keygroupname と同じである必要があります。
		
		構成ファイルを作成したら、nbdevconfig コマンドを実行します。
		
		`/usr/openv/netbackup/bin/admincmd/nbdevconfig`
		`-setconfig -storage_server <storage server>`
		`-stype PureDisk`
		`-configlist <configuration file path>`

手順	作業	手順の詳細
		メモ: パラメータ <storage server> は、手順 4 のパラメータ <storage server> と同じである必要があります。
手順 7	ディスクプールを作成します。	nbdevconfig コマンドを実行して、ディスクプールを作成します。次に、nbdevconfig コマンドの使用例を示します。 例 1: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv -storage_servers <storage server name> -stype PureDisk	grep <LSU name> > /tmp/dvlist` 例 2: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp <disk pool name> -stype PureDisk -dvlist /tmp/dvlist -storage_servers <storage server name>` **メモ:** また、NetBackup Web UI または NetBackup 管理コンソールからディスクプールを作成することもできます。
手順 8	ストレージユニットを作成します。	bpstuadd コマンドを使用して、ストレージユニットを作成します。次に、bpstuadd コマンドの使用例を示します。 `/usr/openv/netbackup/bin/admincmd/bpstuadd -label <storage unit name> -odo 0 -dt 6 -dp <disk pool name> -nodevhost` **メモ:** また、NetBackup Web UI または NetBackup 管理コンソールからストレージサーバーを作成することもできます。

メモ: Web UI を使用し、[クレデンシャル管理 (Credential management)]内で更新トークンを更新します。

Amazon と Amazon Government 用の Cohesity Alta Recovery Vault の `csconfig cldinstance` の変更について

`csconfig cldinstance` コマンドはエイリアス情報を取得する**[トークンの更新が必要 (Need Token Renew)]** フラグを表示します (はい/いいえ)。**[はい (Yes)]**の場合、

Recovery Vault はストレージアカウントとアクセスキーではなく、ストレージアカウントとトークンの更新クレデンシャルを想定します。

クラウドインスタンスには、[トークンの更新が必要 (Need Token Renew)] (-ntr) オプションを無効 (0) または有効 (1) にするオプションがあります。この `Veritas-Alta-Recovery-Vault-Amazon` と `Veritas-Alta-Recovery-Vault-Amazon-Gov` のデフォルト値は[はい (Yes)](1) です。

`csconfig cldinstance` と `-ntr` の使用例:

```
csconfig cldinstance -us -in <instance name> -sts <alias name> -ntr
 <0,1>
```

メモ: CLI を使用して旧バージョンのメディアサーバーにクラウド LSU を追加する場合は、`-ntr` オプションを `No` (0) に設定する必要があります。古いバージョンのメディアサーバーではトークンベースのクレデンシャルがサポートされていないため、このオプションを[いいえ (No)]に設定する必要があります。バージョン 10.3.1 以降の NetBackup ストレージサーバーを使用する場合、クラウドエイリアスインスタンスの `-ntr` オプションは `Yes` に設定されている必要があります。設定を `No` に設定することはできません。

Amazon と Amazon Government 用の Cohesity Alta Recovery Vault の `nbcldutil` の変更について

NetBackup 10.3.1 以降の `nbcldutil` コマンドは、Amazon および Amazon Government 用の Cohesity Alta Recovery Vault を構成した場合、`-validatecreds` オプションをサポートしません。

Amazon と Amazon Government 用の Cohesity Alta Recovery Vault の `msdpcldutil` の変更について

このユーティリティを使用するには、NetBackup Web UI を使用してクレデンシャル名を作成し、`csconfig` コマンドを次の例のように使用してクラウドエイリアスを作成する必要があります。

```
/usr/openv/netbackup/bin/admincmd/csconfig cldinstance
-as -in Veritas-Alta-Recovery-Vault-Amazon -sts <storage_server_name>

-stype PureDisk -lsu_name test1

Successfully added storage server(s): <storage_server_name>_test1
```

Cohesity Alta Recovery Vault Amazon に使用する `--enable_sts` オプションが追加されました。さらに、`--enable _sts` オプションを使用する場合は、次の環境変数をエクスポートする必要があります。

- MSDPC_MASTER_SERVER - このオプションは NetBackup プライマリサーバーの名前です。
- MSDPC_ALIAS - このオプションは、csconfig を使用して作成されたクラウドエイリアスです。
- MSDPC_ACCESS_KEY - クレデンシャル名。MSDPC_SECRET_KEY はダミーの文字列です。
  アクセスキーとシークレットキーのほか、NetBackup は MSDPC_CMS_CRED_NAME 変数をサポートします。
- MSDPC_CMS_CRED_NAME - これはクレデンシャル名です。

出力例

```
export MSDPC_PROVIDER=vamazon
export MSDPC_REGION="us-east-1"
export MSDPC_CMS_CRED_NAME=<credential name>
export MSDPC_MASTER_SERVER=<primary server>
export MSDPC_ALIAS=<storage_server_name>_testnew

/usr/openv/pdde/pdcr/bin/msdpcldutil create -b rv-worm1
-v dv-worm --mode GOVERNANCE --min 1D --max 3D --enable_sts
```

または、Cohesity から受信したアクセストークンを指定して WORM バケットまたはボリュームを作成することもできます。メディアサーバーが Recovery Vault Web サーバーに接続し、Cohesity が Recovery Vault Web サーバー URI を指定する必要があるため、このオプションは推奨されません。

- MSDPC_RVLT_API_URI - Cohesity が別のエンドポイントを提供する場合に使用する新しい環境パラメータ。
- MSDPC_ACCESS_TOKEN - Cohesity が提供するクレデンシャルの一部であるアクセストークン。

Recovery Vault の標準認証からトークンベースの認証への移行

古いバージョンの NetBackup を使用して Cohesity Alta Recovery Vault をすでに構成している場合は、新しいバージョンにアップグレードする必要があります。セキュリティ強化のためにトークンベースの認証を利用するには、この機能を使用するためにプライマリサーバーとメディアサーバーを次のバージョンにアップグレードする必要があります。

- Azure 用の NetBackup 10.2 リリース。
- Amazon 用の NetBackup 10.3.1 リリース。

クレデンシャルを移行するには

1. NetBackupテクニカルサポートに問い合わせて、Cohesity Alta Recovery Vault Azure または Cohesity Alta Recovery Vault Amazon の新しいクレデンシャルを要求します。
2. NetBackup Web UI にログインし、[クレデンシャルの管理 (Credential management)]に新しいクレデンシャルを追加します。
   - 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
   - [指定したクレデンシャル (Named credentials)]タブで[追加 (Add)]をクリックし、次のプロパティを指定します。
     - クレデンシャル名 (Credential name)
     - タグ (Tag)
     - 説明 (Description)
   - [次へ (Next)]をクリックします。
   - ドロップダウンで、[Cohesity Alta Recovery Vault]を選択します。
   - [Cohesity Alta Recovery Vault Azure]または[Cohesity Alta Recovery Vault Amazon]をクリックします。
   - ストレージアカウントと更新トークンを追加します。
   - このクレデンシャルにアクセスできる役割を選択または追加します。
   - 情報を確認して[完了 (Finish)]をクリックします。
3. `csconfig cldinstance` コマンドを使用して `-ntr` オプションを更新します。

   例:

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -us -in
   <instance name> -sts <alias name> -ntr 1
   ```

   要トークン更新オプションの `-ntr` が、ストレージサーバーで有効になるように `1` に設定されていることを確認して、変更を確認します。

   ```
   <install path>/netbackup/bin/admincmd/csconfig cldinstance -i
   ```

4 nbdevconfig を使用してクレデンシャルを更新します。

[クレデンシャルの管理 (Credential management)]を使用して作成したクレデンシャル名として cmsCredName を使用して、構成ファイルを作成します。

構成ファイルの例:

```
V7.5 "operation" "update-lsu-cloud" string
V7.5 "lsuName" "myvolume" string
V7.5 "cmsCredName" "RVLT-creds" string
V7.5 "lsuCloudBucketName" "mybucket" string
V7.5 "lsuCloudBucketSubName" "myvolume" string
```

5 新しい構成ファイルを使用してクレデンシャルを更新します。

```
<install path>/netbackup/bin/admincmd/nbdevconfig
-setconfig -stype PureDisk -storage_server <storage_server>
-configlist <config file path>
```

プライマリサーバーとメディアサーバーでサービスを再起動して、変更を有効にします。

6 古いバックアップのリストアを確認し、新しいバックアップを実行します。新しいバックアップをリストアします。

MSDP クラウド変更不可 (WORM) ストレージのサポートについて

クラウド変更不可ストレージを使用すると、クラウドにバックアップデータを格納できます。このデータは 1 回書き込むと、変更や削除は行えません。この機能は Red Hat Enterprise Linux および SUSE Linux Enterprise オペレーティングシステムでのみサポートされます。

この機能はリーガルホールドとバケットのデフォルトの保持をサポートしません。

NetBackup は、次のクラウド変更不可ストレージをサポートします。

- Amazon S3 変更不可ストレージ
p.350 の「AWS S3 の変更不可オブジェクトのサポートについて」を参照してください。
- Amazon S3 と互換性のあるストレージ
p.355 の「AWS S3 互換プラットフォームでの変更不可オブジェクトのサポートについて」を参照してください。
- Microsoft Azure 変更不可ストレージ

p.356 の「Azure Blob Storage の変更不可ストレージのサポートについて 」を参照してください。

- Google Cloud Storage
  p.357 の「Google Cloud Storage のオブジェクトレベルの変更不可ストレージのサポートについて」を参照してください。

NetBackup 10.0.1 では、クラスタ環境でクラウド変更不可ストレージを使用できます。詳しくは、p.359 の「クラスタ環境でのクラウド変更不可ストレージの使用について」を参照してください。を参照してください。

Web UI を使用したクラウド変更不可ストレージユニットの作成

クラウド変更不可ストレージユニットを作成するには、NetBackup Web UI を使用します。次の手順では、クラウド変更不可ストレージユニットを作成するプロセスについて説明します。

次の手順を実行する前に、MSDP ストレージサーバーが作成されていることを確認します。

Azure クラウド変更不可ストレージの場合は、バージョンレベルの変更不可サポートが有効になっているストレージアカウントが作成されていることを確認します。

クラウド変更不可ストレージユニットを作成するには

1. NetBackup Web UI で、[ストレージ (Storage)]、[ディスクプール (Disk pools)]の順に移動し、[追加 (Add)]をクリックします。
2. [ディスクプールオプション (Disk pool options)]で、[変更 (Change)]をクリックしてストレージサーバーを選択します。

   [ディスクプール名 (Disk pool name)]に入力します。

   [I/O ストリーム数を制限 (Limit I/O streams)]をオフのままにすると、デフォルト値は[無制限 (Unlimited)]になり、パフォーマンスの問題が発生する可能性があります。

   必要なすべての情報を追加した後、[次へ (Next)]をクリックします。

3 [ボリューム (Volume)]ドロップダウンリストから、ボリュームを選択するか新しいボリュームを追加します。

[クラウドストレージプロバイダ (Cloud storage provider)]ウィンドウで、リストからプロバイダを選択します。

[地域 (Region)]で、適切な地域を選択します。

クレデンシャルを入力して、設定を完了します。プロキシサーバーの追加など、追加のオプションをここで設定できます。

[WORM]で、[オブジェクトロックを使用 (Use object lock)]にチェックマークを付けます。保持モードを選択し、ロック期間を日数または年数で入力します。

[クラウドバケット (Cloud bucket)]で、[クラウドバケットを選択または作成してください (Select or create a cloud bucket)]を選択して[取得リスト (Retrieve list)]をクリックします。リストからバケットを選択します。バケット名を指定することもできます。

暗号化が必要な場合は、データ圧縮と暗号化のためにデータの暗号化オプションを選択します。MSDP では、管理キーを使用してデータを暗号化する KMS 暗号化を使用できます。KMS を使用するには、KMS サーバーが事前に構成されている必要があります。

選択内容に応じて必要なすべての情報を入力し、[次へ (Next)]をクリックします。

4 [レプリケーション (Replication)]で、[次へ (Next)]をクリックします。

5 [確認 (Review)]ページで、すべての設定と情報が正しいことを確認します。[完了 (Finish)]をクリックします。

ウィンドウを閉じると、ディスクプールの作成とレプリケーション構成がバックグラウンドで続行されます。クレデンシャルとレプリケーションの構成の検証に問題がある場合は、[変更 (Change)]オプションを使用して設定を調整できます。

6 [ストレージユニット (Storage unit)]タブで、[追加 (Add)]をクリックします。

7 [メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP))]を選択して、[開始 (Start)]をクリックします。

8 [基本プロパティ(Basic properties)]で、MSDP ストレージユニットの[名前 (Name)]を入力し、[次へ (Next)]をクリックします。

9 作成されたディスクプールを選択し、[WORM の有効化 (Enable WORM)]または[有効期限までロック (Lock until expiration)]ボックスを選択して、[次へ (Next)]をクリックします。

10 [メディアサーバー (Media server)]で、デフォルトで選択されている[自動的に選択することを NetBackup に許可する (Allow NetBackup to automatically select)]を使用し、[次へ (Next)]をクリックします。

複数のメディアサーバーがある場合は、バージョン 9.1 以降を選択してください。

11 ストレージユニットの設定を確認し、[保存 (Save)]をクリックします。

クラウドの変更不可ボリュームの更新

すでに存在するクラウドの変更不可ボリュームの保持モードとロック期間を更新できます。

クラウドの変更不可ボリュームを更新するには

1. NetBackup Web UI で、[ストレージ (Storage)]、[ディスクプール (Disk pools)]の順に移動し、ボリューム名をクリックします。
2. [ボリュームオプション (Volume options)]で、ボリュームの処理メニューをクリックします。
3. [保持モードの編集 (Edit retention mode)]をクリックして、ボリュームの保持モードを更新します。

   [保持モードの編集 (Edit retention mode)]ウィンドウで、保持モードに[エンタープライズ (Enterprise)]または[コンプライアンス (Compliance)]を選択します。

   既存のアカウントクレデンシャルまたはクラウド管理者のクレデンシャルを選択します。

   [保存 (Save)]をクリックします。
4. [ロック期間の編集 (Edit lock duration)]をクリックして、ボリュームのロック期間を更新します。

   [ロック期間の編集 (Edit lock duration)]ウィンドウで、最小および最大のロック期間を日数または年数で指定します。

   既存のアカウントクレデンシャルまたはクラウド管理者のクレデンシャルを選択します。

   [保存 (Save)]をクリックします。

AWS S3 の変更不可オブジェクトのサポートについて

NetBackup 9.1 以降のバージョンは、S3 オブジェクトロックを使用してクラウド変更不可 (WORM) ストレージをサポートします。Amazon S3 オブジェクトロックについて詳しくは、https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/object-lock-overview.html を参照してください。

クラウド管理者とバックアップ管理者は、変更不可ストレージを構成して使用するために特定の権限を必要とします。クラウド管理者はクラウドのバケットとクラウドボリュームを管理するための一連の権限を必要とし、バックアップ管理者はバックアップデータを管理するための権限を必要とします。

p.352 の「クラウドの変更不可ボリュームを作成するための AWS ユーザー権限」を参照してください。

バックアップイメージは、次の 2 つの保持モードのいずれかでロックできます。

- コンプライアンスモード

ユーザーは、定義された保持期間にコンプライアンスモードを使用して保護されているデータを上書きまたは削除できません。データストレージの保持期間を設定すると、期間は延長できますが、短縮できません。

- エンタープライズモード
  保持ロックを無効にしてイメージを削除するには、ユーザーに特別な権限が必要です。クラウド管理者ユーザーのみが、必要に応じて保持ロックを無効にしてイメージを削除できます。コンプライアンスモードを使用する前に、エンタープライズモードを使用して保持期間の動作をテストできます。

クラウドの変更不可ボリューム (クラウド LSU) は、通常のクラウドボリュームと次の点で異なるクラウドボリュームです。

- バケットでオブジェクトロックが有効です。
- 保持範囲がクラウドボリュームに対して定義されます。バックアップイメージの保持は、この範囲内である必要があります。この条件は、バックアップポリシーが作成されると NetBackup によってチェックされます。
  この範囲は、NetBackup Web UI で定義および変更できます。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

p.350 の「クラウドの変更不可ボリュームの更新」を参照してください。

p.351 の「クラウドの変更不可ボリュームのライブ期間の自動延長」を参照してください。

p.351 の「パフォーマンスチューニング」を参照してください。

p.352 の「クラウドの変更不可ボリュームを作成するための AWS ユーザー権限」を参照してください。

p.353 の「変更不可ストレージのバケットポリシーについて」を参照してください。

クラウドの変更不可ボリュームのライブ期間の自動延長

オブジェクトのロックが設定されているクラウド変更不可ボリュームには、有効期限が設定されています。有効期限後、クラウドの変更不可ボリュームは保護されません。ただし、クラウドの変更不可ボリュームのライブ期間は、ボリューム構成で設定した最大値に自動的に延長されます。

Amazon S3 ストレージでバケットポリシーを有効にすると、MSDP クラウドにはクラウドの変更不可ボリュームのライブ期間を延長する権限がないため、自動延長は無効になります。この場合、クラウドの変更不可ボリュームのライブ期間を手動で延長するために `msdpcldutil` を使用する必要があります。

パフォーマンスチューニング

MSDP の spad プロセスには保持キャッシュがあります。これにより、データコンテナの保持時間が短縮します。データコンテナの保持期間が `retentionCacheTimeThreshold`

未満の場合、ストレージをすばやく再利用するために重複排除が再度実行されません。重複排除がある場合、保持期間を延長したり、削除したりすることはできません。

構成項目は cloudlsu.cfg にあります。

パラメータ	説明	デフォルト値
retentionCacheSizeThreshold	保持キャッシュに保存されるデータコンテナの保持情報の最大数です。 数を最小にするとメモリの節約になります。	10000000
retentionCacheTimeThreshold	データコンテナの保持期間がこのしきい値未満の場合、重複排除は再度実行されません。	432000

クラウドの変更不可ボリュームを作成するための AWS ユーザー権限

MSDP は、S3 変更不可ストレージをプロビジョニングおよび使用するための最小限の権限の原則に従っています。

リソース管理を行い、リソースを使用することで、変更不可ストレージでデータを保護します。バケットの作成や削除、バケットでのオブジェクトロックの有効化などのリソース管理タスクは、システムレベルのタスクです。S3 変更不可ストレージとの間でデータを転送するバックアップジョブやリストアジョブの実行などのリソースタスクの使用は、ユーザーレベルのタスクです。

これらの 2 つのタスクには、異なる権限セットが必要です。最初の権限セットを持つプリンシパルはクラウド管理者であり、2 番目の権限セットを持つプリンシパルはバックアップ管理者です。

Amazon クラウドのユーザーは、クラウドの変更不可ボリュームを管理および使用するための権限を必要とします。

クラウド管理者は、クラウドボリュームを管理するために msdpcldutil を実行する権限を必要とします。

```
"s3:BypassGovernanceRetention",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketVersioning",
```

```
"s3:GetObject",
"s3:GetObjectRetention",
"s3:GetObjectVersion"
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListBucketVersions",
"s3:PutBucketObjectLockConfiguration",
"s3:PutBucketVersioning",
"s3:PutObject",
"s3:PutObjectRetention",
```

バックアップ管理者は、Web UI から変更不可クラウド LSU を構成し、バックアップ、リストア、複製、レプリケーションなどのデータ保護ジョブを実行するために、次の権限を必要とします。

```
"s3:BypassGovernanceRetention",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketVersioning",
"s3:GetObject",
"s3:GetObjectRetention",
"s3:GetObjectVersion",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListBucketVersions",
"s3:PutObject",
"s3:PutObjectRetention",
```

変更不可ストレージのバケットポリシーについて

バケットポリシーは、各ボリュームまたはサブバケットの `lockdown-mode.conf` や `lsu-worm.conf` など、変更不可ストレージのメタデータオブジェクトを保護します。バケットポリシーを更新するには、`msdpcldutil update bucket-policy` コマンドを実行する必要があります。

バケットにバケットポリシーがすでにある場合、クラウド管理者は、変更不可ストレージ用のポリシーと既存のバケットポリシーを手動でマージする必要があります。S3 バケットポリシーの編集について詳しくは、AWS のマニュアルの Amazon S3 コンソールを使用したバケットポリシーの追加に関するトピックを参照してください。

AWS S3 の変更不可ストレージ用のバケットポリシーの例を次に示します。

```
{
    "Version": "2012-10-17",
    "Id": "vtas-lockdown-mode-file-protection",
    "Statement": [
        {
            "Sid": "vrts-lockdown-file-read-only",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:PutObjectRetention"
            ],
            "Resource": [

"arn:aws:s3:::bucket-name/volume-name/lockdown-mode.conf",
              "arn:aws:s3:::bucket-name/volume-name/lsu-worm.conf",


"arn:aws:s3:::bucket-name/volume-name/lockdown-mode.conf",
              "arn:aws:s3:::bucket-name/volume-name/lsu-worm.conf",


"arn:aws:s3:::bucket-name/volume-name/lockdown-mode.conf",
               "arn:aws:s3:::bucket-name/volume-name/lsu-worm.conf"

            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:userid": "YOUR-USER-ID-HERE"
                }
            }
        }
    ]
}
```

p.352 の「クラウドの変更不可ボリュームを作成するための AWS ユーザー権限」を参照してください。

AWS S3 互換プラットフォームでの変更不可オブジェクトのサポートについて

NetBackup 10.0 リリースから、次の S3 互換プラットフォームに対してクラウド変更不可オブジェクトのサポートが追加されました。

- HCP (Hitachi Content Platform) for Cloud Scale バージョン 2.3
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
  - コンプライアンスモードのみがサポートされます。
- Cloudian HyperStore、バージョン 7.2
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
- Seagate Lyve Cloud (パブリッククラウド)
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
- Veritas Access Cloud
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
  - コンプライアンスモードのみがサポートされます。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

NetBackup 10.1 リリースから、次の S3 互換プラットフォームに対してクラウド変更不可オブジェクトのサポートが追加されました。

- Wasabi (Wasabi cloud storage)
  クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
- Scality RING/ARTESCA
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
- EMC-ECS (バージョン 3.6.2)
  クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

NetBackup 10.1.1 リリースから、次の S3 互換プラットフォームに対してクラウド変更不可オブジェクトのサポートが追加されました。

- Quantum ActiveScale
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
  - コンプライアンスモードのみがサポートされます。
- NetApp StorageGRID Webscale - WAN

- クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
- コンプライアンスモードのみがサポートされます。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

NetBackup 10.3 リリースから、次の S3 互換プラットフォームに対してクラウド変更不可オブジェクトのサポートが追加されました。

- IBM Cloud Object Storage (iCOS)
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
  - コンプライアンスモードのみがサポートされます。
- DataCore クラウドクラスタストレージ
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
  - コンプライアンスモードのみがサポートされます。
- NetApp StorageGrid LAN
  NetAPP StorageGRID バージョン 11.7.0.4 以降を使用することをお勧めします。古いバージョンではパフォーマンスの問題が発生する可能性があります。
  - クラウド管理者とバックアップ管理者の役割が 1 つの役割に統合されています。
  - コンプライアンスモードのみがサポートされます。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

p.350 の「クラウドの変更不可ボリュームの更新」を参照してください。

Azure Blob Storage の変更不可ストレージのサポートについて

NetBackup 10.0 以降のバージョンは、Azure Blob Storage の変更不可ストレージをサポートし、バックアップデータを格納します。Azure の変更不可ストレージについて詳しくは、「不変ストレージを使用してビジネスに不可欠な BLOB データを保存する」を参照してください。

変更不可の BLOB データには、次のいずれかの時間ベースの保持ポリシーを使用できます。

- ロック済みポリシー
  定義された保持期間について、ロック済みポリシーを使用して、保護されているデータを上書きまたは削除することはできません。データストレージの保持期間を設定すると、期間は延長できますが、短縮できません。
- ロック解除済みポリシー

定義された保持期間について、ロック解除済みポリシーを使用して、保護されているデータを上書きまたは削除することはできません。データストレージの保持期間を設定した後、期間の延長、短縮、または削除が可能です。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

p.350 の「クラウドの変更不可ボリュームの更新」を参照してください。

Google Cloud Storage のオブジェクトレベルの変更不可ストレージのサポートについて

NetBackup 10.4 以降のバージョンは、バックアップデータを格納するために、Google Cloud Storage のオブジェクトレベルの変更不可クラウドストレージをサポートします。Google Cloud Storage について詳しくは、「オブジェクト保持ロック」を参照してください。

クラウド管理者とバックアップ管理者は、変更不可ストレージを構成して使用するために特定の権限を必要とします。クラウド管理者はクラウドのバケットとクラウドボリュームを管理するための一連の権限を必要とし、バックアップ管理者はバックアップデータを管理するための権限を必要とします。

バックアップイメージは、次の 2 つの保持モードのいずれかでロックできます。

- コンプライアンスモード
  ユーザーは、定義された保持期間にコンプライアンスモードを使用して保護されているデータを上書きまたは削除できません。データストレージの保持期間を設定すると、期間は延長できますが、短縮できません。
- エンタープライズモード
  保持ロックを無効にしてイメージを削除するには、ユーザーに特別な権限が必要です。クラウド管理者ユーザーのみが、必要に応じて保持ロックを無効にしてイメージを削除できます。コンプライアンスモードを使用する前に、エンタープライズモードを使用して保持期間の動作をテストできます。

クラウドの変更不可ボリューム (クラウド LSU) は、通常のクラウドボリュームと次の点で異なるクラウドボリュームです。

- バケットでオブジェクトロックが有効です。
- 保持範囲がクラウドボリュームに対して定義されます。バックアップイメージの保持は、この範囲内である必要があります。この条件は、バックアップポリシーが作成されると NetBackup によってチェックされます。この範囲は、NetBackup Web UI で定義および変更できます。

NetBackup は、Google S3 XML API を使用して、Google Cloud Storage のデータ管理を効果的に処理します。ただし、Google S3 XML API には、バケットのデフォルトの保持期間の取得と構成を管理するために必要な機能がありません。そのため、NetBackup は S3 バケットにデフォルトの保持ポリシーが構成されているかどうかを判断できず、その

結果、それらを非オブジェクトロックバケットとして認識します。Google Cloud Storage でデフォルトの保持ポリシーを使用してバケットを選択すると、期限が切れていない特定のオブジェクトを削除できません。

Google Cloud コンソールでのバケットの作成は避けることをお勧めします。すべてのバケットは NetBackup Web UI 内でのみ作成してください。また、デフォルトの保持ポリシーを使用しているバケットを Google Web コンソールで特定し、それらを NetBackup で使用しないようにしてください。

p.348 の「Web UI を使用したクラウド変更不可ストレージユニットの作成」を参照してください。

p.350 の「クラウドの変更不可ボリュームの更新」を参照してください。

p.351 の「クラウドの変更不可ボリュームのライブ期間の自動延長」を参照してください。

p.351 の「パフォーマンスチューニング」を参照してください。

クラウドの変更不可ボリュームを作成するための Google Cloud Storage ユーザー権限

MSDP は、S3 変更不可ストレージをプロビジョニングおよび使用するための最小限の権限の原則に従っています。

リソース管理を行い、リソースを使用することで、変更不可ストレージでデータを保護します。バケットの作成や削除、バケットでのオブジェクトロックの有効化などのリソース管理タスクは、システムレベルのタスクです。S3 変更不可ストレージとの間でデータを転送するバックアップジョブやリストアジョブの実行などのリソースタスクの使用は、ユーザーレベルのタスクです。

これらの 2 つのタスクには、異なる権限セットが必要です。最初の権限セットを持つプリンシパルはクラウド管理者であり、2 番目の権限セットを持つプリンシパルはバックアップ管理者です。

クラウド管理者は、クラウドボリュームを管理するために変更不可クラウドストレージ構成を行う権限を必要とします。

```
"storage.buckets.create",
"storage.buckets.delete",
"storage.buckets.enableObjectRetention",
"storage.buckets.get",
"storage.buckets.list",
"storage.buckets.update",
"storage.objects.create",
"storage.objects.delete",
"storage.objects.list",
"storage.objects.overrideUnlockedRetention",
```

```
"storage.objects.setRetention",
"storage.objects.update"
```

バックアップ管理者は、Web UI から変更不可クラウド LSU を構成し、バックアップ、リストア、複製、レプリケーションなどのデータ保護ジョブを実行するために、次の権限を必要とします。

```
"storage.buckets.get",
"storage.buckets.list",
"storage.buckets.update",
"storage.objects.create",
"storage.objects.delete",
"storage.objects.list",
"storage.objects.overrideUnlockedRetention",
"storage.objects.setRetention",
"storage.objects.update",
"storage.multipartUploads.create",
"storage.multipartUploads.abort",
"storage.multipartUploads.listParts",
"storage.multipartUploads.list"
```

クラスタ環境でのクラウド変更不可ストレージの使用について

以前は、NetBackup は単一ノードでのクラウド変更不可ストレージの配備をサポートしました。NetBackup 10.1 からは、NetBackup は Azure Kubernetes Service (AKS)、Amazon Elastic Kubernetes Service (EKS)、NetBackup Flex Scale などのクラスタ環境でのクラウド変更不可ストレージの配備をサポートします。

p.347 の「MSDP クラウド変更不可 (WORM) ストレージのサポートについて」を参照してください。

データが一定期間削除または上書きされないように、クラウド WORM ストレージにデータをバックアップできます。現在、MSDP は次のクラウド変更不可ストレージをサポートします。これらすべてのクラウド変更不可ストレージを NetBackup クラスタ環境に配備できます。

- Amazon S3 オブジェクトロック
  p.350 の「AWS S3 の変更不可オブジェクトのサポートについて」を参照してください。
- Amazon S3 と互換性のあるストレージ
  p.355 の「AWS S3 互換プラットフォームでの変更不可オブジェクトのサポートについて」を参照してください。
- Azure 変更不可ストレージ

p.356 の「Azure Blob Storage の変更不可ストレージのサポートについて」を参照してください。

Web UI を使用したディスクボリュームの作成が失敗した場合のエラーのトラブルシューティング

メディアまたはストレージサーバーが互換性のない古いバージョンであることが原因で、Web UI でディスクボリュームを作成できない場合があります。メディアサーバーとストレージサーバーの両方が 10.3 以降であることを確認します。

次のエラーメッセージは、メディアサーバーまたはストレージサーバーに互換性がないことを示します。

- `One or more invalid arguments`
  このエラーは無効な入力をしたか、メディアサーバーに互換性がないために表示されます。入力内容を確認して、メディアサーバーとストレージサーバーの両方が 10.3 以降であることを確認します。
- `The object "<bucket>/<disk volume name>/lockdown-mode.conf" or the object "<bucket>/<disk volume name>/lsu-worm.conf" does not exist, or neither object "<bucket>/<disk volume name>/lockdown-mode.conf" nor object "<bucket>/<disk volume name>/lsu-worm.conf" exists`
  ストレージサーバーはクラウドボリュームの作成に失敗しました。`msdpcldutil` を使用してクラウドボリュームを作成する場合、ディスクボリュームを引き続き作成できます。`msdpcldutil` によって設定されるボリュームの保持モードと保持範囲は保持されます。Web UI の入力は無視されます。
  『NetBackup コマンドリファレンスガイド』の msdpcldutil に関するトピックを参照してください。

エンタープライズモードを使用した変更不可イメージの削除

エンタープライズモードの保持ロックを使用して、変更不可イメージを削除できます。

エンタープライズモードを使用して変更不可イメージを削除するには

1. クラウド管理者の環境変数 `MSDPC_ACCESS_KEY`、`MSDPC_SECRET_KEY` をエクスポートします。

   ```
   export MSDPC_ACCESS_KEY=<your access key id>

   export MSDPC_SECRET_KEY=<your secret key>
   ```

2. 次のコマンドを実行して、バックアップ ID とコピー番号を見つけます。

   ```
   catdbutil --worm list --allow_worm
   ```

3 保持ロックを解除します。

```
catdbutil --worm disable --backupid ${my_backup_id} --copynum
${my_copy_num} --allow_worm
```

4 NetBackup プライマリサーバーで NetBackup コマンドを使用して WORM イメージを期限切れにします。

```
bpexpdate -backupid ${my_backup_id} -d 0 -try_expire_worm_copy
-copy ${my_copy_num}
```

S3 オブジェクトの永続的な削除

変更不可バケットを作成すると、バケットのバージョン管理が有効になります。これにより、誤って削除または上書きされたオブジェクトをリストアできます。オブジェクトを (永続的な削除ではなく) 削除すると、変更不可の S3 クラウドは削除マーカーを挿入し、これが現在のオブジェクトバージョンになります。

その後、前のバージョンをリストアできます。オブジェクトを上書きすると、バケット内に新しいオブジェクトバージョンが作成されます。保護されたオブジェクトを完全に削除するには、バージョン管理を使用してオブジェクトを削除する必要があります。

MSDP クラウド管理ツールについて

10.2 以降のバージョンの NetBackup で、Web UI を介して WORM パラメータを作成、変更、表示できます。このため、`msdpcldutil` コマンドラインの使用が削減されるようになりました。

ほとんどのタスクを Web UI から実行できます。ただし、次のタスクは、`msdpcldutil` を使用してのみ実行できます。

- `msdpcldutil update inherit`
- `msdpcldutil history list`
- `msdpcldutil history download`
- `msdpcldutil platform checkperm`
- `msdpcldutil bucket`

詳しくは、『NetBackup Appliance コマンドリファレンスガイド』の `msdpcldutil` のセクションを参照してください。

AWS IAM Role Anywhere のサポートについて

AWS IAM Role Anywhere を使用すると、一時的なセキュリティクレデンシャルを使用して、安全な方法で AWS S3 ストレージを認証できます。AWS アカウントで IAM Role Anywhere を設定し、必要な証明書と秘密鍵を使用して認証できます。

メモ: IAM Role Anywhere は AWS Recovery Vault ではサポートされません。また、IAM Role Anywhere と、アクセスキーなどの他の認証タイプを切り替えることはできません。

AWS IAM Role Anywhere 構成の前提条件

- AWS アカウントで IAM Role Anywhere を作成し、必要な証明書や秘密鍵を使用して認証するには、そのための権限が必要です。
- 構成を開始する前に、次を作成して情報を手元に用意してください。
  - プロファイル ARN
  - 役割 ARN
  - トラストアンカー ARN
  - IAM Role Anywhere CA 証明書
  - IAM Role Anywhere 秘密鍵
- AWS でのリソースの設定について詳しくは、次を参照してください。
  https://docs.aws.amazon.com/rolesanywhere/latest/userguide/getting-started.html

AWS での IAM Role Anywhere の構成

AWS で IAM Role Anywhere を設定するには、次の手順を実行します。

- 「必要な証明書の作成」
- 「トラストアンカーの作成」
- 「ポリシーの作成」
- 「役割の作成」
- 「プロファイルの作成」

必要な証明書の作成

CA 証明書は、Amazon のプライベート CA 認証局を通じて作成 (有料) するか、プライベート CA 認証局を設定して CA 証明書を作成 (無料) します。

Amazon のプライベート CA リソースを使用するには、次の AWS のマニュアルを参照してください。

https://docs.aws.amazon.com/acm-pca/latest/userguide/PcaWelcome.html

プライベート CA 認証局を設定し、CA 証明書を作成することで、無料で CA 証明書を作成するには、次を参照してください。

https://docs.aws.amazon.com/rolesanywhere/latest/userguide/getting-started.html

証明書とキーの使用

1. ルート CA 証明書ファイルを使用して、AWS にトラストアンカーを作成します。
2. 認証には、自己署名した CA 証明書ファイルと、NetBackup のルート CA 証明書から作成した秘密鍵を使用します。

AWS 証明書の仕様については、次を参照してください。

https://docs.aws.amazon.com/rolesanywhere/latest/userguide/trust-model.html

署名の検証

クレデンシャル要求を認証するため、IAM Roles Anywhere は、証明書のキータイプに必要な署名検証アルゴリズム (RSA や ECDSA など) を使用して、受け取った署名を検証します。署名の検証後、IAM Roles Anywhere は、公開鍵インフラストラクチャ X.509 (PKIX) 標準によって定義されたアルゴリズムを使用して、アカウントのトラストアンカーとして構成された認証局によって証明書が発行されたことを確認します。

エンドエンティティ証明書は、認証に使用するため、次の制約を満たす必要があります。

- 証明書は *X.509v3* である必要があります。
- 基本的な制約に *CA: false* が含まれている必要があります。
- キーの使用法に *Digital Signature* が含まれている必要があります。
- 署名アルゴリズムに *SHA256* 以上が含まれている必要があります。*MD5* と *SHA1* の署名アルゴリズムは拒否されます。

トラストアンカーとして使用される証明書は、署名アルゴリズムと同じ要件を満たす必要がありますが、次の違いがあります。

- キーの使用法に *Certificate Sign* が含まれている必要があります。*CRL Sign* が含まれる場合もあります。CRL (証明書失効リスト) は、IAM Roles Anywhere のオプション機能です。
- 基本的な制約に *CA: true* が含まれている必要があります。

トラストアンカーの作成

トラストアンカーを作成するには、AWS のマニュアルを参照してください。

https://docs.aws.amazon.com/rolesanywhere/latest/userguide/getting-started.html

ポリシーの作成

AWS コンソールでポリシーを作成し、NetBackup に必要な次の権限を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetBucketObjectLockConfiguration",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketPolicyStatus",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:GetBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteBucket",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketVersioning",
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:PutObjectRetention",
                "s3:RestoreObject"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages"
```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

役割の作成

AWS コンソールで役割を作成します。詳しくは AWS のマニュアルを参照してください。

https://docs.aws.amazon.com/rolesanywhere/latest/userguide/getting-started.html#getting-started-step2

必要なパラメータが入力されたポリシーは次のようになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "rolesanywhere.amazonaws.com"
                ]
            },
            "Action": [
              "sts:AssumeRole",
              "sts:TagSession",
              "sts:SetSourceIdentity"
            ],
            "Condition": {
              "ArnEquals": {
                "aws:SourceArn": [
                  "arn:aws:rolesanywhere:<REGION>:<ACCOUNT
NUMBER>:trust-anchor/<TRUST ANCHOR ID>"
                ]
              },
              "StringEquals": {
                    "<PRINCIPAL TAG CHECK>"
              }
            }
        }
    ]
}
```

NetBackup では ArnEquals と Principal Tag StringEquals のチェックは必要ありませんが、これらは推奨されるセキュリティ制約です。

プロファイルの作成

AWS コンソールでプロファイルを作成します。詳しくは、以下を参照してください。

https://docs.aws.amazon.com/rolesanywhere/latest/userguide/getting-started.html

AWS IAM Anywhere を使用した新しいディスクプールの構成

AWS IAM Anywhere を使用して新しいディスクプールを作成するには、次の手順を実行します。

表 6-8

手順	作業	手順の詳細
手順 1	(オプション) MSDP ストレージサーバーが存在しない場合は作成します。	詳しくは、『NetBackup 重複排除ガイド』の「MSDP サーバー側の重複排除の構成」を参照してください。
手順 2	ディスクプールを追加します。	NetBackup Web UI で、ディスクプールを作成します。『NetBackup Web UI 管理者ガイド』の「ディスクプールの作成」の手順に従います。 ■ [ボリューム (Volumes)] 手順で、次の手順を実行します。 ■ [クラウドストレージプロバイダ (Cloud storage provider)] ドロップダウンから、Amazon または Amazon Government のオプションを選択します。 ■ 適切な地域を選択します。 ■ [Amazon アカウントのアクセスの詳細 (Access details for Amazon account)] セクションの [認証形式 (Authentication type)] で IAM Role Anywhere を選択し、[Add a New Credential (新しいクレデンシャルの追加)] を選択します。p.264 の「MSDP-C のクレデンシャルの管理」を参照してください。 Amazon のクレデンシャルがある場合は、[既存のクレデンシャルの選択 (Select existing credentials)] を使用することもできます。 ■ クレデンシャルを指定したクラウドバケット名を入力します。

手順	作業	手順の詳細
手順 3	ストレージユニットを追加します。	NetBackup Web UI で、ストレージユニットを作成します。『NetBackup Web UI 管理者ガイド』の「ストレージユニットの作成」の手順に従います。 ストレージユニットを作成するときに、[メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP))] オプションを選択します。[ディスクプール (Disk pool)] の手順で、手順 3 で作成したディスクプールを選択します。

Azure サービスプリンシパルのサポートについて

Azure サービスプリンシパルを使用すると、シークレットキーの公開や自動更新を行わずに、安全な方法で Azure Blob Storage を認証できます。NetBackup は、指定されたストレージアカウント、クライアント ID、テナント ID、シークレットキーを使用して、クラウドリソースにアクセスするための一時的なクレデンシャルを取得します。

メモ: Azure Recovery Vault では、サービスプリンシパルはサポートされません。また、Azure サービスプリンシパルと他の認証形式との切り替えはサポートされません。

メモ: MSDP クラウド配備での Azure サービスプリンシパルの使用は FIPS 準拠ではありません。

Azure サービスプリンシパル構成の前提条件

- サービスプリンシパルを設定および使用して認証するには、そのための権限が必要です。詳しくは、Azure のマニュアルを参照してください。
  https://learn.microsoft.com/ja-jp/azure/active-directory/develop/howto-create-service-principal-portal
- サービスプリンシパルを作成するときは、NetBackup で必要な API 呼び出しを実行できるようにするための役割を付与する必要があります。次の処理権限を使用して、カスタム役割の定義を作成する必要があります。

  ```
  "Microsoft.Storage/storageAccounts/blobServices/containers/delete"
  "Microsoft.Storage/storageAccounts/blobServices/containers/read"
  "Microsoft.Storage/storageAccounts/blobServices/containers/write"
  "Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action"
  "Microsoft.Storage/storageAccounts/blobServices/read"
  "Microsoft.Storage/storageAccounts/read"
  ```

  必要なデータ処理権限を次に示します。

```
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete"
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read"
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action"
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action"
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/deleteBlobVersion/action"
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/immutableStorage/runAsSuperUser/action"
```

- 構成を開始する前に、次を作成して情報を手元に用意してください。
  - ストレージアカウント
  - クライアント ID
  - テナント ID
  - シークレットキー

Azure サービスプリンシパルの構成

Azure サービスプリンシパルを設定するには、次の手順を実行します。

- 「カスタム役割の作成」
- 「新しいサービスプリンシパルの作成」

カスタム役割の作成

NetBackup のサービスプリンシパルで使用する Azure RBAC のカスタム役割を作成するには、Azure のマニュアルを参照してください。

https://learn.microsoft.com/ja-jp/azure/role-based-access-control/custom-roles

次の点に注意してください。

- 役割の範囲は、サブスクリプションレベルである必要があります。これにより、サービスプリンシパルは、サブスクリプション内のすべてのストレージアカウントで動作します。
- 必要な処理権限とデータ処理権限を付与します。

新しいサービスプリンシパルの作成

新しいサービスプリンシパルを作成するには、Azure のマニュアルを参照してください。

https://learn.microsoft.com/ja-jp/entra/identity-platform/howto-create-service-principal-portal

サービスプリンシパルを作成する際は、作成したアプリケーション (クライアント) ID、ディレクトリ (テナント) ID、シークレットキーを使用します。

カスタム役割をサービスプリンシパルに確実に割り当ててください。

Azure サービスプリンシパルを使用したディスクプールの構成

Azure サービスプリンシパルを使用して新しいディスクプールを作成するには、次の手順を実行します。

表 6-9

手順	作業	手順の詳細
手順 1	(オプション) MSDP ストレージサーバーが存在しない場合は作成します。	詳しくは、『NetBackup 重複排除ガイド』の「MSDP サーバー側の重複排除の構成」を参照してください。
手順 2	ディスクプールを追加します。	NetBackup Web UI で、ディスクプールを作成します。『NetBackup Web UI 管理者ガイド』の「ディスクプールの作成」の手順に従います。 ■ [ボリューム (Volumes)] 手順で、次の手順を実行します。 ■ [クラウドストレージプロバイダ (Cloud storage provider)] ドロップダウンから、Microsoft Azure または Microsoft Azure Government のオプションを選択します。 ■ 適切な地域を選択します。 ■ [Azure アカウントのアクセスの詳細 (Access details for Azure account)] セクションの [認証形式 (Authentication type)] でサービスプリンシパルを選択し、[Add a New Credential (新しいクレデンシャルの追加)] を選択します。p.264 の「MSDP-C のクレデンシャルの管理」を参照してください。 Azure のクレデンシャルがある場合は、[既存のクレデンシャルの選択 (Select existing credentials)] を使用することもできます。 ■ クレデンシャルを指定したクラウドバケット名を入力します。
手順 3	ストレージユニットを追加します。	NetBackup Web UI で、ストレージユニットを作成します。『NetBackup Web UI 管理者ガイド』の「ストレージユニットの作成」の手順に従います。 ストレージユニットを作成するときに、[メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP))] オプションを選択します。[ディスクプール (Disk pool)] の手順で、手順 3 で作成したディスクプールを選択します。

オブジェクトストレージのインスタントアクセスについて

次の表に、オブジェクトストレージのインスタントアクセスでサポートされるプラットフォームを示します。

表 6-10 サポート対象プラットフォーム

サポート対象プラットフォーム	説明
Azure Kubernetes Service (AKS)	このプラットフォームはサポートされており、デフォルトでは有効になっています。
Amazon Elastic Kubernetes Service (EKS)	このプラットフォームはサポートされており、デフォルトでは有効になっています。
Azure または AWS 内の VM (独自構築クラウド (BYO-In-Cloud))	このプラットフォームはサポートされています。このオプションは手動で有効にする必要があります。
オンプレミスの MSDP (BYO、Flex メディアサーバー、NetBackup Appliance)	このプラットフォームはサポートされています。このオプションは手動で有効にする必要があります。MSDP からオブジェクトストアへの接続には、良好なネットワーク帯域幅と遅延が必要です。

AKS または EKS プラットフォームでは、オブジェクトストレージのインスタントアクセスがデフォルトで有効になっています。インスタントアクセスがデフォルトで有効になっていない場合は、次の手順を手動で実行して有効にする必要があります。

1. ストレージサーバーで */etc/msdp-release* ファイルに `instant-access-object-store = 1` オプションを追加します。
2. 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て `IA_OBJECT_STORE` 名が `extendedcapabilities` オプションに含まれているかどうかを確認します。

   例:

   ```
   nbdevconfig -getconfig -stype PureDisk
   -storage_server your_storage_server_name
   |grep IA_OBJECT_STORE
   ```

3. プライマリまたはメディアサーバーで、次のコマンドを実行してストレージサーバーの属性を再ロードします。

   ```
   nbdevconfig -getconfig -stype PureDisk
   -storage_server your_storage_server_name > /tmp/flags

   nbdevconfig -setconfig -stype PureDisk
   -storage_server your_storage_server_name -configlist /tmp/flags
   ```

AWS Snowball Edge の NetBackup のサポートについて

NetBackup は、AWS S3 に対してデータをインポートまたはエクスポートするためにオンボードストレージを使用する AWS Snowball Edge デバイスをサポートします。デバイスがオンプレミスに到着したら、NetBackup はデータをデバイスに格納し、その後 AWS にインポートできます。NetBackup では、イメージ共有によってデバイスにロードされた NetBackup データもリカバリできます。

デバイスとの通信

NetBackup の外部にあるデバイスと通信するための 2 つの主要なツールは、Snowball Edge クライアント CLI と Ops Hub UI です。これらは、Snowball Edge デバイスがインストールされているのと同じデータセンターに存在する VM にインストールして使用する必要があります。

クライアントと AWS Ops Hub による AWS Snowball Edge との通信には、ロック解除コードと、AWS ポータルから取得できるマニフェストファイルが必要です。Snowball Edge デバイスをインポートするリージョンで、Snow Family コンソールに移動し、サイドバーの［Jobs］を選択します。インポートジョブが表示されます。ジョブをクリックし、ページを下にスクロールしてロック解除コードとマニフェストファイルを取得します。デバイスとの通信に使用する VM にロック解除コードとマニフェストファイルをコピーします。

クレデンシャルの使用

通常の S3 IAM クレデンシャルではなく、デバイスのローカルユーザーのクレデンシャルを使用します。root クレデンシャルは、AWS Snowball Edge クライアントから取得できます。

最初にアクセスキーを取得します。

```
<client install location>/snowballEdge list-access-keys
--manifest-file <manifest file location>
--unlock-code <code>
--endpoint https://<ip-address-of-snowball-edge-device>
```

次にシークレットキーを取得します。

```
<client install location>/snowballEdge get-secret-access-key
--manifest-file <manifest file location> --unlock-code <code>
--endpoint https://<ip-address-of-snowball-edge-device>
--access-key-id <access key from previous command output>
```

メモ: ベストプラクティスは、root 以外のユーザーを構成することです。ローカルユーザーを作成するには、次の手順を参照してください。

ローカルユーザー AWS Snowball の設定

AWS Snowball Edge 用の NetBackup の構成

AWS Snowball Edge と連携するように NetBackup を構成するには、次の手順を使用します。

メモ: 手順 2 では別のインスタンス名を使用できますが、残りの手順でも必ずそのインスタンス名を使用してください。

AWS Snowball Edge 用に NetBackup を構成するには

1. プライマリサーバーにログオンします。
2. 新しいインスタンスを追加するには、次のコマンドを実行します。

```
/usr/openv/netbackup/bin/admincmd/csconfig cldinstance -a
-in <instance name> -pt
amazon -sh <IP address of snowball>
-http_port <8080>
-https_port <8443>
-access_style 2
```

3. 地域または場所の制約を追加するには、次のコマンドを実行します。

```
/usr/openv/netbackup/bin/admincmd/csconfig cldinstance -ar
-in <instance name>
-rn "<region where AWS Snowball edge device is imported>"
-lc "<location constraint for the region>"
-sh <ip address of AWS Snowball Edge device>
```

4. Web UI で MSDP クラウドを通常どおり構成します。
   - ディスクプールを追加する場合は、Amazon をプロバイダとして使用してカスタム地域を選択してください。
   - ディスクプールを構成するときの SSL オプションについては、AWS Snowball Edge デバイスが SSL を使用して構成されていない場合は SSL を無効にします。SSL を使用したデバイスの構成については、「「AWS Snowball Edge 用の SSL の構成」」セクションを参照してください。
   - バケット名は手動で入力する必要があります。AWS Snowball Edge デバイス上のバケットと一致することを確認します。

AWS Snowball Edge デバイスを指す MSDP クラウドストレージを構成したら、デバイスに直接データを書き込むバックアップポリシーを作成できます。ストレージライフサイクルポリシー (SLP) を作成して、ローカル MSDP ストレージから AWS Snowball Edge デバイスにデータを複製することもできます。このデバイスは、サポートされている他の NetBackup 操作の実行にも使用できます。

メモ: AWS Snowball Edge デバイスのバケットは、必要に応じて AWS に存在します。AWS Snowball Edge デバイスをインポートジョブに使用するには、AWS に既存のバケットが必要です。

AWS Snowball Edge 用の SSL の構成

AWS Snowball Edge 用に SSL を構成する方法

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

```
<client install location>/snowballEdge list-certificates
--manifest-file <path-to-manifest-file> --unlock-code
<unlock-code-from-aws-portal> --endpoint
https://<snowball-edge-IP>
```

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

```
<client install location>/snowballEdge get-certificate
--certificate-arn <arn-value-from-last-cmd> --manifest-file
<path-to-manifest-file> --unlock-code
<unlock-code-from-aws-portal> --endpoint
https://<snowball-edge-IP>
```

3 手順 2 の出力の証明書を、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。

SSL を有効にした AWS Snowball Edge 用の NetBackup の構成

SSL を有効にした AWS Snowball Edge 用の NetBackup を構成する方法

1 インスタンスを作成し、`https_port 8443` を使用する必要があります。

```
/usr/openv/netbackup/bin/admincmd/csconfig cldinstance -a -in
<snowball instance name> -pt amazon -sh <IP of snowball device>
-http_port 8080 -https_port 8443 -access_style 2
```

2 MSDP Cloud AWS Snowball Edge 用のディスクプールの作成中は、[セキュリティ (Security)]で[SSL を使用する (Use SSL)]を選択し、[証明書の失効を確認する (Check certificate revocation)]を選択解除します。

3 他の手順は、「「AWS Snowball Edge 用の NetBackup の構成」」セクションと同じにする必要があります。

デバイスの発送

データをデバイスに書き込み、Amazon にデバイスを発送する準備ができたら、ネットワークからデバイスを切断する前に、次の手順を実行します。

1. 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一時停止にします。次のコマンドを実行して、セカンダリ操作を一時停止します。

```
/usr/openv/netbackup/bin/admincmd/nbstlutil inactive -lifecycle
<slp_name>
```

2. AWS Snowball Edge ボリュームを停止します。

```
/usr/openv/netbackup/bin/admincmd/nbdevconfig -changestate -stype
PureDisk -dp disk_pool_name -dv <disk_volume_name> -state DOWN
```

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

デバイスが AWS に到着後、S3 バケットにデータをインポートするのに数日かかります。インポート時間は、デバイスに存在するデータのサイズによって異なります。[AWS portal]、[AWS Snow Family]の順に選択すると、インポートジョブの進捗状況を表示できます。インポートジョブが完了したら、成功ログとエラーログを確認して、必要なデータが S3 バケットに正常にインポートされたことを確認します。

バックアップが S3 バケットにインポートされた後、NetBackup 操作を実行する前に、「「S3 と連携するための NetBackup の再構成」」セクションの手順を実行します。

S3 と連携するための NetBackup の再構成

AWS リージョンの次のリストは、デフォルトの AWS リージョンとしてと見なされます: 中国北京、中国寧夏、米国東部、GovCloud-US-West、US-East。これらのリージョンを使用するには、「「バケットがデフォルトの AWS リージョンにある場合」」の手順を使用して、S3 と連携するように NetBackup を再構成する必要があります。

次の点に注意してください。

- `csconfig` コマンドを使用する場合、プライマリサーバーでコマンドを実行する必要があります。
- `pdde` コマンドは、メディアサーバー、または AWS Snowball Edge で構成されたストレージサーバーが配置されている場所で実行する必要があります。
- バックアップポリシーを有効にする前に、AWS アカウントのクレデンシャルを使用するようにクレデンシャルを更新する必要があります。Snowball Edge デバイス自体には独自のクレデンシャルセットがあるため、NetBackup がストレージエンドポイントとして Snowball デバイスを使用するように構成されている場合、このセットが最初に使用されます。
- CMS がサポートされている場合、AWS Snowball Edge のクレデンシャルと AWS クレデンシャルを CMS に格納する必要があります。NetBackup の初期構成時には、CMS から AWS Snowball Edge クレデンシャルを使用する必要があります。再構成が実行されたら、CMS の AWS アカウントのクレデンシャルを使用するようにストレージを更新して、NetBackup がクラウドのバケットで認証できるようにする必要があります。

バケットがデフォルトの AWS リージョンにある場合

バケットがデフォルトの AWS リージョンにあって、AWS Snowball Edge へのバックアップを実行した後に S3 と連携するように NetBackup を再構成する場合は、次の手順を使用します。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。

バックアップの実行後に S3 と連携するように NetBackup を再構成するには

1. AWS Snowball Edge をターゲットとするバックアップポリシーと SLP が無効になっていることを確認します。無効になっていない場合は、再構成手順を続行する前に無効にします。

   次のコマンドを実行して、SLP のセカンダリ操作を一時停止します。

   ```
   /usr/openv/netbackup/bin/admincmd/nbstlutil inactive -lifecycle
   <slp_name>
   ```

2. カスタムインスタンス用に作成されたストレージサーバー名を取得するには、次のコマンドを実行し、ディスクプールの作成時に構成されたストレージサーバーを書き留めます。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -i -in
   <name of your instance>
   ```

3. カスタムインスタンスからストレージサーバーを削除するには、次のコマンドを実行します。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -rs -in
   <instance name> -sts <storage server name from step 2>
   ```

4. amazon.com インスタンスにストレージサーバーを追加するには、次のコマンドを実行します。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in
   amazon.com -sts <storage server name from step 2>
   ```

5. `/usr/openv/netbackup/bin/admincmd/csconfig r` を実行して、クラウドインスタンスを更新します。

6. AWS Snowball Edge ボリュームを起動します:
   `/usr/openv/netbackup/bin/admincmd/nbdevconfig -changestate -stype PureDisk -dp <disk_pool_name> -dv <disk_volume_name> -state UP`

7. NetBackup Web UI にログオンします。

8. NetBackup Web UI で[ディスクプール (Disk pool)]に移動し、AWS アカウントのクレデンシャルを使用してクレデンシャルを更新します。

9. メディアサーバーで `pdde` サービスを再起動します。

   - `/usr/openv/pdde/pdconfigure/pdde stop`
   - `/usr/openv/pdde/pdconfigure/pdde start`

10. NetBackup Web UI で、[ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ディスクプール (Disk pools)]の順に移動し、ディスクプールを選択して[ディスクボリュームの更新 (Update disk volume)]をクリックします。

11 次のコマンドを実行して Status = UP を検証します:

```
/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype
PureDisk -U -dp <disk_pool_name>
```

12 NetBackup Web UI で[ディスクプールの詳細 (Disk pool details)]ページを開き、[クラウドの詳細 (Cloud details)]セクションで、[サービスホスト (Service host)]がリージョンの AWS サービスホストに更新されていることを確認します。

13 バックアップポリシーをアクティブ化するか、SLP のセカンダリ操作の処理をアクティブ化します。次のコマンドを使用して SLP のセカンダリ操作をアクティブ化できます。

```
/usr/openv/netbackup/bin/admincmd/nbstlutil active -lifecycle
<slp_name>
```

14 リストアを実行し、データを確認します。NetBackup Web UI を使用してイメージを検証します。

バケットがデフォルト以外の AWS リージョンに存在する場合 (またはストレージが AWS リージョンにすでに存在する)

デフォルト以外の AWS リージョンで S3 と連携するために NetBackup を再構成する方法

1 AWS Snowball Edge をターゲットとするバックアップポリシーと SLP が無効になっていることを確認します。無効になっていない場合は、再構成手順を続行する前に無効にします。

次のコマンドを実行して、SLP のセカンダリ操作を一時停止します。

```
/usr/openv/netbackup/bin/admincmd/nbstlutil inactive -lifecycle
<slp_name>
```

2 NetBackup Web UI で、[ホスト (Hosts)]、[マスターサーバー (Master servers)]、<お使いのマスターサーバー>、[クラウドストレージ (Cloud Storage)]の順に移動して、Snowball Edge デバイスを指すクラウドストレージを編集します。サービスホストは S3 エンドポイント (s3.dualstack.<region ID>.amazonaws.com)、HTTP/HTTPS ポートは 80/443、リージョンは <region ID> で、サービスホストと同じエンドポイントにします。

3 AWS Snowball Edge インスタンスで SSL を無効にした場合は、再度有効にします。

NetBackup 管理コンソールからのみ SSL を有効にできます。

- [ホストプロパティ (Host Properties)]、[マスターサーバー (Master Servers)]、<お使いのマスターサーバー>、[クラウドストレージ (Cloud Storage)]の順に移動します。
- AWS Snowball Edge デバイスを指すクラウドストレージをクリックします。

- ［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)］の表で、ストレージサーバー名を選択し、［変更 (Change)］をクリックします。
- ［SSL を使用する (Use SSL)］と［データ転送 (Data Transfer)］を選択します。
- ［保存 (Save)］をクリックします。

4 NetBackup Web UI で［ディスクプール (Disk pool)］に移動し、AWS アカウントのクレデンシャルを使用してクラウドクレデンシャルを更新します。

5 クラウドインスタンスを更新するには、次のコマンドを実行します。

```
/usr/openv/netbackup/bin/admincmd/csconfig r
```

6 AWS Snowball Edge ボリュームを起動します。

```
/usr/openv/netbackup/bin/admincmd/nbdevconfig -changestate
-stypePureDisk -dp <disk_pool_name> -dv <disk_volume_name>
-stateUP
```

7 メディアサーバーで pdde サービスを再起動します。

- /usr/openv/pdde/pdconfigure/pdde stop
- /usr/openv/pdde/pdconfigure/pdde start

8 次のコマンドを実行して Status= UP を検証します:

```
/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype
PureDisk -U -dp <disk_pool_name>
```

9 バックアップポリシーをアクティブ化するか、SLP のセカンダリ操作の処理をアクティブ化します。次のコマンドを使用して SLP のセカンダリ操作をアクティブ化します。

```
/usr/openv/netbackup/bin/admincmd/nbstlutil active -lifecycle
<slp_name>
```

10 リストアを実行し、データを確認します。

CLI を使用した AWS Snowball Edge 用の NetBackup の構成

CLI を使用して AWS Snowball Edge 用に NetBackup を構成するには

1. プライマリサーバーにログオンします。
2. AWS Snowball Edge デバイスのカスタムインスタンスを追加するには、次のコマンドを実行します。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -a -in
   <instance name> -pt amazon -sh <hostname of your snowball server>
   -http_port_8080 -access_style 2
   ```

   メモ: SSL を有効にして AWS Snowball Edge 用の NetBackup を構成する場合は、`-https_port 8443` を使用します。

3. AWS Snowball Edge 用のカスタムインスタンスを作成します。次のコマンドを実行します。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -ar -in
   <instance name> -rn <region snowball edge device is imported> -lc
   <location constraint of the region> -sh <IP address of snowball
   edge device>
   ```

4. カスタムインスタンスのエイリアスを作成します。

   ```
   /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in
   <instance name> -sts <storage server name> -lsu_name <name of
   LSU> -crl 0 -ssl 0
   ```

5. 次のように構成ファイルを作成します。

   - [root@instancename# cat /add_lsu.txt

     V7.5 "operation" "add-lsu-cloud" string

     V7.5 "lsuName" "<lsu name used in last step> string

     V7.5 "cmsCredName" "<Snowball CMS CredName>" string

     V7.5 "lsuCloudBucketName" "<Bucket name on Snowball>" string

     V7.5 "lsuCloudBucketSubName" "<Volume name in the bucket>"
     string

メモ: クラウド認証に CMS を使用する場合は、"lsuCloudUser" および "lsuCloudPassword" の代わりに、構成ファイルの CMS クレデンシャル名を使用します。次の形式を使用します。

```
V7.5 "cmsCredName" "<Snowball_credential_name>" string
```

- 作成した構成ファイルを使用してストレージサーバーの構成を更新するには、次のコマンドを実行します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
  -storage_server <storage server name> -stype PureDisk
  -configlist /add_lsu.txt
  ```

- ディスクボリュームをプレビューして一時ファイルにコピーするには、次のコマンドを実行します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv
  -storage_server <storage server name> -stype PureDisk | grep
  <Volume name> > /tmp/dvlist
  ```

- ディスクプールを作成するには、次のコマンドを実行します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp
  <disk pool name> -stype PureDisk -dvlist /tmp/dvlist
  -storage_servers <storage server name>
  ```

6 ストレージユニットを作成するには、次のコマンドを実行します。

```
/usr/openv/netbackup/bin/admincmd/bpstuadd -label <storage unit
name> -odo 0 -dt 6 -dp <disk pool name> -nodevhost
```

大規模なバックアップリストアでの AWS Snowball Edge の使用

データセンターから AWS クラウドへのバックアップデータの移動を高速化する Snowball バックアップの使用例で、顧客データセンターから AWS クラウドへのネットワーク帯域幅が制限されている場合と同様です。AWS Snowball Edge デバイスに AWS バックアップを格納し、顧客データセンターに発送してリストアするという方法でリストア処理を高速化するためにも AWS Snowball Edge を使用できます。

バケットからリストアするデータの量によっては、目的のイメージを別のバケットに複製するためにかかる時間に相当する場合があります。その後、AWS Snowball Edge からエクスポートを実行します。このエクスポートは、クラウドのイメージ共有サーバーを使用することで実現できます。

バケット内の AWS バックアップを Snowball にリストアするには、次の 2 つの方法があります。

- Snowball へのバックアップに使用されるバケット全体のリストア。

- 必要なバックアップを新しいバックアップに複製し、新しいバケットを Snowball にリストア。

最初のオプションではバックアップ全体をリストアする必要があり、多くのバックアップが含まれ、データの量が非常に多くなる場合があります。2 つ目のオプションでは、必要なバックアップだけを移動できます。

AWS Snowball Edge のエクスポートジョブの間、エクスポートされるバケットのデータは読み取り専用になります。この制限は、データの競合状態を防ぐための AWS の制限事項です。データの移動中、バケットへのバックアップは作成できません。

ネットワーク速度によっては、EC2 インスタンスのイメージ共有サーバーを使用した S3 バケット間での 1 TB のデータ複製に、時間がかかることがあります。したがって、大量の TB データを含む一般的な Snowball 作業負荷の場合、複製には数時間から数日間かかる場合があります。イメージ共有の代わりの手段として、ソースバケットから直接エクスポートし、デバイスの移動中にはデータにアクセスできないようにする方法があります。デバイスの移動には通常数日かかります。これらの 2 つのソリューションの利点と欠点は、特定のエクスポートのニーズに応じて検討する必要があります。

イメージ共有を使用して AWS Snowball Edge によってデータをエクスポートするには

1. ソースバケットとターゲットバケットの両方が存在するのと同じリージョン内に EC2 インスタンスを作成します。このワークフローでは、ネットワークパフォーマンスが重要です。VM が属する VPC に S3 エンドポイントが構成されていることを確認します。これにより、EC2 と S3 間のネットワーク速度が高速化するためです。
2. EC2 インスタンスに NetBackup をインストールします。
3. イメージ共有用に MSDP ストレージサーバーを構成します。
4. Web UI を使用して、ソースバケットを指すディスクプール、ディスクボリューム、ストレージユニットを構成します。

   ボリュームは、データが作成された元のボリュームと同じ名前である必要があります。
5. イメージをインポートします。
6. CLI を使用して、(空の) 宛先バケットを指すディスクプール、ディスクボリューム、ストレージユニットを構成します。
   - クラウドインスタンスエイリアスを作成します。次のコマンドを実行します。

     ```
     /usr/openv/netbackup/bin/admincmd/csconfig cldinstance -as -in
     amazon.com -sts <storage server> -lsu_name <lsu name>
     ```
   - 構成ファイルを作成して、nbdevconfig コマンドを実行します。
     新しいクラウド LSU を追加するための構成ファイルの内容:

     ```
     V7.5 "operation" "add-lsu-cloud" string
     V7.5 "lsuName" "<lsu name used in last step> string
     V7.5 "cmsCredName" "<cms_cred_name>" string
     ```

```
V7.5 "lsuCloudBucketName" <destination_bucket_name>" string
V7.5 "lsuCloudBucketSubName" "<volume_name_in_bucket>" string

/usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server <storage server> -stype PureDisk -configlist
<configuration file path>
```

- nbdevconfig コマンドを使用して、ディスクプールを作成します。次のコマンドを実行します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -previewdv
  -storage_servers <storage server name> -stype PureDisk | grep
  <LSU name> > /tmp/dvlist
  #/usr/openv/netbackup/bin/admincmd/nbdevconfig -createdp -dp
  <disk pool name> -stype PureDisk -dvlist /tmp/dvlist
  -storage_server <storage server name>
  ```

- bpstuadd コマンドを使用して、ストレージユニットを作成します。次のコマンドを実行します。

  ```
  /usr/openv/netbackup/bin/admincmd/bpstuadd -label <storage
  unit name> -odo 0 -dt 6 -dp <disk pool name> -nodevhost
  ```

現在、Web UI では、イメージ共有サーバーに追加のディスクプールを作成できません。

7. 目的のイメージを宛先ストレージに複製します。
8. Snowball を使用して、宛先バケットからエクスポートジョブを開始します。
9. デバイスがオンプレミスに到着したら、目的のリストアを実行するために AWS Snowball Edge デバイスを指すイメージ共有サーバーを作成します。

AWS Snowball Edge を使用する場合の制限事項

NetBackup で AWS Snowball Edge を使用する場合の制限事項を次に示します。

- AWS Snowball Edge は、次の AWS ストレージ階層をサポートしません。
  - Glacier
  - Deep Archive
  - 低頻度アクセス (IA)
- 変更不可ストレージまたは WORM ストレージはサポートされません。
  - S3 オブジェクトロックを有効にしている場合、またはバケットの IAM ポリシーでバケットへの書き込みが禁止されている場合、AWS Snowball Edge はバケットへの書き込みを実行できません。

- バケットの一覧表示はサポートされていません (AWS はバケットの一覧表示の S3 API をサポートしていません)
  - バケットを取得しようとすると、NetBackup Web UI に[利用可能なクラウドバケットがありません (No cloud buckets available)]と表示されます。
- デバイスはバケットの作成をサポートしていません。この制限は、デバイスへの新しいバケットの作成を許可されていないことが原因です。
- データをアップロードするために AWS に移動中のデバイスにはアクセスできません。そのため、このデバイスを対象にしたすべてのバックアップポリシーと SLP を無効にする必要があります。さらに、アップロード処理が正常に完了するまで、バケットからデータにアクセスできません。
- AWS からデータをエクスポートするためにデバイスが移動中の場合、S3 のバケット内のデータは読み取り専用モードになります。そのため、そのバケットを対象にするすべてのバックアップポリシーと SLP を無効にする必要があります。イメージ共有の場合、データを別のバケットに複製できます。バックアップを元のバケットで実行し続ける必要がある場合は、新しく作成されたバケットがエクスポートジョブのターゲットバケットとして使用されます。

NetBackup 10.3 へのアップグレードとクラスタ環境

NetBackup Cloud Scale や NetBackup Flex Scale などのクラスタ環境では、クラウドボリュームに関連付けられたクレデンシャルを移行して、NetBackup 10.3 以降で新しいエンジンを追加できるようにする必要があります。

クラウドクレデンシャルを CMS に保存し、クレデンシャルを既存のクラウドボリュームに関連付けるには、『NetBackup Web UI 管理者ガイド』の「MSDP クラウドと CMS の移行またはアップグレード」のトピックを参照してください。

クラウドダイレクトについて

MSDP はストレージサーバーにデータコンテナを生成し、それらをバックアップのためにクラウドストレージにアップロードします。クライアントからメディアサーバーとストレージサーバーに、受信するデータストリームを送信します。リストアの場合、ストレージサーバーはクラウドストレージからデータコンテナをダウンロードし、データコンテナファイルからデータセグメントを読み取り、クライアントに送信します。

クライアントまたはメディアサーバーで実行されている `mtstrmd` サービスは、クラウドストレージとの間でイメージデータを直接読み書きします。メタデータのみが、ストレージサーバーに送信されます。これにより、クライアントリソースが活用され、ストレージとメディアサーバーのデータ伝送オーバーヘッドが減少します。

バックアップ用のクラウドダイレクトの構成

この機能を使用するには、Client Direct バックアップを有効にする必要があります。クラウドダイレクトは、pdagutil コマンドを使用して構成できます。クラウドダイレクトバックアップは、Red Hat Linux でのみサポートされます。

バックアップ用にクラウドダイレクトを構成する前に、クライアント側の重複排除を有効にします。

バックアップ用にクラウドダイレクトを構成するには

1. バックアップ用にクラウドダイレクトを構成します。

   ```
   /usr/openv/pdde/pdag/bin/pdagutil --config-cloud-direct-backup
   --storage-path <storage path> --cache-size <cache size>
   ```

2. バックアップ用にクラウドダイレクトを有効にします。

   ```
   /usr/openv/pdde/pdag/bin/pdagutil --update-cloud-direct-backup
   --enable
   ```

3. バックアップ用のクラウドダイレクトを無効にします。

   ```
   /usr/openv/pdde/pdag/bin/pdagutil --update-cloud-direct-backup
   --disable
   ```

4. キャッシュサイズを更新します。

   ```
   /usr/openv/pdde/pdag/bin/pdagutil --update-cloud-direct-backup
   --cache-size <cachesize>
   ```

5. 構成を有効にするために、mtstrmd サービスを再起動します。

   ```
   /usr/openv/pdde/pdag/bin/mtstrmctl --shut-down
   ```

リストア用のクラウドダイレクトの構成

クライアントに対する Client Direct リストアを有効にする必要があります。クラウドダイレクトは、pdagutil コマンドを使用して構成できます。クラウドダイレクトリストアは、Red Hat Linux でのみサポートされます。

リストア用にクラウドダイレクトを構成する前に、Client Direct リストアを有効にします。

p.529 の「 MSDP のクライアントへの直接リストアの構成」を参照してください。

リストア用にクラウドダイレクトを構成するには

1 リストア用にクラウドダイレクトを構成します。

```
/usr/openv/pdde/pdag/bin/pdagutil --config-cloud-direct-restore
--storage-path <storage path> --cache-size <cache size>
```

2 リストア用のクラウドダイレクトの構成後、この機能を有効にします。

```
/usr/openv/pdde/pdag/bin/pdagutil --update-cloud-direct-restore
--enable
```

3 リストア用のクラウドダイレクトの構成後、この機能を無効にします。

```
/usr/openv/pdde/pdag/bin/pdagutil --update-cloud-direct-restore
--disable
```

4 キャッシュサイズを更新します。

```
/usr/openv/pdde/pdag/bin/pdagutil --update-cloud-direct-restore
--cache-size <cachesize>
```

5 構成を有効にするために、mtstrmd サービスを再起動します。

```
/usr/openv/pdde/pdag/bin/mtstrmctl --shut-down
```

MSDP 遅延削除について

MSDP 遅延削除を使用すると、失敗したジョブについて、クラウドにアップロードされたデータを一定期間保持できます。これにより、再試行中のジョブで、すでに正常にアップロードされたデータを参照することが可能になるため、データの重複が削減されて効率が向上し、ストレージコストを削減できます。たとえば、エラーが発生する前に 80% のデータがアップロードされた場合、再試行されたジョブはその 80% を使用し、残りの 20% のみをアップロードします。この機能は、保持要件が最小の AWS Glacier や Azure Archive などのアーカイブ層で特に役立ちます。

MSDP 遅延削除はデフォルトで有効になっています。失敗したジョブのメタデータは、デフォルトでは 2 日間保持されます。msdpcldutil lazy-delete コマンドを使用して、更新または無効化できます。コマンドの使用方法について詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

MSDP 遅延削除が無効になっている場合に NetBackup イメージクリーンアップを実行すると、クラウドにアップロードされたイメージのフラグメントが削除されます。データがまだオブジェクトストレージに格納されている場合でも、MSDP は削除されたイメージの一意のデータを使用しません。ジョブを再実行すると、同じデータが再びクラウドに格納されます。重複データは、ジョブが再試行されるたびにオブジェクトストレージで増加します。

7

MSDP の S3 インターフェース

この章では以下の項目について説明しています。

MSDP の S3 インターフェースについて

S3 は、クラウドで一般的なストレージインターフェースです。クラウドネイティブアプリケーションとシームレスに連携できます。MSDP の S3 インターフェースは、MSDP サーバー

で S3 API を提供します。MSDP の S3 インターフェースは、Amazon S3 クラウドストレージサービスと互換性があります。バケットの作成、バケットの削除、オブジェクトの格納、オブジェクトの取得、オブジェクトの一覧表示、オブジェクトの削除、マルチパートアップロードなど、一般的に使用される S3 API のほとんどをサポートします。

MSDP の S3 インターフェースは、オブジェクトのバージョン管理、IAM、ID ベースのポリシーもサポートします。snowball-auto-extract を使用して、小さいオブジェクトのバッチアップロードをサポートします。

MSDP の S3 インターフェースは、MSDP の独自の (BYO) サーバー、Flex Appliance、Flex WORM、AKS/EKS の NetBackup で構成できます。

Flex Appliance で MSDP 構成用の S3 インターフェースを使用する場合は、Flex メディアサーバーにログインし、p.388 の「MSDP の独自の (BYO) サーバーでの MSDP 用 S3 インターフェースの構成」を参照してください。。

Flex WORM の MSDP 構成用の S3 インターフェースの場合は、p.709 の「重複排除シェルからの S3 サービスの管理」を参照してください。

AKS/EKS の NetBackup での MSDP 構成用の S3 インターフェースの場合は、『Kubernetes クラスタ向け NetBackup 配備ガイド』マニュアルの MSDP スケールアウトでの S3 サービスの使用に関するトピックを参照してください。

メモ: API 呼び出しが正常に実行されるように、クライアントと S3 サーバー間の時間を同期する必要があります。

MSDP の独自の (BYO) サーバーの前提条件

MSDP の S3 インターフェースを構成するための前提条件を次に示します。

- ストレージサーバーのオペレーティングシステムは Red Hat Enterprise Linux である必要があります。

  メモ: MSDP の S3 インターフェースは、SUSE Linux Enterprise ではサポートされません。

- ストレージサーバーには 64 GB を超えるメモリと 8 個の CPU を搭載することをお勧めします。
- NGINX がストレージサーバーにインストールされていることを確認します。
  - NGINX バージョンは、対応する正式な RHEL バージョンのリリースに存在するものと同じである必要があります。対応する RHEL yum ソースからインストールする必要があります。

- 次のコマンドを実行して、NGINX の準備ができていることを確認します。

  ```
  systemctl is-active <ngnix service name>
  ```

- /etc/<nginx service>/conf.d の設定が、NGINX の設定に含まれている必要があります。

- SE Linux を有効にした場合は、policycoreutils と policycoreutils-python (RHEL 7 用) パッケージまたは policycoreutils-python-utils (RHEL 8 用) パッケージが同じ RHEL yum ソース (RHEL サーバー) からインストールされていることを確認します。次のコマンドを実行して、MSDP の S3 インターフェースが特別なポートで応答準備できるようにします。

  ```
  semanage port -a -t http_port_t -p tcp <nginx port>
  ```

  次のコマンドを実行して、MSDP の S3 インターフェースがネットワークに接続できるようにします。

  ```
  setsebool -P httpd_can_network_connect 1
  ```

MSDP の独自の (BYO) サーバーでの MSDP 用 S3 インターフェースの構成

MSDP を構成した後、NetBackup Web UI または s3srv_config.sh スクリプトを使用して、MSDP の S3 インターフェースを構成できます。

NetBackup Web UI を使用して MSDP の S3 インターフェースを構成するには、『NetBackup Web UI 管理者ガイド』の「MSDP オブジェクトストアの構成」のトピックを参照してください。

s3srv_config.sh スクリプトを使用して S3 サーバーを構成するには

- MSDP の S3 インターフェースで NBCA または ECA タイプの証明書を使用する場合は、次のコマンドを実行します。

  ```
  /usr/openv/pdde/vxs3/cfg/script/s3srv_config.sh --catype=<type>
  [--port=<port>] [--loglevel=<0-4>]
  ```

  MSDP の S3 インターフェースで証明書を使用する場合は、次のコマンドを実行します。

  ```
  /usr/openv/pdde/vxs3/cfg/script/s3srv_config.sh --cert=<certfile>
  --key=<keypath> [--port=<port>] [--loglevel=<0-4>]
  ```

--catype=<type>	認証局のタイプ。NBCA: 1 または ECA: 2。
--cert=<certfile>	HTTPS の証明書ファイル。
--key=<keypath>	HTTPS の秘密鍵。

`--port=<port>`	S3 サーバーポート。デフォルトのポートは 8443 です。
`--loglevel=<0-4>`	S3 サーバーのログレベル。 ■ なし: 0 ■ エラー: 1 ■ 警告: 2 ■ 情報: 3 (デフォルト) ■ デバッグ: 4
`--help|-h`	使用状況を印刷します。

- S3 サービスは HTTPS サービスです。デフォルトのポートは 8443 です。
- このスクリプトは root ユーザーが直接実行できます。他のサービスユーザーの場合は、このコマンドを次の形式で実行します。
  `sudo -E /usr/openv/pdde/pdcr/bin/msdpcmdrun /usr/openv/pdde/vxs3/cfg/script/s3srv_config.sh <arguments>`
- `/usr/openv/var/vxss/credentials` に複数の証明書が存在する場合、次の設定エラーが表示されることがあります。
  `Too many ca files under /usr/openv/var/vxss/credentials/keystore`
  オプション `--cert` と `--key` を使用して、使用する証明書を指定できます。
- MSDP の S3 インターフェースでは、認証局によって署名されていない証明書で HTTPS を有効にできます。MSDP の S3 インターフェースが SSL 証明書として NBCA で構成されている場合、CA 証明書は S3 サーバーホストの `/usr/openv/var/webtruststore/cacert.pem` になります。MSDP の S3 インターフェースに接続するために AWS CLI を使用する場合、次の 2 つのオプション (`--ca-bundle` と `--no-verify-ssl`) があります。オプション `--ca-bundle` は、SSL 証明書を対応する CA 証明書バンドルに対して検証します。オプション `--no-verify-ssl` は、AWS CLI コマンドでの SSL 証明書の検証を上書きします。次の警告メッセージは無視して構いません。
  `urllib3/connectionpool.py:1043: InsecureRequestWarning: Unverified HTTPS request is being made to host 'xxxx.xxxx.com'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings`
- 証明書とシークレットキーの PEM 形式のみがサポートされます。他の形式の証明書とシークレットキーは PEM 形式に変換してください。
- S3 サーバーを構成した後、S3 サーバーの状態を確認できます。
  root ユーザー: `systemctl status pdde-s3srv`
  その他のサービスユーザー: `sudo -E /usr/openv/pdde/pdcr/bin/msdpcmdrun /usr/openv/pdde/vxs3/cfg/script/s3srv_adm.sh status`

- S3 サーバーを構成した後、S3 サーバーを停止または開始できます。
  root ユーザー: `systemctl stop/start pdde-s3srv`
  その他のサービスユーザー: `sudo -E /usr/openv/pdde/pdcr/bin/msdpcmdrun /usr/openv/pdde/vxs3/cfg/script/s3srv_adm.sh stop|start`
- S3 サーバーについての NGINX 構成は `/etc/<nginx path>/conf.d/s3srvbyo.conf` と `/etc/<nginx path>/locations/s3srv.conf` に保存されます。設定ファイルを修正した場合は、アップグレード後に再度修正する必要があります。

S3 サーバーでの証明書の変更

S3 サーバーの HTTPS 証明書の期限が切れたら、手動で更新する必要があります。または、NBCA を ECA に変更できます。

NBCA を ECA に変更する方法

◆ 次のコマンドを実行します。

```
s3srv_config.sh --changeca --catype=<type>

s3srv_config.sh --changeca --cert=<certfile> --key=<keypath>
```

S3 オブジェクトの ETAG タイプの変更

MSDP S3 サーバーは、サーバーに配置されたオブジェクトごとに ETAG を返します。デフォルトの ETAG タイプは SHA256 です。一部の S3 クライアントで必要な場合は、ETAG タイプを MD5 に変更できます。

S3 オブジェクトの ETAG タイプを変更する方法

1 S3 サーバー構成ファイル `<storage>/etc/puredisk/s3srv.cfg` を開きます。

2 `EtagType` の値を編集します。

```
; Etag type. Valid values are: SHA256, MD5, DOFP
; Note: MD5 cannot be used with FIPS mode
; Note: DOFP uses MSDP DO finger print as ETAG value. Use this
value for best performance.
; @restart
EtagType=SHA256
```

3 S3 サーバーを再起動します。

```
systemctl restart pdde-s3srv
```

MSDP の S3 インターフェースの IAM (Identity and Access Management)

S3 Identity and Access Management (IAM) は、S3 サーバーへのアクセスの制御に役立ちます。

IAM と S3 API 要求の署名

MSDP S3 サーバーは、AWS と同じ署名方法を使用します。署名バージョン 4 とバージョン 2 の両方がサポートされます。要求の署名について詳しくは、次のページを参照してください。

- 署名バージョン 4 の署名プロセス
- 署名バージョン 2 の署名プロセス

IAM ワークフロー

このセクションでは、IAM の典型的なワークフローについて説明します。AWS CLI をインストールして、IAM 関連の API 要求を送信してタスクを完了できます。

IAM ワークフロー

1 S3 サーバーの root ユーザーのクレデンシャルをリセットして取得します。

root ユーザーのクレデンシャルを作成します。root ユーザーを使用して、権限が制限されたユーザーを作成できます。

MSDP の S3 インターフェースを構成した後、次のコマンドを実行して root ユーザーのクレデンシャルを作成します。

```
/usr/openv/pdde/vxs3/cfg/script/s3srv_config.sh --reset-iam-root
```

このコマンドは、root ユーザーのアクセスキーを紛失した場合にも使用できます。root ユーザーの新しいアクセスキーとシークレットキーはコマンド出力で利用可能です。

NetBackup Web UI を使用して root ユーザーのクレデンシャルを作成またはリセットするには、『NetBackup Web UI 管理者ガイド』で MSDP オブジェクトストアの root クレデンシャルのリセットに関するトピックを参照してください。

2 ユーザーを作成します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam create-user --user-name <USER_NAME>
```

3 ユーザーに 1 つ以上のポリシーを接続します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam put-user-policy --user-name <USER_NAME>
--policy-name <POLICY_NAME> --policy-document
file://<POLICY_DOCUMENT_FILE_PATH>
```

4 ユーザーのアクセスキーを作成します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam create-access-key [--user-name <USER_NAME>]
```

メモ: --user-name オプションを省略すると、要求を送信するユーザーの下にアクセスキーが作成されます。

5 ユーザーのアクセスキーを削除します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam delete-access-key [--user-name <USER_NAME>]
--access-key-id <ACCESS_KEY>
```

メモ: --user-name オプションを省略すると、要求を送信するユーザーの下でアクセスキーが削除されます。root ユーザーの最後に有効なアクセスキーを削除することはできません。

6 ユーザーのアクセスキーを一覧表示します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam list-access-keys [--user-name <USER_NAME>]
```

メモ: --user-name オプションを省略すると、要求を送信するユーザーの下にアクセスキーが表示されます。

7 ユーザーのアクセスキーの状態を更新します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam update-access-key [--user-name <USER_NAME>]
--access-key-id <ACCESS_KEY> --status [Active | Inactive]
```

--user-name オプションを省略すると、要求を送信するユーザーの下でアクセスキーが更新されます。

オプション --status は[有効 (Active)]または [無効 (Inactive)]パラメータに従う必要があります (大文字と小文字は区別されます)。

root ユーザーの最後に有効なアクセスキーを[無効 (Inactive)]状態に更新することはできません。

8 特定のユーザーポリシーを取得します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam get-user-policy --user-name <USER_NAME>
--policy-name <POLICY_NAME>
```

9 ユーザーに関連付けられているすべてのポリシーを一覧表示します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam list-user-policies --user-name <USER_NAME>
```

10 ユーザーポリシーを削除します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam delete-user-policy --user-name <USER_NAME>
--policy-name <POLICY_NAME>
```

11 ユーザー情報を取得します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam get-user --user-name <USER_NAME>
```

12 すべてのユーザーを一覧表示します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam list-users
```

13 ユーザーを削除します。

```
aws --endpoint https://<MSDP_HOSTNAME>:8443 [--ca-bundle
<CA_BUNDLE_FILE>] iam delete-user --user-name <USER_NAME>
```

メモ: ユーザーを削除する前に、ユーザーに関連付けられているユーザーポリシーとアクセスキーを削除する必要があります。root ユーザーは削除できません。

MSDP の S3 インターフェースの IAM API

IAM (Identity and Access Management) は、MSDP S3 インターフェースへのアクセスを安全に制御するための Web サービスです。IAM を使用すると、ユーザー、アクセスキーなどのセキュリティクレデンシャル、ユーザーがアクセスできるリソースを制御する権限を一元管理できます。

MSDP S3 インターフェースの IAM 関連の API は、すべての IAM アクションに HTTP POST メソッドのみをサポートします。

共通パラメータ

次の表に、クエリー文字列を使用した署名バージョン 4 の署名リクエストに、すべての処理で使用するパラメーターを示します。

表 7-1 共通パラメータ

パラメータ	説明
`Action`	実行される処理。 タイプ: 文字列 必要/不要: 必要
`Version`	リクエストを作成する API バージョン。形式は YYYY-MM-DD です。 タイプ: 文字列 必要/不要: 不要
`X-Amz-Algorithm`	アクセスキー、日付、リージョン、サービス、終了文字列を含むクレデンシャルスコープの値。値は次の形式で構成されます: `access_key/YYYYMMDD/region/service/aws4_request`。 詳しくは、「タスク 2: 署名バージョン 4 の署名文字列を作成する」を参照してください。 条件: HTTP 認証ヘッダーの代わりにクエリー文字列に認証情報を含める場合は、このパラメータを指定します。 タイプ: 文字列 必要/不要: 該当する場合

パラメータ	説明
X-Amz-Credential	アクセスキー、日付、リージョン、サービス、終了文字列を含むクレデンシャルスコープの値。値は次の形式で構成されます: access_key/YYYYMMDD/region/service/aws4_request。 詳しくは、「タスク 2: 署名バージョン 4 の署名文字列を作成する」を参照してください。 条件: HTTP 認証ヘッダーの代わりにクエリー文字列に認証情報を含める場合は、このパラメータを指定します。 タイプ: 文字列 必要/不要: 該当する場合
X-Amz-Date	署名の作成時に指定した日時。形式は ISO 8601 基本形式 (YYYYMMDD'T'HHMMSS'Z') である必要があります。たとえば、20220525T120000Z は、X-Amz-Date の有効な日時の値です。 条件: X-Amz-Date は、すべてのリクエストで必要に応じて指定します。このオプションを使用して、署名リクエストに使用された日付を上書きできます。Date ヘッダーが ISO 8601 基本形式で指定されている場合、X-Amz-Date は不要です。X-Amz-Date を使用すると、常に Date ヘッダーの値が上書きされます。詳しくは、「署名バージョン 4 の日付の処理」を参照してください。 タイプ: 文字列 必要/不要: 該当する場合
X-Amz-Signature	署名文字列と取得した署名キーから計算した 16 進エンコード署名を指定します。 条件: HTTP 認証ヘッダーの代わりにクエリー文字列に認証情報を含める場合は、このパラメータを指定します。 タイプ: 文字列 必要/不要: 該当する場合
X-Amz-SignedHeaders	正規リクエストの一部として含まれていたすべての HTTP ヘッダーを指定します。署名付きヘッダーの指定について詳しくは、『AWS 全般のリファレンス』の「タスク 1: 署名バージョン 4 の正規リクエストを作成する 」を参照してください。 条件: HTTP 認証ヘッダーの代わりにクエリー文字列に認証情報を含める場合は、このパラメータを指定します。 タイプ: 文字列 必要/不要: 該当する場合

共通エラーコード

次のエラーコードは、IAM API に共通です。API 処理に固有のエラーについては、「IAM API」セクションで説明しています。

表 7-2 共通エラーコード

エラーコード	説明
InvalidClientTokenId	指定されたアクセスキー ID がレコードに存在しません。 HTTP 状態コード: 403
SignatureDoesNotMatch	計算したリクエストの署名が、指定した署名と一致しません。 HTTP 状態コード: 403
ValidationError	入力は、AWS サービスによって指定された制約を満たしていません。 HTTP 状態コード: 400
AccessDeniedException	この処理を実行するための十分なアクセス権がありません。 HTTP 状態コード: 400
MissingAction	リスエストに処理または必須パラメータがありません。 HTTP 状態コード: 400
NotImplemented	指定したヘッダーは、実装されていない機能を示しています。 HTTP 状態コード: 501

CreateUser

MSDP S3 の新しい IAM ユーザーを作成します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `UserName`
  作成するユーザーの名前。
  IAM ユーザー名は一意である必要があります。ユーザー名には、大文字と小文字の区別があります。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。

パターン: [¥w+=,.@-]+
必要/不要: 必要

応答要素

サーバーから次の要素が返されます。

- User
  新しい IAM ユーザーに関する詳細を含む構造。
  タイプ: ユーザーオブジェクト

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- EntityAlreadyExists
  すでに存在するリソースの作成が試行されたため、要求が拒否されました。
  HTTP 状態コード: 409
- InvalidInput
  入力パラメータに無効または範囲外の値が指定されているため、要求が拒否されました。
  HTTP 状態コード: 400
- ServiceFailure
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=CreateUser
&UserName=User1
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateUserResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>16481914289311827O3</RequestId>
  </ResponseMetadata>
  <CreateUserResult>
    <User>
      <CreateDate>2022-03-25T06:57:08Z</CreateDate>
```

```
      <UserName>User1</UserName>
    </User>
  </CreateUserResult>
</CreateUserResponse>
```

GetUser

指定した IAM ユーザーに関する情報を取得します。

ユーザー名を指定しない場合、IAM は、この操作への要求の署名に使用される MSDP S3 アクセスキー ID に基づいて、ユーザー名を暗黙的に決定します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `UserName`
  情報を取得するユーザーの名前。
  このパラメータは必要に応じて指定します。指定しない場合は、要求を行ったユーザーがデフォルト値になります。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: [¥w+=,.@-]+
  必要/不要: 不要

応答要素

サーバーから次の要素が返されます。

- `User`
  新しい IAM ユーザーに関する詳細を含む構造。
  タイプ: ユーザーオブジェクト

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- `NoSuchEntity`
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404
- `ServiceFailure`
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=GetUser
&UserName=User1
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<GetUserResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>16481914289311827O3</RequestId>
  </ResponseMetadata>
  <GetUserResult>
    <User>
      <CreateDate>2022-03-25T06:57:08Z</CreateDate>
      <UserName>User1</UserName>
    </User>
  </GetUserResult>
</GetUserResponse>
```

ListUsers

サーバーのすべての IAM ユーザーを一覧表示します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

この API には、特定の要求パラメータは必要ありません。

応答要素

サーバーから次の要素が返されます。

- `Users.member.N`
  ユーザーのリスト。
  タイプ: ユーザーオブジェクトの配列
- `IsTruncated`
  返す項目が他にあるかどうかを示すフラグ。
  タイプ: ブール値

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- ServiceFailure
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=ListUsers
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<ListUsersResponse
   xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648203604905893069</RequestId>
  </ResponseMetadata>
  <ListUsersResult>
    <Users>
      <member>
        <CreateDate>2022-03-22T13:35:03Z</CreateDate>
        <UserName>root</UserName>
      </member>
      <member>
        <CreateDate>2022-03-25T06:57:08Z</CreateDate>
        <UserName>User1</UserName>
      </member>
    </Users>
    <IsTruncated>false</IsTruncated>
  </ListUsersResult>
</ListUsersResponse>
```

DeleteUser

指定した IAM ユーザーを削除します。

ユーザーを削除する前に、ユーザーに関連付けられている項目 (アクセスキー、ポリシーなど) を手動で削除する必要があります。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- UserName
  削除するユーザーの名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: [¥w+=,.@-]+
  必要/不要: 必要

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- DeleteConflict
  下位エンティティがあるリソースの削除が試行されたため、要求が拒否されました。エラーメッセージにはこれらのエンティティが表示されます。
  HTTP 状態コード: 409
- NoSuchEntity
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404
- ServiceFailure
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=DeleteUser
&UserName=User1
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<GetUserResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648214899748730966</RequestId>
  </ResponseMetadata>
</DeleteUserResponse>
```

CreateAccessKey

指定したユーザーの新しい AWS シークレットアクセスキーと対応する MSDP S3 アクセスキー ID を作成します。新しいキーのデフォルトの状態は[有効 (Active)]です。

ユーザー名を指定しない場合、IAM は、要求に署名する MSDP S3 アクセスキー ID に基づいて、ユーザー名を暗黙的に決定します。

ユーザーは、最大 2 つのアクセスキーを所有できます。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `UserName`
  新しいキーが属する IAM ユーザーの名前。
  このパラメータは必要に応じて指定します。指定しない場合は、要求を行ったユーザーがデフォルト値になります。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 不要

応答要素

サーバーから次の要素が返されます。

- `AccessKey`
  アクセスキーに関する詳細を含む構造。
  タイプ: アクセスキーオブジェクトp.414 の「データ形式」を参照してください。

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- `LimitExceeded`
  上限を超えるリソースを作成しようとしたため、要求は拒否されました。エラーメッセージには、超過した上限が表示されます。
  HTTP 状態コード: 409
- `NoSuchEntity`
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404
- `ServiceFailure`
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=CreateAccessKey
&UserName=User1
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessKeyResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648431826555152698</RequestId>
  </ResponseMetadata>
  <CreateAccessKeyResult>
    <AccessKey>
      <AccessKeyId>2PPM4XHAKMG5JHZIUPEUG</AccessKeyId>
      <CreateDate>2022-03-28T01:43:46Z</CreateDate>
      <SecretAccessKey>9TvXcpw2YRYRZXZCyrCELGVWMNBZyJYY95jhDc1xgH
      </SecretAccessKey>
      <Status>Active</Status>
      <UserName>User1</UserName>
    </AccessKey>
  </CreateAccessKeyResult>
</CreateAccessKeyResponse>
```

ListAccessKeys

指定した IAM ユーザーに関連付けられているアクセスキー ID に関する情報を返します。存在しない場合は空のリストを返します。

UserName フィールドを指定しない場合、要求の署名に使用する MSDP S3 アクセスキー ID に基づいて、ユーザー名が暗黙的に決定されます。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- UserName
  IAM ユーザーの名前。
  このパラメータは必要に応じて指定します。指定しない場合は、要求を行ったユーザーがデフォルト値になります。
  タイプ: 文字列

長さの制約: 最小 1 文字。最大 64 文字。
パターン: `[¥w+=,.@-]+`
必要/不要: 不要

応答要素

サーバーから次の要素が返されます。

- `AccessKeyMetadata.member.N`
  アクセスキーに関するメタデータを含むオブジェクトのリスト。
  タイプ: `AccessKeyMetadata` オブジェクトの配列 p.414 の「データ形式」を参照してください。
- `IsTruncated`
  返す項目が他にあるかどうかを示すフラグ。
  タイプ: ブール値

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- `NoSuchEntity`
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404
- `ServiceFailure`
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=ListAccessKeys
&UserName=User1
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<ListAccessKeysResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648432612600646944</RequestId>
  </ResponseMetadata>
  <ListAccessKeysResult>
```

```
    <AccessKeyMetadata>
      <member>
        <AccessKeyId>2PPM4XHAKMG5JHZIUPEUG</AccessKeyId>
        <CreateDate>2022-03-28T01:43:46Z</CreateDate>
        <Status>Active</Status>
        <UserName>User1</UserName>
      </member>
      <member>
        <AccessKeyId>GAATH0QN9N5W8TBQPSKPJ</AccessKeyId>
        <CreateDate>2022-03-28T01:53:02Z</CreateDate>
        <Status>Active</Status>
        <UserName>User1</UserName>
      </member>
    </AccessKeyMetadata>
    <IsTruncated>false</IsTruncated>
  </ListAccessKeysResult>
</ListAccessKeysResponse>
```

DeleteAccessKey

指定した IAM ユーザーに関連付けられているアクセスキーペアを削除します。

ユーザー名を指定しない場合、IAM は、要求に署名する MSDP S3 アクセスキー ID に基づいて、ユーザー名を暗黙的に決定します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `AccessKeyId`
  削除するアクセスキー ID とシークレットアクセスキーのアクセスキー ID。
  タイプ: 文字列
  長さの制約: 最小 16 文字。最大 128 文字。
  パターン: `[¥w]+`
  必要/不要: 必要

- `UserName`
  IAM ユーザーの名前。
  このパラメータは必要に応じて指定します。指定しない場合は、要求を行ったユーザーがデフォルト値になります。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 不要

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- `NoSuchEntity`
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404
- `ServiceFailure`
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=DeleteAccessKey
&AccessKeyId=GAATH0QN9N5W8TBQPSKPJ
&UserName=User1
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteAccessKeyResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648451304149485569</RequestId>
  </ResponseMetadata>
</DeleteAccessKeyResponse>
```

UpdateAccessKey

指定したアクセスキーの状態を[有効 (Active)]から[無効 (Inactive)]、またはその逆に変更します。この操作は、キーのローテーションワークフローの一環としてユーザーのキーを無効にするために使用できます。

`UserName` を指定しない場合、要求の署名に使用する MSDP S3 アクセスキー ID に基づいて、ユーザー名が暗黙的に決定されます。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `AccessKeyId`

更新するアクセスキーのアクセスキー ID。
タイプ: 文字列
長さの制約: 最小 16 文字。最大 128 文字。
パターン: `[¥w]+`
必要/不要: 必要

- `Status`
  シークレットアクセスキーに割り当てる状態。[有効 (Active)]は、MSDP S3 サーバーへのプログラムの呼び出しにキーを使用できることを意味し、[無効 (Inactive)]はキーを使用できないことを意味します。
  タイプ: 文字列
  有効な値: 有効 (Active)/無効 (Inactive)
  必要/不要: 必要

- `UserName`
  IAM ユーザーの名前。
  このパラメータは必要に応じて指定します。指定しない場合は、要求を行ったユーザーがデフォルト値になります。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 不要

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- `NoSuchEntity`
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404

- `ServiceFailure`
  不明なエラー、例外、障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=UpdateAccessKey
&AccessKeyId=GAATH0QN9N5W8TBQPSKPJ
&Status=Inactive
&UserName=User1
```

```
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<UpdateAccessKeyResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ResponseMetadata>
    <RequestId>1648451481105563455</RequestId>
  </ResponseMetadata>
</UpdateAccessKeyResponse>
```

PutUserPolicy

指定した IAM ユーザーに埋め込まれたインラインポリシー文書を追加または更新します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `PolicyDocument`
  ポリシー文書。
  IAM では JSON 形式のポリシーを指定する必要があります。
  タイプ: 文字列
  必要/不要: 必要
- `PolicyName`
  ポリシー文書の名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 128 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 必要
- `UserName`
  ポリシーと関連付けるユーザーの名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 必要

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- MalformedPolicyDocument
  ポリシー文書の形式が不正であるため、要求が拒否されました。
  HTTP 状態コード: 400
- NoSuchEntity
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404
- ServiceFailure
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=PutUserPolicy
&UserName=User1
&PolicyName=ExamplePolicy
&PolicyDocument={"Version":"2012-10-17","Statement":[{"Effect":"Allow",
"Action":["s3:*"],"Resource":["arn:aws:s3:::bkt3/*"]}]}
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<PutUserPolicyResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648451612346994599</RequestId>
  </ResponseMetadata>
</PutUserPolicyResponse>
```

GetUserPolicy

指定した IAM ユーザーに埋め込まれた特定のインラインポリシー文書を取得します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- PolicyName
  取得するポリシー文書の名前。
  タイプ: 文字列

長さの制約: 最小 1 文字。最大 128 文字。
パターン: [¥w+=,.@-]+
必要/不要: 必要

- UserName
  ポリシーと関連付けるユーザーの名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: [¥w+=,.@-]+
  必要/不要: 必要

応答要素

サーバーから次の要素が返されます。

- PolicyDocument
  ポリシー文書。
  IAM は JSON 形式でポリシーを格納します。
  タイプ: 文字列

- PolicyName
  ポリシーの名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 128 文字。
  パターン: [¥w+=,.@-]+

- UserName
  ポリシーと関連付けるユーザー。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 128 文字。
  パターン: [¥w+=,.@-]+

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- NoSuchEntity
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404

- ServiceFailure
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=GetUserPolicy
&UserName=User1
&PolicyName=ExamplePolicy
&Version=2010-05-08
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<GetUserPolicyResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>16484414174495822l2</RequestId>
  </ResponseMetadata>
  <GetUserPolicyResult>
    <UserName>User1</UserName>
    <PolicyName>ExamplePolicy</PolicyName>

<PolicyDocument>{"Version":"2012-10-17","Statement":[{"Effect":"Allow",


"Action":["s3:*"],"Resource":["arn:aws:s3:::bkt3/*"]}]}</PolicyDocument>

  </GetUserPolicyResult>
</GetUserPolicyResponse>
```

ListUserPolicies

指定した IAM ユーザーに埋め込まれたインラインポリシーの名前を一覧表示します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `UserName`
  ポリシーを一覧表示するユーザーの名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 必要

応答要素

サーバーから次の要素が返されます。

- PolicyNames.member.N
  ポリシー名のリスト。
  タイプ: 文字列の配列
  長さの制約: 最小 1 文字。最大 128 文字。
  パターン: [¥w+=,.@-]+

- IsTruncated
  返す項目が他にあるかどうかを示すフラグ。
  タイプ: ブール値

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- NoSuchEntity
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404

- ServiceFailure
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=ListUserPolicies
&UserName=User1
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<ListUserPoliciesResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648441729868934088</RequestId>
  </ResponseMetadata>
  <ListUserPoliciesResult>
    <PolicyNames>
      <member>ExamplePolicy</member>
    </PolicyNames>
    <IsTruncated>false</IsTruncated>
  </ListUserPoliciesResult>
</ListUserPoliciesResponse>
```

DeleteUserPolicy

指定した IAM ユーザーに埋め込まれた特定のインラインポリシーを削除します。

要求パラメータ

すべての処理に共通するパラメータについては、p.394 の「共通パラメータ」を参照してください。

- `PolicyName`
  削除するポリシー文書を識別する名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 128 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 必要

- `UserName`
  ポリシーが埋め込まれているユーザーを識別する名前。
  タイプ: 文字列
  長さの制約: 最小 1 文字。最大 64 文字。
  パターン: `[¥w+=,.@-]+`
  必要/不要: 必要

エラー

すべての処理に共通するエラーについては、p.396 の「共通エラーコード」を参照してください。

- `NoSuchEntity`
  存在しないリソースエンティティが参照されているため、要求が拒否されました。エラーメッセージにはリソースが表示されます。
  HTTP 状態コード: 404

- `ServiceFailure`
  不明なエラー、例外、または障害が発生したため、要求の処理に失敗しました。
  HTTP 状態コード: 500

例

要求のサンプル:

```
https://msdps3.veritas.com:8443/?Action=DeleteUserPolicy
&PolicyName=ExamplePolicy
&UserName=User1
&AUTHPARAMS
```

応答のサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteUserPolicyResponse
  xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1648451943468940588</RequestId>
  </ResponseMetadata>
</DeleteUserPolicyResponse>
```

データ形式

表 7-3　　データ形式

データ形式	説明
User	IAM ユーザーエンティティに関する情報が含まれます。 ■ UserName ユーザーを識別する分かりやすい名前。 タイプ: 文字列 長さの制約: 最小 1 文字。最大 64 文字。 パターン: [¥w+=,.@-]+ 必要/不要: 必要 ■ CreateDate ユーザーが作成された日時 (ISO 8601 日時形式)。 タイプ: タイムスタンプ 必要/不要: 必要

データ形式	説明
AccessKey	MSDP S3 アクセスキーに関する情報が含まれます。 ■ AccessKeyId このアクセスキーの ID。 タイプ: 文字列 長さの制約: 最小 16 文字。最大 128 文字。 パターン: [¥w]+ 必要/不要: 必要 ■ CreateDate アクセスキーが作成された日付。 タイプ: タイムスタンプ 必要/不要: 不要 ■ SecretAccessKey 要求に署名するために使用されるシークレットキー。 タイプ: 文字列 必要/不要: 必要 ■ Status アクセスキーの状態。[有効 (Active)]は、キーが API 呼び出しに対して有効であることを意味し、[無効 (Inactive)]は有効ではないことを意味します。 タイプ: 文字列 有効な値: 有効 (Active) | 無効 (Inactive) 必要/不要: 必要 ■ UserName アクセスキーが関連付けられている IAM ユーザーの名前。 タイプ: 文字列 長さの制約: 最小 1 文字。最大 64 文字。 パターン: [¥w+=,.@-]+ 必要/不要: 必要

データ形式	説明
AccessKeyMetadata	MSDP S3 アクセスキーに関する情報が含まれます。シークレットキーは含まれません。 ■ AccessKeyId このアクセスキーの ID。 タイプ: 文字列 長さの制約: 最小 16 文字。最大 128 文字。 パターン: [¥w]+ 必要/不要: 不要 ■ CreateDate アクセスキーが作成された日付。 タイプ: タイムスタンプ 必要/不要: 不要 ■ Status アクセスキーの状態。Active はキーが API 呼び出しに対して有効であることを意味し、Inactive は無効であることを意味します。 タイプ: 文字列 有効な値: 有効 (Active) | 無効 (Inactive) 必要/不要: 不要 ■ UserName アクセスキーが関連付けられている IAM ユーザーの名前。 タイプ: 文字列 長さの制約: 最小 1 文字。最大 64 文字。 パターン: [¥w+=,.@-]+ 必要/不要: 不要

IAM ポリシー文書の構文

ポリシー文書は、Version オブジェクトと Statement オブジェクトを含む JSON 形式の文書です。次に例を示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": [
```

```
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

ポリシー文書のサポート対象バージョン:

「2012-10-17」のみがサポートされます。

サポート対象の処理:

表 7-4　　サポート対象の処理

処理	説明	許容 API
`s3:*`	任意の S3 操作と IAM 操作。これは管理者権限です。	すべての S3 API と IAM API。 **メモ:** CreateBucket API には、この権限が必要です。 権限 `s3:BypassGovernanceRetention` は処理 `s3:*` にのみ適用されます。

`s3:Put*`	S3 書き込み操作。	`UploadPart`
		`CompleteMultipartUpload`
		`CreateMultipartUpload`
		`AbortMultipartUpload`
		`PutObject`
		`DeleteObject`
		`DeleteObjects`
		`PutBucketVersioning`
		`DeleteBucket`
		`CopyObject`
		`PutObjectLockConfiguration`
		`PutObjectRetention`

処理	説明	許容 API
s3:Get*	S3 読み取り操作。	HeadObject GetObject GetBucketVersioning GetBucketLocation GetBucketEncryption HeadBucket CopyObject GetObjectLockConfiguration GetObjectRetention
s3:List*	S3 表示操作。	ListBuckets ListObjects ListObjectsV2 ListObjectVersions ListMultipartUploads

サポート対象の結果:

結果としては[許可 (Allow)]のみがサポートされます。

メモ: ルートユーザーには管理者権限が埋め込まれているため、ポリシーは適用できません。

サポート対象のリソースパターン:

表 7-5 サポート対象のリソースパターン

リソースパターン	説明
arn:aws:s3:::*	すべての S3 リソース。 **メモ:** このリソースパターンを s3:* 処理と併用すると、すべての S3 リソースに対するすべての権限 (root ユーザーと同じ権限) がユーザーに付与されます。 権限 s3:BypassGovernanceRetention は処理 s3:* にのみ適用されます。

リソースパターン	説明
`arn:aws:s3:::<BUCKET_NAME>/*`	<BUCKET_NAME> 内のすべてのオブジェクト。バケット自体も含まれます。 権限 `s3:BypassGovernanceRetention` は現在のリソースには適用されません。

Flex WORM の S3 オブジェクトロック

S3 オブジェクトロックを使用すると、WORM (Write Once Read Many) モデルを使用してオブジェクトを格納できます。現在、この機能は Flex WORM でのみ機能し、リーガルホールド API はサポートされません。

オブジェクトロックが有効なバケットにすべてのデータを格納することをお勧めします。Flex WORM の S3 オブジェクトロックと Flex WORM の MSDP の設定は、デフォルトで同じです。ただし、オブジェクトロック保持の形式は異なります。たとえば、S3 バケットオブジェクトのロック保持の「日」または「年」は、「時間」や「年」を使用する MSDP WORM ストレージサーバーとは異なります。バックアップ保持に与える影響を最小限に抑えるため、間隔の範囲を広くすることをお勧めします。

MSDP WORM 設定が更新された場合は、s3srv と MSDP サービスを再起動する必要があります。WORM 設定の更新後は、既存のオブジェクトの保持設定は変更されないままになり、新しく作成されたオブジェクトのみが影響を受けます。

メモ: Flex WORM S3 オブジェクトロックのガバナンスモードは、Flex WORM の MSDP LSU ではエンタープライズモードです。Flex WORM S3 オブジェクトロックのコンプライアンスモードは、Flex WORM の MSDP LSU ではコンプライアンスモードです。

Flex WORM のオブジェクトロックには、次の S3 API を使用できます。

- Create Bucket
  p.421 の「CreateBucket 」を参照してください。
- Put Object
  p.462 の「PutObject」を参照してください。
- Copy Object
  p.463 の「Copy Object」を参照してください。
- Get Object
  p.457 の「GetObject」を参照してください。
- Head Object
  p.459 の「HeadObject」を参照してください。
- Delete Object

p.453 の「DeleteObject」を参照してください。

- Delete Objects
p.455 の「DeleteObjects」を参照してください。
- Create Multipart Upload
p.451 の「CreateMultipartUpload」を参照してください。
- Put Object Retention (Flex WORM のみ)
p.469 の「Put Object Retention (Flex WORM のみ)」を参照してください。
- Get Object Retention (Flex WORM のみ)
p.470 の「Get Object Retention (Flex WORM のみ)」を参照してください。
- Put Object Lock Configuration (Flex WORM のみ)
p.444 の「Put Object Lock Configuration (Flex WORM のみ)」を参照してください。
- GET Object Lock Configuration (Flex WORM のみ)
p.445 の「GET Object Lock Configuration (Flex WORM のみ)」を参照してください。

MSDP の S3 インターフェースの S3 API

一般的なエラー応答

エラーの場合、次の xml 応答が REST クライアントに返されます。

- 応答コンテンツタイプは「application/xml」です。
- `RequestId` は、要求ごとに生成される一意の ID です。
- 応答の内容は次のような XML 形式で示されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
    <Code>InvalidKeyMarker</Code>
    <Message>The key marker is invalid. It should start with prefix.

    </Message>
    <Resource>/azure-versioned/</Resource>
    <RequestId>1653377472751453758</RequestId>
```

S3 API によるバケット操作

S3 API によるバケット操作で、次のデータ配置機能を実行できます。

- バケットを作成する。
- バケットを削除する。

- バケットの状態を確認する。
- バケットを一覧表示する。

CreateBucket

新しいバケットを作成します。バケット名は、すべての LSU で一意です。一部の文字列はバケット名として使用できません。バケットの命名制限について詳しくは、「バケットの命名規則」を参照してください。要求の本文に `Region(=lsu name)` を指定する必要があります。匿名の要求を使用したバケットの作成は許可されません。

要求の構文

```
PUT /bucket HTTP/1.1
Host: msdps3.server:8443
<?xml version="1.0" encoding="UTF-8"?>
<CreateBucketConfiguration
xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <LocationConstraint>string</LocationConstraint>
</CreateBucketConfiguration>
```

要求パラメータ

- `Bucket`
  作成するバケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- `x-amz-bucket-object-lock-enabled` (Flex WORM のみ)
  新しいバケットで S3 オブジェクトロックが有効かどうかを指定します。

  メモ: `CreateBucket` 要求で `ObjectLockEnabledForBucket` が true に設定されている場合、`s3:PutObjectLockConfiguration` 権限が必要になり、バケットのバージョン管理が自動的に有効になります。`s3:PutBucketVersioning` 権限は必要ありません。

要求の本文

- `CreateBucketConfiguration`
  `CreateBucketConfiguration` パラメータのルート階層タグ。
  必要/不要: 必要
- `LocationConstraint`
  バケットが作成される地域を指定します。

メモ: S3Srv の地域は LSU 名です。地域を指定しない場合、バケットは地域 PureDiskVolume (ローカル LSU) に作成されます。

タイプ: 文字列
有効な値: PureDiskVolume、CLOUD_LSU_NAME
必要/不要: 不要

応答の構文

```
HTTP/1.1 200
```

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。
- `InvalidArgument`
  引数が無効です。
  HTTP 状態コード 400。
- `InvalidBucketName`
  指定されたバケットが無効です。
  HTTP 状態コード 400。
- `AccessDenied`
  アクセスが拒否されました。
  HTTP 状態コード 403。
- `BucketAlreadyExists`
  要求されたバケット名が利用できません。バケットの名前空間は、システムのすべてのユーザーで共有されます。別の名前を選択して再試行してください。
  HTTP 状態コード 409。
- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

DeleteBucket

バケットを削除します。バケット自体を削除するには、まずバケット内のすべてのオブジェクト (すべてのオブジェクトバージョンと削除マーカーを含む) を削除する必要があります。

要求の構文

```
DELETE /bucket HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  削除するバケットの名前。
  必要/不要: 必要
  タイプ: 文字列

応答の構文

```
HTTP/1.1 204
```

考えられるエラー応答

- Success
  HTTP 状態コード 204。
- AccessDenied
  アクセスが拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- BucketNotEmpty
  削除しようとしたバケットが空ではありません。
  HTTP 状態コード 409。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

GetBucketEncryption

バケットのデフォルトの暗号化構成を返します。

要求の構文

```
GET /bucket?encryption HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200 <?xml version="1.0" encoding="UTF-8"?>
<ServerSideEncryptionConfiguration>
    <Rule>
        <ApplyServerSideEncryptionByDefault>
            <SSEAlgorithm>string</SSEAlgorithm>
        </ApplyServerSideEncryptionByDefault>
    </Rule>
</ServerSideEncryptionConfiguration>
```

応答の本文

- `ServerSideEncryptionConfiguration`
  `ServerSideEncryptionConfiguration` パラメータのルート階層タグ。
  必要/不要: 必要
  - Rule
    特定のサーバー側の暗号化構成ルールに関する情報を格納するコンテナ。
    - `ApplyServerSideEncryptionByDefault`
      バケット内のオブジェクトに適用するデフォルトのサーバー側の暗号化を指定します。
      - `SSEAlgorithm`
        デフォルトの暗号化に使用するサーバー側の暗号化アルゴリズム。

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。
- `NoSuchBucket`
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

GetBucketLocation

そのオブジェクトの `LocationConstraint` を使用してバケットのリージョンを返します。バケットのリージョンは MSDP LSU です。

要求の構文

```
GET /bucket?location HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<LocationConstraint>
    <LocationConstraint>string</LocationConstraint>
</LocationConstraint>
```

応答の本文

- LocationConstraint
  LocationConstraint パラメータのルート階層タグ。
  必要/不要: 必要
- LocationConstraint
  そのオブジェクトの LocationConstraint は MSDP LSU です。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

GetBucketVersioning

バケットのバージョン管理の状態を返します。

要求の構文

```
GET /bucket?versioning HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket

バージョン管理情報を取得するバケット名。
必要/不要: 必要
タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<VersioningConfiguration>
    <Status>string</Status>
</VersioningConfiguration>
```

応答の本文

- `VersioningConfiguration`
  `VersioningConfiguration` パラメータのルート階層タグ。
  必要/不要: 必要
- `Status`
  バケットのバージョン管理状態。
  有効な値: 有効 (Enabled)

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。
- `NoSuchBucket`
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

HeadBucket

バケットが存在するかどうかを判断します。バケットが存在し、ユーザーがそのバケットにアクセスする権限を持っている場合、この操作は 200 OK を返します。

要求の構文

```
HEAD /bucket HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- `Bucket`

バケットの名前。
必要/不要: 必要
タイプ: 文字列

応答の構文

```
HTTP/1.1 200
```

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。
- `NoSuchBucket`
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

ListBuckets

すべてのバケットを一覧表示します。

要求の構文

```
GET / HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

要求に URI パラメータは使用しません。

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListAllMyBucketsResult>
    <Buckets>
        <Bucket>
            <CreationDate>timestamp</CreationDate>
            <Name>string</Name>
        </Bucket>
    </Buckets>
</ListAllMyBucketsResult>
```

応答の本文

- ListAllMyBucketsResult
  すべてのバケット結果のルート階層タグ。
  必要/不要: 必要
  - Buckets
    要求に対して認証されたユーザーが所有するバケットのリスト。
    - Bucket
      バケットの情報。
      - CreationDate
        バケットの作成日時。
      - Name
        バケットの名前。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

ListMultipartUploads

進行中のマルチパートアップロードを一覧表示します。進行中のマルチパートアップロードとは、マルチパートアップロードの作成要求を使用して開始されたが、まだ完了していないか、または中止されていないマルチパートアップロードです。この操作は、オブジェクトキーで昇順にソートされた応答で、最大 10000 個のマルチパートアップロードをランダムに返します。この操作はページングをサポートしません。

要求の構文

```
GET /bucket?uploads&prefix=Prefix
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  マルチパートアップロードが開始されたバケットの名前。
  必要/不要: 必要
  タイプ: 文字列

- prefix
  応答を、指定した接頭辞で始まるアップロードに制限します。
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListMultipartUploadsResult>
    <Bucket>string</Bucket>
    <KeyMarker>string</KeyMarker>
    <UploadIdMarker>string</UploadIdMarker>
    <NextKeyMarker>string</NextKeyMarker>
    <Prefix>string</Prefix>
    <NextUploadIdMarker>string</NextUploadIdMarker>
    <MaxUploads>integer</MaxUploads>
    <IsTruncated>boolean</IsTruncated>
    <Upload>
        <Initiated>timestamp</Initiated>
        <Key>string</Key>
        <StorageClass>string</StorageClass>
        <UploadId>string</UploadId>
    </Upload>
    ...
</ListMultipartUploadsResult>
```

応答の本文

- ListMultipartUploadsResult
  ListMultipartUploadsResult パラメータのルート階層タグ。
  必要/不要: 必要
  - Bucket
    マルチパートアップロードが開始されたバケットの名前。
  - IsTruncated
    検索条件を満たすすべての結果が MSDP S3 によって返されたかどうかを示すフラグ。
  - KeyMarker
    MSDP の S3 インターフェースでは、最後の要求でサーバーによって返されたキーマーカーが必要です。要求で、応答の「NextKeyMarker」の値をキーマーカーとして使用する必要があります。
  - MaxUploads
    応答で返されるマルチパートアップロードの数を制限します。

- NextKeyMarke
  応答が切り捨てられた場合、後続の要求でこの値をマーカーとして使用して、次のオブジェクトセットを取得できます。
- NextUploadIdMarker
  応答が切り捨てられた場合、後続の要求でこの値をマーカーとして使用して、次のオブジェクトセットを取得できます。
- UploadIdMarker
  要求で渡された UploadIdMarker の値。
- Prefix
  応答を、指定した接頭辞で始まるキーに制限します。
- Upload
  特定のマルチパートアップロードに関連する情報。応答には、ゼロまたは複数のアップロードを含められます。
  - Initiated
    マルチパートアップロードが開始された日時。
    タイプ: タイムスタンプ
  - Key
    マルチパートアップロードが開始されたオブジェクト名。
  - StorageClass
    アップロードされたパートのストレージクラス。
  - UploadId
    マルチパートアップロードを識別するアップロード ID。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument
  引数が無効です。HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。

HTTP 状態コード 500。

ListObjects

バケット内のすべてのオブジェクトのリストを返します。要求パラメータを選択条件として使用して、バケット内のオブジェクトのサブセットを返すことができます。バケットでバージョン管理が有効になっている場合、API は最新バージョンのオブジェクトを返します。200 OK の応答に有効または無効な XML を含められます。応答の内容を解析し、適切に処理するようにアプリケーションが設計されていることを確認します。

要求の構文

```
GET /bucket?delimiter=Delimiter&marker=Marker&max-keys
=Maxkeys&prefix=Prefix HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- `Bucket`
  オブジェクトが含まれているバケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- `delimiter`
  区切り文字はキーをグループ化するために使用する文字です。接頭辞と最初に出現する区切り文字の間に同じ文字を含むキーを、`CommonPrefixes` コレクション内の 1 つの結果要素にロールアップします。これらのロールアップキーは、応答の他の場所には返されません。各ロールアップ結果は、`MaxKeys` 値に対して 1 回のみ返されたものとしてカウントされます。MSDP S3 は区切り文字として「/」文字列のみをサポートします。
  タイプ: 文字列
- `marker`
  マーカーは、MSDP の S3 インターフェースがオブジェクトの一覧表示を開始するポイントです。MSDP の S3 インターフェースでは、最後の要求でサーバーによって返されたマーカーが必要です。要求で、応答の `NextMarker` の値をマーカーとして使用する必要があります。
  タイプ: 文字列
- `max-keys`
  応答で返されるキーの数を制限します。デフォルトでは、最大 1,000 個のキー名が返されます。
  タイプ: 整数
- `prefix`
  応答を、指定した接頭辞で始まるキーに制限します。

タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult>
    <IsTruncated>boolean</IsTruncated>
    <Marker>string</Marker>
    <NextMarker>string</NextMarker>
    <Contents>
        <ETag>string</ETag>
        <Key>string</Key>
        <LastModified>timestamp</LastModified>
        <Size>integer</Size>
        <StorageClass>string</StorageClass>
    </Contents>
    ...
    <Name>string</Name>
    <Prefix>string</Prefix>
    <Delimiter>string</Delimiter>
    <MaxKeys>integer</MaxKeys>
    <CommonPrefixes>
        <Prefix>string</Prefix>
    </CommonPrefixes>
    ...
</ListBucketResult>
```

応答の本文

- `ListBucketResult`
  `ListBucketResult` パラメータのルート階層タグ。
  必要/不要: 必要
  - `CommonPrefixes`
    戻り値の数を決定する際、すべてのキー (最大 1,000 個) は共通の接頭辞でまとめられ、1 つとしてカウントされます。`CommonPrefixes` には、接頭辞と、区切り文字で指定された次に出現する文字列の間にあるすべてのキーが含まれます。
  - `Delimiter`
    要求で渡される区切り文字の値。
  - `IsTruncated`
    検索条件を満たすすべての結果が MSDP S3 によって返されたかどうかを示すフラグ。

- Marker
  バケット内の一覧表示の開始位置を示します。マーカーは、要求で渡された場合にのみ応答に含まれます。
- MaxKeys
  応答の本文で返すことができるオブジェクトの最大数。
- Name
  バケットの名前。
- NextMarker
  応答が切り捨てられた場合、後続の要求でこの値をマーカーとして使用して、次のオブジェクトセットを取得できます。
- Prefix
  応答を、指定した接頭辞で始まるキーに制限します。
- Contents
  返される各オブジェクトに関するメタデータ。
  - ETag
    オブジェクトの SHA256 ダイジェスト。
  - Key
    オブジェクト名。
  - LastModified
    オブジェクトの前回の変更日時。
  - Size
    オブジェクトのサイズ。
  - StorageClass
    オブジェクトのストレージクラス。

バージョン管理対象バケットの場合、List Object Versions API を使用して、すべてのオブジェクトに関する情報を取得することをお勧めします。バージョン管理対象バケットで「list objects」を使用する場合、結果が切り捨てられると、結果のキー数が最大キー数未満になる可能性があり、改ページ要求で残りのキーを確認できます。

バージョン管理対象バケットで list objects API を使用する場合、指定した接頭辞以下のすべてのオブジェクトが delete マーカーであると、指定した接頭辞が CommonPrefixes 要素として表示されます。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument(Marker is invalid.)

引数が無効です。HTTP 状態コード 400。

- `InvalidArgument(maxKeys is invalid)`
  引数が無効です。
  HTTP 状態コード 400。
- `S3srvExtInvalidPrefix`
  接頭辞はスラッシュで始めることはできません。
  HTTP 状態コード 400。
- `S3srvExtInvalidDelimiter`
  区切り文字としてスラッシュのみをサポートします。
  HTTP 状態コード 400。
- `AccessDenied`
  アクセスが拒否されました。
  HTTP 状態コード 403。
- `NoSuchBucket`
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

ListObjectsV2

バケット内のすべてのオブジェクトのリストを返します。要求パラメータを選択条件として使用して、バケット内のオブジェクトのサブセットを返すことができます。バケットでバージョン管理が有効になっている場合、API は最新バージョンのオブジェクトを返します。200 OK の応答に有効または無効な XML を含められます。応答の内容を解析し、適切に処理するようにアプリケーションが設計されていることを確認します。

要求の構文

```
GGET /bucket?list-type=2&continuation-token=Continuation
Token&delimiter=Delimiter&max-keys=MaxKeys&prefix=Prefix HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- `Bucket`
  オブジェクトが含まれているバケットの名前。
  必要/不要: 必要
  タイプ: 文字列

- continuation-token
  継続トークンは、MSDP の S3 インターフェースでオブジェクトの一覧表示を開始するポイントです。MSDP の S3 インターフェースでは、最後の要求でサーバーによって返された継続トークンが必要です。要求で、応答の NextContinuationToken の値を ContinuationToken として使用する必要があります。トークンは 1 回のみ使用でき、デフォルトでは 2 分間有効です。
  タイプ: 文字列

- delimiter
  区切り文字はキーをグループ化するために使用する文字です。接頭辞と最初に出現する区切り文字の間に同じ文字を含むキーを、CommonPrefixes コレクション内の 1 つの結果要素にロールアップします。これらのロールアップキーは、応答の他の場所には返されません。各ロールアップ結果は、MaxKeys 値に対して 1 回のみ返されたものとしてカウントされます。MSDP S3 は区切り文字として「/」文字列のみをサポートします。
  タイプ: 文字列

- max-keys
  応答で返されるキーの数を制限します。デフォルトでは、最大 1,000 個のキー名が返されます。
  タイプ: 整数

- prefix
  応答を、指定した接頭辞で始まるキーに制限します。
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult>
    <IsTruncated>boolean</IsTruncated>
    <Contents>
        <ETag>string</ETag>
        <Key>string</Key>
        <LastModified>timestamp</LastModified>
        <Size>integer</Size>
        <StorageClass>string</StorageClass>
    </Contents>
    ...
    <Name>string</Name>
    <Prefix>string</Prefix>
    <Delimiter>string</Delimiter>
    <MaxKeys>integer</MaxKeys>
    <CommonPrefixes>
```

```
        <Prefix>string</Prefix>
    </CommonPrefixes>
    ...
    <KeyCount>integer</KeyCount>
    <ContinuationToken>string</ContinuationToken>
    <NextContinuationToken>string</NextContinuationToken>
</ListBucketResult>
```

応答の本文

- `ListBucketResult`
  `ListBucketResult` パラメータのルート階層タグ。
  必要/不要: 必要
  - `CommonPrefixes`
    戻り値の数を決定する際、すべてのキー (最大 1,000 個) は共通の接頭辞でまとめられ、1 つとしてカウントされます。`CommonPrefixes` には、接頭辞と、区切り文字で指定された次に出現する文字列の間にあるすべてのキーが含まれます。
  - `Contents`
    返される各オブジェクトに関するメタデータ。
    - `ETag`
      オブジェクトの SHA256 ダイジェスト。
    - `Key`
      オブジェクト名。
    - `LastModified`
      オブジェクトの前回の変更日時。
    - `Size`
      オブジェクトのサイズ。
    - `StorageClass`
      オブジェクトのストレージクラス。
  - `Delimiter`
    要求で渡される区切り文字の値。
  - `IsTruncated`
    検索条件を満たすすべての結果が MSDP S3 によって返されたかどうかを示すフラグ。
  - `ContinuationToken`
    `ContinuationToken` は、MSDP の S3 インターフェースでオブジェクトの一覧表示を開始するポイントです。MSDP の S3 インターフェースでは、最後の要求でサーバーによって返された `ContinuationToken` が必要です。要求で、応答

の NextContinuationToken の値を ContinuationToken として使用する必要があります。

- KeyCount
  応答の本文で返すオブジェクトの数。
- MaxKeys
  応答の本文で返すことができるオブジェクトの最大数。
- Name
  バケットの名前。
- NextContinuationToken
  応答が切り捨てられた場合、後続の要求でこの値を ContinuationToken として使用して、次のオブジェクトセットを取得できます。
- Prefix
  応答を、指定した接頭辞で始まるキーに制限します。

バージョン管理対象バケットの場合、List Object Versions API を使用して、すべてのオブジェクトに関する情報を取得することをお勧めします。バージョン管理対象バケットで「list objects」を使用する場合、結果が切り捨てられると、結果のキー数が最大キー数未満になる可能性があり、改ページ要求で残りのキーを確認できます。

スラッシュ (/) 区切り文字で区切って指定した接頭辞以下の CommonPrefixes 要素は 1,000 個未満にすることをお勧めします。指定した接頭辞以下に 10,000 個を超える CommonPrefixes 要素が存在する場合、要求で接頭辞と区切り文字パラメータを使用した list objects により 10,000 個の要素のみが返されます。指定した接頭辞以下のすべての要素を一覧表示する場合は、区切り文字なしで list objects を使用します。

バージョン管理対象バケットで list objects API を使用する場合、指定した接頭辞以下のすべてのオブジェクトが削除マーカーであると、指定した接頭辞が CommonPrefixes 要素として表示されます。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument(continuation-token is invalid)
  引数が無効です。
  HTTP 状態コード 400。
- InvalidArgument(max-keys is invalid)
  引数が無効です。
  HTTP 状態コード 400。
- S3srvExtInvalidPrefix
  接頭辞はスラッシュで始めることはできません。

HTTP 状態コード 400。

- S3srvExtInvalidDelimiter
  区切り文字としてスラッシュのみをサポートします。
  HTTP 状態コード 400。
- AccessDenied
  アクセスが拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

ListObjectVersions

バケット内のすべてのバージョンのオブジェクトに関するメタデータを返します。要求パラメータを選択条件として使用して、すべてのオブジェクトバージョンのサブセットに関するメタデータを返すこともできます。MSDP の S3 インターフェースでは、1 つの要求ですべてのオブジェクトバージョンを一覧表示するために、最大 1,000 個のキーとオブジェクト名を接頭辞としてこの API を使用することをお勧めします。

要求の構文

```
GET /bucket/?versions&delimiter=Delimiter&key-marker=
KeyMarker&max-keys=MaxKeys&prefix=Prefix HTTP/1.1
Host: msdps3.server:8443
```

または

```
GET /bucket/?versions&delimiter=Delimiter&max-keys=
MaxKeys&prefix=Prefix&version-id-marker=VersionIdMarker HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  オブジェクトが含まれているバケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- key-marker

要求で、応答の NextKeyMarker の値をマーカーとして使用する必要があります。マーカーは 1 回のみ使用でき、デフォルトでは 2 分間有効です。このパラメータは、version-id-marker と併用する必要があります。
タイプ: 文字列

- delimiter
  区切り文字はキーをグループ化するために使用する文字です。接頭辞と最初に出現する区切り文字の間に同じ文字を含むキーを、CommonPrefixes コレクション内の 1 つの結果要素にロールアップします。これらのロールアップキーは、応答の他の場所には返されません。各ロールアップ結果は、MaxKeys 値に対して 1 回のみ返されたものとしてカウントされます。MSDP S3 は区切り文字として「/」文字列のみをサポートします。
  タイプ: 文字列

- max-keys
  応答で返されるキーの数を制限します。デフォルトでは、最大 1,000 個のキー名が返されます。
  タイプ: 整数

- prefix
  応答を、指定した接頭辞で始まるキーに制限します。
  タイプ: 文字列

- version-id-marker
  要求で、応答の NextVerionIDMarker の値を VersionIdMarker として使用する必要があります。マーカーは 1 回のみ使用でき、デフォルトでは 2 分間有効です。このパラメータは、key-marker と併用する必要があります。
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListVersionsResult>>
    <IsTruncated>boolean</IsTruncated>
    <KeyMarker>string</KeyMarker>
    <VersionIdMarker>string</VersionIdMarker>
    <NextKeyMarker>string</NextKeyMarker>
    <NextVersionIdMarker>string</NextVersionIdMarker>
    <Version>
        <ETag>string</ETag>
        <IsLatest>boolean</IsLatest>
        <Key>string</Key>
        <LastModified>timestamp</LastModified>
        <Size>integer</Size>
```

```
            <StorageClass>string</StorageClass>
            <VersionId>string</VersionId>
        </Version>
        ...
        <DeleteMarker>
            <IsLatest>boolean</IsLatest>
            <Key>string</Key>
            <LastModified>timestamp</LastModified>
            <VersionId>string</VersionId>
        </DeleteMarker>
        ...
        <Name>string</Name>
        <Prefix>string</Prefix>
        <Delimiter>string</Delimiter>
        <MaxKeys>integer</MaxKeys>
        <CommonPrefixes>
            <Prefix>string</Prefix>
        </CommonPrefixes>
        ...
</ListVersionsResult>>
```

応答の本文

- `ListVersionsResult`
  `ListVersionsResult` パラメータのルート階層タグ。
  必要/不要: 必要
  - `DeleteMarker`
    各削除マーカーに関するメタデータ。応答には、0 個以上の削除マーカーを含めることができます。
  - Contents
    返される各オブジェクトに関するメタデータ。
    - `IsLatest`
      オブジェクトが最新かどうかを示します。
      タイプ: ブール値
    - `Key`
      マーカー名を削除します。
    - `LastModified`
      削除マーカーの前回の変更日時。
      タイプ: タイムスタンプ
    - `VersionId`

削除マーカーのバージョン ID を示します。

- Delimiter
  要求で渡される区切り文字の値。
- IsTruncated
  検索条件を満たすすべての結果が MSDP S3 によって返されたかどうかを示すフラグ。
- KeyMarker
  要求で、応答の NextKeyMarker の値を KeyMarker として使用する必要があります。
- MaxKeys
  応答の本文で返すことができるオブジェクトの最大数。
- Name
  バケットの名前。
- NextKeyMarker
  応答が切り捨てられた場合、後続の要求でこの値を KeyMarker として使用して、次のオブジェクトセットを取得できます。
- NextVersionIdMarker
  応答が切り捨てられた場合、後続の要求でこの値を VersionIdMarker として使用して、次のオブジェクトセットを取得できます。
- Prefix
  応答を、指定した接頭辞で始まるキーに制限します。
- VersionIdMarker
  要求で、応答の NextVersionIdMarker の値を VersionIdMarker として使用する必要があります。
- Version
  オブジェクトバージョンに関するメタデータ。
  - ETag
    オブジェクトの SHA256 ダイジェスト。
  - IsLatest
    オブジェクトが最新かどうかを示します。
    タイプ: ブール値
  - Key
    オブジェクト名。
  - LastModified
    オブジェクトの前回の変更日時。

- DELETE /bucket/Key+?uploadId=UploadId HTTP/1.1
  オブジェクトのサイズ。
- StorageClass
  オブジェクトのストレージクラス。
- VersionId
  オブジェクトのバージョン ID を示します。

スラッシュ (/) 区切り文字で区切って指定した接頭辞以下の CommonPrefixes 要素は 1,000 個未満にすることをお勧めします。指定した接頭辞以下に 10,000 個を超える CommonPrefixes 要素が存在する場合、要求で接頭辞と区切り文字パラメータを使用した list objects により 10,000 個の要素のみが返されます。指定した接頭辞以下のすべての要素を一覧表示する場合は、区切り文字なしで list objects を使用します。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument(continuation token is invalid)
  引数が無効です。HTTP 状態コード 400。
- InvalidArgument(maxKeys is invalid)
  引数が無効です。
  HTTP 状態コード 400。
- S3srvExtInvalidPrefix
  接頭辞はスラッシュで始めることはできません。
  HTTP 状態コード 400。
- S3srvExtInvalidDelimiter
  区切り文字としてスラッシュのみをサポートします。
  HTTP 状態コード 400。
- S3srvExtInvalidKeyMarker
  キーマーカーが無効です。
  HTTP 状態コード 400。
- AccessDenied
  アクセスが拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError

内部サーバーエラーのため、要求が失敗しました。
HTTP 状態コード 500。

PutBucketVersioning

既存のバケットのバージョン管理の状態を設定します。バージョン管理の状態を値 Enabled に設定すると、バケット内のオブジェクトのバージョン管理が有効になります。

バケットでバージョン管理の状態が一度も設定されていない場合、バケットのバージョン管理状態は存在しません。バケットでバージョン管理を有効にすると、バケットはバージョン管理状態になり、バージョン管理なしの状態に戻すことはできません。

要求の構文

```
PUT /bucket/?versioning HTTP/1.1
Host: msdps3.server:8443
<?xml version="1.0" encoding="UTF-8"?>
<VersioningConfiguration
xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Status>string</Status>
</VersioningConfiguration>
```

要求パラメータ

- Bucket
  オブジェクトが含まれているバケットの名前。
  必要/不要: 必要
  タイプ: 文字列

要求の本文

- Status
  バケットのバージョン管理の状態。
  有効な値: 有効 (Enabled)
  必要/不要: 必要
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
```

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- AccessDenied
  アクセスが拒否されました。

HTTP 状態コード 403。

- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

Put Object Lock Configuration (Flex WORM のみ)

指定したバケットにオブジェクトロックの構成を配置します。オブジェクトロック構成で指定されたルールが、指定したバケットに配置されたすべての新しいオブジェクトにデフォルトで適用されます。

要求の構文

```
PUT /{bucket}/?object-lock HTTP/1.1
Host: msdps3.server:8443

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration
xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <ObjectLockEnabled>string</ObjectLockEnabled>
   <Rule>
      <DefaultRetention>
         <Days>integer</Days>
         <Mode>string</Mode>
         <Years>integer</Years>
      </DefaultRetention>
   </Rule>
</ObjectLockConfiguration>
```

要求パラメータ

- Bucket
  オブジェクトロック構成を作成または置換するバケット。
  必要/不要: 必要
  タイプ: 文字列

要求の本文

- ObjectLockConfiguration
  ObjectLockConfiguration パラメータのルート階層タグ。
  必要/不要: 必要

- `ObjectLockEnabled`
  このバケットでオブジェクトロックの構成が有効になっているかどうかを示します。バケットに `ObjectLockConfiguration` を適用する場合は、`ObjectLockEnabled` を有効にします。
  有効な値: 有効 (Enabled)
  必要/不要: 不要
  タイプ: 文字列

- `Rule`
  指定したオブジェクトのオブジェクトロックルールを指定します。バケットに `ObjectLockConfiguration` を適用する場合は、ルールを有効にします。
  設定にはモードと期間の両方が必要です。期間には、日または年を指定できます。日と年を同時に指定することはできません。
  必要/不要: 不要
  種類: `ObjectLockRule` データ形式

応答の構文

```
HTTP/1.1 200
```

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。

- `AccessDenied`
  アクセスが拒否されました。
  HTTP 状態コード 403。

- `NoSuchBucket`
  指定されたバケットが存在しません。
  HTTP 状態コード 404。

- `InvalidBucketState`
  既存のバケットでオブジェクトロックの構成を有効にできません。
  HTTP 状態コード 409。

- `InvalidRequest`
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

GET Object Lock Configuration (Flex WORM のみ)

バケットのオブジェクトロック構成を取得します。

要求の構文

```
GET /{bucket}?object-lock HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  オブジェクトロック構成を取得するバケット。
  必要/不要: 必要
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration>
   <ObjectLockEnabled>string</ObjectLockEnabled>
   <Rule>
      <DefaultRetention>
         <Days>integer</Days>
         <Mode>string</Mode>
         <Years>integer</Years>
      </DefaultRetention>
   </Rule>
</ObjectLockConfiguration>
```

応答の本文

- ObjectLockConfiguration
  ObjectLockConfiguration パラメータのルート階層タグ。
  必要/不要: 必要

- ObjectLockEnabled
  このバケットでオブジェクトロックの構成が有効になっているかどうかを示します。バケットに ObjectLockConfiguration を適用する場合は、ObjectLockEnabled を有効にします。
  有効な値: 有効 (Enabled)
  必要/不要: 不要
  タイプ: 文字列

- Rule
  指定したオブジェクトのオブジェクトロックルールを指定します。バケットに ObjectLockConfiguration を適用する場合は、ルールを有効にします。
  設定にはモードと期間の両方が必要です。期間には、日または年を指定できます。日と年を同時に指定することはできません。
  必要/不要: 不要

種類: ObjectLockRule データ形式

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- AccessDenied
  アクセスが拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- S3srvExtObjectLockConfigurationNotFound
  このバケットのオブジェクトロック構成が存在しません。
  HTTP 状態コード 404。
- InvalidRequest
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

S3 API によるオブジェクト操作

S3 API によるオブジェクト操作で、次の主な機能を実行できます。

- MSDP サーバーにデータ (オブジェクト) をアップロードする
- MSDP サーバーからデータをダウンロードする
- MSDP サーバーからデータを削除する
- MSDP サーバーのデータを一覧表示する

AbortMultipartUpload

マルチパートアップロードを中止します。マルチパートアップロードが中止された後に、そのアップロード ID を使用して他のパートをアップロードすることはできません。アップロード済みのパートが使用するストレージは解放されます。

要求の構文

```
DELETE /bucket/Key+?uploadId=UploadId HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket

バケットの名前。
必要/不要: 必要
タイプ: 文字列

- Key
  マルチパートアップロードが開始されたオブジェクト名。
  必要/不要: 必要
  タイプ: 文字列
- uploadId
  マルチパートアップロードのアップロード ID。
  必要/不要: 必要
  タイプ: 文字列

応答の構文

```
HTTP/1.1 204
```

考えられるエラー応答

- Success
  HTTP 状態コード 204。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- InvalidPrefix
  接頭辞が無効です。
  HTTP 状態コード 400。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

CompleteMultipartUpload

以前にアップロードされたパートを集めてマルチパートアップロードを完了させます。

要求の構文

```
POST /bucket/Key+?uploadId=UploadId HTTP/1.1
Host: msdps3.server:8443
<?xml version="1.0" encoding="UTF-8"?>
```

```
<CompleteMultipartUpload
xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Part>
<ETag>string</ETag>
<PartNumber>integer</PartNumber>
</Part>
...
</CompleteMultipartUpload>
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- Key
  オブジェクトの名前。
  必要/不要: 必要
  タイプ: 文字列
- uploadId
  マルチパートアップロードのアップロード ID。
  必要/不要: 必要
  タイプ: 文字列

要求の本文

- CompleteMultipartUpload
  CompleteMultipartUpload パラメータのルート階層タグ。
  必要/不要: 必要
  - Part
    最終オブジェクトを作成するパートのリスト。ETag と PartNumber が含まれます。
    - ETag
      アップロードされたパートの ETag。
    - PartNumber
      アップロードされたパートの PartNumber。

応答の構文

```
HTTP/1.1 200
x-amz-version-id: VersionId
<?xml version="1.0" encoding="UTF-8"?>
<CompleteMultipartUploadResult>
```

```
    <Bucket>string</Bucket>
    <Key>string</Key>
    <ETag>string</ETag>
</CompleteMultipartUploadResult>
```

応答ヘッダー

- x-amz-version-id
  作成されたオブジェクトのバージョン ID。

応答の本文

- CompleteMultipartUploadResult
  CompleteMultipartUploadResult parameters のルート階層タグ。
  必要/不要: 必要
  - Bucket
    バケットの名前。
    必要/不要: 必要
    タイプ: 文字列
  - Key
    オブジェクトの名前。
    必要/不要: 必要
    タイプ: 文字列
  - ETag
    オブジェクトの SHA256 ダイジェスト。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidDigest
  指定した Content-MD5 が、受け取った内容と一致しませんでした。
  HTTP 状態コード 400。
- InvalidArgument
  引数が無効です。
  パート番号は、1 から 10000 までの整数にする必要があります。
  HTTP 状態コード 400。
- InvalidPartOrder
  パートのリストが昇順ではありませんでした。
  パートのリストは、パート番号順に指定する必要があります。
  HTTP 状態コード 400。

- EntityTooLarge
  指定したアップロードがオブジェクトの最大許容サイズを超えています。
  HTTP 状態コード 400。
- ErrEntityTooSmall
  指定したアップロードがオブジェクトの最小許容サイズを下回っています。
  HTTP 状態コード 400。
- ErrNoSuchUpload
  指定したマルチパートアップロードが存在しません。アップロード ID が有効でないか、マルチパートアップロードが中止または完了している可能性があります。
  HTTP 状態コード 400。
- ErrInvalidPart
  指定したパートの 1 つ以上が見つかりませんでした。パートがアップロードされていないか、指定したエンティティタグがパートのエンティティタグと一致していない可能性があります。
  HTTP 状態コード 400。
- MalformedPOSTRequest
  POST 要求の本文が適切な形式のマルチパート/フォームデータではありません。
  HTTP 状態コード 400。

- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

CreateMultipartUpload

マルチパートアップロードを開始してアップロード ID を返します。このアップロード ID を使用して、特定のマルチパートアップロードのすべてのパートを関連付けます。

要求の構文

```
POST /bucket/{Key+}?uploads HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- `Bucket`
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- `Key`
  マルチパートアップロードが開始されたオブジェクト名。
  必要/不要: 必要
  タイプ: 文字列
- `x-amz-object-lock-mode` (Flex WORM のみ)
  アップロードされたオブジェクトに適用するオブジェクトロックモードを指定します。
  有効な値: GOVERNANCE、COMPLIANCE
- `x-amz-object-lock-retain-until-date` (Flex WORM のみ)
  オブジェクトロックを期限切れにする日時を指定します。

メモ: このオプションを指定しない場合、保持値はバケットのデフォルトのオブジェクトロック構成を使用して計算されます。

```
object_lock_retain_until_date = current_system_timestamp +
bucket_default_object_lock_retention
```

応答の構文

```
HTTP/1.1 200
x-amz-version-id: VersionId
<?xml version="1.0" encoding="UTF-8"?>
<InitiateMultipartUploadResult>
    <Bucket>string</Bucket>
    <Key>string</Key>
    <UploadId>string</UploadId>
</InitiateMultipartUploadResult>
```

応答の本文

- `InitiateMultipartUploadResult`
  `InitiateMultipartUploadResult` パラメータのルート階層タグ。
  必要/不要: 必要
  - `Bucket`
    バケットの名前。
  - `Key`
    オブジェクトの名前。

- UploadId
  開始されたマルチパートアップロードの ID。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument
  引数が無効です。
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。
- InvalidRequest
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

DeleteObject

バージョン管理外のバケット内の指定されたオブジェクトを削除します。バケットでバージョン管理が有効で、VersionId が渡された場合は、指定したバージョンのオブジェクトが削除されます。バケットでバージョン管理が有効で、VersionId が渡されなかった場合は、オブジェクトに DeleteMarker が作成されます。

要求の構文

```
DELETE /bucket/Key+?versionId=VersionId HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列

- Key
  マルチパートアップロードが開始されたオブジェクト名。
  必要/不要: 必要
  タイプ: 文字列
- versionId
  オブジェクトのバージョン ID。
  タイプ: 文字列
- x-amz-bypass-governance-retention (Flex WORM のみ)
  この操作を処理するために、S3 オブジェクトロックがガバナンスモードの制限をバイパスする必要があるかどうかを示します。このヘッダーを使用するには、s3:BypassGovernanceRetention 権限が必要です。

応答の構文

```
HTTP/1.1 204
x-amz-delete-marker: DeleteMarker
x-amz-version-id: VersionId
```

応答ヘッダー

- x-amz-delete-marker
  削除されたオブジェクトが削除マーカーであるかどうかを示します。
- x-amz-version-id
  削除されたオブジェクトのバージョン ID を示します。

考えられるエラー応答

- Success
  HTTP 状態コード 204。
- InvalidArgument
  引数が無効です。
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchKey
  指定したキーは存在しません。
  HTTP 状態コード 404。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。

- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。
- `InvalidRequest`
  現在のオブジェクトはオブジェクトロックによって保護されており、上書きできません。
  HTTP 状態コード 400。

DeleteObjects

1 つの要求でバケットから複数のオブジェクトを削除します。

Content-MD5 ヘッダーはマルチオブジェクト削除要求に必要です。S3 インターフェースでは、ヘッダー値を使用して、送信中に要求の本文が変更されていないことを確認します。

要求の構文

```
DELETE /bucket?delete HTTP/1.1
Host: msdps3.server:8443
<?xml version="1.0" encoding="UTF-8"?>
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Object>
        <Key>string</Key>
        <VersionId>string</VersionId>
    </Object>
    ...
    <Quiet>boolean</Quiet>
</Delete>
```

要求パラメータ

- `Bucket`
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- `x-amz-bypass-governance-retention` (Flex WORM のみ)
  この操作を処理するために、S3 オブジェクトロックがガバナンスモードの制限をバイパスする必要があるかどうかを示します。このヘッダーを使用するには、`s3:BypassGovernanceRetention` 権限が必要です。

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DeleteResult>
```

```
    <Deleted>
        <DeleteMarker>boolean</DeleteMarker>
        <DeleteMarkerVersionId>string</DeleteMarkerVersionId>
        <Key>string</Key>
        <VersionId>string</VersionId>
    </Deleted>
    ...
    <Error>
        <Code>string</Code>
        <Key>string</Key>
        <Message>string</Message>
        <VersionId>string</VersionId>
    </Error>
    ...
</DeleteResult>
```

応答の本文

- `DeleteResult`
  `DeleteResult` パラメータのルート階層タグ。
  必要/不要: 必要
  - `Deleted`
    正常に削除されたオブジェクトの情報。
    - `DeleteMarker`
      削除されたオブジェクトが削除マーカーであったかどうかを示します。
    - `DeleteMarkerVersionId`
      削除された削除マーカーの `versionId` を示します。
    - `Key`
      オブジェクトの名前。
    - `VersionId`
      削除されたオブジェクトの `VersionId`。
  - `Error`
    削除に失敗したオブジェクトの情報。
    - `Code`
      オブジェクトの削除中に発生したエラーのエラーコード。
    - `Key`
      オブジェクトの名前。
    - `Message`

エラーメッセージ。

- VersionId
  エラーが発生したオブジェクトまたは削除マーカーの VersionId。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。
- InvalidRequest
  現在のオブジェクトはオブジェクトロックによって保護されており、上書きできません。
  HTTP 状態コード 400。

GetObject

S3 バケットからオブジェクトを取得します。大きいオブジェクトをダウンロードする場合は、範囲ベースの Get Object API を使用します。

要求の構文

```
GET /bucket/Key+?partNumber=PartNumber&versionId=VersionId HTTP/1.1

Host: msdps3.server:8443
Range: Range
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- Key
  オブジェクトの名前。
  必要/不要: 必要
  タイプ: 文字列
- partNumber
  読み込むオブジェクトのパート数。これは、1 から 10000 の正の整数です。

タイプ: 整数

- versionId
  オブジェクトのバージョン ID。
  タイプ: 文字列

リクエストヘッダー

- Range
  指定されたオブジェクト範囲 (バイト) を返します。
  タイプ: 整数

応答の構文

```
HTTP/1.1 200
x-amz-delete-marker: DeleteMarker
accept-ranges: AcceptRanges
Last-Modified: LastModified
Content-Length: ContentLength
ETag: ETag
x-amz-version-id: VersionId
Content-Range: ContentRange
x-amz-storage-class: StorageClass
Body
```

応答ヘッダー

- x-amz-delete-marker
  返されたオブジェクトが削除マーカーであるかどうかを示します。オブジェクトが削除マーカーでない場合、このヘッダーは応答に追加されません。
- Last-Modified
  オブジェクトの最終変更時刻。
- Content-Length
  返された本文のサイズ (バイト)。
- ETag
  返されたオブジェクトの SHA256 を示します。
- x-amz-version-id
  返されたオブジェクトのバージョン ID を示します。
- Content-Range
  応答で返されたオブジェクトの範囲。
- x-amz-storage-class
  返されたオブジェクトのストレージクラスを示します。

- x-amz-object-lock-mode (Flex WORM のみ)
  このオブジェクトに現在設定されているオブジェクトロックモード。
  有効な値: GOVERNANCE、COMPLIANCE
- x-amz-object-lock-retain-until-date (Flex WORM のみ)
  このオブジェクトのオブジェクトロックの期限が切れる日時。
- x-amz-meta-msdps3-object-creator
  オブジェクトのアップロードに使用する API。値 PutGroupObject は、「ヘッダー x-amz-meta-snowball-auto-extract を持つ PutObject」を意味します。
  有効な値: PutObject、PutGroupObject、UploadPart

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument
  引数が無効です。
  無効なバージョン ID が指定されました。HTTP 状態コード 400。
- EntityTooLarge
  指定したアップロードがオブジェクトの最大許容サイズを超えています。
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchKey
  指定したキーは存在しません。
  HTTP 状態コード 404。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

HeadObject

オブジェクト自体を返さずに、オブジェクトからメタデータを取得します。この操作は、オブジェクトのメタデータにのみ関心がある場合に使用します。

要求の構文

```
HEAD /bucket/Key+?partNumber=PartNumber&versionId=VersionId HTTP/1.1

Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- Key
  オブジェクトの名前。
  必要/不要: 必要
  タイプ: 文字列
- partNumber
  読み込むオブジェクトのパート数。これは、1 から 10000 の正の整数です。
  タイプ: 整数
- versionId
  オブジェクトのバージョン ID。
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
x-amz-delete-marker: DeleteMarker
accept-ranges: AcceptRanges
Last-Modified: LastModified
Content-Length: ContentLength
ETag: ETag
x-amz-version-id: VersionId
Content-Range: ContentRange
```

応答ヘッダー

- x-amz-delete-marker
  返されたオブジェクトが削除マーカーであるかどうかを示します。オブジェクトが削除マーカーでない場合、このヘッダーは応答に追加されません。
- Last-Modified
  オブジェクトの最終変更時刻。
- Content-Length
  返された本文のサイズ (バイト)。
- ETag

返されたオブジェクトの SHA256 を示します。

- `x-amz-version-id`
  返されたオブジェクトのバージョン ID を示します。
- `Content-Range`
  応答で返されたオブジェクトの範囲。
- `x-amz-object-lock-mode` (Flex WORM のみ)
  このオブジェクトに現在設定されているオブジェクトロックモード。
  有効な値: GOVERNANCE、COMPLIANCE
- `x-amz-object-lock-retain-until-date` (Flex WORM のみ)
  このオブジェクトのオブジェクトロックの期限が切れる日時。
- `x-amz-meta-msdps3-object-creator`
  オブジェクトのアップロードに使用する API。値 `PutGroupObject` は、「ヘッダー `x-amz-meta-snowball-auto-extract` を持つ `PutObject`」を意味します。
  有効な値: `PutObject`、`PutGroupObject`、`UploadPart`

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。
- `InvalidArgument`
  引数が無効です。無効なバージョン ID が指定されました。
  HTTP 状態コード 400。
- `AccessDenied`
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- `NoSuchKey`
  指定したキーは存在しません。
  HTTP 状態コード 404。
- `NoSuchBucket`
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- `InternalError`
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

PutObject

バケットにオブジェクトを追加します。バケットでバージョン管理が有効になっている場合、Put Object API はオブジェクトの `VersionId` を返します。

要求の構文

```
PUT /bucket/Key HTTP/1.1
Host: msdps3.server:8443
Content-Length: ContentLength
Content-MD5: ContentMD5
Body
```

要求パラメータ

- `Bucket`
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- `Key`
  オブジェクトの名前。
  必要/不要: 必要
  タイプ: 文字列
- `x-amz-object-lock-mode` (Flex WORM のみ)
  このオブジェクトに適用するオブジェクトロックモード。
  有効な値: GOVERNANCE、COMPLIANCE
- `x-amz-object-lock-retain-until-date` (Flex WORM のみ)
  このオブジェクトのオブジェクトロックの期限が切れる日時。タイムスタンプパラメータとしてフォーマットする必要があります。

応答の構文

```
HTTP/1.1 200
ETag: ETag
x-amz-version-id: VersionId
```

応答ヘッダー

- `x-amz-version-id`
  バケット内のオブジェクト PUT のバージョン ID。

考えられるエラー応答

- `Success`
  HTTP 状態コード 200。

- EntityTooLarge
  オブジェクトのサイズが最大許容サイズを超えています。
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。
- InvalidRequest
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

Copy Object

ストレージサーバーにオブジェクトのコピーを作成します。ソースオブジェクトへの読み取りアクセス権と宛先バケットへの書き込みアクセス権が必要です。バケットでバージョン管理が有効になっている場合、Copy Object API はオブジェクトの VersionId を返します。オブジェクトをコピーすると、メタデータと ACL の両方が保持されません。

要求の構文

```
PUT /bucket/Key HTTP/1.1
Host: msdps3.server:8443
x-amz-copy-source: CopySource
x-amz-object-lock-mode: ObjectLockMode
x-amz-object-lock-retain-until-date: ObjectLockRetainUntilDate
```

要求パラメータ

- Bucket
  宛先バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- Key
  宛先オブジェクトのキー。
  必要/不要: 必要

タイプ: 文字列

- x-amz-copy-source
  コピー操作のソースオブジェクトを指定します。
  値の形式: ソースバケットの名前とソースオブジェクトのキーをスラッシュ (/) で区切って指定します。
  たとえば、バケット srcbk からオブジェクト msdps3/copyright.txt をコピーするには、srcbk/msdps3/copyright.txt を使用します。値は URL エンコードされている必要があります。
  オブジェクトの特定のバージョンをコピーするには、値に ?versionId=<version-id> を追加します。例: srcbk/msdps3/copyright.txt?versionId=AAAA1234567890
  バージョン ID を指定しない場合、ソースオブジェクトの最新バージョンがコピーされます。
  パターン: ¥/.+¥/.+
  必要/不要: 必要

- x-amz-object-lock-mode (Flex WORM のみ)
  このコピーされたオブジェクトに適用するオブジェクトロックモード。
  有効な値: GOVERNANCE、COMPLIANCE

- x-amz-object-lock-retain-until-date (Flex WORM only)
  このコピーされたオブジェクトのオブジェクトロックの期限が切れる日時。タイムスタンプパラメータとしてフォーマットする必要があります。

応答の構文

```
HTTP/1.1 200
x-amz-copy-source-version-id: CopySourceVersionId
x-amz-version-id: VersionId
<?xml version="1.0" encoding="UTF-8"?>
<CopyObjectResult>
   <ETag>string</ETag>
   <LastModified>timestamp</LastModified>
</CopyObjectResult>
```

応答ヘッダー

- x-amz-copy-source-version-id
  ソースバケット内にあるコピーされたオブジェクトのバージョン。

- x-amz-version-id
  新しく作成されたコピーのバージョン ID。

- ETag
  新しいオブジェクトの ETag を返します。
  タイプ: 文字列

- LastModified
  オブジェクトの作成日。
  タイプ: タイムスタンプ

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- EntityTooLarge
  オブジェクトのサイズが最大許容サイズを超えています。
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。
- InvalidRequest
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

UploadPart

マルチパートアップロードのパートをアップロードします。

要求の構文

```
PUT /bucket/Key+?partNumber=PartNumber&uploadId=UploadId HTTP/1.1
Host: msdps3.server:8443
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列
- Key
  オブジェクトの名前。

必要/不要: 必要
タイプ: 文字列

- partNumber
  アップロードするパート数。
  必要/不要: 必要
  タイプ: 文字列
- uploadId
  マルチパートアップロードのアップロード ID。
  必要/不要: 必要
  タイプ: 文字列
- Content-MD5
  部分データの base64 エンコードされた 128 ビット MD5 ダイジェスト。このパラメータは、オブジェクトロックパラメータが指定されている場合に必要です。

応答の構文

```
HTTP/1.1 200
```

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchUpload
  アップロード ID またはキーが無効である可能性があります。
  HTTP 状態コード 404。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。

PutObject (小さいファイルの場合は snowball-auto-extract)

各コピー操作では何らかのオーバーヘッドが発生するため、個々の小さいファイルで多くの転送を実行すると、大きいファイルで同じデータを転送するよりも全体的なパフォーマンスが低下します。小さいファイル (1 MB 未満のファイル) の転送速度を大幅に向上させるには、小さいファイルをまとめてバッチ処理します。ファイルのバッチ処理は手動で行います。x-amz-meta-snowball-auto-extract ヘッダーを指定してバッチファイルを S3 サーバーに追加する場合、データを MSDP S3 サーバーにインポートするときに、バッチが自動的に抽出されます。

メモ: バージョン管理対象外のバケットでは x-amz-meta-snowball-auto-extract ヘッダーは許可されないため、バッチ処理されたすべての小さいファイルは S3 サーバーで同じバージョンを共有します。

---

tar または gzip コマンドを実行して小さいファイルを手動でバッチ処理してから、MSDP の S3 インターフェースに転送します。

例: `tar -czf <archive-file> <small files or directory of small files>`

```
aws --endpoint https://<hostname>:8443 --profile <profile name> s3api
[--ca-bundle <CA_BUNDLE_FILE>] put-object --bucket <bucket name>
--key <key path> --body <xxx.tgz> --metadata
snowball-auto-extract=true
```

小さいファイルをバッチ処理する場合は、次の点に注意してください。

- 最大バッチサイズは 5 GB。
- バッチあたりの推奨最大ファイル数は 10,000 個。
- サポート対象のアーカイブ形式は TGZ。

要求の構文

```
PUT /bucket/Key HTTP/1.1
Host: msdps3.server:8443
Content-Length: ContentLength
Content-MD5: ContentMD5
x-amz-meta-snowball-auto-extract:true
Body
```

要求パラメータ

- Bucket
  バケットの名前。
  必要/不要: 必要
  タイプ: 文字列

- Key
  オブジェクトの名前。
  必要/不要: 必要
  タイプ: 文字列
- x-amz-object-lock-mode (Flex WORM のみ)
  このオブジェクトに適用するオブジェクトロックモード。
  有効な値: GOVERNANCE、COMPLIANCE
- x-amz-object-lock-retain-until-date (Flex WORM のみ)
  このオブジェクトのオブジェクトロックの期限が切れる日時。タイムスタンプパラメータとしてフォーマットする必要があります。

リクエストヘッダー

- Enable snowball-auto-extract
  必要/不要: 必要
  値: true

応答の構文

```
HTTP/1.1 200
ETag: ETag
x-amz-version-id: VersionId
```

リクエストヘッダー

- x-amz-version-id
  バケット内のオブジェクト PUT のバージョン ID。

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- EntityTooLarge
  オブジェクトのサイズが最大許容サイズを超えています。
  HTTP 状態コード 400。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。

HTTP 状態コード 500。

- InvalidRequest
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

Put Object Retention (Flex WORM のみ)

オブジェクトにオブジェクトの保持構成を配置します。

要求の構文

```
PUT /{bucket}/{Key+}?retention&versionId=VersionId HTTP/1.1
Host: msdps3.server:8443
x-amz-bypass-governance-retention: BypassGovernanceRetention
Content-MD5: ContentMD5
<?xml version="1.0" encoding="UTF-8"?>
<Retention xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Mode>string</Mode>
   <RetainUntilDate>timestamp</RetainUntilDate>
</Retention>
```

要求パラメータ

- Bucket
  このオブジェクト保持構成を適用するオブジェクトを含むバケット名。
  必要/不要: 必要
  タイプ: 文字列
- Key
  このオブジェクト保持構成を適用するオブジェクトのキー名。
  必要/不要: 必要
  タイプ: 文字列
- versionId
  このオブジェクト保持構成を適用するオブジェクトのバージョン ID。
- x-amz-bypass-governance-retention
  この操作で、ガバナンスモードの制限をバイパスする必要があるかどうかを示します。

要求の本文

- Retention
  保持パラメータのルート階層タグ。
  必要/不要: 必要
- Mode

指定したオブジェクトの保持モードを示します。
有効な値: GOVERNANCE、COMPLIANCE
必要/不要: 不要
タイプ: 文字列

- RetainUntilDate
  このオブジェクトロックの保持が期限切れになる日付。
  必要/不要: 不要
  タイプ: タイムスタンプ

応答の構文

```
HTTP/1.1 200
```

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。
- InternalError
  内部サーバーエラーのため、要求が失敗しました。
  HTTP 状態コード 500。
- InvalidRequest
  このエラーは何らかの理由で発生することがあります。詳しくは、エラーメッセージを参照してください。
  HTTP 状態コード 400。

Get Object Retention (Flex WORM のみ)

オブジェクトの保持設定を取得します。

要求の構文

```
GET /{bucket}/Key+?retention&versionId=VersionId HTTP/1.1 Host:
msdps3.server:8443
```

要求パラメータ

- Bucket
  保持設定を取得するオブジェクトを含むバケット名。
  必要/不要: 必要
  タイプ: 文字列
- Key
  保持設定を取得するオブジェクトのキー名。
  必要/不要: 必要
  タイプ: 文字列
- versionId
  保持設定を取得するオブジェクトのバージョン ID。
  タイプ: 文字列

応答の構文

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<Retention>
   <Mode>string</Mode>
   <RetainUntilDate>timestamp</RetainUntilDate>
</Retention>
```

応答の本文

- Retention
  保持パラメータのルート階層タグ。
  必要/不要: 必要
- Mode
  指定したオブジェクトの保持モードを示します。
  有効な値: GOVERNANCE、COMPLIANCE
  タイプ: 文字列
- RetainUntilDate
  このオブジェクトロックの保持が期限切れになる日付。
  タイプ: タイムスタンプ

考えられるエラー応答

- Success
  HTTP 状態コード 200。
- InvalidArgument
  引数が無効です。無効なバージョン ID が指定されました。
  HTTP 状態コード 400。

- AccessDenied
  ユーザー認証が失敗したため、要求が拒否されました。
  HTTP 状態コード 403。
- NoSuchKey
  指定したキーは存在しません。
  HTTP 状態コード 404。
- NoSuchBucket
  指定されたバケットが存在しません。
  HTTP 状態コード 404。

バケットとオブジェクトの命名規則

バケットの命名規則:

- バケット名は 3 ～ 63 文字の長さにする必要があります。
- バケット名には小文字、数字、ドット (.)、ハイフン (-) のみを使用できます。
- バケット名の先頭と末尾は英字または数字である必要があります。
- バケット名に IP アドレスは使用できません。たとえば、192.168.5.4 などです。
- バケット名の先頭に接頭辞 xn-- を付けることはできません。
- バケット名の末尾に接尾辞 -s3alias を付けることはできません。
- バケット名にドット (.) を使用しないでください。

オブジェクトの命名規則:

- オブジェクトの命名規則は、UNIX ファイルシステムのファイル命名規則と同じです。
- URL エンコードタイプのみがサポートされます。エスケープが必要な場合は、URL Escape で名前をエンコードする必要があります。
- オブジェクト名の先頭や末尾にスラッシュは使用できません。
- オブジェクト名は次の規則で処理されます。
  - 複数のスラッシュは 1 つのスラッシュに置き換えられます。
  - 各 . パス名要素 (現在のディレクトリ) は削除されます。
  - 内部の各 .. パス名要素 (親ディレクトリ) と、その前にある .. 以外の要素は削除されます。
  - ルート指定のパスの先頭の .. 要素は削除されます。つまり、パスの先頭にある「/..」が「/」に置き換わります。
  - 返されるパスは、ルート「/」の場合のみスラッシュで終了します。

- この処理の結果が空の文字列の場合は、文字列「.」が返されます。
- オブジェクト名に「%」が含まれている場合は、エンコード名として扱われます。

MSDP オブジェクトストアの保護ポリシーの作成

MSDP-Object-Store ポリシー形式は、MSDP S3 ストレージに配置されたデータを保護します。

MSDP オブジェクトストアのバックアップに関する制限事項を次に示します。

- メディアサーバーは Red Hat オペレーティングシステムである必要があります。
- バケットのバージョン管理が有効になっている場合、最新のオブジェクトバージョンのみをバックアップできます。
- NBCA と ECA を使用して構成された MSDP S3 のみがサポートされます。
- 1 つのバックアップポリシーで複数のバックアップ対象を指定できます。ただし、これらのバックアップ対象は同じバケットに属している必要があります。
- 指定した MSDP S3 パスがオブジェクトと接頭辞の両方と一致する場合、バックアップジョブは失敗します。
  たとえば、パスが `/bucket1/obj1` として指定され、次のオブジェクト構造が存在する場合、バックアップジョブは失敗します: /bucket1/obj1、/bucket1/obj1/obj2。
- MSDP オブジェクトストアのバックアップジョブの実行中は、バックアップジョブが完了するまで、バックアップ対象のオブジェクトを削除したり、(バージョン管理されていないバケットを) 上書きしたりすることはできません。

MSDP オブジェクトストアの保護ポリシーを作成するには

1. NetBackup Web UI を使用してポリシーを作成します。
2. [属性 (Attributes)]タブで、ポリシー形式リストの[MSDP-Object-Store]を選択します。
3. [宛先 (Destination)]で、ポリシーストレージリストからストレージユニットを選択します。

   MSDP-Object-Store ポリシーのストレージユニットは、MSDP S3 が作成されるのと同じディスクプールボリュームに配置する必要があります。

   ポリシーストレージの設定について詳しくは、『NetBackup 管理者ガイド Vol. 1』のポリシーストレージ (ポリシー属性) に関する説明を参照してください。
4. [スケジュール (Schedules)]タブで、[完全バックアップ (Full backup)]、[差分増分バックアップ (Differential incremental backup)]、または[累積増分バックアップ (Cumulative incremental backup)]を選択します。

5 [バックアップ対象 (Backup Selections)]タブで、[追加 (Add)]をクリックします。MSDP S3 バケットのパスの接頭辞をパス名に入力します。形式は /<BucketName>/<Prefix> です。[リストに追加 (Add to list)]をクリックします。

MSDP-Object-Store ポリシーのクライアント名は、形式 MSDP_<StorageServerName>_<BucketName> を使用して自動的に生成されます。

6 MSDP-Object-Store ポリシーを実行します。

バックアップの作成後、リストア、複製、自動イメージレプリケーションなどの NetBackup の機能でバックアップを管理できます。

バックアップイメージからの MSDP オブジェクトストアデータのリカバリ

MSDP-Object-Store バックアップイメージからバックアップデータをリカバリし、NetBackup クライアントのファイルシステムに書き込むことができます。

MSDP オブジェクトストアのリカバリに関する制限事項:

- サポートされるのは、MSDP オブジェクトストアのバックアップデータを NetBackup クライアントのファイルシステムにリカバリすることのみで、NetBackup クライアントのオペレーティングシステムは Linux である必要があります。
- 安全性を高めるため、リカバリされたオブジェクトの権限はファイルシステムで 600 となっており、オブジェクトへのアクセスには管理者権限が必要です。

MSDP-Object-Store のバックアップデータをリカバリするには

1 NetBackup Web UI で、左側の[リカバリ (Recovery)]をクリックします。

2 [標準リカバリ (Regular recovery)]で[リカバリの開始 (Start recovery)]をクリックします。

3 [基本プロパティ (Basic properties)]ページで、ポリシー形式リストから[MSDP-Object-Store]を選択します。

4 [クライアントの選択 (Select client)]をクリックしてソースクライアントを選択します。

5 宛先クライアントのホスト名を入力します。宛先クライアントは有効な NetBackup クライアントである必要があります。MSDP-Object-Store ポリシー用に自動的に生成されたクライアント名は、宛先クライアントとして使用できません。

[次へ (Next)]をクリックします。

6 [リカバリの詳細 (Recovery details)]ページで、リカバリするバックアップイメージおよびオブジェクトを選択します。[次へ (Next)]をクリックします。

7 [リカバリオプション (Recovery options)]ページで、リカバリ先を選択します。これは宛先クライアントのファイルシステムパスです。[次へ (Next)]をクリックします。

8 [確認 (Review)]ページで、詳細を確認して[リカバリの開始 (Start recovery)]をクリックします。

リストアジョブが完了すると、リカバリされたオブジェクトは、宛先の NetBackup クライアントの宛先ファイルシステムパスに配置されます。

MSDP オブジェクトストアのインスタントアクセス

NetBackup イメージを使用して、MSDP オブジェクトストアのインスタントアクセスバケットを作成できます。

インスタントアクセスの前提条件

- MSDP オブジェクトストアのインスタントアクセスは、BYO (Build-Your-Own) を使用する Red Hat MSDP ストレージサーバーと、NetBackup Flex Appliance 環境にのみ適用できます。
- MSDP S3 バケットに MSDP オブジェクトストア用のバックアップイメージを少なくとも 1 つ生成する必要があります。
- MSDP S3 インターフェースは、NetBackup イメージが配置されている MSDP ストレージに構成する必要があります。

インスタントアクセス機能を使用する前の考慮事項

インスタントアクセス MSDP オブジェクトストア機能について、次の点に注意します。

- インスタントアクセスターゲットストレージサーバーでは、MSDP S3 インターフェースが構成されている必要があります。
p.386 の「MSDP の S3 インターフェースについて」を参照してください。
- インスタントアクセスターゲットバケットでバージョン管理を無効にする必要があります。新しいバケットを指定すると、デフォルトでバージョン管理は無効になります。バージョン管理が有効になっている既存のバケットを指定すると、インスタントアクセスは失敗します。
- インスタントアクセスターゲットバケットは、バックアップイメージが格納されているストレージに配置されている必要があります。新しいバケットを指定すると、デフォルトでは、バックアップイメージが格納されているのと同じストレージに作成されます。バックアップイメージが格納されているのとは異なるストレージサーバーにある既存のバケットを指定すると、インスタントアクセスは失敗します。
- ソース MSDP S3 バケットでは、以前の NetBackup リリースでバックアップイメージが生成された場合、インスタントアクセス用にバックアップイメージが識別されない場合があります。MSDP オブジェクトストアのインスタントアクセスを使用するには、最新のリリースでバックアップイメージを生成する必要があります。

- MSDP オブジェクトストアのバックアップとインスタントアクセスを、同じ MSDP ストレージサーバーで同時に使用しないことをお勧めします。
- MSDP-Object-Store ポリシーを使用して、NetBackup バックアップイメージを作成する必要があります。

インスタントアクセス MSDP オブジェクトストアの作成

NetBackup イメージから、インスタントアクセス MSDP オブジェクトストアを作成できます。[バケット (Buckets)]タブにはソースバケットが表示され、[インスタントアクセス MSDP オブジェクトストア (Instant access MSDP object store)]タブには、作成したすべてのターゲットバケットが表示されます。

メモ: MSDP オブジェクトストアのインスタントアクセス機能は、BYO および NetBackup Flex メディアプラットフォームのみをサポートします。

「インスタントアクセス機能を使用する前の考慮事項」

インスタントアクセス MSDP オブジェクトストアを作成するには

1. 左側で、[作業負荷 (Workloads)]、[MSDP オブジェクトストア (MSDP object store)]の順に選択します。
2. [バケット (Buckets)]タブでバケットを見つけてクリックします。
3. [リカバリポイント (Recovery points)]タブをクリックし、バックアップが発生した日付をクリックします。

   利用可能なイメージは、各イメージのバックアップタイムスタンプ付きで各行に表示されます。
4. インスタントアクセスを使用したリカバリのオプションがあるイメージまたはイメージのコピーで、[リカバリ (Recover)]をクリックします。

   [インスタントアクセス MSDP オブジェクトストアの作成 (Create an instant access MSDP object store)]ページに、MSDP オブジェクトストレージサーバー名が表示されます。
5. [ターゲットバケット名 (Target bucket name)]フィールドに、インスタントアクセス MSDP オブジェクトストアを作成するバケットの名前を入力し、[保存 (Save)]をクリックします。

   ターゲットバケット名は 3 から 63 文字の間で、文字または数字で開始および終了し、小文字、数字、ドット、およびハイフンのみが含まれるようにする必要があります。
6. インスタントアクセスジョブが開始された後、[リストアアクティビティ (Restore activity)]タブをクリックして進捗状況を表示できます。
7. ターゲットバケットについて詳しくは、[インスタントアクセス MSDP オブジェクトストア (Instant access MSDP object store)]タブでバケットの表示名をクリックします。

インスタントアクセス MSDP オブジェクトストアの削除

インスタントアクセスターゲットバケットが存在する MSDP ストレージサーバーで、次のコマンドラインオプションを実行する必要があります。この操作は、NetBackup Web UI ではサポートされません。

- `aws --cli-read-timeout 0 --endpoint <endpoint url> s3 rm s3://<bucket name> --recursive` (バケットを空にする)
- `aws --endpoint <endpoint url> s3 rb s3://<bucket name>` (バケットを削除する)
- `rm -f <storage dir>/s3_ia_instances/<bucketname>.json`

MSDP の S3 インターフェースでのディザスタリカバリ

ローカル LSU をリカバリした後、`s3srv_config.sh --recover` コマンドを実行して MSDP の S3 インターフェースをリカバリします。

p.539 の「MSDP ストレージサーバーのディスクエラーからのリカバリ」を参照してください。

p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。

MSDP クラウドのクラウド LSU をリカバリできます。p.288 の「クラウド LSU のディザスタリカバリについて」を参照してください。

シナリオ 1 とシナリオ 2 (ローカルストレージが失われる場合) については、S3 構成コマンドを実行して S3 を構成します。

シナリオ 3 とシナリオ 4 (ローカルストレージが失われない場合) については、`s3srv_config.sh --recover` コマンドを実行して S3 を構成します。

クラウド LSU からの MSDP S3 IAM 構成のリカバリ

MSDP S3 が有効になっている場合は、ディザスタリカバリ後のクラウド LSU から MSDP S3 IAM 構成をリカバリできます。

クラウド LSU から MSDP S3 IAM 構成をリカバリする方法

◆ MSDP サーバーで、次のコマンドを実行します。

```
/usr/openv/pdde/vxs3/cfg/script/s3srv_config.sh
--recover-iam-config <LSU name>
```

このコマンドは、クラウド LSU の IAM 構成と現在の IAM 構成を表示します。

次の警告メッセージが表示されます。

```
WARNING: This operation overwrites current IAM configurations
with the IAM configurations in cloud LSU.
```

現在の IAM 構成を上書きするには、次を入力して Enter キーを押します。

```
overwrite-with-<cloud_LSU_name>
```

メモ: このコマンドの前に `/usr/openv/pdde/vxs3/cfg/script/s3srv_config.sh --reset-iam-root` コマンドを実行しないでください。クラウド LSU の IAM 構成が上書きされます。

MSDP の S3 インターフェースの制限事項

MSDP の S3 インターフェースには次の制限事項があります。

- 1 台の S3 サーバーに 1,000 個のバケット。
- MSDP サーバーのパフォーマンスに基づいて 500 ～ 800 件の並列実行要求をお勧めします。
- 小さいファイルは 1 MB 未満である必要があります。小さいファイルの tar 圧縮ファイルは 5 GB 未満である必要があります。小さいファイルの tar 圧縮ファイルに含まれる小さいファイルの数は 10,000 個未満である必要があります。
- 1 つのオブジェクトサイズは 5 TB 未満である必要があります。
- マルチパートアップロードの制限事項。「Amazon S3 マルチパートアップロードの制限」を参照してください。
- MSDP の S3 インターフェースでは、Amazon S3 Glacier、Deep Archive、Microsoft Azure Archive はサポートされません。
- S3 サーバーを構成するときに、OST プラグインのクライアント名に #s3storage は使用しないでください。
- バックエンド WORM モードを変更する前に、すべてのマルチパートアップロードが完了していることを確認します。
- オブジェクトを異なるストレージサーバー間でコピーすることはできません。

- 5 GB を超えるオブジェクトはコピーできません。
- UploadPartCopy API はサポートされません。UploadPart によってアップロードされたオブジェクトをコピーすると、作成されたオブジェクトはパートなしのシングルオブジェクトになります。
- MSDP の S3 インターフェースは、AWS コマンドラインインターフェースバージョン 2.23.0 以降をサポートしていません。これらのバージョンでは、PutObject や UploadPart などの PUT 処理にトレーラーを含むチャンクアップロードを使用するためです。

ログとトラブルシューティング

MSDP の S3 インターフェースのログは <storage>/log/vxs3 に保存されます。また、この場所で S3 API に関連するエラーを見つけることもできます。一部のエラーは spad/spoold の下にあります。

ログの設定

1 ログレベルを手動で設定します。

S3 サーバー構成ファイル <storage>/etc/puredisk/s3srv.cfg の編集

```
; None: 0; Error: 1; Warning: 2; Info: 3; Debug: 4

 ; @restart

 LogLevel=<log level>
```

2 S3 サーバーを再起動します。

```
systemctl restart pdde-s3srv
```

NGINX は S3 サーバーに要求を転送します。NGINX のログ記録はデフォルトでは無効になっています。使用する場合は、S3 NGINX の設定で NGINX ログを有効にする必要があります。

NGINX ログの有効化

1. /etc/<nginx server name>/conf.d/s3srvbyo.conf を編集します。
2. アクセスとエラーの部分を次のように変更します。

```
access_log <access log path> main;

        error_log <error log path> debug;
```

3. NGINX の設定を再ロードします。

```
systemctl reload <nginx server name>
```

ベストプラクティス

MSDP に S3 インターフェースを使用する場合のベストプラクティスを次に示します。

- オブジェクトキーに接頭辞を使用します。
- バケット名にドット (.) を使用しないでください。
- BYO コンピュータのパフォーマンスに基づいて 50 ～ 100 件の並列実行要求をお勧めします。
- スラッシュ (/) 区切り文字で区切って指定した接頭辞以下の CommonPrefixes 要素は 1,000 個未満にすることをお勧めします。
- AWS CLI を使用する場合は、.aws/config ファイルに --cli-read-timeout 0 と -cli-connect-timeout 0 を追加してから、payload_signing_enabled = true を追加します。
- S3 クライアントのタイムアウト設定は要求の手順に影響する場合があります。タイムアウト前にサーバーが応答しない場合、クライアントは要求を自動的に取り消します。

8

重複排除アクティビティの監視

この章では以下の項目について説明しています。

- MSDP 重複排除率と圧縮率の監視
- MSDP ジョブの詳細の表示
- MSDP ストレージの容量と使用状況のレポートについて
- MSDP コンテナファイルについて
- MSDP コンテナファイル内のストレージ使用状況の表示
- MSDP プロセスの監視について
- 自動イメージレプリケーションジョブに関するレポート
- イメージの暗号化状態の確認

MSDP 重複排除率と圧縮率の監視

重複排除率は、重複排除エンジンで保存されたデータの割合です。このデータが再度保存されることはありません。圧縮率は、データを格納する前にバックアップデータを圧縮して節約された領域の割合です。

次の方式は MSDP 重複排除率を示します。

- 「グローバルな MSDP 重複排除率を表示する方法」
- 「アクティビティモニターでバックアップジョブの MSDP 重複排除率を表示する方法」

MSDP 圧縮率を示す方式については、p.482 の「MSDP ジョブの詳細の表示」を参照してください。

UNIX と Linux では、NetBackup の bpdbjobs コマンドを使って重複排除率を表示できます。ただし、表示するように構成する必要があります。

グローバルな MSDP 重複排除率を表示する方法

1. Web UI を開きます。
2. 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。
3. [ストレージサーバー (Storage servers)]タブをクリックします。
4. ストレージサーバー名をクリックして、グローバルな MSDP 重複排除率を表示します。

アクティビティモニターでバックアップジョブの MSDP 重複排除率を表示する方法

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. [ジョブ (Jobs)]タブをクリックします。

   [重複排除率 (Deduplication Ratio)]列に、各ジョブの比率が表示されます。

個別の重複排除率と圧縮率の表示を無効にする

個別の圧縮率の表示を無効にするには:

- 次の場所にある pd.conf ファイルを開きます。

  Windows

  ```
  <install_location>¥lib¥ost-plugins¥pd.conf
  ```

  UNIX

  ```
  /usr/openv/lib/ost-plugins/pd.conf
  ```

- ファイルに次のパラメータを追加します。

  ```
  DISPLAY_COMPRESSION_SPACE_SAVING = 0
  ```

  このパラメータを削除するか、値を 1 に変更して、個別の値としての圧縮率の表示を有効にできます。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

p.37 の「MSDP クライアントの重複排除の必要条件と制限事項について」を参照してください。

MSDP ジョブの詳細の表示

重複排除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。

MSDP ジョブの詳細を表示する方法

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. [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)]タブペインに表示されているジョブをダブルクリックします。
4. [ジョブの詳細 (Job Details)]ダイアログボックスで、[状態の詳細 (Detailed Status)]タブをクリックします。

   重複排除ジョブの詳細は別のトピックに記述されています。

   p.483 の「MSDP ジョブの詳細」を参照してください。

MSDP ジョブの詳細

アクティビティモニターでは、ジョブの詳細に、重複排除ジョブの詳細が表示されます。詳細は、ジョブがメディアサーバーの重複排除か、またはクライアント側の重複排除かによって異なります。

メディアサーバーの重複排除ジョブの詳細

メディアサーバーの重複排除の場合、[詳細 (Details)]タブには、重複排除を実行したサーバー上の重複排除率が表示されます。次のジョブの詳細例の引用では MSDP_Server.example.com がデータを重複排除したクライアントの詳細を示します (dedup フィールドは重複排除率を示し、compression フィールドは圧縮によって保存されたストレージ領域を示します)。

```
LOG 1551428319 4 Info MSDP_Server.example.com 27726
StorageServer=PureDisk:MSDP_Server.example.com; Report=PDDO Stats
(multi-threaded stream used) for (MSDP_Server.example.com):
scanned: 105098346 KB, CR sent: 2095410 KB, CR sent over FC: 0 KB,
dedup: 98.0%, cache hits: 337282 (41.0%), where dedup space
saving:89.7%,
compression space saving:8.3%
```

クライアント側の重複排除ジョブの詳細

クライアント側の重複排除ジョブの場合、[詳細 (Details)]タブには、2 つの重複排除率が表示されます。最初の重複排除率は常にクライアントデータに対応しています。2 つ目の重複排除率はメタデータ (ディスクイメージヘッダーと[True Image Restore]情報 (該当する場合)) に対応しています。その情報は常にサーバーで重複排除されます。通常、その情報の重複排除率はゼロまたは非常に低いです。

また、クライアント側の重複排除の場合、先頭の Info 行に dedupe と compression の各値が個別に表示されます。

次のジョブの詳細例の引用は 2 つの率を示します。1/8/2013 11:58:09 PM のエントリはクライアントデータに対応しています。1/8/2013 11:58:19 PM のエントリはメタデータに対応しています。

```
1/8/2013 11:54:21 PM - Info MSDP_Server.example.com(pid=2220)
  Using OpenStorage client direct to backup from client
  Client_B.example.com to MSDP_Server.example.com
1/8/2013 11:58:09 PM - Info MSDP_Server.example.com(pid=2220)
  StorageServer=PureDisk:MSDP_Server.example.com; Report=PDDO
  Stats for (MSDP_Server.example.com: scanned: 110028 KB,
CR sent: 16654 KB, CR sent over FC: 0 KB, dedup: 84.9%,
cache disabled, where dedup space saving:3.8%,
compression space saving:81.1%
1/8/2013 11:58:09 PM - Info MSDP_Server.example.com(pid=2220)
  Using the media server to write NBU data for backup
  Client_B_1254987197.example.com to MSDP_Server.example.com
1/8/2013 11:58:19 PM - Info MSDP_Server.example.com(pid=2220)
  StorageServer=PureDisk:MSDP_Server.example.com; Report=PDDO
  Stats for (MSDP_Server.example.com: scanned: 17161 KB,
CR sent: 17170 KB, dedup: 0.0%, cache hits: 0 (0.0%)
```

フィールドの説明

表 8-1 に、重複排除のアクティビティフィールドを示します。

表 8-1 MSDP のアクティビティフィールドの説明

フィールド	説明
重複排除領域の節約	データ重複排除によって節約された領域の割合 (データは再度書き込まれません)。
圧縮領域の節約	データをストレージに書き込む前に重複排除エンジンが一部のデータを圧縮したために節約された領域の割合。
cache hits	ローカルの指紋キャッシュで表されるバックアップのデータセグメントの割合。重複排除プラグインは、セグメントについてデータベースを問い合わせる必要がありませんでした。 pd.conf ファイルの FP_CACHE_LOCAL パラメータがストレージで 0 に設定されている場合は、cache hits の出力はストレージサーバーで動作するジョブでは行われません。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

フィールド	説明
CR sent	重複排除プラグインからデータを保存するコンポーネントに送られるデータの量。NetBackup で、NetBackup 重複排除エンジンはデータを保存します。 ストレージサーバーがデータを重複排除する場合、データはネットワーク経由で移動しません。重複排除データは、重複排除プラグインが次のとおりストレージサーバー以外のコンピュータで動作するとき、ネットワーク経由で移動します。 ■ 自身のデータを重複排除する NetBackup クライアント (クライアント側の重複排除)。 ■ データを重複排除する指紋メディアサーバー。指紋サーバーの重複排除プラグインはストレージサーバーにデータを送り、ストレージサーバーはメディアサーバー重複排除プールにそのデータを書き込みます。
CR sent over FC	重複排除プラグインからファイバーチャネルを介して、データを保存するコンポーネントに送られるデータの量。NetBackup で、NetBackup 重複排除エンジンはデータを保存します。
dedup	すでに保存されたデータの割合。このデータが再度保存されることはありません。
multi-threaded stream used	重複排除マルチスレッドエージェントがバックアップを処理したことを示します。 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。
PDDO の統計	次の宛先ストレージ用のジョブ詳細であることを示します: ■ メディアサーバー重複排除プール
リベース	バックアップ中にリベース (デフラグ) されたセグメントの割合。このようなセグメントのデータ局所性は低いです。 NetBackup は、バックアップのリベースの完了後にのみバックアップジョブの完了を報告します。 p.525 の「MSDP ストレージのリベースについて」を参照してください。
scanned	重複排除プラグインがスキャンしたデータの量。
Using OpenStorage client direct to restore...	復元がクライアント主導データパスを経由し、データ処理に NetBackup メディアサーバーのコンポーネントを使用しないことを示します。
encrypted	重複排除プールに書き込まれる新しい転送されたデータが暗号化されているかどうかを示します。

重複排除と関連していないジョブ詳細の説明は別のトピックにあります。

MSDP ストレージの容量と使用状況のレポートについて

次に示すように、複数の要因が、予測される NetBackup 重複排除の容量と使用状況の結果に影響します。

- バックアップの期限が切れても、利用可能なサイズと使われたサイズが変わらない場合があります。期限切れのバックアップに一意のデータセグメントがないことがあります。したがって、セグメントは他のバックアップでは有効なままになります。

- NetBackup Deduplication Manager のクリーンアップはまだ実行されていない可能性があります。Deduplication Manager はクリーンアップを 1 日に 2 回実行します。クリーンアップが実行されるまで、削除されたイメージのフラグメントはディスクにそのまま残ります。

ストレージ容量の使用状況を調べるためにオペレーティングシステムツールを使う場合は、次のように結果が NetBackup によって報告された使用状況と異なることがあります。

- NetBackup の使用状況データには、オペレーティングシステムのツールには含まれない予約済み領域が含まれています。
- 他のアプリケーションでストレージが使用される場合、NetBackup は使用状況を正確には報告できません。NetBackup ではストレージの排他的な使用が要求されます。

表 8-2 に、容量と使用状況を監視するためのオプションを示します。

表 8-2　　容量と使用状況のレポート

オプション	説明
[ストレージサーバーの変更 (Change Storage Server)]ダイアログボックス	[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)]タブには、ストレージの容量と使用状況が表示されます。また、グローバルな重複排除率も表示されます。 このダイアログボックスは NetBackup Web UI で利用可能な最新の容量の使用状況を表示します。 別のトピックではダイアログボックスの例を参照できます。 p.481 の「MSDP 重複排除率と圧縮率の監視」を参照してください。
[ディスクプール (Disk Pools)]ウィンドウ	NetBackup Web UI の[ディスクプール (Disk Pools)]ウィンドウには、NetBackup がディスクプールをポーリングしたときに保存された値が表示されます。NetBackup は 5 分ごとにポーリングします。したがって、値は[ストレージサーバーの変更 (Change Storage Server)]ダイアログボックスに表示される値よりも古いことがあります。 ウィンドウを表示するには、[ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ディスクプール (Disk pools)]の順に選択します。
`crcontrol` コマンド	`crcontrol` コマンドは、重複排除コンテナファイル内のストレージ容量および使用状況を表示します。 p.487 の「MSDP コンテナファイルについて」を参照してください。 p.488 の「MSDP コンテナファイル内のストレージ使用状況の表示」を参照してください。

オプション	説明
[ディスクプールの状態 (Disk Pool Status)]レポート	[ディスクプールの状態 (Disk Pool Status)]レポートはディスクプールの状態と使用状況情報を表示します。
[ディスクのログ (Disk Logs)]レポート	[ディスクのログ (Disk Logs)]レポートはイベントとメッセージ情報を表示します。容量を監視するのに有用なイベントはイベント 1044 です。次は[ディスクのログ (Disk Logs)]レポートのイベントの説明です。 `The usage of one or more system resources has exceeded a warning level.` デフォルトでは、このメッセージのしきい値 (高水準点) は容量の 98% です。これ以上のデータは保存できません。 p.741 の「MSDP イベントのコードとメッセージ」を参照してください。
`nbdevquery` コマンド	`nbdevquery` コマンドはディスクボリュームの状態とそのプロパティおよび属性を表示します。また容量、使用状況および使用済みの割合も表示します。 p.513 の「MSDP ディスクボリュームの状態の判断」を参照してください。

MSDP コンテナファイルについて

重複排除ストレージの実装では、バックアップデータを保持するためにコンテナファイルを割り当てます。削除されたセグメントはコンテナファイルに空き容量を残すことができますが、コンテナファイルサイズは変更されません。バックアップイメージが期限切れになり、NetBackup 重複排除マネージャがクリーンアップを実行するときにセグメントがコンテナから削除されます。

NetBackup Deduplication Manager は 20 秒毎にストレージ領域のチェックを行います。その後、定期的にコンテナファイル内の空き領域を圧縮します。したがって、コンテナ内の領域は解放されてもすぐには利用できません。さまざまな内部パラメータによって、コンテナファイルを圧縮するかどうかが制御されます。領域がコンテナファイル内で利用可能な場合も、ファイルは圧縮に適していない場合があります。

p.485 の「MSDP ストレージの容量と使用状況のレポートについて」を参照してください。

p.488 の「MSDP コンテナファイル内のストレージ使用状況の表示」を参照してください。

p.739 の「MSDP ストレージの空きのない状態」を参照してください。

MSDP コンテナファイル内のストレージ使用状況の表示

NetBackup crcontrol コマンドは、コンテナ内のストレージの使用状況をレポートします。

MSDP コンテナファイル内のストレージ使用状況を表示する方法

- 重複排除ストレージサーバーで crcontrol コマンドと --dsstat オプションを使います。コマンドオプションのヘルプ情報については、--help オプションを使用します。

  次に示すのはコマンドの使用法の例です。

  - UNIX および Linux: /usr/openv/pdde/pdcr/bin/crcontrol --dsstat
  - Windows の場合: *install_path*¥¥Veritas¥¥pdde¥¥Crcontrol.exe --dsstat

  次に、この出力の例を示します。

```
************ Data Store statistics ************
Data storage   Raw        Size      Used     Avail    Use%  Free%

               199.95GiB  63.70GiB  1.23GiB  62.48GiB  2%   98.1%

Number of containers                 : 1
Average container size               : 1049 bytes (0.00MiB)
Space allocated for containers       : 1049 bytes (1.02KiB)
Reserved space                       : 136.25GiB (68.1%)
Reserved space for cloud cache       : 14.00GiB (22.0%)
Reserved space for vpfs cloud cache  : 128.00GiB (64.0%)
```

  メディアサーバー重複排除プールをホストするシステムの場合、次の crcontrol コマンドを使用して、各パーティションに関する情報を表示できます。

```
/usr/openv/pdde/pdcr/bin/crcontrol --dsstat 3
```

  コマンド出力から、次のことを判断できます。

  Raw　ストレージの未加工のサイズ。

  Size　NetBackup で利用可能なストレージのサイズ: ストレージの Raw サイズからファイルシステムの Reserved space を引きます。

  ファイルシステムにルート予約済み領域の概念 (EXT3 または VxFS など) がある場合、その領域はストレージのために使用できません。crcontrol コマンドは利用可能な容量に予約領域を含めません。一部のオペレーティングシステムのツールでは、crcontrol コマンドとは異なり、ルート予約済み領域を利用可能な領域として報告します。

Used	ファイルシステムに保存される複排除されたデータの量。NetBackup はオペレーティングシステムからファイルシステムの使用済み領域を取得します。
Avail	Size から Used 領域を引きます。
Use%	Used 領域を Size で割ります。

p.485 の「MSDP ストレージの容量と使用状況のレポートについて」を参照してください。

p.487 の「MSDP コンテナファイルについて」を参照してください。

p.517 の「MSDP トランザクションキューの手動処理」を参照してください。

p.739 の「MSDP ストレージの空きのない状態」を参照してください。

MSDP プロセスの監視について

次の表は NetBackup によって報告される重複排除のプロセスを示します。

p.549 の「MSDP サーバーコンポーネント」を参照してください。

表 8-3 MSDP の主要なプロセスを監視する場所

対象	監視する場所
NetBackup Deduplication Engine	NetBackup Web UI で、NetBackup 重複排除エンジンが[アクティビティモニター (Activity Monitor)]の[デーモン (Daemons)]タブで spoold として表示されます。 NetBackup の bpps コマンドは spoold プロセスも示します。
NetBackup 重複排除マネージャ	NetBackup Web UI で、NetBackup 重複排除マネージャ[アクティビティモニター (Activity Monitor)]の[デーモン (Daemons)]タブで spad として表示されます。 NetBackup の bpps コマンドは spad プロセスも示します。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

p.51 の「MSDP 負荷分散サーバーを徐々に導入する」を参照してください。

自動イメージレプリケーションジョブに関するレポート

アクティビティモニターは、ターゲットのプライマリサーバードメインにレプリケートする構成の[レプリケーション (Replication)]ジョブと[インポート (Import)]ジョブの両方を表示します。

表 8-4 アクティビティモニターに表示される自動イメージレプリケーションジョブ

ジョブ形式	説明
レプリケーション (Replication)	ターゲットプライマリへのバックアップイメージをレプリケートするジョブは、[レプリケーション (Replication)] ジョブとしてアクティビティモニターに表示されます。[ターゲットマスター (Target Master)]ラベルは、この形式のジョブの[ストレージユニット (Storage Unit)]列に表示されます。 他の[レプリケーション (Replication)]ジョブと同様に、ターゲットプライマリにイメージをレプリケートするジョブは 1 つのインスタンス内の複数のバックアップイメージで実行できます。 このジョブの詳しい状態には、レプリケートされたバックアップ ID リストが含まれています。
インポート (Import)	ターゲットプライマリドメインにバックアップコピーをインポートするジョブは、[インポート (Import)]ジョブとしてアクティビティモニターに表示されます。[インポート (Import)]ジョブは、1 つのインスタンスの複数コピーをインポートできます。この[インポート (Import)]ジョブの状態の詳細には、処理されたバックアップ ID のリストと失敗したバックアップ ID のリストが含まれます。 レプリケーションが成功しても、ターゲットプライマリにイメージがインポートされたかどうかはわかりません。 データの分類が両方のドメインで異なる場合、[インポート (Import)]ジョブは失敗し、NetBackup はイメージを再びインポートしていません。 [インポート (Import)]ジョブが状態 191 で失敗し、ターゲットのプライマリサーバーで実行された時点で[問題 (Problems)]レポートに表示されます。 イメージは[イメージクリーンアップ (Image Cleanup)]ジョブの間に期限切れになり、削除されます。レプリケート元のドメイン (ドメイン 1) は失敗したインポートを追跡しません。

イメージの暗号化状態の確認

`msdpimgutil encryptionreport` コマンドラインユーティリティを使用して、ストレージサーバーの MSDP プールの暗号化の状態またはイメージの暗号化の状態を確認できます。

このコマンドラインユーティリティでは、次の処理が実行されます。

- MSDP プールの暗号化の状態を報告します。
  すべての LSU のデータ暗号化設定と KMS 暗号化設定が一覧表示されます。
- 指定したイメージのイメージデータの暗号化状態を報告します。
- 指定したイメージのイメージ KMS 暗号化状態を報告します。
- 指定した暗号化イメージに使用される KMS キー ID を提供します。
- 暗号化されていないデータコンテナ ID を提供します。
- 暗号化が無効になっている場合は、暗号化保護に関するガイダンスが提供されます。

`msdpimgutil encryptionreport` コマンドラインユーティリティは次の場所にあります。

- UNIX の場合: `/usr/openv/pdde/pdcr/bin/msdpimgutil`
- Windows の場合: `install_path¥Veritas¥pdde¥msdpimgutil.exe`

イメージの暗号化状態を確認するには

1 次のコマンドを実行して、MSDP プールの暗号化の状態を確認します。すべての LSU のデータ暗号化設定と KMS 暗号化設定が一覧表示されます。

```
msdpimgutil encryptionreport --systemcheck
```

次に例を示します。

```
msdpimgutil encryptionreport --systemcheck
==== Dedup system encryption check ====
Found Local LSU
      LSU's Data encryption setting is enabled.
      LSU's KMS encryption setting is enabled.

Found Cloud LSU aws_vraxmyan9148
      LSU's Data encryption setting is disabled.
      LSU's KMS encryption setting is disabled.

Found Cloud LSU aws2_vraxmyan9148
      LSU's Data encryption setting is enabled.
      LSU's KMS encryption setting is enabled.

** Follow the NetBackup Deduplication Guide to enable Data/KMS
encryption (contentrouter.cfg).

** Encryption Crawler:
   Encryption Crawler is unavailable for WORM Deduplication pools
 or data stored on Cloud Tier.
```

2 MSDP プールのイメージの暗号化設定を確認します。

イメージデータの暗号化状態、イメージ KMS 暗号化状態、KMS キー ID、指定したイメージで使用される暗号化されていないデータコンテナ ID が報告されます。暗号化が無効になっている場合は、暗号化保護に関するガイダンスが提供されます。

```
msdpimgutil encryptionreport --backupid <backup id> --copy <copy
number> [--verbose | -v]
```

--backupid: イメージのバックアップ ID。

--copy: イメージのコピー番号。

--verbose または -v: [詳細 (Verbose)]は、KMS 暗号化イメージの KMS キー ID または暗号化されていないイメージのデータコンテナ ID を出力するために使用されます。

メモ: イメージが多数のデータコンテナを消費する場合、このコマンドの実行時間が長くなることがあります。

次に例を示します。

```
msdpimgutil encryptionreport --backupid backupid --copy 1
--verbose
==== Dedup system encryption check ====
Found Local LSU
      LSU's Data encryption setting is enabled.
      LSU's KMS encryption setting is enabled.

==== Dedup image encryption check ====
Found image (2|/client/policy|backupid_C1) in Local LSU.
      Image Data encryption setting is enabled.
      Image KMS encryption setting is enabled.

      Image data segments are found in 16 data containers, 16
data containers are KMS encrypted.

      The following unique KeyID is needed for image recovery.
      KeyID:
87f49487cd13e9d30c4891e146721354f53f26b82945a8b23eb859a0b8416929
```

9

重複排除の管理

この章では以下の項目について説明しています。

- MSDP クラスタでのマルチストリームバックアップに対する複数 MSDP ノードの使用
- MSDP クラスタでのメディアサーバーと MSDP エンジンの親和性の有効化

MSDP サーバーの管理

重複排除を構成した後、重複排除サーバーを管理する各種作業を実行できます。

p.495 の「MSDP ストレージサーバーの表示」を参照してください。

p.496 の「MSDP ストレージサーバーの状態の判断」を参照してください。

p.496 の「MSDP ストレージサーバーの属性の表示」を参照してください。

p.496 の「MSDP ストレージサーバーの属性の設定」を参照してください。

p.497 の「MSDP ストレージサーバーのプロパティの変更」を参照してください。

p.498 の「MSDP ストレージサーバーの属性の消去」を参照してください。

p.498 の「MSDP ストレージサーバー名またはストレージパスの変更について」を参照してください。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

p.500 の「MSDP 負荷分散サーバーの削除」を参照してください。

p.501 の「MSDP ストレージサーバーの削除」を参照してください。

p.502 の「MSDP ストレージサーバーの構成を削除する」を参照してください。

MSDP ストレージサーバーの表示

NetBackup で構成されている重複排除ストレージサーバーのリストを表示できます。

MSDP ストレージサーバーを表示する方法

1. Web UI を開きます。
2. 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。
3. [ストレージサーバー (Storage servers)]タブをクリックします。

   このリストには、構成済みのすべてのストレージサーバーが表示されます。重複排除ストレージサーバーでは、[ストレージサーバー形式 (Storage server type)]列に PureDisk が表示されます。

MSDP ストレージサーバーの状態の判断

重複排除ストレージサーバーの状態を判断するには、NetBackup の nbdevquery コマンドを使います。状態は、起動または停止です。

MSDP ストレージサーバーの状態を判断する方法

- NetBackup プライマリサーバーまたは重複排除ストレージサーバーで、次のコマンドを実行します。

  UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbdevquery -liststs -storage_server server_name -stype PureDisk -U`

  Windows の場合: `install_path¥NetBackup¥bin¥admincmd¥nbdevquery -liststs -storage_server server_name -stype PureDisk -U`

  次に出力例を示します。

```
Storage Server      : bit.example.com
Storage Server Type : PureDisk
Storage Type        : Formatted Disk, Network Attached
State               : UP
```

  この出力例は短縮されています。実際の出力にはこれより多くのフラグが表示されることがあります。

MSDP ストレージサーバーの属性の表示

重複排除ストレージサーバーの属性を表示するには、NetBackup の nbdevquery コマンドを使います。

nbdevquery コマンドで使う nbdevquery は、ストレージサーバーの構成名に一致している必要があります。ストレージサーバー名がその完全修飾ドメイン名の場合、その名前を *server_name* に使う必要があります。

MSDP ストレージサーバーの属性を表示する方法

-

MSDP ストレージサーバーの属性の設定

新しい機能を有効にするためにストレージサーバーの属性を設定する必要があることがあります。

ストレージサーバーの属性を設定する場合、既存の重複排除プールの同じ属性を設定する必要があることがあります。要件については、新しい機能の概要または構成手順で説明します。

p.507 の「メディアサーバー重複排除プールの属性の設定」を参照してください。

MSDP ストレージサーバーの属性を設定する方法

1 次はストレージサーバーの属性を設定するコマンドの構文です。プライマリサーバーまたはストレージサーバーでコマンドを実行します。

```
nbdevconfig -changests -storage_server storage_server -stype
PureDisk -setattribute attribute
```

次に、ドメインに固有の引数を必要とするオプションについて説明します。

`-storage_server` *`storage_server`*	ストレージサーバーの名前。
`-setattribute` *`attribute`*	***attribute*** は、新しい機能を表す引数の名前です。 たとえば、OptimizedImage は、最適化された合成バックアップ方式を環境がサポートするように指定します。

`nbdevconfig` コマンドへのパスは次のとおりです。

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

2 確認するには、ストレージサーバーの属性を表示します。

p.496 の「MSDP ストレージサーバーの属性の表示」を参照してください。

p.42 の「MSDP の最適化された合成バックアップについて」を参照してください。

MSDP ストレージサーバーのプロパティの変更

NetBackup Deduplication Manager の保持期間とログレベルを変更できます。

MSDP ストレージサーバーのプロパティを変更する方法

1 Web UI を開きます。

2 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。

3 [ストレージサーバー (Storage servers)]タブをクリックします。

4 重複排除ストレージサーバーの名前をクリックします。

5 [編集 (Edit)]をクリックし、必要な変更を加えます。

6 [保存 (Save)]をクリックします。

p.25 の「MSDP 重複排除ノードについて」を参照してください。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

p.89 の「MSDP のストレージパスのプロパティ」を参照してください。

p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。

MSDP ストレージサーバーの属性の消去

ストレージサーバーの属性を削除するには、コマンドを使います。nbdevconfig

MSDP ストレージサーバーの属性を消去する方法

- NetBackup プライマリサーバーまたはストレージサーバーで次のコマンドを実行します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -changests
  -storage_server storage_server -stype PureDisk -clearattribute
  attribute
  ```

  ```
  nbdevconfig -changests -storage_server storage_server -stype
  PureDisk -clearattribute attribute
  ```

  `-storage_server storage_server` ストレージサーバーの名前。

  `-setattribute attribute` ***attribute*** は、機能を表す引数の名前です。

  `nbdevconfig` コマンドへのパスは次のとおりです。

  - UNIX の場合: `/usr/openv/netbackup/bin/admincmd`
  - Windows の場合: *install_path*¥NetBackup¥bin¥admincmd

MSDP ストレージサーバー名またはストレージパスの変更について

既存の NetBackup の重複排除環境のストレージサーバーのホスト名とストレージパスを変更できます。

既存の重複排除環境の変更が必要なユースケースの一部を次に示します。

- ホスト名を設定したいとします。たとえば、ホスト A の名前が B に変わり、新しいネットワークカードがプライベートインターフェース C でインストールされました。ホスト名 B またはプライベートインターフェース C を使用するには、ストレージサーバーを再構成する必要があります。
  p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。
- ストレージのパスを変更したいとします。そうするには、ストレージサーバーを新しいパスで再構成する必要があります。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

- ディザスタリカバリ用にストレージを再利用する必要があります。ストレージはそのままですが、ストレージサーバーは破壊されました。リカバリするためには、新しいストレージサーバーを構成する必要があります。
  この場合、同じホスト名とストレージパスを使用するか、別のホスト名とストレージパスを使用できます。
  p.541 の「MSDP ストレージサーバーのエラーからのリカバリ」を参照してください。

MSDP ストレージサーバーの名前またはストレージパスの変更

NetBackup Deduplication 構成には、EMM データベース内の重複排除ストレージのレコードおよび物理的に存在するディスク上のストレージ (データを含むストレージディレクトリ) という 2 つの要素があります。

警告: 有効なバックアップイメージを削除すると、データが損失する可能性があります。

p.498 の「MSDP ストレージサーバー名またはストレージパスの変更について」を参照してください。

表 9-1　　ストレージサーバーの名前またはストレージパスの変更

手順	作業	手順詳細
手順 1	重複排除アクティビティが実行されていないことを確認します	重複排除ストレージを使うすべてのバックアップポリシーを無効にします。 『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 2	バックアップイメージを期限切れにします。	重複排除ディスクストレージに存在するすべてのバックアップイメージを期限切れにします。 **警告:** イメージを削除しないでください。後でイメージを NetBackup にインポートして戻します。 `bpexpdate` コマンドを使ってバックアップイメージを期限切れにする場合は、`-nodelete` パラメータを使います。 『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 3	ディスクプールを使用するストレージユニットを削除します	『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 4	ディスクプールを削除します	p.514 の「メディアサーバー重複排除プールの削除」を参照してください。
手順 5	重複排除ストレージサーバーを削除します	p.501 の「MSDP ストレージサーバーの削除」を参照してください。

手順	作業	手順詳細
手順 6	設定を削除します	重複排除の構成を削除します。 p.502 の「MSDP ストレージサーバーの構成を削除する」を参照してください。
手順 7	重複排除ホストの構成ファイルを削除します	各負荷分散サーバーには、重複排除ホストの構成ファイルが含まれます。負荷分散サーバーを使う場合は、サーバーから重複排除ホストの構成ファイルを削除します。 p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。
手順 8	ID ファイルとファイルシステムテーブルファイルを削除します。	オペレーティングシステムにより、次のファイルを MSDP ストレージサーバーから削除します。 UNIX の場合: */storage_path*/data/.identity */storage_path*/etc/puredisk/fstab.cfg Windows の場合: *storage_path*¥data¥.identity *storage_path*¥etc¥puredisk¥fstab.cfg
手順 9	ストレージサーバーの名前または格納場所を変更します	コンピュータまたはストレージベンダーのマニュアルを参照してください。 p.49 の「完全修飾ドメイン名を使用する」を参照してください。 p.89 の「MSDP のストレージパスのプロパティ」を参照してください。
手順 10	ストレージサーバーを再構成します	重複排除を構成するときに、新しい名前でホストを選択し、(パスを変更した場合は) 新しいストレージのパスを入力します。新しいネットワークインターフェースを使うこともできます。 p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。
手順 11	バックアップイメージをインポートします	『NetBackup 管理者ガイド Vol. 1』を参照してください。

MSDP 負荷分散サーバーの削除

重複排除ノードから負荷分散サーバーを削除できます。メディアサーバーではクライアントデータが重複排除されなくなりました。

p.33 の「MSDP ストレージサーバーについて」を参照してください。

負荷分散サーバーを削除した後、NetBackup Enterprise Media Manager サービスを再起動します。NetBackup Disk Polling Service は、削除されたサーバーを使用して

ディスク状態を問い合わせようとすることがあります。サーバーはすでに負荷分散サーバーではないため、ディスクストレージに問い合わせることができません。その結果、NetBackup はディスクボリュームに[停止 (DOWN)]とマーク付けすることがあります。EMM サービスを再起動すると、ディスクストレージの監視には異なる重複排除サーバーが選択されます。

ホストに障害が発生して利用不能になった場合は、メニューモードで tpconfig デバイス構成ユーティリティを使用して、サーバーを削除できます。ただし、UNIX または Linux の NetBackup サーバーで tpconfig ユーティリティを実行する必要があります。

手順については、『NetBackup 管理者ガイド Vol. 2』を参照してください。

メディアサーバーを MSDP ノードから削除する方法

1. Web UI を開きます。
2. 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。
3. [ストレージサーバー (Storage servers)]タブをクリックします。
4. [メディアサーバー (Media servers)]列を確認します。1 つ以上のメディアサーバーを手動で選択した各ストレージユニットに対して、[自動的に選択することを NetBackup に許可する (Allow NetBackup to automatically select)]オプション (任意) を選択します。
5. ストレージサーバー名をクリックします。
6. [メディアサーバー (Media servers)]リストで、メディアサーバーを見つけて[削除 (Delete)]をクリックし、MSDP ノードからメディアサーバーを削除します。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

p.50 の「MSDP の調整について」を参照してください。

p.51 の「MSDP 負荷分散サーバーを徐々に導入する」を参照してください。

MSDP ストレージサーバーの削除

重複排除ストレージサーバーを削除すると、NetBackup によってストレージサーバーであるホストが削除され、そのメディアサーバーで重複排除ストレージサーバー機能が無効になります。

NetBackup は構成からメディアサーバーを削除しません。メディアサーバーを削除するには、NetBackup の nbemmcmd コマンドを使用します。

重複排除ストレージサーバーを削除しても、物理ディスク上のストレージの内容は変更されません。不注意なデータ損失を防ぐために、ストレージサーバーを削除しても、NetBackup はストレージを自動的には削除しません。

重複排除ストレージサーバーが管理しているディスクボリュームからディスクプールが構成されている場合、その重複排除ストレージサーバーは削除できません。

警告: 期限が切れていない NetBackup イメージがストレージに含まれている重複排除ストレージサーバーは削除しないでください。削除すると、データが消失する場合があります。

MSDP ストレージサーバーを削除する方法

1. Web UI を開きます。
2. 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。
3. [ストレージサーバー (Storage servers)]タブをクリックします。
4. ストレージサーバーを選択し、[削除 (Delete)]をクリックします。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

MSDP ストレージサーバーの構成を削除する

この手順は、重複排除ストレージサーバーの構成を削除するのに使います。この手順で使われるスクリプトはアクティブな構成を削除し、構成ファイルをインストール時の事前設定された状態に戻します。

この手順は、プロセストピックから指示された場合にのみ使用してください。プロセストピックは一連の個別手順から構成された高レベルのユーザータスクです。

p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。

p.547 の「MSDP の無効化」を参照してください。

MSDP ストレージサーバーの構成を削除する方法

1 NetBackup Web UIを使用して、NetBackup Deduplication Engine (spoold) および NetBackup Deduplication Manager (spad) を停止します。

2 ストレージサーバーで、次のいずれかのスクリプト (オペレーティングシステムによって異なる) を実行します。

UNIX の場合:
/usr/openv/pdde/pdconfigure/scripts/installers/PDDE_deleteConfig.sh

Windows の場合:install_path¥Program Files¥Veritas¥pdde¥PDDE_deleteConfig.bat

コマンド出力には、次の内容が含まれます。

```
**** Starting PDDE_deleteConfig.sh ***
You need to stop the spad and spoold daemons to proceed
This script will delete the PDDE configuration on this system
Would you want to continue? [ y | n ]
```

3 「y」と入力し、次に Enter キーを押します。

NetBackup Deduplication Engine クレデンシャルの管理

NetBackup で既存のクレデンシャルを管理できます。

p.503 の「重複排除クレデンシャルがあるメディアサーバーの確認」を参照してください。

p.504 の「NetBackup Deduplication Engine クレデンシャルの追加」を参照してください。

p.504 の「NetBackup Deduplication Engine クレデンシャルの変更」を参照してください。

p.504 の「負荷分散サーバーからのクレデンシャルの削除」を参照してください。

重複排除クレデンシャルがあるメディアサーバーの確認

どのメディアサーバーに NetBackup Deduplication Engine 用のクレデンシャルが構成されているかを確認できます。クレデンシャルがあるサーバーは負荷分散サーバーです。

NetBackup Deduplication Engine のクレデンシャルがあるかどうかを確認する方法

1 Web UI を開きます。

2 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。

3 ［ストレージサーバー (Storage servers)］タブをクリックします。

4 ストレージサーバー名をクリックします。

5 ［メディアサーバー (Media servers)］リストを見つけます。

NetBackup Deduplication Engine クレデンシャルの追加

既存のストレージサーバーか負荷分散サーバーに NetBackup Deduplication Engine のクレデンシャルを追加することが必要になる場合があります。たとえば、ディザスタリカバリではクレデンシャルの追加が必要になる場合があります。

ユーザーの環境ですでに使用しているのと同じクレデンシャルを追加します。

構成に負荷分散サーバーを追加する別の手順が存在します。

p.170 の「MSDP 負荷分散サーバーの追加」を参照してください。

tpconfig コマンドを使用して NetBackup Deduplication Engine のクレデンシャルを追加する方法

◆ クレデンシャルを追加したいホストで次のコマンドを実行します。

Windows の場合:

```
install_path¥Veritas¥NetBackup¥Volmgr¥bin¥tpconfig -add
-storage_server sshostname -stype PureDisk -sts_user_id UserID
-password PassWord
```

UNIX または Linux の場合:

```
/usr/openv/volmgr/bin/tpconfig -add -storage_server sshostname
-stype PureDisk -sts_user_id UserID -password PassWord
```

sshostname には、ストレージサーバーの名前を使用します。

NetBackup Deduplication Engine クレデンシャルの変更

NetBackup Deduplication Engine のクレデンシャルは、入力した後に変更できません。クレデンシャルを変更する必要がある場合は、Cohesity のサポート担当者にお問い合わせください。

p.39 の「NetBackup Deduplication Engine のクレデンシャルについて」を参照してください。

負荷分散サーバーからのクレデンシャルの削除

負荷分散サーバーから NetBackup Deduplication Engine のクレデンシャルを削除することが必要になる場合があります。たとえば、ディザスタリカバリでは負荷分散サーバーのクレデンシャルの削除が必要になる場合があります。

重複排除ノードから負荷分散サーバーを削除する別の手順が存在します。

p.500 の「MSDP 負荷分散サーバーの削除」を参照してください。

負荷分散サーバーからクレデンシャルを削除する方法

- 負荷分散サーバーで、次のコマンドを実行します。

  Windows の場合:

  ```
  install_path¥Veritas¥NetBackup¥Volmgr¥bin¥tpconfig -delete
  -storage_server sshostname -stype PureDisk -sts_user_id UserID
  ```

  UNIX または Linux の場合:

  ```
  /usr/openv/volmgr/bin/tpconfig -delete -storage_server sshostname
  -stype PureDisk -sts_user_id UserID
  ```

  sshostname には、ストレージサーバーの名前を使用します。

メディアサーバー重複排除プールの管理

NetBackup 重複排除を構成した後、重複排除ディスクプールを管理する各種作業を実行できます。

p.505 の「メディアサーバー重複排除プールの表示」を参照してください。
p.508 の「メディアサーバー重複排除プールのプロパティの変更」を参照してください。
p.506 の「メディアサーバー重複排除プールの状態の判断」を参照してください。
p.513 の「MSDP ディスクボリュームの状態の判断」を参照してください。
p.514 の「MSDP ディスクボリュームの状態の変更」を参照してください。
p.506 の「メディアサーバー重複排除プールの属性の表示」を参照してください。
p.507 の「メディアサーバー重複排除プールの属性の設定」を参照してください。
p.512 の「メディアサーバー重複排除プールの属性の消去」を参照してください。
p.528 の「MSDP ストレージパーティションのサイズ調整」を参照してください。
p.514 の「メディアサーバー重複排除プールの削除」を参照してください。

メディアサーバー重複排除プールの表示

構成されたディスクプールを表示できます。

ディスクプールを表示する方法

1. NetBackup Web UI を開きます。
2. 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。
3. [ディスクプール (Disk pools)]タブをクリックします。

メディアサーバー重複排除プールの状態の判断

ディスクプールの状態は、起動または停止です。

ディスクプールの状態を判断する方法

1. NetBackup Web UI を開きます。
2. 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。
3. [ディスクプール (Disk pools)]タブをクリックします。
4. [状態 (Status)]列を確認します。

メディアサーバー重複排除プールの属性の表示

重複排除プールの属性を表示するには、NetBackup のコマンドを使います。nbdevquery

MSDP プールの属性を表示する方法

- 次は重複排除プールの属性を表示するコマンドの構文です。NetBackup プライマリサーバーまたは重複排除ストレージサーバーで、このコマンドを実行します。

  UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdp -dp pool_name -stype PureDisk -U`

  Windows の場合: `install_path¥NetBackup¥bin¥admincmd¥nbdevquery -listdp -dp pool_name -stype PureDisk -U`

  次に出力例を示します。

```
Disk Pool Name   : MediaServerDeduplicationPool
Disk Pool Id     : MediaServerDeduplicationPool
Disk Type        : PureDisk
Status           : UP
Flag             : OpenStorage
Flag             : AdminUp
Flag             : InternalUp
Flag             : LifeCycle
Flag             : CapacityMgmt
Flag             : OptimizedImage
Raw Size (GB)    : 235.76
Usable Size (GB) : 235.76
Num Volumes      : 1
High Watermark   : 98
Low Watermark    : 80
Max IO Streams   : -1
Storage Server   : DedupeServer.example.com (UP)
```

  この出力例は短縮されています。実際の出力にはこれより多くのフラグが表示されることがあります。

メディアサーバー重複排除プールの属性の設定

既存のメディアサーバーの重複排除プールの属性を設定する場合があります。たとえば、ストレージサーバーの属性を設定する場合、既存の重複排除ディスクプールの同じ属性を設定する必要があることがあります。

MSDP ディスクプールの属性を設定する方法

1. 次は重複排除プールの属性を設定するコマンドの構文です。プライマリサーバーまたはストレージサーバーでコマンドを実行します。

   `nbdevconfig -changedp -dp pool_name -stype PureDisk -setattribute attribute`

次に、ドメインに固有の引数を必要とするオプションについて説明します。

`-changedp` *`pool_name`*	ディスクプールの名前。
`-setattribute` *`attribute`*	*attribute* は、新しい機能を表す引数の名前です。 たとえば、OptimizedImage は、最適化された合成バックアップ方式を環境がサポートするように指定します。

`nbdevconfig` コマンドへのパスは次のとおりです。

- UNIX の場合: `/usr/openv/netbackup/bin/admincmd`
- Windows の場合: *`install_path`*`¥NetBackup¥bin¥admincmd`

2 確認するには、ディスクプールの属性を表示します。

p.506 の「メディアサーバー重複排除プールの属性の表示」を参照してください。

p.92 の「NetBackup の重複排除用ディスクプールについて」を参照してください。

メディアサーバー重複排除プールのプロパティの変更

重複排除ディスクプールのプロパティを変更できます。

ディスクプール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[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。

3 [ディスクプール (Disk pools)]タブをクリックします。

4 ディスクプールの名前をクリックします。

5 [詳細 (Details)]タブをクリックします。

6 [編集 (Edit)]をクリックし、必要な変更を加えます。

7 [保存 (Save)]をクリックします。

自動イメージレプリケーションのボリューム変更を解決する方法

[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスを開くと、NetBackup はディスクプールのプロパティをカタログからロードします。[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスのNetBackup[更新 (Refresh)]ボタンをクリックするか、またはストレージサーバーのための新しいディスクプールを構成すると、はストレージサーバーに変更を問い合わせます。

ボリュームのトポロジーが変化したときに次の処置をとることを推奨します。

- ストレージ管理者と変更について話し合います。必要に応じてディスクプールを変更して NetBackup がディスクプールを使い続けることができるようにするために、変更を把握する必要があります。
- NetBackup に変更が計画されていなかった場合、NetBackup が正しく機能するように変更を元に戻すようにストレージ管理者に依頼します。

NetBackup は次のボリュームプロパティへの変更を処理できます。

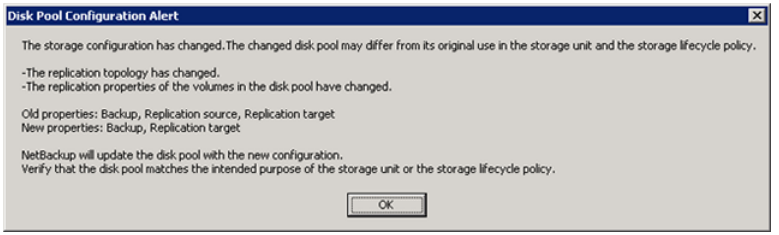
- レプリケーションソース (Replication Source)
- レプリケーションターゲット (Replication target)
- なし

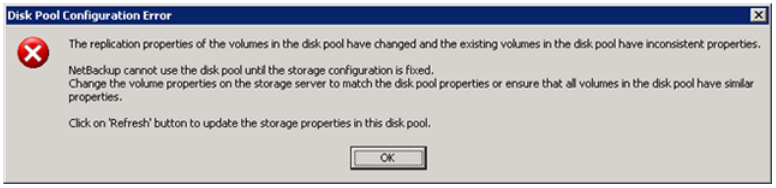
これらのボリュームプロパティが変化した場合、NetBackup はその変化と一致するようにディスクプールを更新できます。NetBackup はそのディスクプールを使い続けることができますが、ディスクプールはストレージユニットまたはストレージライフサイクルの目的に合わなくなっている可能性があります。

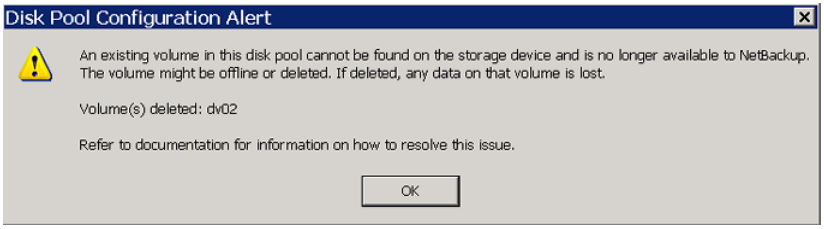
次の表で、考えられる結果と、それらを解決する方法を説明します。

表 9-2　　更新の結果

結果	説明
変更は検出されません。	変更は必要ありません。
NetBackup はディスクプールに追加できる新しいボリュームを検出します。	新しいボリュームは[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスに表示されます。ダイアログボックスのテキストは、ディスクプールに新しいボリュームを追加できることを示す内容に変わります。

結果	説明
すべてのボリュームのレプリケーションプロパティは変わりましたが、一貫性はまだ維持されています。	[ディスクプール構成の警告 (Disk Pool Configuration Alert)]ポップアップには、ディスクプール内のすべてのボリュームのプロパティが変わったが、プロパティがすべて同じ (同質) であることを知らせるメッセージが表示されます。  [ディスクプールの変更 (Change Disk Pool)]ダイアログボックスのディスクプールプロパティが新しいボリュームプロパティと一致するように更新された後は、警告ダイアログボックスで[OK]をクリックする必要があります。 新しいプロパティと一致する新しいプロパティが利用可能になると、NetBackup は[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスにそれらのプロパティを表示します。ディスクプールにそれらの新しいボリュームを追加できます。 [ディスクプールの変更 (Change Disk Pool)]ダイアログボックスでは、次の 2 つの選択肢から 1 つを選択してください。 ■ OK。ディスクプールの変更を受け入れるには、[OK]を[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスでクリックします。NetBackup はディスクプールの新しいプロパティを保存します。 NetBackup はディスクプールを使うことができますが、このディスクプールはストレージユニットまたはストレージライフサイクルポリシーの意図した目的と合わなくなっている可能性があります。レプリケーション操作で正しいソースとターゲットのディスクプール、ストレージユニット、ストレージユニットグループが使われるようにするために、ストレージライフサイクルポリシー定義を変更してください。あるいは、管理者と協力してボリュームプロパティを元の値に戻します。 ■ キャンセル (Cancel): ディスクプールの変更を破棄するには、[キャンセル (Cancel)]を[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスでクリックします。NetBackup は新しいディスクプールプロパティを保存しません。NetBackup はディスクプールを使うことができますが、このディスクプールはストレージユニットまたはストレージライフサイクルポリシーの意図した目的と合わなくなっている可能性があります。

結果	説明
ボリュームのレプリケーションプロパティが変更され、今は一貫性が失われています。	[ディスクプール構成エラー (Disk Pool Configuration Error)]ポップアップボックスには、ディスクプール内の一部のボリュームのレプリケーションプロパティが変わったことを知らせるメッセージが表示されます。ディスクプールのボリュームのプロパティが同質ではありません。  警告ダイアログボックスの[OK]をクリックする必要があります。 [ディスクプールの変更 (Change Disk Pool)]ダイアログボックスでは、ディスクプールのプロパティは変更されないままで、プロパティを選択することができません (つまり淡色表示されます)。ただし、個々のボリュームのプロパティは更新されます。 ボリュームプロパティが同質ではないので、NetBackup はストレージ構成が修正されるまでディスクプールを使うことができません。 NetBackup はディスクプール内の既存のボリュームが同質ではないので、(新しいボリュームがあったとしても) 新しいボリュームを表示しません。 変更されたボリュームを特定するには、ディスクプールプロパティとボリュームプロパティを比較します。 p.140 の「自動イメージレプリケーションのレプリケーショントポロジーの表示」を参照してください。 ストレージ管理者と協力して、変更点とその変更を行った理由を把握します。レプリケーション関係の再確立は必要な場合と不要な場合があります。関係がエラーで削除された場合、関係の再確立は必要であると考えられます。レプリケーションターゲットデバイスを廃止中または交換中の場合、関係の再確立はおそらく必要ではありません。 ディスクプールは、ディスクプール内の各ボリュームのプロパティが同種になるまで使用できません。 [ディスクプールの変更 (Change Disk Pool)]ダイアログボックスで[OK]または[キャンセル (Cancel)]をクリックすると、[ディスクプールの変更 (Change Disk Pool)]ダイアログボックスが終了します。

結果	説明
NetBackup はディスクプール内にあったボリュームを検出できません。	[ディスクプール構成の警告 (Disk Pool Configuration Alert)]ポップアップボックスには、1 つまたは複数の既存のボリュームがストレージデバイスから削除されたことを知らせるメッセージが表示されます。  NetBackup はディスクプールを使うことができますが、データが失われる可能性があります。 手違いによるデータ損失を避けるために、NetBackup ではディスクプールからボリュームを削除することはできません。 ディスクプールを使い続けるには、次のことを実行してください。 ■ bpimmediaコマンドまたは[ディスク上のイメージ (Images On Disk)]レポートを使用して、特定のボリュームのイメージを表示する。 ■ ボリューム上のイメージを期限切れにする。 ■ nbdevconfig コマンドを使用して、ボリュームを停止状態に設定する。そうすることで、NetBackup では使われません。

メディアサーバー重複排除プールの属性の消去

既存のメディアサーバーの重複排除プールの属性を消去しなければならないことがあります。

[メディアサーバー重複排除プール (Media Server Deduplication Pool)]属性を消去する方法

◆ 次は重複排除プールの属性を消去するコマンドの構文です。プライマリサーバーまたはストレージサーバーでコマンドを実行します。

```
nbdevconfig -changedp -dp pool_name -stype PureDisk
-clearattribute attribute
```

次に、入力を必要とするオプションについて説明します。

`-changedp pool_name` ディスクプールの名前。

`-setattribute attribute` ***attribute*** は、新しい機能を表す引数の名前です。

nbdevconfig コマンドへのパスは次のとおりです。

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

MSDP ディスクボリュームの状態の判断

NetBackup の nbdevquery コマンドを使用して、重複排除ディスクプールのボリュームの状態を判断します。NetBackup は単一ボリュームである PureDiskVolume として MSDP のストレージすべてを開示します。このコマンドは PureDiskVolume のプロパティと属性を示します。

MSDP ディスクボリュームの状態を判断する方法

◆ 次のコマンドを使用してボリュームの状態を表示します。

UNIX の場合: /usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype PureDisk -U -dp *disk_pool_name*

Windows の場合: *install_path*¥NetBackup¥bin¥admincmd¥nbdevquery -listdv -stype PureDisk -U -dp *disk_pool_name*

state には、UP または DOWN のいずれかを指定します。

次に出力例を示します。

```
Disk Pool Name      : MSDP_Disk_Pool
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
Disk Media ID       : @aaaab
Total Capacity (GB) : 49.98
Free Space (GB)     : 43.66
Use%                : 12
Status              : UP
Flag                : ReadOnWrite
Flag                : AdminUp
Flag                : InternalUp
Num Read Mounts     : 0
Num Write Mounts    : 1
Cur Read Streams    : 0
Cur Write Streams   : 0
```

p.514 の「MSDP ディスクボリュームの状態の変更」を参照してください。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.543 の「NetBackup カタログリカバリ後の MSDP ストレージサーバーのリカバリ」を参照してください。

MSDP ディスクボリュームの状態の変更

ディスクボリュームの状態は、[起動 (UP)]または[停止 (DOWN)]です。NetBackup は単一ボリュームである PureDiskVolume として MSDP のストレージすべてを開示します。

状態を[停止 (DOWN)]に変更するには、ボリュームが存在するディスクプールがビジー状態でない必要があります。バックアップジョブがディスクプールに割り当てられている場合、状態の変更は失敗します。バックアップジョブを取り消すか、ジョブが完了するまで待機します。

MSDP ディスクボリュームの状態を変更する方法

- ディスクボリュームの状態を変更します。コマンドの構文は次のとおりです。

  UNIX の場合:`/usr/openv/netbackup/bin/admincmd/nbdevconfig -changestate -stype PureDisk -dp` *`disk_pool_name`* `-dv PureDiskVolume -state` *`state`*

  Windows の場合: *`install_path`*`¥NetBackup¥bin¥admincmd¥nbdevconfig -changestate -stype PureDisk -dp` *`disk_pool_name`* `-dv PureDiskVolume -state` *`state`*

  `-state` には、[起動 (UP)] または [停止 (DOWN)] を指定します。

p.513 の「MSDP ディスクボリュームの状態の判断」を参照してください。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.543 の「NetBackup カタログリカバリ後の MSDP ストレージサーバーのリカバリ」を参照してください。

メディアサーバー重複排除プールの削除

有効な NetBackup バックアップイメージかイメージのフラグメントを含んでいない場合は、ディスクプールを削除できます。その場合は、最初にそれらのイメージまたはフラグメントを期限切れにして削除する必要があります。期限切れのイメージフラグメントがディスクに残っている場合は、それも削除する必要があります。

p.734 の「MSDP ディスクプールを削除できない」を参照してください。

ディスクプールを削除すると、NetBackup によってそのディスクプールが構成から削除されます。

ディスクプールがストレージユニットの宛先ストレージである場合は、最初にストレージユニットを削除する必要があります。

MSDP ディスクプールを削除する方法

1. NetBackup Web UI を開きます。
2. 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。
3. ディスクプールを選択します。
4. [削除 (Delete)]、[はい (Yes)]の順に選択します。

バックアップイメージのディスク容量の消費量の分析

`msdpimgutil spacereport` コマンドを使用して、バックアップイメージが消費するディスク容量を分析します。このユーティリティは、予想外の重複排除率になっているイメージを特定し、重複排除プール領域の使用率が高くなったときにどのイメージを期限切れにするかを適切に判断するのに役立ちます。

`msdpimgutil` ユーティリティは次の場所にあります。

- UNIX の場合: `/usr/openv/pdde/pdcr/bin/msdpimgutil`
- Windows の場合: `install_path¥Veritas¥pdde¥msdpimgutil.exe`

制限事項:

- このコマンドは、ユニバーサル共有のダンプデータの統計をサポートしていません。
- このコマンドを実行してデータサイズを確認するときは、コマンド入力パラメータで指定したバックアップイメージの有効期限を期限切れにしないでください。
- このユーティリティを実行する前に、期限切れのストレージ領域が再利用されていることを確認してください。
- このコマンドは、MSDP-Object-Store ポリシー形式のデータ統計をサポートしていません。

必要なオプションを指定して次のコマンドを実行し、消費されているディスク容量を分析します。

```
msdpimgutil spacereport <[--backup_id_list <backupid list>] [--client
<client name>] [--policy <policy name>] [--startdate <start date>]
[--enddate <end date>]> [--copynumber <copy number>]
```

例:

```
msdpimgutil spacereport --client sadiexxvmxx.xxx.xxx.veritas.com
--policy PCloud --startdate 2023-09-02T01:23:22 --enddate 2023-
12-03T01:23:22 -copynumber 1
```

バックアップイメージのディスク容量の消費量を分析するには

1 指定したバックアップイメージが消費するサイズを取得します。

```
msdpimgutil spacereport --backup_id_list
sadiexxvmxx.xxx.xxx.veritas.com_xxxxx02360
sadiexxvmxx.xxx.xxx.veritas.com_xxxxx02243
```

2 指定したクライアントのすべてのバックアップイメージが消費するサイズを取得します。

```
msdpimgutil spacereport --client sadiexxvmxx.xxx.xxx.veritas.com
```

3 指定したポリシー、またはクライアントとポリシーのすべてのバックアップイメージが消費するサイズを取得します。

```
msdpimgutil spacereport --client sadiexxvmxx.xxx.xxx.veritas.com
--policy dirPlocal2
```

4 指定した開始日から終了日までの、すべてのバックアップイメージによって消費されているサイズを取得します。

```
msdpimgutil spacereport --startdate 2023-09-02T01:23:22 --enddate
2023-12-03T01:23:22
```

バックアップイメージの削除

イメージの削除には時間がかかることがあります。したがって、イメージを手動で削除する場合、Cohesity では次の方法をお勧めします。

p.527 の「MSDP のデータ削除処理について」を参照してください。

バックアップイメージを手動で削除する方法

1 bpexpdate コマンドと -notimmediate オプションを使用して、すべてのイメージを期限切れにします。-notimmediate オプションは、bpexpdate がイメージを削除する nbdelete コマンドを呼び出すのを防ぎます。

このオプションがなければ、bpexpdate は nbdelete を呼び出してイメージを削除します。nbdelete を呼び出すたびに、アクティビティモニターでのジョブの作成、リソースの割り当て、およびメディアサーバーでのプロセスの起動が行われます。

2 最後のイメージを期限切れにした後、nbdelete オプションを指定した -allvolumes コマンドを使用して、すべてのイメージを削除します。

アクティビティモニターに 1 つのジョブだけが作成され、割り当てられるリソースとメディアサーバーで起動されるプロセスは少なくなります。イメージを期限切れにして削除する処理全体にかかる時間が短縮されます。

MSDP キュー処理について

データベースの更新が必要になる操作は、トランザクションキューに蓄積されます。1 日に 2 回、NetBackup Deduplication Manager はキューを 1 つのバッチとして処理するように Deduplication Engine に指示します。デフォルトでは、キューの処理は 12 時間ごとに、その時間の 20 分過ぎに実行されます。

本来トランザクションキューにはクリーンアップトランザクションと整合性検査トランザクションが含まれます。これらのトランザクションは参照データベースを更新します。

キューの処理は状態情報を Deduplication Engine の `storaged.log` ファイルに書き込みます。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

これらのキューの処理が他の重複排除処理をブロックすることはないので、再スケジュールは必要ありません。ユーザーはメンテナンス処理のスケジュールを変更できません。ただし、これらの処理を再スケジュールする必要がある場合は、Cohesity のサポート担当者にお問い合わせください。

キューの処理は自動的に実行されるため、手動で呼び出す必要はありません。ただし、そうすることもできます。

p.517 の「MSDP トランザクションキューの手動処理」を参照してください。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

MSDP トランザクションキューの手動処理

NetBackup では、MSDP データベーストランザクションのキューが保持されます。

p.517 の「MSDP キュー処理について」を参照してください。

通常、重複排除データベーストランザクションキュー処理を手動で実行する必要はないはずです。ただし、バックアップから MSDP カタログをリカバリする場合、MSDP トランザクションキューを処理する必要があります。トランザクションキューの処理はより大きい処理の一部です。

デフォルトでは、MSDP はすべてのローカル LSU およびクラウド LSU のデータベーストランザクションキューを処理します。ただし、クラウド LSU の dsid 値を指定することで、クラウド LSU またはローカル LSU ごとにキュープロセスを個別に実行できます。クラウド LSU の dsid 値を取得するには `/usr/openv/pdde/pdcr/bin/pddecfg -a listcloudlsu` を使用します。dsid 値が「0」に指定されている場合、ローカル LSU が処理されます。

MSDP トランザクションキューを手動で処理する方法

1 MSDP ストレージサーバーで、次のコマンドを実行します。

UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --processqueue --dsid <dsid>`

Windows の場合: `install_path¥Veritas¥pdde¥Crcontrol.exe --processqueue --dsid <dsid>`

`--dsid` は省略可能なパラメータです。dsid 値を指定しなかった場合は、すべてのローカル LSU とクラウド LSU が MSDP トランザクションキューを処理します。

2 キューの処理がまだアクティブであるかどうかを判断するには、次のコマンドを実行します。

UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --processqueueinfo --dsid <dsid>`

Windows の場合: `install_path¥Veritas¥pdde¥Crcontrol.exe --processqueueinfo --dsid <dsid>`

出力に `Busy : yes` と表示されている場合、キューはまだアクティブです。

`--dsid` は省略可能なパラメータです。dsid 値を指定しなかった場合にいずれかのローカル LSU またはクラウド LSU がアクティブだと、コマンドの出力は `busy` になります。

3 結果を検査するには、次のコマンドを実行します (小文字の l ではなく数字の 1)。

UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --dsstat 1`

Windows の場合: *`install_path`*`¥Veritas¥pdde¥Crcontrol.exe --dsstat 1`

コマンドは長い間動作することがあります。`1` を省略すると、結果はもっとすばやく返されますが、正確性は低下します。

MSDP データ整合性チェックについて

重複排除メタデータやデータは、ディスクエラー、I/O エラー、データベース破損、操作エラーのために、不整合になったり破損することがあります。NetBackup は重複排除データの整合性を定期的に調べます。NetBackup はストレージサーバーがアイドル状態の時に整合性チェックの一部を実行します。その他の整合性チェックは、作業を妨げないように、ストレージサーバーリソースを少量しか使用しない設計になっています。

データ整合性チェックプロセスには次の検査と処理が含まれます。

- 自動的にデータ損失やデータ破損を制約し、新しいバックアップが完全な状態であることを確認します。

- データコンテナの巡回冗長検査 (CRC) を自動的に実行します。
- 自動的にストレージのガーベジを収集し、クリーンアップします。
- コンテナベースの参照データベースが破損または欠落している場合に、そのデータベース (またはその一部) を自動的にリカバリします。
- ストレージの漏えいを自動的に見つけて修復します。

NetBackup はユーザーの介入なしで多くの整合性の問題を解決し、一部の問題は次回のバックアップ実行時に解決されます。ただし、重大な問題では Cohesity のサポートによる介入を必要とすることがあります。そのような場合、NetBackup は NetBackup の[ディスクのログ (Disk Logs)]レポートにメッセージを書き込みます。

データ整合性メッセージコードは 1057 です。

p.741 の「MSDP イベントのコードとメッセージ」を参照してください。

NetBackup は、NetBackup 重複排除エンジンの `storaged.log` ファイルに整合性チェックのアクティビティを書き込みます。クラウド LSU の場合、メッセージは `Storaged_<dsid>.log` に書き込まれます。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

データ整合性チェックの動作の一部を構成できます。

p.519 の「MSDP データ整合性チェックの動作の構成」を参照してください。

MSDP データ整合性チェックの動作の構成

NetBackup はいくつかのデータ整合性チェックを実行します。これらの検査の動作は構成できます。クラウド LSU の場合、`dsid` 値によって異なるクラウド LSU の動作を個別に構成できます。

MSDP データ整合性チェックの動作を構成するには、次のような 2 つの方式があります。

- コマンドを実行する。
  p.520 の「コマンドの使用によりデータ整合性チェックの動作を構成する方法」を参照してください。
- 構成ファイルパラメータを編集する。
  p.521 の「構成ファイルの編集によりデータ整合性チェックの動作を構成する方法」を参照してください。

警告: Cohesity データ整合性チェックは無効にしないことをお勧めします。無効にすると、NetBackup はデータの破損の発見、修復、または報告ができません。

---

p.518 の「MSDP データ整合性チェックについて」を参照してください。

p.521 の「MSDP データ整合性検査の構成パラメータ」を参照してください。

コマンドの使用によりデータ整合性チェックの動作を構成する方法

- 動作を構成するには、次のように、データ整合性チェックのそれぞれに値を指定します。
  - データ整合性チェック。次のコマンドを使用して動作を構成します。

    有効　UNIX の場合: `/usr/openv/pdde/pdcr/bin/pddecfg -a enabledataintegritycheck -d <dsid>`

    Windows の場合: `install_path¥Veritas¥pdde¥pddecfg -a enabledataintegritycheck -d <dsid>`

    無効　UNIX の場合: `/usr/openv/pdde/pdcr/bin/pddecfg -a disabledataintegritycheck -d <dsid>`

    Windows の場合: `install_path¥Veritas¥pdde¥pddecfg -a disabledataintegritycheck -d <dsid>`

    状態の取得　UNIX の場合: `/usr/openv/pdde/pdcr/bin/pddecfg -a getdataintegritycheck -d <dsid>`

    Windows の場合: `install_path¥Veritas¥pdde¥pddecfg -a getdataintegritycheck -d <dsid>`

    メモ: `-d` はクラウド LSU の dsid 値で、省略可能なパラメータです。クラウド LSU の dsid 値を取得するには `/usr/openv/pdde/pdcr/bin/pddecfg -a listcloudlsu` を使用します。dsid 値が「0」の場合は、ローカル LSU が処理されます。

  - 巡回冗長検査 (CRC)。次のコマンドを使用して動作を構成します。

    有効　CRC は、キュー処理がアクティブな場合およびディスクの書き込みや読み込み操作の間は実行されません。

    UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckon`

    Windows の場合: *`install_path`*`¥Veritas¥pdde¥Crcontrol.exe --crccheckon`

    無効　UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckoff`

    Windows の場合: *`install_path`*`¥Veritas¥pdde¥Crcontrol.exe --crccheckoff`

高速検査の有効化	高速 CRC 検査モードでは、コンテナ 64 から検査が開始され、コンテナの検査間でスリープ状態になりません。 高速 CRC が終了すると、CRC の動作は高速検査が呼び出される前の動作に復帰します。 UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckrestart` Windows の場合: *install_path*¥Veritas¥pdde¥Crcontrol.exe --crccheckrestart
状態の取得	UNIX の場合: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckstate` Windows の場合: *install_path*¥Veritas¥pdde¥Crcontrol.exe --crccheckstate

構成ファイルの編集によりデータ整合性チェックの動作を構成する方法

1. テキストエディタを使ってデータ整合性チェックの動作を制御する `contentrouter.cfg` ファイルまたは `spa.cfg` ファイルを開きます。

   ファイルは次のディレクトリにあります。

   - UNIX の場合: *storage_path*`/etc/puredisk`
   - Windows の場合: *storage_path*`¥etc¥puredisk`

2. パラメータを変更するには、新しい値を指定します。

   p.521 の「MSDP データ整合性検査の構成パラメータ」を参照してください。

3. ファイルを保存して閉じます。

4. NetBackup Deduplication Engine と NetBackup Deduplication Manager を再起動します。

   これはアクティビティモニターの[デーモン (Daemons)]タブから実行できます。

MSDP データ整合性検査の構成パラメータ

重複排除データ整合性検査を制御する構成ファイルのパラメータは、次の 2 つの構成ファイルにあります。

- `contentrouter.cfg` ファイル。
  パラメータについて詳しくは、表 9-3 を参照してください。
  p.190 の「MSDP contentrouter.cfg ファイルについて」を参照してください。
- `spa.cfg` ファイル。

パラメータについて詳しくは、表 9-3 を参照してください。

それらのファイルは次のディレクトリに存在します。

- UNIX の場合: *storage_path*/etc/puredisk
- Windows の場合: *storage_path*¥etc¥puredisk

警告: データ整合性検査は無効にしないことを Cohesity がお勧めします。無効にすると、NetBackup はデータの破損の発見、修復、または報告ができません。

p.518 の「MSDP データ整合性チェックについて」を参照してください。

表 9-3 contentrouter.cfg ファイルのデータ整合性検査用のパラメータ

設定	デフォルト	説明
EnableCRCCheck	true	データコンテナファイルの巡回冗長検査 (CRC) を有効または無効にします。 可能な値は true または false です。 CRC 検査は、バックアップ、リストア、またはキュー処理のジョブが実行されていない場合にのみ行われます。
CRCCheckSleepSeconds	5	コンテナ検査間のスリープ時間 (秒単位)。 スリープ間隔が長いほど、コンテナの検査に時間がかかります。
CRCCheckBatchNum	40	一度にチェックするコンテナの数。 このコンテナ数が多いほど、すべてのコンテナを検査するための所要時間は短くなりますが、必要なシステムリソースは多くなります。
ShutdownCRWhenError	false	データ損失が検出された場合に NetBackup Deduplication Manager を停止します。 このパラメータは、デバッグ目的で Cohesity のサポート担当者によって予約されます。 可能な値は true または false です。
GarbageCheckRemainDCCount	100	ガーベジを確認しない失敗したジョブのコンテナ数。失敗したバックアップまたはレプリケーションジョブは引き続きデータコンテナを生成します。失敗したジョブは再試行されるため、それらのコンテナを保持することは NetBackup が再度フィンガープリント情報を送信する必要がないことを意味します。その結果、再試行されたジョブが消費する時間とシステムリソースは最初に実行されたときより少なくなります。

設定	デフォルト	説明
CRCDaysToRaiseCritical DataScannedNotification	7	クリティカルイベントは、指定した日数の間にローカル LSU で CRC に対してデータがスキャンされない場合に生成されます。 このパラメータは、初期使用のために、DataCheck の新しいエントリとして追加する必要があります。
EnableCRCDataScan Notification	true	ローカル LSU の CRC 通知を無効にします。このパラメータは、初期使用のために、DataCheck の新しいエントリとして追加する必要があります。 例: EnableCRCDataScanNotification=false

表 9-4 データ整合性検査用 spa.cfg ファイルパラメータ

設定	デフォルト	説明
EnableDataCheck	true	データ整合性検査の有効と無効を切り替えます。 可能な値は True または False です。
DataCheckDays	14	データの一貫性を検査する日数。 日数が多いほど、毎日検査するオブジェクト数が少なくなります。日数が多いほど、毎日消費されるストレージサーバーリソースが少なくなります。
EnableDataCheckAlert	true	アラートの有効と無効を切り替えます。 true の場合に NetBackup がデータが損失したセグメントを検出すると、[ディスクのログ (Disk Logs)]レポートにメッセージが書き込まれます。 p.720 の「NetBackup MSDP ログファイル」を参照してください。

ローカル LSU の CRC 通知について

NetBackup はローカル LSU の CRC の状態に関連する通知を送信します。これらの通知は、NetBackup Web UI で確認できます。NetBackup API を使用して、これらの通知をフェッチすることもできます。詳しくは、NetBackup API のマニュアルを参照してください。

ローカル LSU の CRC 通知はデフォルトで有効になっています。これは、EnableCRCDataScanNotification パラメータを使用して無効にできます。

p.521 の「MSDP データ整合性検査の構成パラメータ」を参照してください。

表 9-5 CRC 通知

通知	種類	間隔	構成
過去 24 時間で一部のデータがスキャンされました (Some data scanned in the last 24 hrs)	情報	24 時間ごとに 1 回。	構成不可
過去 24 時間でデータはスキャンされていません (No data scanned in the last 24 hrs)	警告	24 時間ごとに 1 回。	構成不可
過去 N 日間でデータはスキャンされていません (No data scanned in the last N days)	危険	24 時間ごとに 1 回。	構成可能 p.521 の「MSDP データ整合性検査の構成パラメータ」を参照してください。
データ破損が見つかりました (Data corruption found)	危険	データ破損が見つかったとき。 24 時間に 1 回だけ通知されます。	構成不可

MSDP ストレージの読み込みパフォーマンスの管理について

NetBackup は読み取り操作に使われる処理を制御します。読み取り操作の制御によって、ストレージから読み込むジョブのパフォーマンスを向上できます。そのようなジョブには、リストアジョブ、複製ジョブおよびレプリケーションジョブが含まれています。

ほとんどの場合、Cohesity のサポート担当者によってそうするように指示されたときにのみ、構成ファイルオプションを変更する必要があります。

ストレージのデフラグ

NetBackup には、重複排除プールのバックアップイメージをデフラグするリベースと呼ばれる処理が含まれています。読み込みパフォーマンスは、重複排除ストレージでクライアントバックアップからのファイルセグメントが互いに近い場合に向上します。

p.525 の「MSDP ストレージのリベースについて」を参照してください。

サーバーではなくクライアントでのデータの解読

RESTORE_DECRYPT_LOCAL ファイルの RESTORE_DECRYPT_LOCAL パラメータは、リストア操作時にデータを解読し、解凍するホストを指定します。

p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。

p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。

MSDP ストレージのリベースについて

最初のバックアップにおいて、NetBackup はバックアップからできるだけ少数のコンテナファイルにデータセグメントを書き込みます。読み込みパフォーマンスは、重複排除ストレージでクライアントバックアップからのデータセグメントが互いに近い場合に最高になります。セグメントが互いに近くにある場合、NetBackup はバックアップファイルの検索と再構築に費やす時間が少なくなります。

ただし、バックアップのデータセグメントはクライアントがバックアップされるたびにディスクストレージ全体に散在することがあります。そのような分散は重複排除の正常な結果です。

NetBackup には、データセグメントがなるべく少ない数のコンテナファイルに格納されるように保守するリベースという処理があります。リベースにより、リストアや複製などのストレージから読み込む操作のパフォーマンスが向上します。NetBackup は、セグメントがすでにストレージにある場合にも、バックアップから新しいコンテナファイルにすべてのデータセグメントを書き込みます。その後のバックアップは、その後のリベースによって何らかの変更があるまで、これらのセグメントの古いコピーではなく新しいコピーを参照します。リベースを実行するバックアップジョブの重複排除率は、データをリベースしないジョブより低くなります。

リベースの後に、NetBackup はリベースされたデータセグメントが使用していたストレージ領域を再利用します。

表 9-6にリベース操作の説明があります。

表 9-6 リベースの形式

形式	説明
通常バックアップのリベース	標準リベースの基準が満たされた場合にバックアップ中に実行されるリベースは次のとおりです。 ■ コンテナが過去 3 カ月間にリベースされました。 ■ そのバックアップの場合、コンテナ内のデータセグメントが消費する領域は FP_CACHE_PERIOD_REBASING_THRESHOLD 値より少なくなります。FP_CACHE_PERIOD_REBASING_THRESHOLD パラメータは pd.conf ファイルにあります。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。 バックアップのリベースは、通常の MSDP バックアップ処理を通過する完全バックアップでのみ実行されます。たとえば、NetBackup アクセラレータのバックアップは MSDP バックアップ処理を通過しません。 NetBackup はバックアップジョブの完了をリベースの完了後に報告します。
定期的なバックアップのリベース	定期的リベースの基準が満たされた場合にバックアップ中に実行されるリベースは次のとおりです。 ■ コンテナは過去 3 カ月間リベースされていません。 ■ そのバックアップの場合、コンテナ内のデータセグメントが消費する領域は FP_CACHE_REBASING_THRESHOLD 値より少なくなります。FP_CACHE_REBASING_THRESHOLD パラメータは pd.conf ファイルにあります。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。 バックアップのリベースは、通常の MSDP バックアップ処理を通過する完全バックアップでのみ実行されます。たとえば、NetBackup アクセラレータのバックアップは MSDP バックアップ処理を通過しません。 NetBackup はバックアップジョブの完了をリベースの完了後に報告します。
サーバー側リベース	リベースの基準が満たされた場合にサーバーで実行されるストレージリベース。サーバー側リベースには、通常 MSDP バックアップ処理を通過しない重複排除データが含まれます。たとえば、NetBackup アクセラレータのバックアップは MSDP バックアップ処理を通過しません。 contentrouter.cfg ファイルの一部のパラメータはサーバー側のリベース動作を制御します。 p.526 の「MSDP サーバー側リベースのパラメータ」を参照してください。

MSDP サーバー側リベースのパラメータ

表 9-7に、サーバー側リベースを制御するパラメータの説明があります。

p.525 の「MSDP ストレージのリベースについて」を参照してください。

通常、パラメータ値を変更する必要はありません。ただし、場合によっては、Cohesity のサポート担当者によって、設定を変更するように指示されることがあります。

パラメータは contentrouter.cfg ファイルに格納されます。

p.190 の「MSDP contentrouter.cfg ファイルについて」を参照してください。

表 9-7　　サーバー側リベースのパラメータ

パラメータ	説明
RebaseMaxPercentage	ファイルでリベースするデータセグメントの最大パーセンテージ。すべてのファイルに対して、データセグメントの割合がこのしきい値に到達すると、残りのデータセグメントはリベースされません。 デフォルトでは、このパラメータは RebaseMaxPercentage=5 です。
RebaseMaxTime	ファイルでリベースするデータセグメントの最長時間 (秒単位)。このしきい値に到達すると、NetBackup は残りのデータセグメントをリベースしません。 デフォルトでは、このパラメータは RebaseMaxTime=150 です。
RebaseMinContainers	ファイルのデータセグメントが格納されているコンテナの最小数で、そのファイルがリベースの対象になるために必要です。ファイルのデータセグメントが格納されているコンテナの数が RebaseMinContainers より少ない場合、NetBackup はデータセグメントをリベースしません。 デフォルトでは、このパラメータは RebaseMinContainers=4 です。
RebaseScatterThreshold	コンテナのデータ局所性のしきい値。コンテナ内のファイルのデータセグメントの合計サイズが RebaseScatterThreshold 未満の場合、NetBackup はすべてのファイルのデータセグメントをリベースします。 デフォルトでは、このパラメータは RebaseScatterThreshold=64MB です。

MSDP のデータ削除処理について

データ削除処理では、NetBackup バックアップイメージを構成するデータセグメントを削除します。バックアップイメージによって参照されないセグメントのみが削除されます。

次のリストに、期限切れのバックアップイメージのデータ削除処理を示します。

- NetBackup は、NetBackup カタログからイメージレコードを削除します。
  NetBackup は、NetBackup Deduplication Manager にイメージを削除するように指示します。
- 重複排除マネージャはすぐに重複排除カタログのイメージエントリを削除し、NetBackup Deduplication Engine のトランザクションキューに削除要求を追加します。
  この時点から、期限切れのバックアップイメージにはアクセスできなくなります。

- NetBackup Deduplication Engine がキューを処理する際、すべての削除要求が処理されます。イメージの削除の要求は再生成されません。
  キューを処理する間、Deduplication Engine はデータセグメントが存在するストレージ領域の一部を再利用します。一部はデータ圧縮時に再利用されます。別のバックアップイメージがデータセグメントを要求する場合、セグメントは削除されません。
  さまざまな内部パラメータによって、コンテナファイルを圧縮するかどうかが制御されます。
  p.487 の「MSDP コンテナファイルについて」を参照してください。

24 時間以内に期限切れになったイメージを手動で削除すると、データは不要データになります。そのデータは、次のガーベジコレクション処理によって削除されるまでディスクに残ります。ガーベジコレクションはデータ整合性チェックの間に起きます。

p.518 の「MSDP データ整合性チェックについて」を参照してください。

p.516 の「バックアップイメージの削除」を参照してください。

MSDP ストレージパーティションのサイズ調整

重複排除ストレージを含んでいるボリュームが動的にサイズ調整をされたら、ストレージサーバーの NetBackup サービスを再起動します。NetBackup がサイズ調整されたパーティションを正しく使うことができるようにサービスを再起動してください。サービスを再起動しなければ、NetBackup は容量に空きがなくなる前に、空きがないと報告します。

MSDP ストレージをサイズ調整する方法

1. ディスクパーティションのサイズを変更するストレージのすべての NetBackup ジョブを停止し、ジョブの終了を待ちます。
2. ストレージサーバーをホストするメディアサーバーを無効にします。
   『NetBackup 管理者ガイド Vol. 1』を参照してください。
   http://www.veritas.com/docs/DOC5332
3. ストレージサーバーの NetBackup サービスを停止します。
   必ずすべてのサービスが停止するのを待ちます。
4. 動的に重複排除ストレージ領域を増やすか、または減らすためにオペレーティングシステムまたはディスクマネージャツールを使います。
5. NetBackup サービスを再起動します。
6. ストレージサーバーをホストするメディアサーバーを有効にします。
   『NetBackup 管理者ガイド Vol. 1』を参照してください。
   http://www.veritas.com/docs/DOC5332
7. 重複排除ジョブを再開します。

MSDP のリストアのしくみ

MSDP のリストア操作には、次の 2 つの方法があります。

表 9-8 MSDP のリストア形式

型	説明
通常のリストア	MSDP ストレージサーバーは、最初にデータを復元(つまり再構築)します。NetBackup は、次に最も使用率が低いメディアサーバーを選択してデータをクライアントに移動します。(NetBackup は、NetBackup Deduplication Engine のクレデンシャルを保有するメディアサーバーから最も使用率が低いサーバーを選択します)。メディアサーバーの bptm プロセスは、データをクライアントに移動します。 次のメディアサーバーは、NetBackup Deduplication Engine のクレデンシャルを保有します。 ■ ストレージサーバーをホストするメディアサーバー。 メディアサーバーとストレージサーバーはホストを共有しますが、ストレージサーバーはそのホストのメディアサーバーの bptm プロセスを使用してデータを送信します。 ■ 同じ重複排除ノードの負荷分散サーバー。 p.34 の「MSDP 負荷分散サーバーについて」を参照してください。 ■ 最適化複製のターゲットである異なる重複排除ノードの重複排除サーバー。 p.120 の「同じドメイン内での MSDP の最適化複製のメディアサーバーについて」を参照してください。 リストアに使うサーバーを指定できます。 p.531 の「リストアサーバーの指定」を参照してください。
クライアントに直接リストアする	ストレージサーバーは、メディアサーバーをバイパスしてクライアントに直接データを移動できます。 メディアサーバーをバイパスし、リストアデータをストレージサーバーから直接受信するように NetBackup を構成する必要があります。 p.529 の「 MSDP のクライアントへの直接リストアの構成」を参照してください。 デフォルトでは、NetBackup は Client Direct Restore を除き、NetBackup メディアサーバーのデータを圧縮解除します。その場合、データの圧縮解除はクライアントで行われます。データをストレージサーバーではなくクライアントで圧縮解除するように NetBackup を構成できます。MSDP の pd.conf ファイルの RESTORE_DECRYPT_LOCAL パラメータを参照してください。 p.176 の「MSDP pd.conf ファイルのパラメータ」を参照してください。 p.175 の「MSDP pd.conf ファイルの編集」を参照してください。

MSDP のクライアントへの直接リストアの構成

NetBackup MSDP ストレージサーバーは、メディアサーバーのコンポーネントをバイパスして MSDP クライアントにリストアデータを直接移動できます。

p.529 の「MSDP のリストアのしくみ」を参照してください。

クライアントへの直接リストアを有効にする方法

1 クライアントで OLD_VNETD_CALLBACK オプションを YES に設定します。
OLD_VNETD_CALLBACK オプションは、UNIX システムの bp.conf ファイルおよび Windows システムのレジストリに格納されます。

p.130 の「コマンドラインの使用による NetBackup 構成オプションの設定」を参照してください。

2 プライマリサーバーで次のコマンドを実行して、クライアントで Client Direct Restore を使用するように NetBackup を構成します。

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/bpclient -client client_name -update -client_direct_restore 2`

Windows の場合: `install_path¥NetBackup¥bin¥admincmd¥bpclient -client client_name -update -client_direct_restore 2`

リモートサイトのファイルのリストアについて

ローカルサイトからリモートサイトにイメージをコピーするために最適化複製を使うと、リモートサイトのコピーからリモートサイトのクライアントにリストアできます。そうするには、元のクライアント以外のクライアントにファイルをリストアする、サーバー主導リストアかクライアントによるリダイレクトリストアを使います。

リダイレクトリストア方法についての情報は別のガイドにあります。

「クライアントのリストアの管理」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。

どのメディアサーバーがリストアを実行するか構成しなければならないことがあります。最適化複製では、複製操作を開始するメディアサーバーは新しいイメージコピーの書き込みホストになります。書き込みホストはそれらのイメージコピーからリストアします。書き込みホストがローカルサイトにある場合、書き込みホストはリモートサイトのそれらのイメージからリモートサイトの代替クライアントにリストアします。このホストは WAN をまたがってイメージを読み込み、次に WAN をまたがって代替クライアントにイメージを書き戻します。この場合、リストアサーバーとしてリモートサイトのメディアサーバーを指定できます。

ターゲットプライマリドメインでのバックアップからのリストアについて

ターゲットプライマリドメインでイメージを使用してクライアントを直接リストアすることはできますが、これは、ディザスタリカバリ時にのみ行ってください。ここでは、ディザスタリカバリは元のドメインがもはや存在せず、クライアントをターゲットのドメインからリカバリする必要があるという状況でのリカバリをいいます。

表 9-9 ディザスタリカバリの例でのクライアントのリストア

ディザスタリカバリの例	クライアントが存在するか	説明
例 1	はい	別のドメインでクライアントを構成し、そのクライアントに直接リストアします。
例 2	なし	リカバリドメインにクライアントを作成し、そのクライアントに直接リストアします。これは可能性が最も高い例です。
例 3	なし	リカバリドメインで代替クライアントへのリストアを実行します。

クライアントをリカバリする手順は他のクライアントのリカバリと同じです。実際の手順はクライアントの形式、ストレージの形式、およびリカバリが代替クライアントのリストアであるかどうかによって異なります。

個別リカバリテクノロジ (GRT) を使うリストアの場合は、アプリケーションインスタンスがリカバリドメインに存在する必要があります。アプリケーションインスタンスは、NetBackup がリカバリ先を持つために必要となります。

リストアサーバーの指定

NetBackup は重複排除データのリストアサーバーとしてバックアップサーバーを使わないことがあります。

p.529 の「MSDP のリストアのしくみ」を参照してください。

リストアに使うサーバーを指定できます。次はリストアサーバーを指定する方式です。

- 常時バックアップサーバーを使用します。次のとおり 2 つの方式が存在します。
  - [メディアホストの上書き (Media host override)]サーバーを指定するために NetBackup の[ホストプロパティ (Host properties)]を使用します。元のバックアップサーバーの任意のストレージユニットのすべてのリストアジョブは指定されたメディアサーバーを使います。[元のバックアップサーバー (Original backup server)]と同じサーバーを[リストアサーバー (Restore server)]に指定します。
    『NetBackup 管理者ガイド Vol. 1』の「リストアでの特定のサーバーの使用」を参照してください。
    この手順は FORCE_RESTORE_MEDIA_SERVER オプションを設定します。構成オプションは Windows システムのレジストリと UNIX システムの bp.conf ファイルに保存されます。
  - NetBackup プライマリサーバーの次のディレクトリに touch ファイル USE_BACKUP_MEDIA_SERVER_FOR_RESTORE を作成します。
    UNIX の場合: usr/openv/netbackup/db/config
    Windows の場合: *install_path*¥Veritas¥Netbackup¥db¥config

このグローバル設定はバックアップをしたサーバーへのリストアを常に強制します。それは重複排除のリストアジョブだけではなくすべての NetBackup リストアジョブに適用されます。この touch ファイルが存在する場合、NetBackup は FORCE_RESTORE_MEDIA_SERVER と FAILOVER_RESTORE_MEDIA_SERVER の設定を無視します。

- 異なるサーバーを常時使用します。
  [メディアホストの上書き (Media host override)]サーバーを指定するために NetBackup の[ホストプロパティ (Host Properties)]を使います。
  [メディアホストの上書き (Media host override)]についての以前の説明を参照してください。[リストアサーバー (Restore server)]に対する異なるサーバーの指定についての説明は除きます。
- 単一のリストアインスタンス。-disk_media_server オプションを指定して bprestore コマンドを使います。
  コマンドの各インスタンスのリストアジョブは指定されたメディアサーバーを使います。
  『NetBackup コマンドリファレンスガイド』を参照してください。

WORM ストレージサーバーインスタンスでの追加の OS STIG 強化の有効化

STIG (セキュリティ技術導入ガイド) では、情報システムとソフトウェアのセキュリティを向上するための技術ガイドを提供し、悪質なコンピュータ攻撃を防ぎます。この種のセキュリティは、強化とも呼ばれます。

OS STIG 強化ルールは、プライマリサーバー、メディアサーバー、ストレージサーバーのインスタンスで自動的に有効になります。これらのルールは、DISA (国防情報システム局) からの次のプロファイルに基づいています。

Red Hat Enterprise Linux Server 用の STIG

セキュリティの向上のため、追加の OS STIG 強化を有効にすることができます。追加ルールにより、sshd プロセスがさらに強化され、より厳格なパスワードポリシーが適用されます。

追加の OS STIG 強化の有効化については、次の注意点があります。

- このコマンドでは、個々のルールの制御は許可されません。
- このオプションを一度有効にすると、無効にはできません。
- インスタンスで追加ルールを有効にする前は、SSH の同時セッションは無制限です。OS STIG 強化を有効にすると、SSH の同時セッションの最大数は 10 個に制限されます。

追加の **OS STIG** 強化を有効にするには

1. msdpadm ユーザー (Flex の場合) または appadmin ユーザー (Flex Scale の場合) として、インスタンスへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting STIG enable-ondemand-hardening
```

MSDP クラスタでのマルチストリームバックアップに対する複数 MSDP ノードの使用

MSDP クラスタ環境では、最適なパフォーマンスを維持するために、複数のノード間で負荷を分散することが不可欠です。MSDP には、単一ノード構成またはクラスタ構成があります。Flex Scale、Cloud Scale、MSDP ボリュームグループなどの MSDP クラスタ構成には、複数のノードがある場合があります。これらのクラスタ構成により、マルチストリームバックアップの拡張性とパフォーマンスが向上します。

NetBackup 11.0 以降、MSDP クラスタストレージサーバーでのマルチストリームバックアップの負荷分散を改善するために、新しいポリシー属性[複数の MSDP ノードの使用 (Use multiple MSDP nodes)]が導入されました。この機能により、複数の MSDP ノード間でバックアップストリームを分散し、スループットを最適化し、個々のノードで潜在的な輻輳を減らすことができます。

11.0 NetBackup より前は、マルチストリームバックアップで複数の MSDP ノードの使用を有効にするために、ポリシー名の接頭辞 MSDPLB+ が使用されていました。運用中、MSDPLB+ の命名規則は必ずしも最適だったとは言えなかったため、NetBackup 11.0 で新しいポリシー属性の導入が進められました。

このオプションを使用する場合は、次の点を考慮してください。

- このポリシー属性は、MSDP クラスタストレージサーバー上のマルチストリームバックアップにのみ使用するように設計されています。単一ノード MSDP ストレージサーバーの場合、この属性には効果がありません。
- このポリシー属性は、次のポリシー形式では利用できません。これらのポリシー形式の一部には、複数の MSDP ノード間でのバックアップストリームの分散を処理する、より高度な機能がすでに備えられています。その他の場合、ポリシーの性質上、複数の MSDP ノードを使用することはできません。
  - Oracle
  - Epic-large-file
  - Universal-share
  - MSDP-object-store

- このオプションを使用するには、メディアサーバーが NetBackup 11.0 以降を実行している必要があります。ストレージサーバーが以前のバージョンのメディアサーバーで構成されている場合、バックアップジョブはジョブ状態コード 213 で失敗します。ただし、以前のバージョンを実行している環境では、MSDPLB+ ポリシー接頭辞を引き続き使用して、複数の MSDP ノード間の負荷分散を有効にできます。
- より小さいバックアップの場合は、このオプションを有効にしないことをお勧めします。このオプションを有効にしない場合、ストレージとネットワークの使用率を最小限に抑えるための最も効率的な方法は、同じノードでの重複排除です。
- クライアントデータが大きく、バックアップジョブがバックアップ処理時間帯内に終了できない場合は、このオプションを有効にして並列データ処理に複数の MSDP ノードを使用して、バックアップ時間を短縮します。
- クライアントアプリケーションによっては、前回のバックアップと同じ順序で NetBackup にバックアップデータを送信しないことがあります。このような場合、MSDP はデータストリームを管理するために、ノード間でより多くのストレージリソースとネットワークリソースを必要とすることがあります。これらのタイプのアプリケーションに対してこのオプションを有効にすると、システム効率が低下する場合があります。

p.534 の「MSDP クラスタでのメディアサーバーと MSDP エンジンの親和性の有効化」を参照してください。

MSDP クラスタでのメディアサーバーと MSDP エンジンの親和性の有効化

MSDP クラスタ環境では、MSDP エンジンとメディアサーバーの両方を同じノードで実行できます。デフォルトでは、NetBackup は 2 つの間の関係を維持しません。バックアップジョブが実行されると、メディアサーバーは MSDP エンジンのいずれかにデータを転送します。メディアサーバーと MSDP エンジンが同じノード上にない場合、データはネットワークを介して転送されるため、より多くのネットワーク帯域幅が必要になる場合があります。

ネットワーク帯域幅に関する問題がある場合は、メディアサーバーの親和性設定を有効にできます。メディアサーバーの親和性を有効にすると、NetBackup はバックアップジョブのために同じノードのメディアサーバーと MSDP エンジンの選択を試みて、ネットワークトラフィックを減らします。

メディアサーバーと MSDP エンジンの親和性を有効にするには

1. NetBackup プライマリサーバーで次のコマンドを実行して、設定を有効にします。

   ```
   /usr/openv/netbackup/bin/admincmd/nbemmcmd -changesetting
   -machinename <primary_server> -ALLOW_MEDIA_SERVER_AFFINITY 1
   ```

2. 次のコマンドを実行して、現在の設定を確認します。

   ```
   /usr/openv/netbackup/bin/admincmd/nbemmcmd -listsettings
   -machinename <primary_server>
   ```

10

MSDP のリカバリ

この章では以下の項目について説明しています。

- MSDP カタログのリカバリについて
- シャドーコピーからの MSDP カタログのリストア
- MSDP ストレージサーバーのディスクエラーからのリカバリ
- MSDP ストレージサーバーのエラーからのリカバリ
- NetBackup カタログリカバリ後の MSDP ストレージサーバーのリカバリ

MSDP カタログのリカバリについて

次に、NetBackup MSDP カタログのリカバリオプションを示します。

表 10-1 MSDP カタログバックアップのリカバリオプション

リカバリオプション	説明
シャドーコピーからのリストア	NetBackup が MSDP カタログで破損を検出した場合には、Deduplication Manager がカタログを最新のシャドーコピーから自動的にリストアします。この自動リストア処理では、リカバリした MSDP カタログが最新になるようにトランザクションログも使います。 シャドーコピーのリストア処理は自動的に実行されますが、シャドーコピーから手動でリカバリする必要がある場合はリストア手順を利用できます。 p.197 の「MSDP シャドーカタログについて」を参照してください。 p.537 の「シャドーコピーからの MSDP カタログのリストア」を参照してください。

リカバリオプション	説明
バックアップからのリカバリ	MSDP カタログのバックアップポリシーを設定し、有効なバックアップがある場合はバックアップからカタログをリカバリできます。一般に、バックアップからの MSDP カタログリカバリは代替がない場合にのみ試みてください。例: ハードウェアの問題またはソフトウェアの問題により MSDP カタログとシャドーコピーが完全に消失することになります。 ガイド付きリカバリを行う場合が、バックアップからの MSDP カタログのリカバリを成功させられる可能性が最も大きくなります。失敗すると、データ喪失の可能性があります。MSDP カタログをリカバリする必要があるお客様のために、Cohesity はプロセスのガイドを行っています。そのため、バックアップから MSDP カタログをリカバリするには、Cohesity のサポート担当者にお問い合わせください。サポート担当者には、リカバリ手順が記載されているナレッジベースの記事 000047346 を参照するように依頼してください。

注意: カタログのリカバリが必要なほど重大な状況であるかどうかを判断する必要があります。Cohesity は、シャドーコピーから MSDP カタログのすべてまたは一部をリストアする前に Cohesity のサポート担当者に問い合わせることをお勧めします。サポート担当者は、カタログをリカバリする必要があるか、または他のソリューションが利用可能かどうかを判断するお手伝いをします。

p.197 の「MSDP カタログの保護について」を参照してください。

p.678 の「外部 MSDP カタログバックアップからのリストア」を参照してください。

シャドーコピーからの MSDP カタログのリストア

NetBackup は破損を検出すると、MSDP カタログの必要な部分を自動的にリストアします。ただし、通常の状況では必要ありませんが、シャドーコピーから MSDP カタログを手動でリストアすることもできます。Cohesity は、シャドーコピーから MSDP カタログのすべてまたは一部をリストアする前に Cohesity のサポート担当者に問い合わせることをお勧めします。

次のように、使う手順はリストアのシナリオによって決まります。

シャドーコピーから MSDP カタログ全体をリストアする	このシナリオでは、シャドーコピーの 1 つからカタログ全体をリストアします。 p.538 の「シャドーコピーから MSDP カタログ全体をリストアする方法」を参照してください。

特定の MSDP データベースファイルをリストアする

MSDP カタログは複数の小さいデータベースファイルから構成されます。それらのファイルは、ファイルシステムでは次のようにクライアント名とポリシー名で構成されます。

UNIX の場合:
/database_path/databases/catalogshadow/2/*ClientName*/*PolicyName*

Windows の場合:
database_path¥databases¥catalogshadow¥2¥*ClientName*¥*PolicyName*

クライアントとポリシーの組み合わせに対してデータベースファイルをリストアできます。特定のクライアントとポリシーのデータベースファイルのリストアは、常に最新のシャドーコピーから実行します。

p.538 の「シャドーコピーから特定の MSDP データベースファイルをリストアする方法」を参照してください。

p.536 の「MSDP カタログのリカバリについて」を参照してください。

シャドーコピーから MSDP カタログ全体をリストアする方法

1. アクティブな MSDP ジョブがある場合、それらを取り消すか、完了するまで待ちます。
2. [メディアサーバー重複排除プール (Media Server Deduplication Pool)]にバックアップするすべてのポリシーとストレージライフサイクルポリシーを無効にします。
3. MSDP ストレージサーバーで、ホスト形式に応じて次のコマンドを実行します。
   - UNIX の場合: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog recover all`
   - Windows の場合: *install_path*¥Veritas¥pdde¥cacontrol --catalog recover all
4. [メディアサーバー重複排除プール (Media Server Deduplication Pool)]にバックアップするすべてのポリシーとストレージライフサイクルポリシーを有効にします。
5. リカバリの前に、取り消されたジョブを再起動します。

シャドーコピーから特定の MSDP データベースファイルをリストアする方法

1. クライアントとバックアップポリシーの組み合わせに対してアクティブな MSDP ジョブがある場合、それらを取り消すか、完了するまで待ちます。
2. [メディアサーバー重複排除プール (Media Server Deduplication Pool)]にバックアップする、クライアントとバックアップポリシーの組み合わせに対するポリシーとストレージライフサイクルポリシーを無効にします。

3 そのデータベースファイルをリカバリするクライアントとポリシーのシャドーディレクトリに移動します。そのディレクトリには、リカバリするデータベースファイルが含まれます。パス名の形式は次のとおりです。

UNIX の場合:
/database_path/databases/catalogshadow/2/*ClientName*/*PolicyName*

Windows の場合:
database_path¥databases¥catalogshadow¥2¥*ClientName*¥*PolicyName*

4 ホスト形式に応じて次のコマンドを実行します。

- UNIX の場合: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog recover 2 "/ClientName/PolicyName"`
- Windows の場合: *install_path*¥Veritas¥pdde¥cacontrol --catalog recover 2 "¥*ClientName*¥*PolicyName*"

5 [メディアサーバー重複排除プール (Media Server Deduplication Pool)]にバックアップするすべてのポリシーとストレージライフサイクルポリシーを有効にします。

6 データベースファイルをリカバリする前にジョブを取り消した場合、それらを再起動します。

MSDP ストレージサーバーのディスクエラーからのリカバリ

リカバリ機構で NetBackup ソフトウェアが存在するディスクが保護されない場合、ディスク障害が発生すると重複排除ストレージサーバーの構成は失われます。このトピックでは、ディスクがバックアップされなかったシステムディスクまたはプログラムディスクの障害からリカバリする方法について説明します。

メモ: この手順では、重複排除されたデータが存在するディスクではなく、NetBackup メディアサーバーソフトウェアが存在するディスクのリカバリについて説明します。ディスクは、システムブートディスクの場合とシステムブートディスクではない場合があります。

リカバリ後、NetBackup の重複排除環境は正常に機能する必要があります。重複排除ストレージ上のすべての有効なバックアップイメージがリストアに利用可能である必要があります。

Cohesity は、NetBackup を使用して、重複排除ストレージサーバーのシステムディスクまたはプログラムディスクを保護することをお勧めします。その後、NetBackup が存在するディスクで障害が発生してディスクを交換する必要がある場合に、NetBackup を使用して、そのメディアサーバーをリストアできます。

表 10-2　メディアサーバーのディスク障害からリカバリする処理

手順	タスク	手順詳細
手順 1	ディスクを交換します	ディスクがシステムブートディスクの場合は、オペレーティングシステムのインストールも行います。 ハードウェアベンダーとオペレーティングシステムのマニュアルを参照してください。
手順 2	ストレージをマウントします	ストレージとデータベースが同じ場所にマウントされていることを確認します。 ストレージベンダーのマニュアルを参照してください。
手順 3	NetBackup メディアサーバーのソフトウェアをインストールし、ライセンスを取得します	『NetBackup インストールガイド UNIX および Windows』を参照してください。 http://www.veritas.com/docs/DOC5332
手順 4	重複排除ホストの構成ファイルを削除します	各負荷分散サーバーには、重複排除ホストの構成ファイルが含まれます。負荷分散サーバーを使う場合は、サーバーから重複排除ホストの構成ファイルを削除します。 p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。
手順 5	重複排除サーバー上のクレデンシャルを削除します	負荷分散サーバーがある場合は、それらのメディアサーバー上の NetBackup Deduplication Engine のクレデンシャルを削除します。 p.504 の「負荷分散サーバーからのクレデンシャルの削除」を参照してください。
手順 6	ストレージサーバーにクレデンシャルを追加します	ストレージサーバーに NetBackup Deduplication Engine のクレデンシャルを追加します。 p.504 の「NetBackup Deduplication Engine クレデンシャルの追加」を参照してください。
手順 7	構成ファイルテンプレートを取得します	ディスク障害の前にストレージサーバーの構成ファイルを保存しなかった場合は、テンプレート構成ファイルを取得します。 p.192 の「MSDP ストレージサーバーの構成の保存」を参照してください。
手順 8	構成ファイルを編集します	p.193 の「MSDP ストレージサーバーの構成ファイルの編集」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	編集したファイルから構成をアップロードすることによって、ストレージサーバーを構成します。 p.194 の「MSDP ストレージサーバーの構成の設定」を参照してください。
手順 10	負荷分散サーバーを追加します	環境で負荷分散サーバーを使用している場合は、それらのサーバーを構成に追加します。 p.170 の「MSDP 負荷分散サーバーの追加」を参照してください。

MSDP ストレージサーバーのエラーからのリカバリ

ストレージサーバーのホストコンピュータの永続的なエラーからリカバリするには、このトピックで説明されている処理を実行します。

NetBackup は、リカバリする前に次の項目を考慮することを推奨します。

- 新しいコンピュータでは、古いコンピュータと同じバイト順序を使用する必要があります。

  警告: 新しいコンピュータで古いコンピュータと同じバイト順序を使用しないと、重複排除されたデータにアクセスできません。演算処理において、エンディアンネスはビッグエンディアンとリトルエンディアンのデータを表すバイト順序を示します。たとえば、SPARC プロセッサと Intel プロセッサでは、異なるバイト順序が使用されます。このため、Oracle Solaris SPARC ホストを Intel プロセッサ搭載の Oracle Solaris ホストと置き換えることはできません。

- Cohesity は、新しいコンピュータで古いコンピュータと同じオペレーティングシステムを使用することを推奨します。
- Cohesity は、新しいコンピュータで古いコンピュータと同じバージョンの NetBackup を使用することを推奨します。
  新しいコンピュータでより最近のバージョンの NetBackup を使用する場合は、新しいリリースで必要とされるデータ変換を行うようにしてください。
  置換ホストでより古いバージョンの NetBackup を使用する場合は、Cohesity のサポート担当者に連絡してください。

表 10-3 MSDP ストレージサーバーのエラーからのリカバリ

手順	作業	手順詳細
手順 1	ディスクプールを使用するストレージユニットを削除します	『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 2	ディスクプールを削除します	p.514 の「メディアサーバー重複排除プールの削除」を参照してください。
手順 3	重複排除ストレージサーバーを削除します	p.501 の「MSDP ストレージサーバーの削除」を参照してください。
手順 4	重複排除ホストの構成ファイルを削除します	各負荷分散サーバーには、重複排除ホストの構成ファイルが含まれます。負荷分散サーバーを使う場合は、サーバーから重複排除ホストの構成ファイルを削除します。 p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。

手順	作業	手順詳細
手順 5	重複排除サーバー上のクレデンシャルを削除します	負荷分散サーバーがある場合は、それらのメディアサーバー上の NetBackup Deduplication Engine のクレデンシャルを削除します。 p.504 の「負荷分散サーバーからのクレデンシャルの削除」を参照してください。
手順 6	重複排除の要件を満たすように新しいホストを構成します	新しいホストを構成するときに、次のことを考慮してください。 ■ 同じホスト名または別の名前を使用できます。 ■ 同じストレージパスまたは異なるストレージパスを使用できます。別のストレージパスを使う場合は、重複排除ストレージをその新しい場所に移動する必要があります。 ■ 元のホストのデータベースパスがストレージパスと異なっている場合、次のいずれかを行えます。 ■ 同じデータベースパスを使う。 ■ 別のデータベースパスを使う。この場合、重複排除データベースを新しい場所に移動する必要があります。 ■ 異なるデータベースパスを使い続ける必要はありません。databases ディレクトリをストレージパスに移動し、ストレージサーバーを構成するときにストレージパスのみを指定することもできます。 ■ ホストの既定のネットワークインターフェースを使うか、ネットワークインターフェースを指定することができます。 元のホストが特定のネットワークインターフェースを使用していた場合、同じインターフェース名を使う必要はありません。 ■ 以前の MSDP ストレージサーバーを、KMS サービスを使用して MSDP 暗号化を使用するように設定した場合は、新しい MSDP ストレージサーバーと同じ設定を使用する必要があります。 p.33 の「MSDP ストレージサーバーについて」を参照してください。 p.34 の「MSDP サーバーの必要条件について」を参照してください。
手順 7	ストレージをホストに接続します	この交換ホスト用に構成したストレージパスを使用してください。 コンピュータまたはストレージベンダーのマニュアルを参照してください。
手順 8	NetBackup のメディアサーバーソフトウェアを新しいホストにインストールします	『NetBackup インストールガイド』を参照してください。
手順 9	重複排除を再構成します	NetBackup Deduplication Engine と同じクレデンシャルを使用する必要があります。 p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

手順	作業	手順詳細
手順 10	バックアップイメージをインポートします。	『NetBackup 管理者ガイド Vol. 1』を参照してください。 **メモ:** NetBackup カタログが存在しない場合にのみ、バックアップイメージのインポートを実行します。それ以外の場合は、bpimage コマンドを使用して、カタログバックアップイメージのストレージサーバー名とディスクプール名を更新します。

NetBackup カタログリカバリ後の MSDP ストレージサーバーのリカバリ

障害で NetBackup カタログのリカバリが必要な場合は、NetBackup カタログのリカバリ後にストレージサーバーの構成を設定する必要があります。

p.194 の「MSDP ストレージサーバーの構成の設定」を参照してください。

Cohesity ストレージサーバーの構成を保存することをお勧めします。

p.54 の「MSDP ストレージサーバーの構成を保存する」を参照してください。

プライマリサーバーのリカバリに関する情報が利用可能です。

『NetBackup トラブルシューティングガイド』を参照してください。

11

MSDP ホストの置換

この章では以下の項目について説明しています。

MSDP ストレージサーバーのホストコンピュータの交換

重複排除ストレージサーバーのホストコンピュータを交換する場合は、次の手順に従って、NetBackup をインストールし、重複排除ストレージサーバーを再構成します。新しいホストは重複排除ストレージサーバーをまだホストできません。

コンピュータを交換する理由には、リース機器の交換、または現在の重複排除ストレージサーバーコンピュータがパフォーマンス要件を満たしていないことなどがあります。

NetBackup は、リカバリする前に次の項目を考慮することを推奨します。

- 新しいコンピュータでは、古いコンピュータと同じバイト順序を使用する必要があります。

  警告: 新しいコンピュータで古いコンピュータと同じバイト順序を使用しないと、重複排除されたデータにアクセスできません。演算処理において、エンディアンネスはビッグエンディアンとリトルエンディアンのデータを表すバイト順序を示します。たとえば、SPARC プロセッサと Intel プロセッサでは、異なるバイト順序が使用されます。このため、Oracle Solaris SPARC ホストを Intel プロセッサ搭載の Oracle Solaris ホストと置き換えることはできません。

- Cohesity は、新しいコンピュータで古いコンピュータと同じオペレーティングシステムを使用することを推奨します。
- Cohesity は、新しいコンピュータで古いコンピュータと同じバージョンの NetBackup を使用することを推奨します。
  新しいコンピュータでより最近のバージョンの NetBackup を使用する場合は、新しいリリースで必要とされるデータ変換を行うようにしてください。

置換ホストでより古いバージョンの NetBackup を使用する場合は、Cohesity のサポート担当者に連絡してください。

表 11-1　MSDP ストレージサーバーのホストコンピュータの交換

手順	作業	手順詳細
手順 1	バックアップイメージを期限切れにします	重複排除ディスクストレージに存在するすべてのバックアップイメージを期限切れにします。 **警告:** イメージを削除しないでください。後でイメージを NetBackup にインポートして戻します。 `bpexpdate` コマンドを使ってバックアップイメージを期限切れにする場合は、`-nodelete` パラメータを使います。 『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 2	ディスクプールを使用するストレージユニットを削除します	『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 3	ディスクプールを削除します	p.514 の「メディアサーバー重複排除プールの削除」を参照してください。
手順 4	重複排除ストレージサーバーを削除します	p.501 の「MSDP ストレージサーバーの削除」を参照してください。
手順 5	重複排除ホストの構成ファイルを削除します	各負荷分散サーバーには、重複排除ホストの構成ファイルが含まれます。負荷分散サーバーを使う場合は、サーバーから重複排除ホストの構成ファイルを削除します。 p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。
手順 6	重複排除サーバー上のクレデンシャルを削除します	負荷分散サーバーがある場合は、それらのメディアサーバー上の NetBackup Deduplication Engine のクレデンシャルを削除します。 p.504 の「負荷分散サーバーからのクレデンシャルの削除」を参照してください。

手順	作業	手順詳細
手順 7	重複排除の要件を満たすように新しいホストを構成します	新しいホストを構成するときに、次のことを考慮してください。 ■ 同じホスト名または別の名前を使用できます。 ■ 同じストレージパスまたは異なるストレージパスを使用できます。別のストレージパスを使う場合は、重複排除ストレージをその新しい場所に移動する必要があります。 ■ 元のホストのデータベースパスがストレージパスと異なっている場合、次のいずれかを行えます。 ■ 同じデータベースパスを使う。 ■ 別のデータベースパスを使う。この場合、重複排除データベースを新しい場所に移動する必要があります。 ■ 異なるデータベースパスを使い続ける必要はありません。databases ディレクトリをストレージパスに移動し、ストレージサーバーを構成するときにストレージパスのみを指定することもできます。 ■ ホストの既定のネットワークインターフェースを使うか、ネットワークインターフェースを指定することができます。 元のホストが特定のネットワークインターフェースを使用していた場合、同じインターフェース名を使う必要はありません。 ■ 以前の MSDP ストレージサーバーを、KMS サービスを使用して MSDP 暗号化を使用するように設定した場合は、新しい MSDP ストレージサーバーと同じ設定を使用する必要があります。 p.33 の「MSDP ストレージサーバーについて」を参照してください。 p.34 の「MSDP サーバーの必要条件について」を参照してください。
手順 8	ストレージをホストに接続します	この交換ホスト用に構成したストレージパスを使用してください。 コンピュータまたはストレージベンダーのマニュアルを参照してください。
手順 9	NetBackup のメディアサーバーソフトウェアを新しいホストにインストールします	『NetBackup インストールガイド』を参照してください。
手順 10	重複排除を再構成します	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。
手順 11	バックアップイメージをインポートします	『NetBackup 管理者ガイド Vol. 1』を参照してください。

12

MSDP のアンインストール

この章では以下の項目について説明しています。

- MSDP のアンインストールについて
- MSDP の無効化

MSDP のアンインストールについて

メディアサーバーの重複排除コンポーネントを NetBackup とは別にアンインストールできません。重複排除コンポーネントは NetBackup ソフトウェアをインストールするときにインストールされ、NetBackup ソフトウェアをアンインストールするときにアンインストールされます。

他のトピックでは関連する手順が次のように記述されています。

- 既存の重複排除環境の再構成。
p.499 の「MSDP ストレージサーバーの名前またはストレージパスの変更」を参照してください。
- 重複排除の無効化と、構成ファイルとストレージファイルの削除。
p.547 の「MSDP の無効化」を参照してください。

MSDP の無効化

NetBackup メディアサーバーから重複排除コンポーネントを削除できません。コンポーネントを無効にし、重複排除ストレージファイルとカタログファイルを削除することはできます。ホストは NetBackup メディアサーバーのままです。

この処理では、重複排除ディスクストレージに存在するすべてのバックアップイメージが期限切れになっていることを想定しています。

警告: 有効な NetBackup イメージが重複排除ストレージに存在する場合に重複排除を削除すると、データ損失が発生することがあります。

表 12-1 MSDP の削除

手順	作業	手順詳細
手順 1	クライアント重複排除を削除します	クライアント重複排除リストから自身のデータを重複排除するクライアントを削除します。 p.103 の「クライアントについての MSDP クライアント側の重複排除の無効化」を参照してください。
手順 2	ディスクプールを使用するストレージユニットを削除します	『NetBackup 管理者ガイド Vol. 1』を参照してください。 http://www.veritas.com/docs/DOC5332
手順 3	ディスクプールを削除します	p.514 の「メディアサーバー重複排除プールの削除」を参照してください。
手順 4	重複排除ストレージサーバーを削除します	p.501 の「MSDP ストレージサーバーの削除」を参照してください。 重複排除ストレージサーバーを削除しても、物理ディスク上のストレージの内容は変更されません。不注意なデータ損失を防ぐために、ストレージサーバーを削除しても、NetBackup はストレージを自動的には削除しません。
手順 5	設定を削除します	重複排除の構成を削除します。 p.502 の「MSDP ストレージサーバーの構成を削除する」を参照してください。
手順 6	重複排除ホストの構成ファイルを削除します	各負荷分散サーバーには、重複排除ホストの構成ファイルが含まれます。負荷分散サーバーを使う場合は、サーバーから重複排除ホストの構成ファイルを削除します。 p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。
手順 7	ストレージディレクトリとデータベースディレクトリを削除します	ストレージディレクトリとデータベースディレクトリを削除します。(別のデータベースディレクトリを使用することは、重複排除を構成した時のオプションでした。) **警告:** 有効な NetBackup イメージが重複排除ストレージに存在する場合にストレージディレクトリを削除すると、データ損失が発生することがあります。 オペレーティングシステムのマニュアルを参照してください。

13

重複排除アーキテクチャ

この章では以下の項目について説明しています。

- MSDP サーバーコンポーネント
- メディアサーバーの重複排除バックアップ処理
- MSDP クライアントコンポーネント
- MSDP クライアント側の重複排除バックアップ処理

MSDP サーバーコンポーネント

図 13-1 は、ストレージサーバーコンポーネントの図です。

図 13-1　　MSDP サーバーコンポーネント

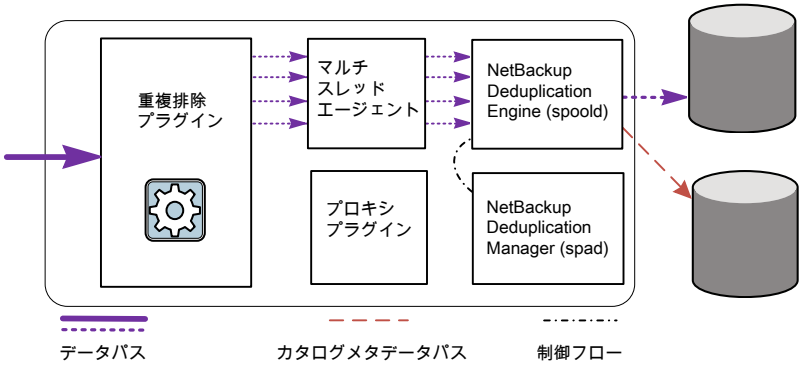


表 13-1 は、MSDP のサーバーのコンポーネントについて説明します。

表 13-1 NetBackup MSDP サーバーコンポーネント

コンポーネント	説明
重複排除プラグイン	重複排除プラグインを使用して、次のことを実行できます。 ■ ファイルの内容からファイルのメタデータを分離します。 ■ 内容を重複排除します (ファイルをセグメントに分割します)。 ■ 必要に応じて、バックアップ用データを圧縮し、リストア用バックアップを解凍します。 ■ 必要に応じて、バックアップ用データを暗号化し、リストア用バックアップを復号します。 ■ 必要に応じて、複製およびレプリケーション転送用データを圧縮します。 ■ 必要に応じて、複製およびレプリケーション転送用データを暗号化します。 プラグインは重複排除ストレージサーバーと負荷分散サーバーで実行されます。
マルチスレッドエージェント	NetBackup 重複排除マルチスレッドエージェントは、非同期ネットワーク I/O と CPU コア計算に対して複数のスレッドを使います。エージェントはストレージサーバー上、負荷分散サーバー上、自身のデータを重複排除するクライアント上で実行されます。 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。
NetBackup Deduplication Engine	NetBackup Deduplication Engine は、ストレージサーバーのコアコンポーネントの 1 つです。これにより数多くの重複排除の機能が提供されます。詳しくは「表 13-2」を参照してください。 バイナリファイル名は、ストレージプールデーモンの省略形である spoold です。これを印刷スプーラデーモンと間違えないでください。spoold プロセスは、NetBackup Web UI に NetBackup 重複排除エンジンとして表示されます。
NetBackup 重複排除マネージャ	Deduplication Manager は、ストレージサーバーのコアコンポーネントの 1 つです。Deduplication Manager は構成を保持し、内部処理、最適化複製、セキュリティおよびイベントのエスカレーションを制御します。 重複排除マネージャのバイナリファイル名は spad です。spad プロセスは、NetBackup Web UI に NetBackup 重複排除マネージャとして表示されます。
プロキシのプラグイン	プロキシプラグインは、自身のデータをバックアップするクライアントとの制御通信を管理します。プロキシプラグインは、クライアント上の OpenStorage プロキシサーバー (nbostpxy) と通信します。
参照データベース	参照データベースには、ファイルを構成するすべてのデータセグメントを指す参照が格納されます。データセグメントは一意のフィンガープリントによって識別されます。拡張性とパフォーマンスを改善するため、参照データベースは複数の小さな参照データベースファイルにパーティション分割されます。 参照データベースは、NetBackup カタログとは別のものです。NetBackup カタログは、通常の NetBackup バックアップイメージの情報を保持します。

表 13-2 は、NetBackup Deduplication Engine のコンポーネントと機能について説明します。

表 13-2 NetBackup Deduplication Engine のコンポーネントと機能

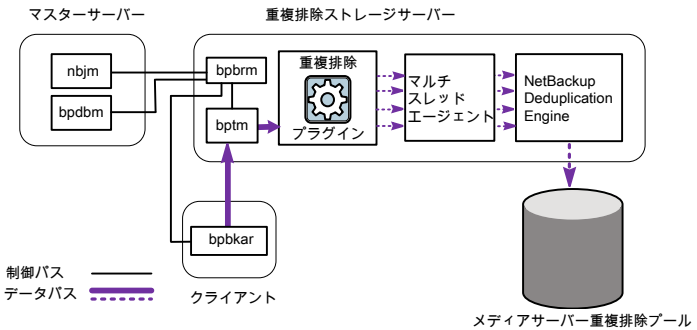
コンポーネント	説明
接続およびタスクマネージャ	接続およびタスクマネージャは負荷分散サーバーおよび各自のデータを重複排除するクライアントからの接続すべてを管理します。接続およびタスクマネージャは以下のことを行う機能とスレッドのセットです。 ■ すべてのクライアントで使用するスレッドプールを提供する。 ■ 各クライアント接続のためのタスクを保持する。 ■ 操作に基づいて Deduplication Engine のモードを管理する。操作とはバックアップ、復元、キュー処理、その他です。
データ整合性検査	NetBackup Deduplication Engine はデータの整合性を調べ、整合性の問題を解決します。 p.518 の「MSDP データ整合性チェックについて」を参照してください。
データストアマネージャ	データストアマネージャはデータコンテナファイルすべてを管理します。データストアマネージャは以下のことを行う機能とスレッドのセットです。 ■ データストアにデータをバックアップするトランザクション機能。 ■ データストアからデータを読み込む機能。 ■ データストアの領域を再利用再生するトランザクションの機能(すなわち、コンテナの小型化とコンテナの削除)。 コンテナの ID は固有です。データストアマネージャは作成されたそれぞれの新しいコンテナでコンテナ数を増分します。コンテナのデータは決して上書きされず、コンテナ ID は決して再利用されません。 p.487 の「MSDP コンテナファイルについて」を参照してください。
インデックスキャッシュマネージャ	インデックスキャッシュマネージャはフィンガープリントキャッシュを管理します。キャッシュによって、フィンガープリントの参照速度が向上します。 p.72 の「MSDP フィンガープリントのキャッシュについて」を参照してください。
キューの処理	NetBackup Deduplication Engine はトランザクションキューを処理します。 p.517 の「MSDP キュー処理について」を参照してください。
Reference Database Engine	参照データベースエンジンは、読み取り元や書き込み先参照などのデータセグメントを指す参照を保存します。一度に操作するデータベースは一つです。

コンポーネント	説明
Reference Database Manager	参照データベース管理プログラムはコンテナ参照のすべてを管理します。単一のデータベースファイルを操作するトランザクション機能を提供します。

メディアサーバーの重複排除バックアップ処理

図 13-2 に、メディアサーバーがバックアップを重複排除するときのバックアップ処理を示します。宛先はメディアサーバー重複排除プールです。説明を次に示します。

図 13-2　　メディアサーバーの重複排除処理



次に、メディアサーバーによるバックアップの重複排除で、宛先がメディアサーバー重複排除プールである場合のバックアップ処理を示します。

- NetBackup Job Manager (nbjm) によって、Backup Restore Manager (bpbrm) がメディアサーバー上で起動します。
- Backup Restore Manager は、メディアサーバー上の bptm プロセスとクライアント上の bpbkar プロセスを開始します。
- クライアントの Backup Archive Manager (bpbkar) は、バックアップイメージを生成し、これらをメディアサーバーの bptm プロセスに移動します。
  また、Backup Archive Manager はイメージ内のファイルについての情報を Backup Restore Manager (bpbrm) に送ります。Backup Restore Manager は NetBackup データベース用のプライマリサーバーの bpdbm 処理にファイル情報を送ります。
- bptm プロセスは、データを重複排除プラグインに移動します。
- 重複排除プラグインは、NetBackup 重複排除エンジンからコンテナファイルの ID のリストを取り込みます。それらのコンテナファイルには、クライアントの最後の完全バックアップからの指紋が含まれます。このリストをキャッシュとして使用することで、プラグインがエンジンの各指紋を要求する必要がなくなります。

- 重複排除プラグインはバックアップイメージのファイルをセグメントに分割します。
- 重複排除プラグインは、セグメントをバッファ処理してから重複排除マルチスレッドエージェントにそれらのバッチを送信します。データ転送には複数のスレッドと共有メモリが使われます。
- NetBackup 重複排除マルチスレッドエージェントは、スループットパフォーマンスを改善するために複数のスレッドを使ってデータセグメントを並列で処理します。その後、エージェントは重複のないデータセグメントのみを NetBackup 重複排除エンジンに送信します。
  ホストが負荷分散サーバーである場合、重複排除エンジンは別のホスト、ストレージサーバーにあります。
- NetBackup 重複排除エンジンは、データをメディアサーバー重複排除プールに書き込みます。
  最初のバックアップでは、重複排除率が 0% になる場合があります。0% は、バックアップデータ内のすべてのファイルセグメントが一意であることを意味します。

MSDP クライアントコンポーネント

表 13-3 に、クライアントの重複排除コンポーネントを示します。

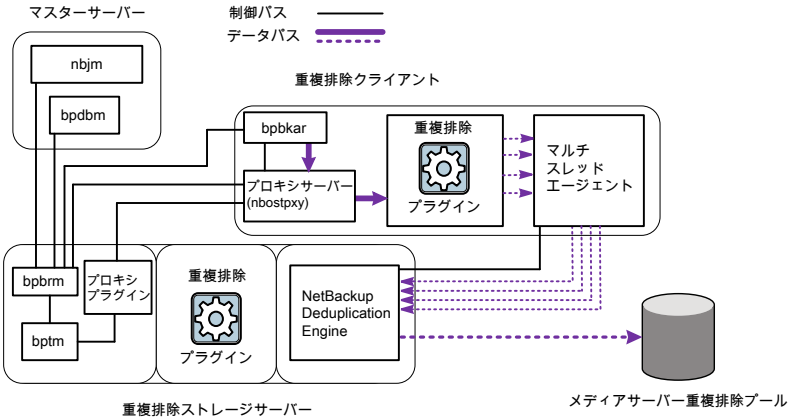
表 13-3　クライアントの MSDP コンポーネント

コンポーネント	説明
重複排除プラグイン	重複排除プラグインを使用して、次のことを実行できます。 ■ ファイルの内容からファイルのメタデータを分離します。 ■ 内容を重複排除します (ファイルをセグメントに分割します)。 ■ 必要に応じて、バックアップ用データを圧縮し、リストア用バックアップを解凍します。 ■ 必要に応じて、バックアップ用データを暗号化し、リストア用バックアップを復号します。
マルチスレッドエージェント	NetBackup 重複排除マルチスレッドエージェントは、非同期ネットワーク I/O と CPU コア計算に対して複数のスレッドを使います。エージェントはストレージサーバー上、負荷分散サーバー上、自身のデータを重複排除するクライアント上で実行されます。 p.65 の「MSDP 重複排除マルチスレッドエージェントについて」を参照してください。
プロキシサーバー	OpenStorage プロキシサーバー (nbostpxy) は、ストレージサーバー上のプロキシプラグインとの制御通信を管理します。

MSDP クライアント側の重複排除バックアップ処理

図 13-3 に、クライアント独自のデータを重複排除するクライアントのバックアップ処理を示します。宛先はメディアサーバー重複排除プールです。説明を次に示します。

図 13-3　　重複排除プールへの MSDP クライアントのバックアップ



次のリストに、MSDP クライアントのメディアサーバー重複排除プールへのバックアップ処理を示します。

- NetBackup Job Manager (nbjm) によって、Backup Restore Manager (bpbrm) がメディアサーバー上で起動します。
- Backup Restore Manager によってクライアントが調べられ、そのクライアントが構成済みであり、重複排除の準備が完了しているかどうかが判別されます。
- クライアントの準備が完了している場合は、Backup Restore Manager によってクライアント上の OpenStorage プロキシサーバー (nbostpxy) およびクライアント上のデータ移動プロセス (bpbkar) およびメディアサーバー上の bptm が開始されます。
  NetBackup では、メディアサーバー上のプロキシのプラグインを使用して、bptm から nbostpxy に制御情報をルーティングします。
- Backup Archive Manager (bpbkar) は、バックアップイメージを生成し、共有メモリによってこれらをクライアントの nbostpxy プロセスに移動します。
  また、Backup Archive Manager はイメージ内のファイルについての情報を Backup Restore Manager (bpbrm) に送ります。Backup Restore Manager は NetBackup データベース用のプライマリサーバーの bpdbm 処理にファイル情報を送ります。
- クライアントの nbostpxy プロセスは、データを重複排除プラグインに移動します。
- クライアント上の重複排除プラグインは以下の順で指紋のリストの取り込みを試行します。

- クライアントの pd.conf ファイルで構成されているクライアントとポリシーから。
  FP_CACHE_CLIENT_POLICY エントリは指紋キャッシュに使うクライアントとポリシーを定義します。エントリは有効である (つまり、期限切れでない) 必要があります。
  p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。
- クライアントとポリシーの以前のバックアップから。
- ストレージサーバーの特別なシードディレクトリから。
  p.74 の「リモートクライアント重複排除の MSDP フィンガープリントキャッシュのシードについて」を参照してください。

指紋のリストをキャッシュとして使用することで、プラグインがエンジンの各指紋を要求する必要がなくなります。
指紋がキャッシュにロードされない場合、バックアップの重複排除率は非常に低いことがあります。

- 重複排除プラグインはバックアップイメージのファイルをセグメントに分割します。
- 重複排除プラグインは、セグメントをバッファ処理してから重複排除マルチスレッドエージェントにそれらのバッチを送信します。データ転送には複数のスレッドと共有メモリが使われます。
- NetBackup 重複排除マルチスレッドエージェントは、スループットパフォーマンスを改善するために複数のスレッドを使ってデータセグメントを並列で処理します。その後、エージェントは重複のないデータセグメントのみを NetBackup 重複排除エンジンに送信します。
- NetBackup 重複排除エンジンは、データをメディアサーバー重複排除プールに書き込みます。
  最初のバックアップでは、重複排除率が 0% になる場合があります。0% は、バックアップデータ内のすべてのファイルセグメントが一意であることを意味します。

14

ユニバーサル共有の構成と管理

この章では以下の項目について説明しています。

ユニバーサル共有の概要

このセクションでは、ユニバーサル共有の概要、ユニバーサル共有の機能と主な利点、およびユニバーサル共有のしくみについて説明します。

ユニバーサル共有の概要

ユニバーサル共有機能は、NFS または CIFS (SMB) 共有を使用して既存の NetBackup 重複排除プール (MSDP) またはサポート対象の Cohesity アプライアンスにデータを取り込みます。

ユニバーサル共有と MSDP の両方で、重複排除と圧縮を使用します。

スペース効率は、このデータを既存の NetBackup ベースのメディアサーバー重複排除プールに直接格納することで実現されます。

主な利点

次に、ユニバーサル共有の主な利点について簡単に説明します。

- NAS ベースのストレージターゲット
  従来の NAS ベースのストレージターゲットとは異なり、ユニバーサル共有は、SLP (ストレージライフサイクルポリシー) を含む、NetBackup によるすべてのデータ保護および管理機能を提供します。
- データベースダンプの場所
  ユニバーサル共有は、領域を節約した (重複排除した) ダンプの場所を提供し、さらに、データの保持、レプリケーション、クラウドテクノロジとの直接統合といった NetBackup テクノロジと直接統合できます。
- コストと時間の節約
  ユニバーサル共有を使用すると、サードパーティの中間ストレージを購入して保守する必要がなくなります。通常、このストレージを使用すると、データを 2 回移動する必要があるため、必要な I/O スループットが 2 倍になります。また、ユニバーサル共有では、価値の高いアプリケーションやデータベースのデータを保護するための所要時間が半分に短縮されます。
- 保護ポイント
  ユニバーサル共有の保護ポイントは、共有に存在するすべてのデータの高速なポイントインタイムコピーを提供します。このデータのコピーは、NetBackup 内で保護されているその他のデータと同様に保持できます。ユニバーサル共有内のすべてのデータで、自動イメージレプリケーション (A.I.R.)、ストレージライフサイクルポリシー、最適化複製、クラウド、テープなど、すべての高度な NetBackup データ管理機能を利用できます。
- CDM (コピーデータ管理)
  ユニバーサル共有の保護ポイントは、強力な CDM ツールも提供します。すべての保護ポイントの読み取り/書き込みコピーは「プロビジョニング」でき、NAS (CIFS/NFS) ベースの共有を介しても利用できます。すべての保護ポイントのプロビジョニングされたコピーは、インスタントリカバリや、プロビジョニングされた保護ポイントのデータへのアクセスなど、一般的な CDM アクティビティに使用できます。たとえば、以前にユニバーサル共有にダンプされたデータベースは、プロビジョニングされた保護ポイントから直接実行できます。
- クライアントソフトウェアなしのバックアップおよびリストアと任意のクライアントへのリストア
  ユニバーサル共有のバックアップまたはリストアには、クライアントソフトウェアは不要です。ユニバーサル共有を任意のクライアントにリストアすることもできます。ユニバー

サル共有は、NFS または CIFS をサポートする POSIX 準拠のオペレーティングシステムと連携して動作します。

ユニバーサル共有を使用する方法

ユニバーサル共有機能は、NetBackup のソフトウェアのみの配備に加えて、サポート対象の Cohesity アプライアンス用のネットワーク接続ストレージ (NAS) オプションを提供します。従来の NAS 製品は、重複排除されない通常のディスクの場所にデータを格納します。ユニバーサル共有内のデータは、スペース効率が高く重複排除された状態で、冗長性の高いストレージに配置されます。このリポジトリに使用される重複排除テクノロジは、標準のクライアントベースのバックアップで使用されるのと同じ MSDP の場所です。

ユニバーサル共有に格納されているデータはすべて MSDP に自動的に配置され、自動的に重複排除されます。その後、このデータは以前にメディアサーバーの MSDP の場所に取り込まれた他のすべてのデータと照らして重複排除されます。一般的な MSDP の場所にはさまざまな種類のデータが格納されるので、ユニバーサル共有では重複排除の効率が大幅に向上します。保護ポイント機能を使用することで、指定したユニバーサル共有に存在するデータのポイントインタイムコピーを作成できます。保護ポイントが作成されると、NetBackup はその時点のデータを自動的にカタログ化し、NetBackup に取り込まれた他のデータと同様に管理します。保護ポイントは、MSDP にすでに存在するユニバーサル共有のデータのみをカタログ化するため、データの移動は行われません。したがって、保護ポイントの作成プロセスは非常に高速です。

クライアントサポート

ユニバーサル共有機能は、さまざまなクライアントとデータの種類をサポートします。共有がマウントされているクライアントに、NetBackup ソフトウェアは不要です。POSIX 準拠のファイルシステムを使用し、CIFS または NFS ネットワーク共有をマウントできるオペレーティングシステムはすべてユニバーサル共有にデータを書き込めます。ユニバーサル共有に取り込まれたデータは、メディアサーバー重複排除プール (MSDP) に直接書き込まれます。データを標準のディスクパーティションに書き込み、その後に重複排除プールに移動する追加の手順やプロセスは不要です。

ユニバーサル共有を構成するための MSDP の独自の (BYO) サーバーの構成と使用

表 14-1では、ユニバーサル共有用に MSDP の独自の (BYO) サーバーを設定する大まかな手順について説明します。(アプライアンスでは、ストレージを構成するとすぐにユニバーサル共有機能を使用できます。) 詳しくは、リンク付きのトピックを参照してください。

表 14-1 ユニバーサル共有を構成するための MSDP の独自の (BYO) サーバーの構成と使用の手順

手順	説明
1	コンピュータを識別します。MSDP の BYO サーバーが前提条件とハードウェア要件を満たしていることを確認します。 p.559 の「ユニバーサル共有を構成するための独自の (BYO) サーバーにおける前提条件とハードウェア要件」を参照してください。
2	NetBackup Web UI で、ユニバーサル共有を作成します。『NetBackup Web UI 管理者ガイド』の「ユニバーサル共有の作成」を参照してください。
3	NetBackup Web UI から作成したユニバーサル共有をマウントします。p.583 の「ユニバーサル共有のマウント」を参照してください。
4	ユニバーサル共有のバックアップポリシーを構成します。
5	必要に応じ、取り込みモードを使用してデータをダンプするか、作業負荷から NFS/CIFS を介してユニバーサル共有にバックアップデータをロードします。 取り込みモードが有効になっている場合、バックアップスクリプトは、バックアップまたはダンプの終了時に、メモリからディスクにすべてのデータをクライアント側で保持するようにユニバーサル共有をトリガします。取り込みモードは、取り込みモードがオフになるまですべての取り込みデータがディスクに保持されることを保証しないため、通常モードよりも高速です。 p.607 の「取り込みモードでのユニバーサル共有へのバックアップデータのロード」を参照してください。
6	ユニバーサル共有のバックアップからリストアします。

ユニバーサル共有を構成するための前提条件

ユニバーサル共有を構成するための前提条件とハードウェア要件があります。要件が満たされたら、ユニバーサル共有用に MSDP の独自の (BYO) サーバーを構成して管理できます。

ユニバーサル共有を構成するための独自の (BYO) サーバーにおける前提条件とハードウェア要件

ユニバーサル共有を構成するための MSDP の独自の (BYO) サーバー機能を使用するための前提条件を次に示します。

- Red Hat Enterprise Linux 7.6 以降を搭載した MSDP の BYO ストレージサーバーでユニバーサル共有機能がサポートされている必要があります。
- ユニバーサル共有機能は、SUSE Linux ではサポートされません。

- ユニバーサル共有のユーザー認証を設定する必要があります。
  p.562 の「ユニバーサル共有のユーザー認証の構成」を参照してください。
- NFS 経由で共有を使用する場合、NFS サービスがインストールされ、実行されている必要があります。
  `nfs-utils` がインストールされていることを確認します。
  - Red Hat: `yum install nfs-utils -y`
  - SUSE: `zypper install yast2-nfs-server -y`
- CIFS または SMB 経由で共有を使用する場合、Samba サービスがインストールおよび実行されている必要があります。
  Linux の `samba` パッケージと `samba winbind` パッケージがインストールされていることを確認します。
  - `yum install samba samba-common samba-winbind samba-winbind-clients samba-winbind-modules -y`
- 対応するストレージサーバーで Samba ユーザーを設定し、クライアントでクレデンシャルを入力する必要があります。
  p.562 の「ユニバーサル共有のユーザー認証の構成」を参照してください。
- `xfsprogs` がインストールされていることを確認します。
  - Red Hat: `yum install xfsprogs -y`
  - SUSE: `zypper install xfsprogs -y`
- SMB 共有に権限を付与するには、次のコマンドが実行されていることを確認します。
  - `setsebool -P samba_export_all_rw on`
  - `setsebool -P samba_export_all_ro on`
- NGINX をインストールして実行します。推奨される最小の NGINX バージョンは 1.24.0 です。
- NGINX のインストール後、ポート 80 の HTTP Web サービスがデフォルトで有効になります。`/etc/nginx/conf.d/default.conf` が必要がない場合は、これを削除するか、HTTP Web サービスを無効にするようにファイルを編集します。
- ストレージサーバーの `/mnt` フォルダが、どのマウントポイントによっても直接マウントされていないことを確認します。マウントポイントはそのサブフォルダに対してマウントされる必要があります。
- MSDP のストレージサーバーを構成したことを確認します。NGINX サービスをインストールせずにストレージを構成またはアップグレードした後に、BYO でユニバーサル共有機能を構成する場合は、ストレージサーバーで次のコマンドを実行します。
  `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

- 必要なネットワークポートが開いていることを確認します。
  『NetBackup ネットワークポートリファレンスガイド』の「NetBackup メディアサーバーのポート」を参照してください。

表 14-2　ユニバーサル共有用の独自の (BYO) サーバーのハードウェア構成要件

CPU	メモリ	ディスク
■ 2.2 GHz 以上のクロックレート。 ■ 64 ビットのプロセッサ。 ■ 最小 4 コア。8 コアを推奨。64 TB のストレージの場合、Intel x86-64 アーキテクチャでは 8 つのコアを必要とします。 ■ CPU 構成で VT-X オプションを有効にします。	■ 16 GB (8 TB から 32 TB のストレージの場合は、ストレージ 1 TB ごとに 1 GB の RAM)。 ■ 32 TB 以上のストレージの場合は 32 GB の RAM。 ■ ライブマウントごとに追加の 500 MB の RAM。	ディスクのサイズは、バックアップのサイズによって異なります。NetBackup とメディアサーバー重複排除プール (MSDP) のハードウェアの必要条件を参照してください。 システムに複数のデータパーティションがある場合、すべてのパーティションは同じサイズである必要があります。例: BYO サーバーに 4 TB の最初のパーティションがある場合、すべての追加データパーティションのサイズは 4 TB である必要があります。

NetBackup へのアップグレード

NFS を介してクライアント側のユニバーサル共有にアクセスするときの問題を避けるために、NetBackup にアップグレードする前に、クライアント側のすべての NFS マウントポイントをマウント解除する必要があります。

メモ: CIFS/SMB 共有では、これらの操作は必要ありません。

1. Linux UNIX クライアントにマウントされたすべてのユニバーサル共有をマウント解除します。
2. NetBackup にアップグレードします。
3. NetBackup サービスを起動します。
4. Linux UNIX クライアント上でユニバーサル共有を再度マウントします。

重複排除 Web サービスユーザーと MSDP BYO サーバーのユーザーグループの管理

MSDP を設定すると、デフォルトでユーザー spws とグループ spwsgrp が作成され、SPWS (Storage Platform Web Service) サービスによって使用されます。

SPWS サービスにデフォルトのユーザーとグループを使用しない場合は、MSDP を構成する前後に SPWS サービスを構成できます。

MSDP サーバーを構成する前に SPWS サービスを管理するには

- MSDP ストレージサーバーがまだ構成されていない場合は、MSDP を構成する前にストレージサーバーで次のコマンドを実行します。

  ```
  /usr/openv/pdde/vpfs/bin/spws_config.sh --spwsuser=<spwsuser>
  --spwsgroup=<spwsgroup>
  ```

  MSDP を構成すると、SPWS サービスは指定したユーザーとグループを使用し、spws とグループ spwsgrp は作成されません。

MSDP サーバーを構成した後で SPWS サービスを管理するには

- MSDP ストレージサーバーがすでに構成されていて、ユーザー spws とグループ spwsgrp が作成されている場合は、ストレージサーバーで次のコマンドを実行して、新しいユーザーとグループを指定します。

  ```
  /usr/openv/pdde/vpfs/bin/spws_config.sh --spwsuser=<spwsuser>
  --spwsgroup=<spwsgroup>
  ```

  SPWS サービスは、指定したユーザーとグループを使用するように変更されます。SPWS サービスによって使用されるファイルの所有者も変更されます。

  作成されたユーザー spws とグループ spwsgrp は削除されません。ユーザーとグループは手動で削除できます。

メモ: root ユーザーで spws_config.sh スクリプトを実行する必要があります。これで、/var/run/vpfs/ にログファイルが作成され、システムサービスが構成されます。

ユニバーサル共有のユーザー認証の構成

CIFS/SMB プロトコルを使用して作成されたユニバーサル共有では、次の 3 つのユーザー認証方法がサポートされています。

- Active Directory ベースのユーザー認証
  p.563 の「Active Directory ベースの認証」を参照してください。
- ローカルユーザーベースの認証
  p.565 の「ローカルユーザーベースの認証」を参照してください。
- Kerberos ベースの認証

p.566 の「Kerberos ベースの認証」を参照してください。

Active Directory ベースの認証

アプライアンス、Flex Scale、Flex Appliance アプリケーションインスタンス、または MSDP BYO サーバーが Active Directory ドメインに含まれている場合は、この方法を使用できます。

NetBackup Web UI からユニバーサル共有を作成する場合は、Active Directory のユーザーまたはグループを指定できます。この方法では、指定したユーザーまたはグループにのみアクセスが制限されます。ユニバーサル共有がマウントされている Windows クライアントから権限を制御することもできます。詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

アプライアンスで Active Directory のユーザーまたはグループを設定する方法について詳しくは、『NetBackup アプライアンスセキュリティガイド』を参照してください。

ユニバーサル共有は、NFS または SMB プロトコルを使用して作成できます。SMB プロトコルを使用する場合、ADS またはローカルユーザーモードで SMB を設定する必要があります。次の表に、さまざまなプラットフォームの Active Directory を使用してメディアサーバーを構成し、SMB を使用してユニバーサル共有を作成する方法を示します。

表 14-3 さまざまなプラットフォームが Active Directory ドメインに参加するための要件を記述します

プラットフォーム	要件

BYO アプライアンス	BYO の場合、Active Directory ドメインへの参加には `/usr/openv/pdde/vpfs/bin/register_samba_to_ad.sh` が使用されます。
	
	`register_samba_to_ad.sh` の使用例:
	
	`/usr/openv/pdde/vpfs/bin/register_samba_to_ad.sh --domain=<domain> --username=<username>`
	
	`register_samba_to_ad.sh` で使用できるその他のオプションを次に示します。
	
	`--domain=<domain> : domain name`
	`--domaincontroller=<domain controller> : domain controller`
	`--username=<username> : windows domain username which has the privilege to join the client to domain`
	`--help|-h : Print the usage`

プラットフォーム	要件
NetBackup アプライアンス (NBA)	『NetBackup アプライアンス管理者ガイド』の「Active Directory サーバー構成の追加」セクションを確認してください。
Flex メディアサーバー	BYO と同様です。
Flex メディアサーバー	BYO と同様です。

WORM 対応ストレージサーバー	ストレージサーバーは、制限付きシェルコマンドを使用して Active Directory に参加または離脱するように構成できます。
	
	`[msdp-16.0] hostname >`
	`setting ActiveDirectory`
	`configure ad_server=<ad_server>`
	`domain=<domain_server>`
	`domain_admin=<domain_adin>`
	
	p.668 の「ユニバーサル共有とインスタントアクセスのための WORM または MSDP ストレージサーバーへの Active Directory ドメインの接続」を参照してください。

Flex Scale	『NetBackup Flex Scale 管理者ガイド』の「ユニバーサル共有とインスタントアクセスのための AD サーバーの構成」セクションを確認してください。
AKS/EKS AD	NetBackup は SMB ローカルユーザーモードのみをサポートします。SMB サーバーは、デフォルトでローカルユーザーモードで構成されています。

ストレージサーバーが Active Directory ドメインに追加されると、ユニバーサル共有を通常どおりに作成できます。指定したユーザーとユーザーグループは、`wbinfo` コマンドを使用して検証されます。次の手順では、Active Directory にユニバーサル共有を追加する方法について説明します。

Active Directory へのユニバーサル共有の追加

1. NetBackup Web UI を開きます。
2. SMB プロトコルを使用してユニバーサル共有を作成します。
3. Windows クライアントで共有ストレージをマウントします。

   必要なすべてのクレデンシャルを指定します。
4. ユニバーサル共有が完全に設定され、ユニバーサル共有ポリシーを使用してバックアップおよびリストアできることを確認します。

Active Directory に Microsoft SQL Server インスタントアクセスを追加するには、次の要件があります。

- ストレージサーバーとクライアントは同じドメインにある必要があります。
- Microsoft SQL Server クライアントにログオンするには、必要な権限を持つドメインユーザーアカウントが必要です。
- Web UI で、ドメインユーザーに Microsoft SQL Server インスタンスを登録します。
- 『NetBackup for Microsoft SQL Server 管理者ガイド』の SQL Server インスタンスの手動での追加に関する説明を参照してください。
- インスタントアクセスを使用するには、ドメインユーザーのクレデンシャルが必要です。

ローカルユーザーベースの認証

対応するストレージサーバーで SMB ユーザーを設定し、クライアントでクレデンシャルを入力する必要があります。

SMB サービスが Windows ドメインに参加している場合、Windows ドメインユーザーは SMB 共有を使用できます。この場合、共有へのアクセスにクレデンシャルは不要です。

メモ: AKS (Azure Kubernetes Service) と EKS (Amazon Elastic Kubernetes Service) クラウドプラットフォームの場合、SMB ローカルユーザーのみが SMB 共有にアクセスできます。SMB 共有にアクセスするには、SMB ユーザーを追加する必要があります。

SMB サービスが Windows ドメインに参加していない場合は、次の手順を実行します。

- NetBackup Appliance の場合:
  NetBackup アプライアンスの場合、ローカルユーザーは SMB ユーザーでもあります。ローカルユーザーを管理するには、CLISH にログインし、[Main]、[Settings]、[Security]、[Authentication]、[LocalUser]の順に選択します。SMB パスワードは、ローカルユーザーのログインパスワードと同じです。
- MDSP の BYO サーバーの場合:
  MDSP の BYO サーバーで、Linux ユーザーが存在しない場合は作成します。次に、SMB にユーザーを追加します。
  たとえば、次のコマンドを実行すると、SMB サービス専用のユーザー名が作成されます。

  ```
  adduser --no-create-home -s /sbin/nologin <username>
  ```

  ```
  smbpasswd -a <username>
  ```

  SMB サービスに既存のユーザーを追加するには、次のコマンドを実行します。

  ```
  smbpasswd -a username
  ```

- Flex アプライアンスのプライマリまたはメディアサーバーアプリケーションインスタンスの場合:

Flex アプライアンスのプライマリまたはメディアサーバーアプリケーションインスタンスの場合、インスタンスにログインし、次のようにローカルユーザーを SMB サービスに追加します。

- 必要に応じて、次のコマンドを使用して新しいローカルユーザーを作成します。

  ```
  useradd <username>
  passwd <username>
  ```

  既存のローカルユーザーを使用することもできます。

- 次のコマンドを実行して SMB サービスのユーザークレデンシャルを作成し、ユーザーを有効にします。

  ```
  smbpasswd -a <username>
  smbpasswd -e <username>
  ```

- WORM ストレージサーバーアプリケーションインスタンスの場合:
  WORM ストレージサーバーインスタンスの場合は、インスタンスにログインし、次のコマンドを使用してローカル SMB ユーザーを追加します。`setting smb add-user username=<username> password=<password>`
  `setting smb list-users` コマンドを使用して新しいユーザーを表示できます。
  ユーザーを削除するには、`setting smb remove-user username=<username>` コマンドを実行します。
- AKS および EKS クラウドプラットフォームの場合:
  - `kubectl` を使用してクラスタの MSDP エンジンポッドにログインします。
  - 次のコマンドを実行して、MSDP エンジンの制限付きシェルにログインします。
    `su - msdpadm`
  - 次の制限付きシェルコマンドを実行して、SMB ユーザーを追加します。
    `setting smb add-user username=<username>`
    次に例を示します。
    `msdp-16.1] > setting smb add-user username=<username>`
    同じコマンドを使用して、既存のユーザーのパスワードを更新できます。
    AKS および EKS クラウドプラットフォームでは、SMB の制限付きシェルコマンドによって、クラスタ内のすべての MSDP エンジンに SMB サーバーが構成されます。

Kerberos ベースの認証

ユニバーサル共有に Kerberos ベースの認証を使用して、クライアントとサーバー間の接続を保護します。ユニバーサル共有構成では、すべての Kerberos セキュリティタイプ krb5、krb5i、krb5p がサポートされます。

ユニバーサル共有の Kerberos 認証を構成するには、次の手順に従う必要があります。

表 14-4

手順	作業	説明
1.	Active Directory ベースの認証を構成します。	Active Directory ドメインにストレージサーバーを追加する方法について詳しくは、p.563 の「Active Directory ベースの認証」を参照してください。
2.	Windows Active Directory ドメインサーバーで、Kerberos 認証用に Active Directory ユーザーを作成します。	p.567 の「Kerberos 認証用の Active Directory ユーザーの作成 」を参照してください。
3.	Kerberos プリンシパルを KDC データベースに登録します。	p.568 の「Kerberos プリンシパルの KDC データベースへの登録」を参照してください。
4.	サーバーで Kerberos ベースの認証を構成します。	p.568 の「サーバーおよびクライアントでの Kerberos ベースの認証の構成」を参照してください。

Kerberos 認証用の Active Directory ユーザーの作成

ストレージサーバーを Active Directory ドメインに追加した後、NetBackup Web UI でユニバーサル共有の Kerberos ベースの認証を構成する前に、次のタスクを実行します。

- Windows Active Directory ドメインサーバーで、Kerberos 認証用に Active Directory ユーザーを作成します。
- Kerberos プリンシパルを KDC (キー配布センター) データベースに登録します。p.568 の「Kerberos プリンシパルの KDC データベースへの登録」を参照してください。

Kerberos 認証用の Active Directory ユーザーを作成する方法

1. Windows Active Directory ドメインサーバーにログインします。
2. [スタート]、[管理ツール]、[Active Directory ユーザーとコンピュータ]の順にクリックします。
3. 左ペインで、正しいドメイン名を選択し、[ユーザー]を選択します。
4. [ユーザー]を右クリックし、[新規]、[ユーザー]の順に選択します。

5 ドメインユーザー情報を入力します。ユーザーログオン名は、Active Directory ドメインのログインと認証に使用されます。

ストレージサーバーの場合、ログオン名は *nfs/<storage server FQDN>* である必要があります。ここで、*nfs* は NFS サービスプリンシパルで、*storage server* はユニバーサル共有が作成されるホストです。たとえば、*nfs/storage-server.mydomain.com* です。

ユニバーサル共有サーバーの場合は、1 人以上のユーザー *host/<storage server FQDN>* を作成します。

ユニバーサル共有サーバーの場合、*nfs/<storage server FQDN>* と *host/<storage server FQDN>* の 2 人の Active Directory ユーザーを作成する必要があります。ユニバーサル共有クライアントの場合、1 人のユーザー *host/<universal share client FQDN>* のみを作成します。

6 新しいユーザーのパスワードを設定します。

7 [完了]をクリックして、ユーザーの作成を終了します。

8 作成したユーザーをダブルクリックして、プロパティウィンドウを開きます。

9 [アカウントオプション]リストで、AES 128 と AES 256 の暗号化項目を選択します。

Kerberos プリンシパルの KDC データベースへの登録

Kerberos 認証用の Active Directory ユーザーが作成されたら、Kerberos プリンシパルを KDC データベースに登録します。

Kerberos プリンシパルを KDC データベースに登録する方法

◆ コマンドラインを開き、`ktpass` コマンドを実行してプリンシパルを KDC データベースに登録します。

次に例を示します。

```
ktpass -princ nfs/storage-server.mydomain.com@MYDOMAIN.COM
-mapuser MYDOMAIN¥username -pass <password> -ptype
KRB5_NT_PRINCIPAL -crypto All -out storage-server.keytab
```

ここで `MYDOMAIN¥username` は、ユーザーのプロパティページのユーザーログオン名 (Windows 2000 より前) です。

メモ: パスワードは、Active Directory ユーザーのパスワードである必要があります。それ以外の場合は、以前のパスワードが変更されます。

サーバーおよびクライアントでの Kerberos ベースの認証の構成

NetBackup BYO、Flex メディアサーバー、Flex WORM、Flex Scale の Kerberos ベースの認証を構成できます。

サーバーおよびクライアントの両方で Kerberos ベースの認証を構成する必要があります。

NetBackup BYO 環境では、NetBackup サーバーとクライアントで Kerberos 認証を構成する前に、必要な krb5 パッケージがシステムにインストールされているかどうかを確認します。次のコマンドを実行して、これらのパッケージがインストールされているかどうかを確認します。

```
yum install krb5-workstation
```

```
pam_krb5 -f
```

サーバーで Kerberos ベースの認証を構成する方法

- NetBackup サーバーで、vpfs_nfs_krb.sh スクリプトを実行して Kerberos プリンシパルの keytab エントリを作成します。

  ```
  /usr/openv/pdde/vpfs/bin/vpfs_nfs_krb.sh
  ```

  NetBackup BYO の場合、コマンドウィンドウでスクリプトを実行します。Flex メディアサーバーの場合は、メディアサーバーインスタンスにログインし、sudo を使用してスクリプトを実行する必要があります。

  - キーエントリを追加します。
    ```
    ./vpfs_nfs_krb.sh add --user nfs/storage-server.mydomain.com
    ```
  - キーエントリを削除します。
    ```
    ./vpfs_nfs_krb.sh delete --user nfs/storage-server.mydomain.com
    ```
  - Kerberos プリンシパルのログインを確認します。
    ```
    ./vpfs_nfs_krb.sh verify --user nfs/storage-server.mydomain.com
    ```
  - Kerberos プリンシパルのパスワードを更新します。
    ```
    ./vpfs_nfs_krb.sh update --user nfs/storage-server.mydomain.com
    ```
  - キーエントリを表示します。
    ```
    ./vpfs_nfs_krb.sh list
    ```
  - Kerberos 認証に関連する構成を表示します。
    ```
    ./vpfs_nfs_krb.sh status
    ```

  Flex WORM と Flex Scale の場合、これらのコマンドを実行するには WORM または MSDP エンジンの制限付きシェルにログインする必要があります。

  - キーエントリを追加します。
    ```
    setting SecureNfs add-krb-user
    krbuser=nfs/storage-server.mydomain.com
    ```
  - キーエントリを削除します。
    ```
    setting SecureNfs delete-krb-user
    krbuser=nfs/storage-server.mydomain.com
    ```

- Kerberos プリンシパルのログインを確認します。

```
setting SecureNfs verify-krb-user
krbuser=nfs/storage-server.mydomain.com
```

- Kerberos プリンシパルのパスワードを更新します。

```
setting SecureNfs update-krb-user
krbuser=nfs/storage-server.mydomain.com
```

- キーエントリを表示します。

```
setting SecureNfs list-krb-users
```

- Kerberos 認証に関連する構成を表示します。

```
setting SecureNfs nfs-secure-status
```

nfs/storage-server.mydomain.com プリンシパルと *host/storage-server.mydomain.com* プリンシパルの両方をストレージサーバーの `/etc/krb5.keytab` に追加する必要があります。

Flex Scale の場合、すべての MSDP エンジンに対して *nfs/storage-server.mydomain.com* と *host/storage-server.mydomain.com* プリンシパルの両方を作成する必要があります。ここで、*storage-server* は、Flex Scale Web UI で構成されている MSDP エンジンのホスト名です。これらの名前は、NetBackup Web UI の［監視 (Monitor)］、［NetBackup］、［ストレージサーバーリスト (Storage servers list)］で確認できます。これらのプリンシパルはすべて、MSDP シェルコマンドを実行して `krb5.keytab` ファイルに追加する必要があります。各エンジンの `/etc/krb5.keytab` ファイルには、クラスタ内のすべてのエンジンに対して作成されたすべてのプリンシパルのキーエントリが含まれています。

複数 VLAN 環境の場合、ストレージサーバーは複数の IP を持つことがあります。セカンダリ VLAN にあるクライアントからユニバーサル共有をマウントする必要がある場合は、ストレージサーバーとクライアントの他の FQDN が DNS に追加され、対応する Active Directory ユーザーが作成されて、Kerberos プリンシパルとして登録されていることを確認します。キーエントリも `/etc/krb5.keytab` ファイルに追加する必要があります。

ユニバーサル共有クライアントで Kerberos ベースの認証を構成する方法

1 Kerberos 認証用に /etc/krb5.conf ファイルを作成します。

ユニバーサル共有が構成されているストレージサーバーから /etc/krb5.conf ファイルをコピーできます。

メモ: krb5.conf ファイルに kdc セクションが定義されている場合は、/etc/krb5.conf ファイルと共に kdc.conf ファイルをコピーします。

---

2 /etc/sysconfig/nfs ファイルで SECURE_NFS を有効にします。

/etc/sysconfig/nfs 構成ファイルに行 SECURE_NFS=yes を追加します。

次のコマンドを実行してサービスを再起動します。

```
systemctl restart nfs-secure
```

メモ: この構成は Red Hat 7 以前のバージョンでのみ必要です。Red Hat 8 と 9 では、この手順は必要ありません。

---

3 Kerberos プリンシパル用の keytab エントリを作成します。

次の 2 つの方法のいずれかを使用して、keytab ファイルを構成できます。

- ストレージサーバーから vpfs_nfs_krb.sh スクリプトをコピーし、そのスクリプトを実行して keytab ファイルを構成します。
- ユニバーサル共有クライアントの Active Directory ユーザーが作成されたら、ktpass ユーティリティを実行して Kerberos プリンシパルの keytab を生成します。
  次に、keytab ファイルを NFS クライアントの /etc フォルダにコピーし、その名前を /etc/krb5.keytab に変更します。

メモ: ユニバーサル共有クライアントに既存の /etc/krb5.keytab ファイルがある場合は、vpfs_nfs_krb.sh スクリプトを使用してキーエントリを追加します。

スクリプト vpfs_nfs_krb.sh では、ユニバーサル共有の構成に関連する操作についてのログを書き込むことができます。ログはユニバーサル共有サーバーでのみ利用可能です。

ログは次の場所にあります: /<storage path>/log/vpfs/yymmdd_*_vpfs_nfs_krb.log

ユニバーサル共有の管理

ユニバーサル共有を NetBackup Appliance、Flex Appliance、Flex Scale、Flex WORM/非 WORM、MSDP AKS/EKS の配備、BYO (build-your-own)、BYO-In-Cloud サーバーにわたって管理できます。ユニバーサル共有を作成、表示、編集、または削除できます。

ユニバーサル共有の作成

ユニバーサル共有は、効率的な領域である SMB (CIFS) または NFS 共有にデータを直接取り込む機能を提供します。領域の効率は、このデータを既存の NetBackup 重複排除プール (MSDP) に直接格納することで達成されます。共有をマウントするクライアントに NetBackup ソフトウェアをインストールする必要はありません。POSIX 準拠のファイルシステムを実行し、SMB (CIFS) または NFS ネットワーク共有をマウントできるオペレーティングシステムは、すべてユニバーサル共有にデータを書き込めます。

オブジェクトストアを使用してユニバーサル共有を作成する場合は、最初にストレージサーバーを作成してからクラウドボリュームを作成する必要があります。ユニバーサル共有を作成するときに、作成したクラウドボリュームを選択します。

ユニバーサル共有を含む特定のストレージサーバーを表示する場合は、右上の[ストレージサーバーの選択 (Select storage server)]をクリックします。次に、ユニバーサル共有を含むストレージサーバーを選択すると、それらが表に表示されます。

NetBackup Web UI でユニバーサル共有を作成するには

1. 必要に応じて、MSDP ストレージサーバーを構成します。

   p.261 の「 NetBackup Web UI でのメディアサーバー重複排除プールストレージサーバーの作成 」を参照してください。

2. 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。

3. [ユニバーサル共有 (Universal Shares)]タブをクリックします。次に[追加 (Add)]をクリックします。

4. 次の必須情報を入力します。

   - [表示名 (Display name)]を入力します。この名前は、ユニバーサル共有パスで使用されます。
   - [タイプ (Type)]を選択します。[クラウドキャッシュのプロパティ (Cloud cache properties)]を設定する場合は、[標準 (Regular)]を選択する必要があります。[アクセラレータ (Accelerator)]タイプを選択した場合は、[ディスクボリューム (Disk volume)]を指定する必要があります。
     ローカルディスクストレージにデータを送るか、クラウドに直接データを送る場合は、種類として[クラスタ (Cluster)]を選択します。

- ストレージサーバーを選択します。
- ディスクボリュームを選択します。
  [タイプ (Type)]で[アクセラレータ (Accelerator)]を選択した場合は、MSDP ストレージサーバーで構成されたクラウドディスクボリュームのみを選択できます。
  検索アイコンをクリックしてボリュームリストを取得し、ディスクボリュームを選択します。デフォルトで PureDiskVolume が選択されます。
  このオプションは、クラウド機能のオブジェクトストレージを使用するユニバーサル共有が有効な場合にのみ利用可能です。
- [クラウドキャッシュのプロパティ (Cloud cache properties)]の[クラウドキャッシュディスク容量の要求 (Request cloud cache disk space)]でローカルディスクキャッシュのサイズを指定します。
  [クラウドキャッシュディスク容量の要求 (Request cloud cache disk space)]をここで設定できるのは、初期設定時のみです。以降の変更は、ストレージサーバーのプロパティページで行う必要があります。

メモ: ストレージサーバーのプロパティページで[クラウドキャッシュのプロパティ (Cloud cache properties)]設定を更新すると、現在の共有マウントが中断します。[保存 (Save)]をクリックすると、`vpfsd` プロセスが再開されて新しい値が適用されます。

さらに、利用可能なサイズが 128 GB 未満の場合は、新しいユニバーサル共有を作成できません。

- [プロトコル (Protocol)]: NFS または SMB (CIFS) を選択します。
  Oracle データベースの標準 NFS を介した NAS (ネットワーク接続ストレージ) のパフォーマンスを改善するには、[Direct NFS]チェックボックスにチェックマークを付けます。Direct NFS を使用すると、NFS サーバーのエクスポートパスに[安全でない (insecure)]エクスポートオプションが追加されます。
  例: `/mnt/vpfs_shares/dnfs/dnfs client-abcd(rw,insecure,mp,fsid=4161bb04-f62f-40f3-af09-0d9a8713694b)`
  p.577 の「Direct NFS (Network File System) を使用してネットワーク接続ストレージのパフォーマンスを向上する」を参照してください。
- 種類として[クラスタ (Cluster)]を選択した場合は、エクスポートされたストレージサーバーを選択します。
  エクスポートされたストレージサーバーは、ユニバーサル共有のエクスポートパスをクライアントへのエクスポートに使用できるサーバーです。
  複数のサーバーを選択することもできます。
- 共有のマウントが許可されている[ホスト (Host)]を指定し、[リストに追加 (Add to list)]をクリックします。ホスト名、IP アドレスまたは範囲、短縮名または FQDN

を使用して、[ホスト (Host)]を指定できます。各共有に対して複数のホストを入力できます。

NetBackup は、一連のルールを使用して、指定したホスト に使用されるワイルドカード文字を検証します。ホストの検証については詳細情報があります。

p.575 の「ユニバーサル共有作成時のホストのワイルドカード検証について」を参照してください。

[タイプ (Type)]で[アクセラレータ (Accelerator)]が選択されている場合、[ホスト (Host)]は FQDN のみにできます。

5 この時点で、残りのフィールドに値を入力するか、[保存 (Save)]をクリックしてユニバーサル共有を保存します。後で、ユニバーサル共有の詳細ページで残りのフィールドを更新できます。

- [クォータの種類 (Quota type)]: ([無制限 (Unlimited)]または[カスタム (Custom)]) を選択します。[カスタム (Custom)]を選択した場合は、クォータも、MB、GB、TB 単位で指定します。
  [カスタム (Custom)]クォータ値は、共有に取り込まれるデータの量を制限します。クォータは、フロントエンド TB (FETB) の計算方法を使用して適用されます。これらは共有ごとに実装され、いつでも変更できます。変更を反映するために共有を再マウントする必要はありません。
  ユニバーサル共有の詳細ページから見積もりの種類または値を更新するには、[クォータ (Quota)]セクションの[編集 (Edit)]をクリックします。
- [ユーザー名 (User names)] (ローカルまたは Active Directory) と[グループ名 (Group names)] (Active Directory のみ) を指定します。指定したユーザーまたはグループのみが共有にアクセスできます。[ユーザー名 (User names)]と[グループ名 (Group names)]は、後で既存のユニバーサル共有の詳細ページから追加および更新できます。

  メモ: 現在、[ユーザー名 (User names)]と[グループ名 (Group names)]は、SMB (CIFS) プロトコルでのみサポートされます。

- 選択したプロトコルが NFS で、選択したストレージサーバーで Kerberos サービスがサポートされている場合は、Kerberos セキュリティ方式を指定します。
  複数の Kerberos セキュリティ方式を選択した場合、クライアントホストからの共有に、任意の方法をマウントコマンドオプションとして指定できます。
  - Kerberos 5
    ローカル UNIX UID と GID の代わりに Kerberos V5 を使用してユーザーを認証します。
  - Kerberos 5i

ユーザー認証に Kerberos V5 を使用し、セキュリティで保護されたチェックサムを使用して NFS 操作の整合性検査を実行し、データの改ざんを防ぎます。

- Kerberos 5p
  ユーザー認証と整合性検査に Kerberos V5 を使用します。NFS トラフィックを暗号化して、トラフィック盗聴を防ぎます。このオプションは最も安全な設定ですが、パフォーマンスのオーバーヘッドも最も多くなります。

メモ: イメージ共有ストレージサーバーは、新しいユニバーサル共有を作成する場合は使用できません。

ユニバーサル共有作成時のホストのワイルドカード検証について

NetBackup は、以下の一連のルールを使用して、ユニバーサル共有を作成するときに指定したホストに使用されるワイルドカード文字を検証します。

ホスト名または FQDN (完全修飾ドメイン名) の検証ルール:

- 単一のホスト名または FQDN を許可します。
- FQDN についてのみ「*」と「?」のワイルドカードを許可します。
  それ以外のワイルドカードは許可しません。
- RFC 標準に従って検証されたホスト名または FQDN を検証します。詳しくは、次のリソースを参照してください。
  https://en.wikipedia.org/wiki/Hostname

IP アドレスまたは IP ネットワーク/範囲の検証ルール:

- 1 つの特定のホストが IP アドレスで指定されている、単一のホストを許可します。
- IP アドレス範囲でのみ「/」を許可します。例: 192.168.0.0/28 は、エクスポートしたファイルシステムにアクセスするため、最初の 16 個の IP アドレス (192.168.0.0 から 192.168.0.15) は許可しますが、192.168.0.16 以上は許可しません。
  それ以外のワイルドカードまたは特殊文字は許可しません。
- 正規表現またはライブラリ関数を使用して、IP アドレス、IP 範囲、FQDN を検証します。

次に、ワイルドカードを使用する有効なホストエントリの例を示します。

```
*.example.com

..example.com

*.vxindia.veritas.com
```

```
*.veritas.com

some.example.com

*.some.example.com

s???me.example.com

s?me.example.com

*.example.com

*.veritas.com

*.example.com

..example.com

*.vxindia.veritas.com

*.veritas.com
```

次の例は無効です。

```
so*me.example.com/

s?me.examp!e.com/

s*me.examp!!!!e.com

so*me.example.com/

s?me.examp!e.com/

s*me.examp!!!!e.com

some.example.com?

some.example.com*

some.example.com?

some.example.com*
```

```
some.ex*ample.com

s*ome.example.com

s*me.example.com

some.example.com?

some.example.com*

some.ex*ample.com

s*ome.example.com

s*me.example.com

*some.example.com
```

MS-Windows、Standard、および Universal-Share ポリシーのインスタントアクセスの使用

非構造化データ資産に対するインスタントアクセスにより、ユーザーは MS-Windows、Standard、または Universal-Share ポリシーを使用して作成されたバックアップイメージからインスタントアクセスマウントを作成できます。

MS-Windows、Standard、または Universal-Share ポリシーを使用してインスタントアクセスを管理するには、ユーザーに RBAC 管理者の役割が必要です。または、類似の権限を持つ役割が必要です。

NetBackup インスタントアクセス API を使用して、ローカルまたはクラウド LSU (論理ストレージユニット) からバックアップコピーに即座にアクセスできます。

NetBackup Web UI または NetBackup インスタントアクセス API を使用して、ユニバーサル共有のバックアップコピーに即座にアクセスできます。

メモ: Flex WORM ストレージでのインスタントアクセスには、次のサービスが必要です: NGINX、NFS、SAMBA、WINBIND (Active Directory が必要な場合)、SPWS、VPFS

Direct NFS (Network File System) を使用してネットワーク接続ストレージのパフォーマンスを向上する

dNFS (Direct Network File System) は、Oracle データベースの標準 NFS を介した NAS (ネットワーク接続ストレージ) のパフォーマンスを改善します。Direct NFS を使用すると、Oracle ソフトウェアは、ストレージサーバーとの通信時にオペレーティングシステ

ムの NFS クライアントをスキップできます。また、Direct NFS は、ストレージへの最大 4 つの並列ネットワークパスをサポートし、これらのパス全体で負荷分散を行うことで、HA (高可用性) と拡張性を向上させます。これらの機能強化により、データベースストレージのコスト削減が実現します。

Direct NFS の要件

- NFS サーバーの書き込みサイズの値 (wsize) は、32768 以上である必要があります。
- NFS マウントポイントは、オペレーティングシステムの NFS クライアントと Direct NFS クライアントの両方によってマウントされる必要があります。
- 次のコマンドを使用して、NFS バッファサイズパラメータである rsize と wsize を少なくとも 1048576 に設定します。

  ```
  rsize and wsize
  nfs_server:/vol/DATA/oradata /mnt/ nfs¥
  rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,vers=3,timeo=600
  ```

- TCP ネットワークバッファサイズが、Direct NFS のパフォーマンスを妨げないだけの十分なサイズであることを確認します。次のコマンドでは、TCP バッファサイズを確認できます。

  ```
  sysctl -a |grep -e net.ipv4.tcp_[rw]mem
  ```

  TCP バッファ出力

  ```
  net.ipv4.tcp_rmem = 4096 87380 1056768
  net.ipv4.tcp_wmem = 4096 16384 1056768
  ```

  バッファサイズを変更するには、`/etc/sysctl.conf` を root として開き、次の値を変更します。

  sysctl.conf

  ```
  net.ipv4.tcp_rmem = 4096 87380 4194304
  net.ipv4.tcp_wmem = 4096 16384 4194304
  ```

  `sysctl -p` を実行する前に、`/etc/rc.d/init.d/network restart` でネットワークを再起動します。

Direct NFS の有効化と無効化

Direct NFS を有効にするには、次のコマンドを実行してデータベースインスタンスを再起動します。

```
cd $ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk dnfs_on
```

Direct NFS を有効にするには、次のコマンドを実行して `oranfstab` ファイルを削除します。

```
cd $ORACLE_HOME/rdbms/lib
```

```
make -f ins_rdbms.mk dnfs_off
```

Direct NFS クライアントの構成

Direct NFS の次のディレクトリで、ファイルの最初に一致するエントリがマウントポイントである oranfstab ファイルを検索します。ファイルを更新してマルチパスを設定し、その他の構成の詳細を処理できます。

- $ORACLE_HOME/dbs
- /var/opt/oracle
- /etc/mnttab

Direct NFS を使用してアクセスする各 NFS サーバーの oranfstab ファイルを作成するには、次のパラメータのリストを使用します。

表 14-5 oranfstab ファイルを作成するためのパラメータ

パラメータ	使用方法
Server	この NFS サーバーの固有の識別子。
Local	データベースホストのネットワークパス (最大 4)。
Path	NFS サーバー上のネットワークパス (最大 4)。
Export	NFS サーバーでエクスポートされたボリューム。
Mount	エクスポートされたボリュームのローカルマウントポイント。
mnt_timeout	最初のマウントを待機する時間 (秒)。
dontroute	発信メッセージのオペレーティングシステムのルーティングは防止されます。
management	NFS サーバー管理インターフェースのネットワークパス。
nfs_version	Direct NFS クライアントが使用する NFS プロトコルのバージョン。
security_default	サーバーエントリのためのエクスポートされたすべての NFS サーバーパスに適用されるデフォルトのセキュリティモード。
security	Direct NFS クライアントで Kerberos 認証プロトコルによってセキュリティを有効にするセキュリティレベル。
community	SNMP クエリーで使用するコミュニティ文字列。

oranfstab ファイルのサンプル出力。

```
server:  myNFSServer1
local: 192.168.1.1 path: 192.168.1.2
```

```
local: 192.168.2.1 path: 192.168.2.2
local: 192.168.3.1 path: 192.168.3.2
local: 192.168.4.1 path: 192.168.4.2
export: /vol/oradata1 mount: /mnt/oradata1
export: /vol/oradata2 mount: /mnt/oradata2
mnt_timeout: 600
```

パス $ORACLE_HOME/bin/oradism に、oradism ファイルを設定していることを確認します。Direct NFS は、この oradism バイナリを使用して、root としてマウントを発行します。このファイルは、各ノードに対してローカルであり、root ユーザーの所有権を持っている必要があります。

ファイルが各ノードに対してローカルであることを確認するには、chown root $ORACLE_HOME/bin/oradism コマンドを実行します。chmod 4755 $ORACLE_HOME/bin/oradism を実行し、oradism ファイルに正しいアクセス権限があることを確認します。

クライアントの監視

クライアントの監視については、次の表の内容を参照してください。

表 14-6 v$ テーブル

項目	説明
v$dnfs_servers	Direct NFS クライアントがマウントした NFS サーバーを一覧表示します。
v$dnfs_files	Direct NFS クライアントが開いたファイルを一覧表示します。
v$dnfs_channels	NFS サーバーから Direct NFS に対して確立された TCP 接続を一覧表示します。
v$dnfs_stats	Oracle プロセスが発行したさまざまな NFS 操作の統計情報を一覧表示します。

Windows プラットフォームでの Direct NFS の構成

Windows サーバー上の Oracle インストーラを使用して、Oracle 11g 以降のソフトウェアがインストールされていることを確認します。

oranfstab ファイルを作成して設定します。oranfstab ファイルは %ORACLE_HOME%¥dbs ディレクトリに追加する必要があります。ファイル名に拡張子 (テキストファイル - txt など) が追加されていることを確認します。

次のように oranfstab を構成します。

```
C:¥>type %ORACLE_HOME%¥dbs¥oranfstab
server: lnxnfs          <=== NFS server Host name
path: 10.171.52.54 <--- First path to NFS server ie NFS server NIC
local: 10.171.52.33 <--- First client-side NIC
export: /oraclenfs  mount: y:¥
uid:1000
gid:1000
C:¥>
```

Direct NFS クライアントは、oranfstab ファイル内に一覧表示されているすべての NFS サーバーにアクセスするために、UID または GID 値を使用します。Direct NFS は UID または GID 値 0 を無視します。前述の例で使用した UID と GID は、NFS サーバーの Oracle ユーザーのものです。

oranfstab ファイルに指定された UID と GID を使用して、Oracle ユーザーが読み取り、書き込み、実行の各操作を行うには、NFS サーバーからのエクスポートされたパスにアクセスできる必要があります。UID と GID のどちらも一覧表示されていない場合は、oranfstab ファイルに一覧表示されているすべての NFS サーバーにアクセスするために、デフォルト値の 65534 が使用されます。

ユニバーサル共有の表示または編集

ユニバーサル共有の詳細を表示したり、ユニバーサル共有の特定の属性を編集できます。

ユニバーサル共有の詳細の表示

ユニバーサル共有の詳細を表示するには

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。次に、[ユニバーサル共有 (Universal Shares)]タブをクリックします。
2. ユニバーサル共有を見つけて、その名前をクリックします。

   [フィルタ (Filters)]を使用して、特定のユニバーサル共有を表示します。たとえば、SMB プロトコルを使用したユニバーサル共有や、状態が[エクスポート済み (Exported)]のユニバーサル共有などです。

   [ID]は、ユニバーサル共有の UUID です。

   [エクスポートパス (Export path)]は、ユニバーサル共有のバックアップポリシーで使用されるパスです。

   [マウントパス (Mount path)]は、クライアントからの接続に使用されるパスです。

ユニバーサル共有の編集

共有のクォータと、共有をマウントできるホストを編集できます。

ユニバーサル共有を編集するには

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。次に、[ユニバーサル共有 (Universal Shares)]タブをクリックします。
2. ユニバーサル共有を見つけて、その名前をクリックします。
3. ユニバーサル共有の次の詳細を編集できます。

クォータ (Quota)	共有のクォータを変更するには、[編集 (Edit)]をクリックします。
エクスポートされたストレージサーバー (Exported storage servers)	ユニバーサル共有の NFS または SMB エクスポートサーバーを変更するには、[編集 (Edit)]をクリックします。
ホスト (Hosts)	共有をマウントできるホストを追加または削除するには、[編集 (Edit)]をクリックします。
Kerberos	選択したプロトコルが NFS で、選択したストレージサーバーで Kerberos サービスがサポートされている場合は、[編集 (Edit)]をクリックして、Kerberos セキュリティ方式を変更します。 p.566 の「Kerberos ベースの認証」を参照してください。 **メモ:** Kerberos セキュリティ方式が更新されると、現在のユニバーサル共有に構成されているクライアントから NFS サーバーに接続する機能に影響します。NFS サーバーを再びマウントするための mount コマンドパラメータとして、更新した Kerberos セキュリティ方式を使用します。

ユニバーサル共有の削除

NetBackup ストレージからユニバーサル共有を削除できます。

ユニバーサル共有を削除すると、共有内のすべてのデータも削除されます。この処理をやり直すことはできません。また、データ量が多い場合は時間がかかることがあります。アクティブなデータ転送はすぐに終了し、マウントされた共有はすぐに削除されてクライアント上でアクセスできなくなります。ユニバーサル共有を削除する前に、クライアント上でマウント解除します。

ユニバーサル共有を削除するには

1. すべてのクライアントでユニバーサル共有をマウント解除します。
2. 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。次に、[ユニバーサル共有 (Universal Shares)]タブをクリックします。
3. 削除するユニバーサル共有を選択し、[削除 (Delete)]、[削除 (Delete)]の順にクリックします。

ユニバーサル共有のマウント

作成したユニバーサル共有の種類と一致するマウントの手順を選択してください。

CIFS/SMB ユニバーサル共有のマウント

Windows エクスプローラを使用して SMB ユニバーサル共有をマウントするには

1. Windows サーバーにログオンし、[ネットワークドライブの割り当て]ツールに移動します。
2. 利用可能なドライブ文字を選択します。
3. 次のようにマウントパスを指定します。

   `¥¥<MSDP storage server>¥<id>`

   例: `¥¥server.example.com¥my-db-share`

   マウントパスは NetBackup Web UI で確認できます ([ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ユニバーサル共有 (Universal shares)])。
4. [完了 (Finish)]をクリックします。

Windows コマンドプロンプトを使用して SMB ユニバーサル共有をマウントするには

1. Windows サーバーにログオンし、コマンドプロンプトを開きます。
2. 次のコマンドを使用してマウントパスを指定します。

   `net use <drive_letter>:¥¥<MSDP storage server >¥<id>`

   例: `net use <drive_letter>:¥¥<MSDP storage server >¥<id>`
3. 次のようにマウントパスを指定します。

   `¥¥<MSDP storage server>¥<id>`

   例: `¥net use ¥¥server.example.com¥my-db-share`

   MSDP ストレージサーバー名とエクスポートパスは、NetBackup Web UI のユニバーサル共有の詳細ページ ([ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ユニバーサル共有 (Universal shares)]) で確認できます。

NFS ユニバーサル共有のマウント

NFS ユニバーサル共有をマウントするには

1. root としてサーバーにログオンします。
2. 次のコマンドを使用してマウントポイント用のディレクトリを作成します。

   ```
   mkdir /mnt/<your_ushare_mount_point_subfolder>
   ```

3. 次のコマンドのいずれかを使用してユニバーサル共有をマウントします。

   - NFSv3:

     ```
     mount -t nfs <MSDP storage server>:<export path> -o
     rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,vers=3,timeo=600
     /mnt/<your_ushare_mount_point_subfolder>
     ```

     例:

     ```
     mount -t nfs
     server.example.com:/mnt/vpfs_shares/3cc7/3cc77559-64f8-4ceb-be90-3e242b89f5e9
     -o
     rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,vers=3,timeo=600
     /mnt/<your_ushare_mount_point_subfolder>
     ```

   - NFSv4:

     ```
     mount -t nfs <MSDP storage server> : <export path> -o
     vers=4.0,rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,
     vers=4,timeo=600 /mnt/ <your_ushare_mount_point_subfolder>
     ```

     メモ: Flex Appliance アプリケーションインスタンスで NFSv4 を使用している場合、エクスポートパスは相対パスとして入力する必要があります。`/mnt/vpfs_shares` は含めないでください。

     例:

     ```
     mount -t nfs
     server.example.com:/3cc7/3cc77559-64f8-4ceb-be90-3e242b89f5e9
     -o
     rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,vers=4,timeo=600
     /mnt/<your_ushare_mount_point_subfolder>
     ```

     NetBackup FlexScale と AKS/EKS クラウドプラットフォームの場合、NFS クライアントで NFSv4 を使用して NFS 共有をマウントする場合は、接頭辞 `/mnt/vpfs_shares` なしの相対共有パスを使用する必要があります。
     たとえば、エクスポート共有パスが engine1.com:/mnt/vpfs_shares/usha/ushare1 の場合は、次のように NFSv4 を使ってクライアントにマウントします。

```
mount -t nfs -o 'vers=4' engine1.com:/usha/ushare1
/tmp/testdir.
```

- NFSv3 または NFSv4 の Kerberos ベースの認証を使用して NFS 共有をマウントするには、次の 3 種類のセキュリティオプションのいずれかを使用します。
  - krb5
  - krb5i
  - krb5p

krb5 を使用した NFSv3:

```
mount -t nfs <MSDP storage server>:<export path> -o
rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,vers=3,timeo=600,sec=krb5
/mnt/<your_ushare_mount_point_subfolder>
```

krb5 を使用した NFSv4:

```
mount -t nfs <MSDP storage server>:<export path> -o
rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,actimeo=0,vers=4,timeo=600,sec=krb5
/mnt/<your_ushare_mount_point_subfolder>
```

- 認証にのみ krb5 を使用します。
- krb5i は、サーバーへのすべての RPC (Remote Procedure Call) 要求と、クライアントへのすべてのレスポンスに対してハッシュを計算します。ハッシュはメッセージ全体 (RPC ヘッダーと NFS の引数または結果) に対して計算されます。
- krb5p は暗号化を使用してプライバシーを確保します。krb5p を使用すると、NFS 引数と結果が暗号化されます。

krb5 はより優れたパフォーマンスを提供し、krb5 > krb5i > krb5p の順序で低下します。

マウントパスは NetBackup Web UI で確認できます ([ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ユニバーサル共有 (Universal shares)])。

ユニバーサル共有の保護ポイントの作成

ユニバーサル共有では、データの保護ポイントを作成して共有内のデータを管理および保護できます。保護ポイントの作成は、Universal-Share バックアップポリシーを作成して行います。

MSDP ストレージサーバーが複数のユニバーサル共有で構成されている場合、一部またはすべての共有に対して 1 つのポリシーを作成できます。また、共有ごとに 1 つずつ個別のポリシーを作成することもできます。複数のストレージサーバーがユニバーサル共有で構成されている場合、各ストレージサーバーのユニバーサル共有を保護するために、各ストレージサーバーを独自のポリシーで構成する必要があります。

p.556 の「ユニバーサル共有の概要」を参照してください。

保護ポイント - ユニバーサル共有データのカタログ化と保護

ユニバーサル共有に最初に取り込まれたデータはすべて、ユニバーサル共有をホストするアプライアンスベースのメディアサーバーにある MSDP に存在します。このデータは NetBackup カタログでは参照されず、保持の適用は有効になりません。したがって、ユニバーサル共有に存在するデータは検索できず、NetBackup を使用して復元できません。共有内のデータの制御は、その共有がマウントされているホストによってのみ管理されます。

保護ポイント機能は、NetBackup との直接統合をサポートします。保護ポイントは、ユニバーサル共有に存在するデータのポイントインタイムコピーです。保護ポイントの作成と管理は、保護ポイントのすべてのスケジュール設定と保持を定義する NetBackup ポリシーを通じて行います。保護ポイントは、NetBackup Web UI を使用して構成できる Universal-Share ポリシーを使用します。ユニバーサル共有内のデータの保護ポイントが作成されると、ユニバーサル共有内のデータのそのポイントインタイムコピーを NetBackup の他の保護対象データと同様に管理できます。保護ポイントデータは、ストレージライフサイクルポリシーを使用して、他の NetBackup ドメインにレプリケートしたり、テープやクラウドなどの他の種類のストレージに移行したりできます。各保護ポイントコピーは、関連付けられたユニバーサル共有の名前に対して参照されます。

ユニバーサル共有の保護ポイントポリシーを作成するには

1. NetBackup 管理コンソールまたは NetBackup Web UI を使用してポリシーを作成します。
2. [属性 (Attributes)]タブで、[ポリシー形式 (Policy type)]リストの[Universal-Share]を選択します。

   [ポリシーストレージ (Policy storage)]で、ユニバーサル共有をホストするストレージユニットを使用する必要があります。それがない場合は作成する必要があります。

   複数のストレージサーバーがユニバーサル共有で構成されている場合は、各ストレージサーバーをそれぞれ独自のポリシーで構成する必要があります。この構成により、そのストレージサーバーのユニバーサル共有が保護されます。
3. [宛先 (Destination)]で、[ポリシーストレージ (Policy storage)]のリストからストレージユニットを選択します。

   ポリシーストレージの設定について詳しくは、『NetBackup 管理者ガイド Vol. 1』のポリシーストレージ (ポリシー属性) に関する説明を参照してください。

   ユニバーサル共有ポリシーのストレージユニットは、ユニバーサル共有が作成されるのと同じディスクプールボリュームに配置する必要があります。
4. [スケジュール (Schedule)]タブで、[完全 (FULL)]または[増分 (INCR)]を選択します。

5 [クライアント (Clients)]タブで、目的のクライアントの名前を入力します。

ユニバーサル共有はエージェントレステクノロジであるため、指定したクライアント名はカタログ作成目的にのみ使用されます。NetBackup Appliance、NetBackup 仮想アプライアンス、Flex Appliance サーバーアプリケーションインスタンス、MSDP BYO サーバー名、またはユニバーサル共有がマウントされているホストを入力できます。クライアント名には、短縮名、FQDN (完全修飾ドメイン名)、または IP アドレスを使用できます。

6 [バックアップ対象 (Backup Selections)]タブにユニバーサル共有のパスを入力します。

エクスポートパスは、NetBackup Web UI のユニバーサル共有の詳細ページ ([ストレージ (Storage)]、[ストレージの構成 (Storage Configuration)]、[ユニバーサル共有 (Universal Share)]) で確認できます。

たとえば、`/mnt/vpfs_shares/3cc7/3cc77559-64f8-4ceb-be90-3e242b89f5e9` です。

複数ストリームのバックアップが必要な場合は、`NEW_STREAM` 指示句を使用できます。

また、`BACKUP X USING Y` 指示句を使用して、ユニバーサル共有パスとは異なるディレクトリにカタログを作成できます。たとえば、`BACKUP /database1 USING /mnt/vpfs_shares/3cc7/3cc77559-64f8-4ceb-be90-3e242b89f5e9` です。この例では、バックアップは `/demo/database1` でカタログ化されます。

7 Universal-Share ポリシーを実行します。

バックアップの作成後、リストア、複製、自動イメージレプリケーションなどの NetBackup の機能でバックアップを管理できます。

Web UI または NetBackup インスタントアクセス API を使用すると、ローカル LSU またはクラウド LSU からのバックアップコピーに即座にアクセスできます。

クラウド LSU のインスタントアクセスについて詳しくは、次を参照してください。

p.369 の「オブジェクトストレージのインスタントアクセスについて」を参照してください。

NetBackup API について詳しくは、次の Web サイトを参照してください。

https://sort.veritas.com/documents

NetBackup を選択し、ページの下部でバージョンを選択します。

ユニバーサル共有を使用したデータのリストア

ユニバーサル共有のバックアップからデータをリストアできます。

保護ポイントのリストア

保護ポイントからのデータの復元は、標準のクライアントバックアップからデータを復元するのとまったく同じです。標準のバックアップアーカイブと、リストアインターフェースまたは NetBackup Web UI を使用してデータをリストアできます。復元に使用されるクライアント名は、Universal-Share ポリシーにあるユニバーサル共有の名前です。代替クライアントの復元を完全にサポートしています。ただし、ユニバーサル共有が元々マウントされていたシステムに復元するには、NetBackup クライアントソフトウェアをそのシステムにインストールする必要があります。このソフトウェアが必要なのは、NetBackup クライアントが最初にユニバーサル共有にデータを配置する必要がないためです。

また、NetBackup は、任意の保護ポイントのポイントインタイムコピーに基づく NFS/SMB 共有のプロビジョニング (インスタントアクセス) または作成に使用できる API など、さまざまな API もサポートしています。このポイントインタイムコピーは、ユニバーサル共有が以前にマウントされていた元のシステムにマウントできます。ネットワーク共有のマウントをサポートする他のシステムでプロビジョニングできます。プロビジョニングされた共有がマウントされているシステムでは、NetBackup クライアントソフトウェアは必要ありません。

ユニバーサル共有のリストア方法

保護ポイントは、高速なデータ保護プロセスを提供するだけでなく、次の 2 つの強力なリストア方式を提供します。

クライアントベースのリストア:

- 保護ポイントを使用して保護されたデータは、標準のクライアントバックアップからデータをリストアする場合とまったく同じ方式を使用してリストアされます。
  - 元のユニバーサル共有にリストア。
    この場合、元のユニバーサル共有が存在する必要があります。ユニバーサル共有パスをリストア先として指定し、ユニバーサル共有が存在するメディアサーバーをクライアントとして指定します。ただし、大規模なデータのリストアの場合は、代替の場所にリストアすることを検討してください。
  - 代替の場所にリストア
    リストア先のシステムには、標準の NetBackup クライアントがインストールされている必要があります。

プロビジョニングされたリストア (インスタントアクセス):

- 保護ポイントは、任意の保護ポイントが開始されたときにユニバーサル共有に存在していたデータのポイントインタイム (PIT) コピーです。データのこの PIT コピーは、保護ポイントデータの個別のネットワーク共有としてエクスポートできます。保護ポイントのこの PIT コピーは、データのプロビジョニングされたコピーと呼ばれます。このプロビジョニングされた共有内のデータは、プライマリユニバーサル共有内のデータに接続されていない場合があります。このデータは、PIT 保護ポイントデータの自律バージョンとして使用できます。このデータのプロビジョニングされたコピーを変更しても、

元のユニバーサル共有内のデータには影響しません。データのソース PIT コピーにも影響しません。

PIT コピーは、ユニバーサル共有が以前にマウントされていた元のシステムにマウントできます。ネットワーク共有のマウントをサポートする他のシステムでプロビジョニングすることもできます。この意味で、NetBackup 保護ポイントは、NetBackup で管理されているデータを使用するための強力な方法を提供する、コピーデータ管理の方式を提供します。保護ポイントのプロビジョニング処理は、NetBackup API を使用して実行します。この API とすべての NetBackup API については、NetBackup プライマリサーバーにある『NetBackup API リファレンス』マニュアルに記載されています。

ユニバーサル共有のディザスタリカバリ

ユニバーサル共有のディザスタリカバリは、共有内のデータまたは共有に固有のメタデータが破損または削除された場合に BYO、AKS、EKS 環境で使用できます。

この手順を始める前に、クラウド構成のユニバーサル共有を使用してデータがバックアップされ、リカバリする共有ごとに少なくとも 1 つの PIT イメージが存在することを確認します。PIT イメージがない場合、この手順は使うことができません。ディザスタリカバリを実行したコンピュータのホスト名は、共有が最初に作成されたホスト名と一致している必要があります。

通常の MSDP ディザスタリカバリの後で次の手順を実行する場合は、NGINX、SPWS、NFS、SMB がこの章で説明したように構成されていることを確認します。

すべてのユニバーサル共有に対するディザスタリカバリの実行

1. `vpfs_cloud.cfg` ファイルが次の場所にあることを確認します。

   ```
   [MSDP storage directory]/etc/puredisk/vpfs_cloud.cfg
   ```

   ファイルが存在しない場合は、次のコマンドを実行します。

   ```
   /usr/openv/pdde/vpfs/bin/vpfscld --download_vpfs_cloud_cfg
   ```

2. nfs エクスポートリストが次の場所にあることを確認します。

   BYO の `[MSDP storage directory]/etc/vpfs-shares.exports` か、AKS または EKS の `[MSDP storage directory]/cat/config/vpfs-shares.exports` (クラウドで構成された NFS 共有がある場合)。

   リストが存在しない場合は、次のコマンドを実行します。

   ```
   /usr/openv/pdde/vpfs/bin/vpfscld --download_export_list
   --share_type nfs
   ```

3 smb エクスポートリストが次の場所にあることを確認します。

BYO の [MSDP storage directory]/etc/vpfs-shares.conf か、AKS または EKS の [MSDP storage directory]/cat/config/samba/vpfs-shares.conf (クラウドで構成された SMB 共有がある場合)。

リストが存在しない場合は、次のコマンドを実行します。

```
/usr/openv/pdde/vpfs/bin/vpfscld --download_export_list
--share_type smb
```

4 次のコマンドを使用して、データを共有にリストアし、メタデータをリカバリします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions -a disasterReovery
--cloudVolume CLOUDVOLUMENAME
```

ここで CLOUDVOLUMENAME は、リストアする共有を含む MSDP クラウドボリュームの名前です。複数のクラウドボリューム間で共有をリストアする場合は、各クラウドボリュームに対してこのコマンドを実行します。

5 次のコマンドを使用して NetBackup サービスを再起動します。

```
/usr/openv/netbackup/bin/bp.kill_all

/usr/openv/netbackup/bin/bp.start_all
```

インスタントアクセスまたは単一ファイルリカバリを使用したユニバーサル共有データのリストア

この機能により、作業負荷管理者は、インスタントアクセスまたは NetBackup Web UI での単一ファイルリカバリを使用してユニバーサル共有データをリストアできます。インスタントアクセスリカバリを使用すると、ユニバーサル共有を作成してデータをマウントし、エンドユーザーがファイルにアクセスするためのパスを提示できます。管理者権限を持たない作業負荷管理者は、NetBackup 管理者の介入なしでデータをリストアできます。

レプリケーションを実行すると、イメージの情報に基づいてターゲットサーバーにユニバーサル共有資産が作成されます。NetBackup は、リカバリポイントがなく、対応するユニバーサル共有ストレージがない場合、ユニバーサル共有を自動的に削除します。

ユニバーサル共有のセルフサービスリカバリの実行

この手順により、必要な RBAC の権限または役割を持つ作業負荷管理者は、1 つの資産を選択し、リカバリポイントとそのリカバリポイントのすべての利用可能なコピーを選択できます。また、ユニバーサル共有のプロビジョニングを実行するために、対象のデフォルトのコピーまたはコピーを選択することもできます。

ユニバーサル共有の回復

1. NetBackup Web UI で、[作業負荷 (Workloads)]、[ユニバーサル共有 (Universal shares)]を選択します。
2. [共有 (Shares)]タブで、使用するユニバーサル共有を選択します。
3. [リカバリポイント (Recovery points)]を選択すると、そのユニバーサル共有のすべてのリカバリイメージが表示されます。
4. [リカバリ (Recover)]をクリックし、使用するイメージの[インスタントアクセスユニバーサル共有の作成 (Create instant access universal share)]をクリックします。
5. 次の必須情報を入力します。
   - [表示名 (Display name)]を入力します。この名前は、ユニバーサル共有パスで使用されます。
   - [プロトコル (Protocol)]: NFS または SMB (CIFS) を選択します。
   - 共有のマウントが許可されている[ホスト (Host)]を指定し、[リストに追加 (Add to list)]をクリックします。ホスト名、IP アドレス、短縮名または FQDN を使用して、ホストを指定できます。各共有に対して複数のホストを入力できます。
6. [保存 (Save)]をクリックします。
7. NetBackup はリカバリジョブを作成します。[リストアアクティビティ (Restore activity)]をクリックすると、このジョブを表示できます。
8. ユニバーサル共有を確認するには、[作業負荷 (Workloads)]、[ユニバーサル共有 (Universal shares)]、[インスタントアクセスユニバーサル共有 (Instant access universal shares)]を選択します。

ユニバーサル共有の拡張機能

ユニバーサル共有の次の拡張機能を活用できます。

- オブジェクトストアを使用したユニバーサル共有
- ユニバーサル共有アクセラレータ
- 取り込みモード
- dNFS (Direct Network File System)
- MSDP データボリューム
- ユニバーサル共有の WORM 機能
- ユニバーサル共有のスケールアウト

オブジェクトストアへのユニバーサル共有データの指定

オブジェクトストアを使用したユニバーサル共有では、ユニバーサル共有内のデータを重複排除形式でオブジェクトストレージに向けられます。

表 14-7 オブジェクトストアを使用したユニバーサル共有のサポート対象プラットフォーム

サポート対象プラットフォーム	説明
Azure Kubernetes Service (AKS)	このプラットフォームはサポートされており、デフォルトでは有効になっています。
Amazon Elastic Kubernetes Service (EKS)	このプラットフォームはサポートされており、デフォルトでは有効になっています。
Azure または AWS の VM	このプラットフォームはサポートされています。このオプションは手動で有効にする必要があります。 p.593 の「オブジェクトストアを使用したユニバーサル共有の有効化」を参照してください。
オンプレミスの RHEL 7.6+/8/9 (オンプレミスのオブジェクトストレージ)	このプラットフォームはサポートされています。このオプションは手動で有効にする必要があります。

オブジェクトストアを使用したユニバーサル共有のライフサイクル管理

ライフサイクル管理の 3 つのフェーズ:

- ユニバーサル共有の作成: ユニバーサル共有を作成する方法について詳しくは、『NetBackup Web UI 管理者ガイド』の「ユニバーサル共有の作成」セクションを参照してください。
- ユニバーサル共有の削除: NetBackup Web UI でユニバーサル共有を削除すると、MSDP クラウドボリュームがユニバーサル共有またはインスタントアクセスで使用されている場合は削除できません。ユニバーサル共有を削除する場合は、ユニバーサル共有のすべてのスナップショットがローカルディスクとクラウドバケットで期限切れになっていることに注意してください。ユニバーサル共有を削除する前に、メディアサーバーにログインして、ユニバーサル共有のすべてのスナップショットコピーを期限切れにする必要があります。
- スナップショットの保持とライフサイクル: `vpfsd` コマンドはバックグラウンドスレッドを実行し、スナップショットコピーの保持を監視し続けます。保持期間に達すると、`vpfsd` コマンドはスナップショットを期限切れにします。完全なスナップショットと増分スナップショットの保持は、`vpfsd_config.json` ファイルで構成できます。

オブジェクトストアを使用したユニバーサル共有の有効化

AKS または EKS では、オブジェクトストアを使用したユニバーサル共有またはインスタントアクセスがデフォルトで有効になっています。ただし、クラウド仮想マシンでオブジェクトストア機能を有効にするには、この機能を手動で有効にする必要があります。

オブジェクトストアを使用したユニバーサル共有の有効化

1. `universal-share-object-store = 1` オプションを `etc/msdp-release` ファイルに追加します。

   例:

   ```
   cat /etc/msdp-release
   universal-share-object-store = 1
   ```

2. `UNIVERSAL_SHARE_OBJECT_STORE` の名前が `extendedcapabilities` オプションにあることを確認します。

   例:

   ```
   nbdevconfig -getconfig -stype PureDisk
   -storage_server your_storage_server_name
   |grep UNIVERSAL_SHARE_OBJECT_STORE
   ```

3. メディアサーバーまたはプライマリサーバーで、次のコマンドを実行してストレージサーバーの属性を再ロードします。

   ```
   nbdevconfig -getconfig -stype PureDisk
   -storage_server your_storage_server_name > /tmp/flags

   nbdevconfig -setconfig -stype PureDisk
   -storage_server your_storage_server_name -configlist /tmp/flags
   ```

オブジェクトストアを使用したユニバーサル共有に追加できるオプションのパラメータを次に示します。これらのオプションは、*storage_path*/etc/puredisk/vpfsd_config.json にあります。

スナップショットの保持:

- `"cloudFullTaskInterval": 36000,`: ユニバーサル共有間隔の完全なスナップショットが自動的に作成され、デフォルト値は 10 時間です。このエントリは、秒単位を使用する整数である必要があります。
- `"cloudIncrTaskInterval": 1800,`: ユニバーサル共有間隔の増分スナップショットが自動的に作成され、デフォルト値は 30 分です。このエントリは、秒単位を使用する整数である必要があります。

- "cloudFullSnapshotRetention": 172800,: 完全なスナップショットコピーの保持期間。保持が期限切れになると、完全なスナップショットがローカルストレージとクラウドバケットストレージから削除されます。デフォルト値は 48 時間です。保持が 48 時間より長く設定されている場合は、領域の再利用に影響する可能性があります。

ローカルディスクキャッシュの設定:

- "CloudCacheSize": 500,: ユニバーサル共有とインスタントアクセスのローカルディスクキャッシュサイズ。このオプションは、オブジェクトストアを使用したユニバーサル共有と、オブジェクトストアを使用したインスタントアクセスにのみ適用されます。vpfsd コマンドは spoold サービスからこの領域を削除するため、キャッシュサイズに十分な領域があることを確認する必要があります。それ以外の場合、オブジェクトストアを使用したユニバーサル共有またはオブジェクトストアのインスタントアクセスは作成されません。MSDP は、ユニバーサル共有を作成する前に十分な構成領域があることを確認します。キャッシュのサイズを増やすと vpfsd を再起動する必要があり、キャッシュサイズに対して十分な空き領域がない場合は vpfsd を開始できないことに注意してください。
  オブジェクトストアを使用したユニバーサル共有またはインスタントアクセスが削除された後、その領域は自動的には spoold に戻りません。CloudCacheSize を減らして、一部の領域を spoold に戻します。削除後に vpfsd を再起動する必要があります。

- "CloudCacheLowThreshold": 50,: キャッシュの領域使用量が低しきい値に達すると、vpfsd サービスはクラウドキャッシュの領域の再利用を開始します。このエントリはパーセント単位で表示されます。

- "CloudCacheHighThreshold": 85,: キャッシュの領域使用量が高いしきい値に達すると、vpfsd サービスはデータの書き込みまたはダウンロードを停止します。空き容量がある場合は、データの書き込みとデータのダウンロードが続行されます。このエントリはパーセント単位で表示されます。

ローカルディスクキャッシュのサイズ決定:

- キャッシュのサイズは、データボリュームの数、ユニバーサル共有の数、すべてのユニバーサル共有内のファイルの合計数によって異なります。ローカルディスクキャッシュには、データコンテナのメタデータと重複排除セグメントという 2 種類のデータストアがあります。ファイルの数が多いほどより多くのディスクキャッシュが必要になり、データボリュームの数が多いほどより多くのディスクキャッシュが必要になります。
  100 万ファイルごとに、ユニバーサル共有のメタデータ用に約 300 GB のディスクキャッシュが必要です。データコンテナキャッシュの場合、各ユニバーサル共有には、デフォルトで各データボリュームについて 32 個のデータコンテナキャッシュがあり、すべてのユニバーサル共有についてデフォルトで読み取りキャッシュ用のデータコンテナが 1,024 個あります。
  ディスクキャッシュサイズを計算するアルゴリズムを次に示します。
  メタデータサイズ: 300 GB * ファイル数 (単位は 100 万)
  データコンテナのサイズ: 64 MB * (32 * データボリュームの数 * 共有の数 + 1024)

合計キャッシュサイズ: (メタデータサイズ + データコンテナサイズ) / 0.85
(CloudCacheHighThreshold)
ローカルディスクのデフォルトサイズは 500 GB です。このサイズであれば、ほとんどのシナリオに対応できます。データボリュームまたはパーティションの数が 4 以下の場合は、以下の構成をお勧めします。キャッシュサイズを調整するには、vpfsd_config.json の CloudCacheSize を構成します。

ファイル数 (100 万単位)	共有の数	パーティションの数	ディスクキャッシュサイズ (GB 単位)
0.5	1	4	400
0.5	20	4	400
1	1	4	600
1	20	4	600
2	1	4	800
3	1	4	1200
4	1	4	1600
5	1	4	2000
5	20	4	2000
6	1	4	2200
7	1	4	2600
8	1	4	3000
9	1	4	3400
10	1	4	3800
10	20	4	3800

スナップショット管理:

- クラウドバケットの完全なスナップショットと増分スナップショットを含むすべてのスナップショットを一覧表示します。

  ```
  /usr/openv/pdde/vpfs/bin/vpfscld -list
  ```

- スナップショットを手動で作成し、スナップショットとデータをクラウドバケットにアップロードします。

```
/usr/openv/pdde/vpfs/bin/vpfscld --snapshot
--share_id <share> --snap_type <full|incr>
```

- ローカルおよびクラウドからスナップショットを手動で削除する場合は、期限切れのスナップショットはリカバリできないことに注意してください。

```
/usr/openv/pdde/vpfs/bin/vpfscld --expire
--share_id <share> --pit <point in time>
```

- クラウドバケットからスナップショットを手動でリカバリする:

```
/usr/openv/pdde/vpfs/bin/vpfscld -recover
--share_id <share> [--tgt_id <target>] [--pit <point in time>]
[--force]
```

- ユニバーサル共有のスナップショットコピーの数を構成します。
  スナップショットコピーのデフォルトの数は 2 です。これは vpfsd_config.json の cloudMaxSnapshotCopy パラメータで構成できます。cloudMaxSnapshotCopy の値を 0 に設定すると、自動的にスナップショットを取得する機能が無効になります。ユニバーサル共有がローカルディスクキャッシュにスナップショットを格納する場合、値を大きくすると、より多くのローカルディスクキャッシュが必要になります。
- スナップショットのコピーがローカルディスクキャッシュに格納されるようにユニバーサル共有を構成します。
  NetBackup 10.4 以降のバージョンでは、スナップショットはローカルディスクキャッシュに保存されるのではなく、クラウドバケットにのみ保存されます。ただし、ローカルディスクキャッシュで、追加のスナップショットのストレージを構成および制御することは可能です。スナップショットを引き続きローカルディスクキャッシュに保持するには、vpfsd_config.json の cloudKeepLocalSnapshotCopy を true に構成する必要があります。また、さらに多くのローカルディスク容量も必要です。

メモ: ユニバーサル共有とインスタントアクセスのオブジェクトストアを有効にするには、/etc/msdp-release に universal-share-object-store = 1 と instance-access-object-store = 1 を追加します。

オブジェクトストレージを使用したインスタントアクセスの有効化

オブジェクトストレージを使用してインスタントアクセスを有効にする

1. /etc/msdp-release ファイルに instant-access-object-store = 1 を追加します。

   例:

   ```
   /etc/msdp-release
    instant-access-object-store = 1
   ```

2. IA_OBJECT_STORE 機能が extendedcapabilities 内にあることを確認します。

   ```
   nbdevconfig -getconfig -stype PureDisk -storage_server
   <your_storage_server_name> |grep IA_OBJECT_STORE
   ```

3. メディアサーバーまたはプライマリサーバーで、次のコマンドを実行してストレージサーバーの属性を再ロードします。

   ```
   nbdevconfig -getconfig -stype PureDisk
   -storage_server <your_storage_server_name> > /tmp/flags
   nbdevconfig -setconfig -stype PureDisk
   -storage_server <your_storage_server_name> -configlist /tmp/flags
   ```

4. /etc/msdp-release に universal-share-object-store = 1 と instant-access-object-store = 1 を追加して、ユニバーサル共有とインスタントアクセスのオブジェクトストアを有効にします。

データ重複排除のユニバーサル共有アクセラレータ

ユニバーサル共有アクセラレータ機能は、作業負荷またはクライアント上にファイルシステムのマウントポイントを直接提供します。NFS/SMB サービスは提供されません。データはストレージサーバーに移動しません。データはクラウドバケットに直接送信され、指紋関連のメタデータのみがストレージサーバーに送信され、データ重複排除が実行されます。データは、アクセラレータからデータを読み込むと、クラウドバケットから直接取得されます。

ユニバーサル共有アクセラレータは、オブジェクトストアを使用したユニバーサル共有機能を利用します。主な違いは、オブジェクトストアを使用したユニバーサル共有はストレージサーバー側にあり、ユニバーサル共有アクセラレータはクライアント側にある点です。ユニバーサル共有アクセラレータは、NetBackup クライアントパッケージとともに提供されます。ユーザーが NetBackup Web UI からユニバーサル共有アクセラレータを作成するには、先にユニバーサル共有アクセラレータ機能を有効にして NetBackup クライアントを該当する作業負荷にインストールする必要があります。NetBackup Web UI でユニバーサル共有アクセラレータを作成したら、クライアント側でアクセラレータを構成できます。

サポート対象プラットフォーム

- クライアント:
  - RHEL 7.6 以降、RHEL 8.x、RHEL 9.x
    - AWS または Azure でのみサポートされます。
- ストレージサーバー:
  - ストレージサーバーバージョン 19.0 以降
  - RHEL 7.6 以降、RHEL 8.x、RHEL 9.x

    メモ: ユニバーサル共有アクセラレータは、SUSE Linux Enterprise ではサポートされません。
  - AWS/Azure を使用する AKS/EKS または MSDP クラスタ
- NetBackup:
  - プライマリサーバー: 10.3 以降
  - メディアサーバー: 10.3 以降
  - クライアント: 10.3 以降

制限事項

- ユニバーサル共有アクセラレータは、複数の `vpfsd` のインスタンスをサポートしません。
- DR はユニバーサル共有アクセラレータではサポートされません。

ユニバーサル共有アクセラレータの NetBackup の準備

AWS、Azure S3、または Blob アカウントとキーを取得して、MSDP クラウド LSU を作成します。

ユニバーサル共有アクセラレータのローカルディスクキャッシュ (<storage-path>) のディスクサイズは、500 GB 以上である必要があります。ディスクの容量は、ユニバーサル共有アクセラレータのローカルディスクキャッシュとして使用され、パフォーマンスの優れたディスクである必要があります。別のディスクを持つマウントポイントまたは既存のマウントポイントの 1 つのフォルダを指定できます。ローカルディスクキャッシュまたはストレージが他のアプリケーションまたはシステムと共有されている場合、NetBackup は構成されたディスク容量を使用できることを確認します。クラウドのキャッシュサイズ (`CloudCacheSize`) は、*<storage-path>*`/etc/puredisk/vpfsd_config.json` にあります。

Cohesityでは、ユニバーサル共有アクセラレータには個別のマウントポイントを使用することをお勧めします。ユニバーサル共有アクセラレータが他のアプリケーションとの共有

ディスクまたはマウントポイントを使用する場合は、ユニバーサル共有アクセラレータに、利用可能な十分な空き容量があることを確認する必要があります。

ユニバーサル共有アクセラレータのインストール

インストールプロセスは、NetBackup クライアントのインストールと非常によく似ています。NetBackup クライアントのインストールについての詳細は、次のリンクから見つけることができます。

- UNIX および Linux での NetBackup クライアントのインストールについて
- UNIX クライアントのローカルインストール

ユニバーサル共有アクセラレータをインストールする方法

1. NBInstallAnswer.conf ファイルにオプション INCLUDE_VRTSPDDEU_CLIENT を追加します。

   アクセラレータのバイナリを自動的にインストールするには、/tmp/NBInstallAnswer.conf にオプション 'INCLUDE_VRTSPDDEU_CLIENT = INCLUDE' を追加する必要があります。デフォルトではバイナリによってインストールされません。

2. 作業負荷 FQDN がある CLIENT エントリを NetBackup プライマリサーバーの /usr/openv/netbackup/bp.conf ファイルに追加します。

3. 作業負荷サーバーに NetBackup Linux クライアントパッケージをコピーします。

   UNIX および Linux での NetBackup クライアントのインストールについて

   UNIX および Linux へのクライアントのインストール方法について詳しくは、『NetBackup インストールガイド』を参照してください。

ユニバーサル共有アクセラレータの保護ポリシーの作成

ユニバーサル共有アクセラレータの保護ポリシーを作成する方法

1. NetBackup 管理コンソールまたは NetBackup Web UI を使用してポリシーを作成します。

2. [属性 (Attributes)]タブで、[ポリシー形式 (Policy type)]の[Universal-Share]を選択します。

   [ポリシーストレージ (Policy storage)]では、ユニバーサル共有アクセラレータと同じディスクボリュームを持つストレージユニットを使用する必要があります。存在しない場合は作成する必要があります。

3 [宛先 (Destination)]で、[ポリシーストレージ (Policy storage)]のリストからストレージユニットを選択します。

ポリシーストレージの設定について詳しくは、『NetBackup 管理者ガイド Vol. 1』のポリシーストレージ (ポリシー属性) に関する説明を参照してください。

ユニバーサル共有ポリシーのストレージユニットは、ユニバーサル共有が作成されるのと同じディスクプールボリュームに配置する必要があります。

4 [スケジュール (Schedules)]タブで[完全バックアップ (Full backup)]または[差分増分バックアップ (Differential incremental backup)]を選択します。

5 [クライアント (Clients)]タブで、[追加 (Add)]をクリックし、[クライアント名 (Client name)]にクライアントのホスト名を入力します。

ホスト名には NetBackup クライアントと同じホスト名が必要です。ホスト名は、[ホスト (Hosts)]、[ホストプロパティ (Host properties)]から NetBackup コンソールで確認できます。または、ユニバーサル共有アクセラレータの詳細ページを開き、[ホスト (Hosts)]セクションでホスト名を見つけます。

6 [バックアップ対象 (Backup Selections)]タブで[追加 (Add)]をクリックし、[パス名または指示句 (Pathname or directive)]にユニバーサル共有のパスを入力し、[リストに追加 (Add to list)]をクリックします。

エクスポートパスは、NetBackup Web UI のユニバーサル共有の詳細ページ ([ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ユニバーサル共有 (Universal shares)]) で確認できます。例: `/mnt/vpfs_shares/accl/accl`

複数ストリームのバックアップが必要な場合は、NEW_STREAM 指示句を使用できます。

また、BACKUP X USING Y 指示句を使用して、ユニバーサル共有パスとは異なるディレクトリにカタログを作成できます。たとえば、`BACKUP /demo/database1 USING /mnt/vpfs_shares/accl/accl` のようにします。この例では、バックアップは `/demo/database1` でカタログ化されます。

7 Universal-Share ポリシーを実行します。

バックアップの作成後、リストア、複製、自動イメージレプリケーションなどの NetBackup の機能でバックアップを管理できます。

ユニバーサル共有アクセラレータの構成

自社構築 (BYO) でユニバーサル共有アクセラレータを作成するには、オブジェクトストアを使用したユニバーサル機能を有効にする必要があります。これを有効にするには、次のトピックを参照してください。ユニバーサル共有アクセラレータには、クラウドディスクボリュームまたはクラウドディスクプールも必要です。

p.593 の「オブジェクトストアを使用したユニバーサル共有の有効化」を参照してください。

ユニバーサル共有アクセラレータの作成

NetBackup Web UI にログオンし、ユニバーサル共有を作成します。詳しくは、『NetBackup Web UI クラウド管理者ガイド』の「ユニバーサル共有の作成」セクションを参照してください。

ユニバーサル共有アクセラレータを作成する場合は、次の情報を入力します。

- 表示名 (Display name): NetBackup クライアントまたは作業負荷でマウントするために使用される共有 ID。
- 形式 (Type): [アクセラレータ (Accelerator)]を選択します。
- ストレージサーバー (Storage server): ストレージサーバーのホスト名。
- ディスクボリューム (Disk volume): MSDP クラウドのディスクボリューム。
- クォータ (Quota): デフォルトでは無制限。
- ホスト (Hosts): NetBackup クライアントのホスト名。

ユニバーサル共有アクセラレータのマウント

まず、NetBackup クライアントコンピュータで `vpfs_accelerator.sh` スクリプトを使用してユニバーサル共有アクセラレータを構成します。次を使用します。

```
/usr/openv/pdde/vpfs/bin/vpfs_accelerator.sh --config
--storage-server=<storage server> --engine-host=<hostname> --mode=byo
--storage-path=<path>
```

- `storage-server`: ストレージサーバーの名前。
- `engine-host`: スタンドアロンサーバーのクラスタまたはストレージサーバーのエンジン名。
- `mode`: アクセラレータモード。byo である必要があります。
- `storage-path`: スペースを使用せず、カンマで区切った、ローカルストレージパスのリスト。それらのパスは事前に作成する必要があります。

次を使用してユニバーサル共有アクセラレータをマウントします。

```
/usr/openv/pdde/vpfs/bin/vpfs_accelerator.sh --create --share-id=<ID>
--cloud-volume=<MSDP cloud disk volume>
```

- `share-id`: NetBackup Web UI の[ディスクストレージ (Disk Storage)]、[ユニバーサル共有 (Universal shares)]タブにあるユニバーサル共有 ID。
- `cloud-volume`: ユニバーサル共有タブの[ボリューム (Volume)]列であるクラウドボリューム。

ユニバーサル共有アクセラレータの削除

ユニバーサル共有アクセラレータを削除するには、次を使用します。

1. クライアントでユニバーサル共有アクセラレータを停止し、削除します。
   - `/usr/openv/pdde/vpfs/bin/vpfs_accelerator.sh --stop --share-id=<id>`
   - `/usr/openv/pdde/vpfs/bin/vpfs_accelerator.sh --delete --share-id=<id>`
   - `/usr/openv/pdde/vpfs/bin/vpfs_accelerator.sh --stop-all`
2. NetBackup Web UI で、ユニバーサル共有が一覧表示されたページを開き、アクセラレータを選択して削除します。

ユニバーサル共有アクセラレータの構成解除

クライアント側でユニバーサル共有アクセラレータを構成解除すると、ユニバーサル共有アクセラレータとそのポイントインタイムが削除されます。構成解除すると、NetBackup プライマリサーバーとの接続は解除されますが、プライマリサーバー側のバックアップイメージは削除されません。ユニバーサル共有アクセラレータを削除するには、NetBackup Web UI から削除する必要があります。

クライアント側でユニバーサル共有アクセラレータを構成解除するには、次を使用します。`/usr/openv/pdde/vpfs/bin/vpfs_accelerator.sh -unconfig`

メモ: `vpfs_accelerator.sh -unconfig` を実行すると、ユニバーサル共有アクセラレータのデータが削除され、データはリカバリできません。

ユニバーサル共有アクセラレータサービスの管理

次を使用して、ユニバーサル共有アクセラレータサービスを管理します。

- `vpfs_accelerator.sh --start --share-id=<id>`: ユニバーサル共有アクセラレータを開始します。
- `vpfs_accelerator.sh --stop --share-id=<id>`: ユニバーサル共有アクセラレータを停止します。
- `vpfs_accelerator.sh --start-all`: すべてのサービスを開始します。
- `vpfs_accelerator.sh --stop-all`: すべてのサービスを停止します。

ユニバーサル共有アクセラレータのストレージパスの追加

新しいパーティションを追加するには、次の手順を実行します。

ユニバーサル共有アクセラレータのストレージパスを追加する方法

1. ユニバーサル共有アクセラレータをシャットダウンします。

   ```
   vpfs_accelerator.sh --stop-all
   ```

2. edit_fstab を編集して、新しいパーティションを追加します。

   ```
   /usr/openv/pdde/vpfs/bin/edit_fstab [partition_1] [partition_2]
   ... [partition_N] Where partition_1 - partition_N are the
   partition paths to be added to the fstab.cfg file. Partitions
   that already exist in fstab.cfg are ignored.
   ```

   例: 新しいパーティション /msdp1/ を追加します。

   ```
   edit_fstab /msdp1/
   ```

3. ユニバーサル共有アクセラレータを起動します。

   ```
   vpfs_accelerator.sh --start-all
   ```

ユニバーサル共有アクセラレータのクォータについて

クォータは NetBackup Web UI で有効にでき、クォータは増減できます。NetBackup Web UI では、クォータの無効化はサポートされません。スパースファイルを削除すると、そのスパースファイルが使用する削除済み領域がクォータに反映されないことがあります。

クォータの有効化または変更

クォータを有効化または変更する方法

1. NetBackup Web UI を開きます。
2. 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。
3. [ユニバーサル共有 (Universal shares)]タブで、[表示名 (Display name)]をクリックしてユニバーサル共有の詳細を表示します。
4. [クォータ (Quota)]セクションを見つけて、[編集 (Edit)]をクリックします。
5. クォータ値を入力し、ユニット GB または TB を選択します。クォータの最小サイズは 1 GB で、最大サイズはストレージシステムの使用可能なサイズより大きくしないようにします。

クォータの使用状況の確認

クォータの使用状況を確認するには、次のいずれかを使用します。

1. NetBackup Web UI の[ディスクストレージ (Disk storage)]ページの[ユニバーサル共有 (Universal shares)]タブで、クォータの使用状況を確認します。[使用済みのクォータ (Quota used)]列には、現在のクォータの使用状況が表示されます。

2. Windows にマウントされている SMB 共有の場合は、マウントポイントまたはドライブのプロパティを指定して df コマンドを実行します。

   例:

   ```
   # df -h /mnt/vpfs_shares/test/test
   Filesystem Size  Used Avail Use% Mounted on
   vpfsd      2.0T  1.9G  2.0T   1% /mnt/vpfs_shares/test/test
   ```

3. コマンド vpfs_quota を使用して、クォータの使用状況を問い合わせます。ユニバーサル共有アクセラレータの場合は、作業負荷コンピュータでコマンドを実行する必要があります。出力はコマンド vpfs_quota に由来し、Web UI と異なる場合があります。

   ```
   vpfs_quota
   Usage:
   vpfs_quota <status> <share_id>
   ```

   例:

   ```
   /usr/openv/pdde/vpfs/bin/vpfs_quota status test
                Quota: 2199023255552
                 Used: 1933574144
                 Enabled: Yes
   ```

ユニバーサル共有のクォータの修復

状況によっては、クォータファイルが破損しているか、使用量クォータが正しくない場合があります。ユニバーサル共有のクォータを修復するには、/usr/openv/pdde/vpfs/bin/vpfs_quota repair *<share ID>* を使用できます。共有のクォータを修復するには、次の手順を実行します。

ユニバーサル共有のクォータを修復する方法

1 ユニバーサル共有に書き込み操作がないことを確認します。

2 *<storage>*/meta_dir/<share_dir>/<share_id>/quota.dat の quota.dat のバックアップコピーを 1 つ作成します。

例:

```
mv /msdp/meta_dir/test/test/quota.dat
/msdp/meta_dir/test/test/quota.dat.bak
```

3 クォータを修復するには、コマンド `vpfs_quota repair` を使用します。

例:

```
/usr/openv/pdde/vpfs/bin/vpfs_quota repair test
```

4 NetBackup サービスを再起動します。

- NetBackup アプライアンス、BYO、または Flex メディア: `netbackup stop/start`
- Flex WORM、Flex Scale、AKS、または EKS: `dedupe vpfs stop, dedupe vpfs start`

メモ: この手順では重複排除シェルでのクォータの修復はサポートされていません。WORM ストレージサーバーでクォータを修復するにはアプライアンスのロックを解除する必要があります。

ユニバーサル共有アクセラレータの指定した時点へのリカバリ

ユニバーサル共有アクセラレータの指定した時点またはスナップショットをリカバリするには、ストレージサーバー側で共有 ID の権限を付与するための作業が必要です。これらの権限により、クライアント側のアクセラレータはその共有 ID を使用してストレージサーバーに接続できます。

指定した時点またはスナップショットからのアクセラレータの作成

次の手順を使用して、1 つのスナップショットをリカバリし、ユニバーサル共有アクセラレータで開始します。`usa_snap` の ID は、次の手順で新しいアクセラレータ ID として使用されます。

ストレージ側

◆ アクセラレータの共有 ID である新しい共有 ID を登録します。

```
vpfscld --manage_accl_id --reg --share_id usa_snap --mode byo
--lsu labvol --client usademo.name.name.domain.com
```

クライアント側:

1 クラウドバケットからスナップショットをリカバリします。 `vpfscld --list` コマンドを使用して、リカバリ前のスナップショット PIT を見つけます。

```
vpfscld --list
/msdp/meta_dir/usa/usa
Name: pit_0f0430a8-4cea-41dc-8e22-ed1b6f7804e9
Type: full
Create_time: 1683642234
```

- Name: 共有のリカバリに使用できるスナップショット ID。
- Type: スナップショット形式。完全または増分のいずれかになります。
- Create_time: スナップショットの作成日時。

2 クライアントでリカバリします。

```
vpfscld --recover
--share_id usa
--tgt_id usa_snap
--pit pit_0f0430a8-4cea-41dc-8e22-ed1b6f7804e9
--lsu labvol
```

- share_id: 元のユニバーサル共有アクセラレータの共有 ID。
- tgt_id: ターゲット共有 ID。
- pit: リカバリの実行に使用されるスナップショット ID。
- lsu: クラウドボリューム名。

3 次を使用して新しいアクセラレータを起動します。

```
vpfs_accelerator.sh --start --share-id usa_snap
```

4 新しいマウントポイントはアクセラレータのすべてのファイルにアクセスできます。

例:

```
/mnt/vpfs_shares/usa_/usa_snap
```

リカバリされたユニバーサル共有アクセラレータの削除

NetBackup Web UI では、リカバリされたユニバーサル共有アクセラレータは管理されません。これは、手動で削除する必要があります。リカバリされたアクセラレータを削除するには、次の手順を実行します。

usa_snap の ID は、次の手順で新しいアクセラレータ ID として使用されます。

クライアント側:

1 ユニバーサル共有アクセラレータを停止します。

```
vpfs_accelerator.sh --stop --share-id=usa_snap
```

2 アクセラレータを削除します。

```
vpfs_accelerator.sh --delete --share-id=usa_snap
```

ストレージサーバー側:

◆ 共有 ID を登録解除します。

```
vpfscld --manage_accl_id --unreg --share_id usa_snap --mode byo
--client usademo.name.name.domain.com
```

ユニバーサル共有アクセラレータのログ

ユニバーサル共有アクセラレータのログメッセージまたはログファイルは、クライアント、ストレージサーバー、メディアサーバー、プライマリサーバーに作成されます。ログファイルは次の場所にあります。

- クライアント:
  - <storage-path>/log/
  - /usr/openv/netbackup/logs/
- ストレージ/メディアサーバー:
  - <storage-path>/log
  - /usr/openv/netbackup/logs/
  - /usr/openv/logs/
- プライマリサーバー:
  - /usr/openv/netbackup/logs/
  - /usr/openv/logs/

取り込みモードでのユニバーサル共有へのバックアップデータのロード

ユニバーサル共有の取り込みモードは、データをダンプしたり、作業負荷からNFS/CIFSを介してユニバーサル共有にバックアップデータをロードしたりすることが目的です。取り込みモードが有効になっている場合、バックアップスクリプトは、バックアップまたはダンプの終了時に、メモリからディスクにすべてのデータをクライアント側で保持するようにユニバーサル共有が要求されます。

取り込みモードは、ユニバーサル共有の通常モードとは少し異なります。取り込みモードでは、残りのバックアップデータまたはダンプデータがユニバーサル共有内のディスクに保持されるようにする操作が追加で必要です。60 秒ごとに、バックグラウンドジョブは定期的にフラッシュし、取り込まれたデータをディスクに保持します。

取り込みモードは、取り込みモードがオフになるまですべての取り込みデータがディスクに保持されることを保証しないため、通常モードよりも高速です。したがって、データダンプの整合性のためには、取り込みモードをオフにすることが重要です。

取り込みモードの使用

1. ユニバーサルを作成し、クライアント側でマウントします。プロトコルには、NFS または CIFS/SMB を指定できます。
2. 取り込みモードをオンにします。

   NFS/SMB クライアント側の特定の共有に対して取り込みモードをオンにできます。この場合、取り込みモードは指定した共有にのみ適用されます。

   たとえば、次のコマンドを使用して、Linux/UNIX または Windows で取り込みモードをオンにできます。

   - NFS を介した Linux/UNIX の場合:

     ```
     (echo [vpfs]&& echo ingest_mode=on) >
      <nfs_mount_point>/.vpfs_special_control_config
     ```

   - CIFS/SMB を介した Windows の場合:

     ```
     (echo [vpfs]&& echo ingest_mode=on) >
      <driver_letter>/.vpfs_special_control_config
     ```

3. ユニバーサル共有にデータをバックアップするか、データをダンプします。
4. バックアップまたはダンプの完了後、NFS/SMB クライアント側で取り込みモードをオフにします。例:

   - NFS を介した Linux/UNIX の場合:

     ```
     (echo [vpfs]&& echo ingest_mode=off) >
      <nfs_mount_point>/.vpfs_special_control_config
     ```

   - CIFS/SMB を介した Windows の場合:

     ```
     (echo [vpfs]&& echo ingest_mode=off) >
      <driver_letter>/.vpfs_special_control_config
     ```

   コマンドの戻り値を確認してください。戻り値が 0 でない場合、データが正常に維持されなかった可能性があります。その場合は、データを再度バックアップまたはダンプする必要があります。

取り込みモードを使用した NFS または SMB を介したスナップショットの取得

この機能は、完全なスナップショットまたは増分スナップショットを作成する機能を提供します。完全なスナップショットが作成されると、vpfsd はメタデータとデータの一貫性を確保し、クラウドバケットにデータをアップロードします。増分スナップショットが作成される

と、vpfsd は最後の完全なスナップショットまたは増分スナップショット以降に変更されたメタデータとデータを識別します。これらの変更はクラウドバケットにアップロードされます。

NFS または SMB を介したスナップショットの作成

- クライアント側からスナップショットを作成します。

  スナップショットで、vpfs_special_control_config コントロールファイルに次のキーと値のペアの内容を追加します。

  ```
  snapshot=[full/incr]
  ```

  例:

  ```
  (echo [vpfs]&& echo snapshot=full && echo ingest_mode=off) >
  <nfs_mount_point>/.vpfs_special_control_config
  ```

取り込みモードを使用した NFS または SMB を使用したポリシーの実行

この機能は、vpfs を使用してユニバーサル共有の NetBackup バックアップポリシーを実行する機能を提供します。この機能を使用する前に、NetBackup プライマリサーバーでユニバーサル共有バックアップポリシーを作成する必要があります。

バックアップポリシーを実行するには、バックアップキーと値のペアと backup_selection のキーと値のペアを .vpfs_special_control_config に追加する必要があります。backup_selection は、バックアップごとに特別なパスまたはディレクトリをバックアップする場合にのみ必要です。backup_selection 機能では、ポリシーが実行されるたびにポリシーのバックアップ対象が更新されます。backup_selection を使用する場合は、backup_selection を常に指定する必要があります。

バックアップキーと値のペアには、次を使用します。

```
backup=<NetBackup policy name>:<backup schedue>:<backup client>
```

バックアップ対象のキーと値のペアには、次を使用します。

```
backup_selection=<path1>:<path2>:<pathN>
```

作業負荷からバックアップを作成する例:

```
(echo [vpfs]&& echo backup=
ushare-policy-01:full-backup-schedule:ushare-client
&& echo ingest_mode=off) >
<nfs_mount_point>/.vpfs_special_control_config
```

backup_selection を使用してバックアップを作成する例:

```
(echo [vpfs]&& echo backup=
ushare-policy-01:full-backup-schedule:ushare-client && echo
backup_selection=
/mnt/vpfs_shares/usha/ushare/dir1:/mnt/vpfs_shares/usha/ushare/dir2

&& echo ingest_mode=off) >
<nfs_mount_point>/.vpfs_special_control_config
```

MSDP データボリュームが無効なユニバーサル共有

ユニバーサル共有は、複数のデータボリュームをサポートします。データとメタデータは、構成されているすべてのデータボリュームに分散されます。複数のデータボリュームがある環境では、ユニバーサル共有は、1 つ以上のデータボリュームをユニバーサル共有のために無効にする機能をサポートします。新しいファイルのデータとメタデータは、無効になっているデータボリュームには書き込まれなくなりました。ただし、ユニバーサル共有は既存のファイルのデータまたはメタデータを読み取ることがあります。オブジェクトストアがユニバーサル共有に対して有効になっていると、ローカルディスクデータは無効なデータボリュームにも書き込まれなくなります。

メモ: 最初のデータボリュームをユニバーサル共有用に無効にすることはできません。

ユニバーサル共有用にデータボリュームを無効にするには:

1. `crcontrol` コマンドを使用してデータボリュームを無効にします。

   ```
   crcontrol --dswriteoff [path]
   ```

2. ユニバーサル共有の再起動:

   ```
   vpfs_mounts stop
   vpfs_mounts start
   ```

ユニバーサル共有の WORM 機能

ユニバーサル共有内のデータに NFS または SMB からアクセスする場合、それらは WORM 対応ではありません。NFS または SMB からデータを変更または修正できます。

WORM ストレージサーバーで、Universal-Share ポリシーを使用して、ユニバーサル共有を NetBackup カタログに取り込み、カタログまたはバックアップイメージを WORM 対応にします。

イメージは別のメディアサーバーに複製でき、別の NetBackup ドメインにレプリケートできます。また、イメージを使用してインスタントアクセスユニバーサル共有を作成でき、元のユニバーサル共有にデータをリストアできます。

ユニバーサル共有のスケールアウト

ユニバーサル共有のスケールアウト機能を使用すると、クラスタ環境のすべてのディスクストレージを使用できます。ユニバーサル共有クラスタは、各エンジンまたはノードがクラスタのデータにアクセスすることが可能なクラスタ環境内にあるすべてのノードまたはエンジンにファイルシステムの操作を分散します。任意のホスト名を使用して、ユニバーサル共有をマウントし、データにアクセスできます。この機能は、NetBackup Web UI で NFS/SMB サーバーのアクセス権限を制御する機能も提供します。データは、オブジェクトバケットまたはローカルディスクストレージで直接使用できます。

通常の単一ノードのユニバーサル共有は、ユニバーサル共有クラスタと共存できます。ユニバーサル共有クラスタへのアップグレードまたは変換はサポートされていません。現在の NetBackup バージョンにアップグレードした場合、通常の単一ノードのユニバーサル共有に変更はありません。

サポート対象プラットフォーム

- NetBackup Cloud Scale
- NetBackup Flex Scale

制限事項

- エンジンまたはノードに対してトリガされるフェールオーバー操作が実行中の一部のファイルにはアクセスできない場合があります。フェールオーバー操作が完了すると、ファイルにアクセスできるようになります。
- この機能は複数の vpfsd インスタンスをサポートしません。

ユニバーサル共有クラスタの構成

ユニバーサル共有クラスタを構成するには、最初にクラスタを作成してから、ユニバーサル共有クラスタをマウントする必要があります。

ユニバーサル共有クラスタの作成

前提条件 - クラスタ内のすべてのエンジン間で TCP 10090 ポートにアクセスできることを確認します。

シナリオ 1: ローカルディスクストレージにデータを転送する

ローカルストレージにデータを転送するには

1 メディアサーバー重複排除プールを作成します。

p.87 の「メディアサーバー重複排除プールのストレージサーバーの構成」を参照してください。

2 ユニバーサル共有を作成します。

形式として[クラスタ (Cluster)]を選択します。

p.572 の「ユニバーサル共有の作成」を参照してください。

シナリオ 2: クラウドバケットにデータを転送する

クラウドストレージにデータを転送するには

1 ユニバーサル共有データをオブジェクトストアに転送します。

この手順は、NetBackup Flex Scale でのみ必要です。

p.592 の「オブジェクトストアへのユニバーサル共有データの指定」を参照してください。

2 ユニバーサル共有を作成します。

形式として[クラスタ (Cluster)]を選択します。

p.572 の「ユニバーサル共有の作成」を参照してください。

ユニバーサル共有クラスタのマウント

次の項の手順を参照してください。

p.583 の「ユニバーサル共有のマウント」を参照してください。

ユニバーサル共有のエクスポート済みマウントパスの編集

次の項の手順を参照してください。

p.581 の「ユニバーサル共有の表示または編集」を参照してください。

ユニバーサル共有クラスタの削除

次の項の手順を参照してください。

p.582 の「ユニバーサル共有の削除」を参照してください。

ユニバーサル共有サービスの管理

次のサービスを使用してユニバーサル共有を管理できます。

- VPFS (Veritas プロビジョニングファイルシステム)
- VLD (可変長の重複排除) アルゴリズム

vpfs_stats ユーティリティを使用したデータボリュームのスキャン

vpfs_stats ユーティリティは、データボリュームをスキャンし、vpfsd が消費するディスク容量の使用状況を計算します。これは、vpfsd またはユニバーサル共有からのデータによって消費されるデータディスク容量を計算するのに役立ちます。

次の場合、ディスク容量のサイズは vpfsd 領域として表示されます。

- vpfsd によってデータが書き込まれたが、そのデータを消費するのがバックアップイメージである。
- ユニバーサル共有または vpfsd データがすべて削除されたが、ユニバーサル共有のバックアップイメージがいくつか残っている。

次の例は、vpfs_stats ユーティリティの形式を示しています。

```
vpfs_stats [options]...
```

オプション:

- `--data-volume [--local] [--cloud]`
  VPFS データボリュームの使用状況の統計を表示します。デフォルトでは、ローカルストレージとクラウドストレージの使用状況の統計が表示されます。ローカルの使用状況の統計のみを表示するには、`--local` オプションを使用します。クラウドの使用状況の統計のみを表示するには、`--cloud` オプションを使用します。
- `-help --help`
  ユーティリティのヘルプテキストを表示します。

次に示すのは vpfs_stats --data-volume の例です。

```
[root@hostname ~]# /usr/openv/pdde/vpfs/bin/vpfs_stats --data-volume


Start to scan data volume /msdp/vol1/data
Start to scan data volume /msdp/vol2
Finished scan data volume /msdp/vol1/data
Finished scan data volume /msdp/vol2

=================== Data volume summary ============================
Number of data volume                        : 2

Data volume 1                                : /msdp/vol1/data
Number of data container groups              : 6
Number of vpfs data container groups         : 4
Vpfs data size                              : 2958014398 bytes(2.8GB)
```

```
Data volume 2                                : /msdp/vol2
Number of data container groups              : 4
Number of vpfs data container groups         : 4
Vpfs data size                               : 103 bytes(0.0MB)

All Data volumes
Number of data container groups              : 10
Number of vpfs data container groups         : 8
Vpfs data size                              : 2958014501 bytes(2.8GB)



==================== Vpfs cloud cache summary ========================
Number of data volume                        : 2

Data volume 1                                : /msdp/vol1/data
Number of data container groups              : 0
Number of vpfs data container groups         : 1
Vpfs data size                              : 4533165734 bytes(4.2GB)


Data volume 2                                : /msdp/vol2
Number of data container groups              : 0
Number of vpfs data container groups         : 1
Vpfs data size                              : 5129660901 bytes(4.8GB)


All Data volumes
Number of data container groups              : 0
Number of vpfs data container groups         : 2
Vpfs data size                              : 9662826635 bytes(9.0GB)



==================== Overall volume usage summary ====================
Number of data volume                        : 2

Data volume 1                                : /msdp/vol1/data
Number of data container groups              : 6
Number of vpfs data container groups         : 5
Vpfs data size                              : 2958014398 bytes(7.0GB)
```

```
Data volume 2                                  : /msdp/vol2
Number of data container groups                : 4
Number of vpfs data container groups           : 5
Vpfs data size                                 : 103 bytes(4.8GB)

All Data volumes
Total number of data container groups          : 10
Total number of vpfs data container groups     : 10
Total vpfs data size                           : 12620841136
bytes(11.8GB)
```

vpfsd インスタンス数の変更

ユニバーサル共有は、デフォルトで 1 つの vpfsd インスタンスを使用します。ほとんどの場合、1 つのインスタンスで十分です。vpfsd インスタンスの数を増やすと、ユニバーサル共有のパフォーマンスが向上する可能性がありますが、必要な CPU とメモリも増えます。vpfsd インスタンスの数は 2 から最大 16 まで増やすことができ、共有はすべての vpfsd インスタンスに分散できます。

ユニバーサル共有の vpfsd インスタンスの数を変更するには

1 メディアサーバーの NetBackup を停止します。

```
systemctl stop netbackup
```

または

```
/usr/openv/netbackup/bin/goodies/netbackup stop
```

2 vpfsd インスタンスの数を変更します。

`vpfsd_config.json` ファイルの `numOfInstance` 値を変更します。値は 2 から 16 の整数である必要があります。例:

```
grep numOfInstance /msdp/vol1/etc/puredisk/vpfsd_config.json
"numOfInstance": 2,
```

BYO (build-your-own): *<storage path>*`/etc/puredisk/vpfsd_config.json`

NetBackup Appliance および NetBackup Flex Scale: `/msdp/data/dp1/pdvol/etc/puredisk/vpfsd_config.json`

NetBackup Flex: `/mnt/msdp/vol0/etc/puredisk/vpfsd_config.json`

3 メディアサーバーで NetBackup を起動します。

```
systemctl start netbackup
```

または

```
/usr/openv/netbackup/bin/goodies/netbackup start
```

メモ: NetBackup 10.3 はマルウェアスキャンに個別の vpfsd インスタンスを使用するため、少なくとも 1 つの vpfsd インスタンスを予約する必要があります。マルウェアスキャン用の vpfsd インスタンスは、numOfScanInstance の値を変更することで構成できます。値は 1 から 4 の整数で、numOfScanInstance は numOfInstance 未満である必要があります。

ユニバーサル共有またはユニバーサル共有内のフォルダの重複排除率の確認

ユニバーサル共有の重複排除率を確認します。

```
/usr/openv/pdde/vpfs/bin/vpfs_metadump dedupe
/mnt/vpfs_shares/<share_dir>/<share_id>
```

ユニバーサル共有フォルダの重複排除率を確認します。

```
/usr/openv/pdde/vpfs/bin/vpfs_metadump dedupe
/mnt/vpfs_shares/<share_dir>/<share_id> <sub_dir>
```

使用例と出力例:

```
/usr/openv/pdde/vpfs/bin/vpfs_metadump dedupe
/mnt/vpfs_shares/02b1/02b1e846-949f-5e55-8e39-e9900cd6a25e LT_0.1_20_1
```

```
File Name   File Size   Stored Size Overall Rate    Dedupe Rate Compress Rate
[INFO]: /LT_0.1_20_1/db_dump.1of14: 3043.42MB, 30.26MB, 99%, 93.31%, 85%
[INFO]: /LT_0.1_20_1/db_dump.2of14: 3043.42MB, 28.10MB, 99%, 93.94%, 84%
[INFO]: /LT_0.1_20_1/db_dump.3of14: 3045.02MB, 32.78MB, 98%, 92.82%, 85%
[INFO]: /LT_0.1_20_1/db_dump.4of14: 3044.93MB, 38.48MB, 98%, 91.44%, 85%
[INFO]: /LT_0.1_20_1/db_dump.5of14: 3044.93MB, 29.05MB, 99%, 93.78%, 84%
[INFO]: /LT_0.1_20_1/db_dump.6of14: 3044.93MB, 30.06MB, 99%, 93.45%, 84%
[INFO]: /LT_0.1_20_1/db_dump.9of14: 3043.42MB, 26.71MB, 99%, 94.27%, 84%
[INFO]: /LT_0.1_20_1/db_dump.8of14: 3043.42MB, 32.05MB, 98%, 93.07%, 84%
[INFO]: /LT_0.1_20_1/db_dump.10of14: 3043.42MB, 31.12MB, 98%, 93.36%, 84%
[INFO]: /LT_0.1_20_1/db_dump.12of14: 3044.93MB, 31.57MB, 98%, 93.13%, 84%
[INFO]: /LT_0.1_20_1/db_dump.11of14: 3044.93MB, 27.08MB, 99%, 94.23%, 84%
[INFO]: /LT_0.1_20_1/db_dump.7of14: 3043.42MB, 25.31MB, 99%, 94.65%, 84%
[INFO]: /LT_0.1_20_1/db_dump.13of14: 3044.93MB, 31.09MB, 98%, 93.33%, 84%
[INFO]: /LT_0.1_20_1/db_dump.14of14: 3044.93MB, 36.60MB, 98%, 91.79%, 85%
[INFO]: total size: 42620.06MB, stored size: 430.25MB, overall rate: 98.99%,
dedupe rate: 93.33%, compress rate:84%
    [0K, 8K): 0.0%
    [8K, 16K): 0.0%
    [16K, 24K): 0.7%
    [24K, 32K): 0.5%
    [32K, 40K): 98.8%
[INFO]: total SO: 1368688, average SO: 31K
```

ユニバーサル共有に対する VLD (可変長の重複排除) アルゴリズムの構成

重複排除エンジンはバックアップイメージをセグメントに分割し、その重複排除ノードに保存されているすべてのセグメントと比較します。一意のセグメントのみがストレージサーバーの NetBackup 重複排除エンジンに送信されます。重複排除エンジンは、データをメディアサーバー重複排除プールに書き込みます。

p.171 の「NetBackup クライアントでの可変長の重複排除について」を参照してください。

NetBackup 重複排除エンジンは、いくつかの種類の可変長の重複排除アルゴリズムを提供します。ユニバーサル共有に可変長の重複排除アルゴリズムを 1 つ使用すると、重複排除率が向上します。

ユニバーサル共有に対しては、可変長の重複排除アルゴリズムはデフォルトでは有効になりません。ただし、MSSQL と Sybase アプリケーションに対しては、可変長の重複排除アルゴリズムは自動的に有効になります。アルゴリズムの構成を管理するには、`vpfs_actions` コマンドラインユーティリティを使用します。

ユニバーサル共有に対する可変長の重複排除アルゴリズムを構成するには

1. メディアサーバーの次の場所に移動します。

   ```
   /usr/openv/pdde/vpfs/bin/
   ```

2. 次のコマンドを実行して、現在の構成を確認します。

   ```
   /usr/openv/pdde/vpfs/bin/vpfs_actions -a tune --imageId <share_id>
   ```

   次に出力例を示します。

   ```
   segment_type: "vld"
   applications: [{"type": "vld", "sw_min": 16, "sw_max": 32}]
   status: 0
   ```

3. 可変長の重複排除のバージョンを構成します。

   ```
   /usr/openv/pdde/vpfs/bin/vpfs_actions -a tune --imageId <share_id>
   --segment <VLD-version> --sw_min <sw_min> --sw_max <sw_max>
   ```

メモ: イメージバックアップがストレージに存在しない新しい環境の場合、初回の構成で `-segment VLD` を指定するときに、ユニバーサル共有では VLD ではなく VLD v2 が自動的に使用されます。

オプション	説明
`imageId`	イメージの一意の識別子。

オプション	説明
segment	■ alignment 固定長の重複排除方式を使用します。これはデフォルト値です。alignment に設定されている場合、sw_min および sw_max は必要ありません。 ■ vld 可変長の重複排除アルゴリズムのバージョン 1。 ■ vldv2 可変長の重複排除アルゴリズムのバージョン 2。このバージョンをデフォルトとして使用することをお勧めします。 ■ vldv3 可変長の重複排除アルゴリズムの別のバージョン。
sw_min	セグメンテーション範囲 (16 から 127) の最小セグメントサイズ (KB)。 推奨値は 16、32、64 です。
sw_max	セグメンテーション範囲 (17 から 128) の最大セグメントサイズ (KB)。この値は sw_min より大きくする必要があります。 推奨値は 32、64、128 です。

ユニバーサル共有操作でのマーカーファイルインターフェースの使用

VPFS スケジューラデーモンは、さまざまなユニバーサル共有操作を実行するためのマーカーファイルインターフェースを備えています。

VPFS スケジューラデーモンを構成するには

1 VPFS スケジューラデーモンを有効にします。

VPFS スケジューラは、次のいずれかの機能が有効になった後、自動的に有効になります。

- ユニバーサル共有の同時ダンプ制御
  詳しくは、「「ユニバーサル共有の同時ダンプ制御を構成するには」」のトピックを参照してください。
- ユニバーサル共有の自動バックアップ

詳しくは、「「ユニバーサル共有の自動バックアップを構成するには 」」のトピックを参照してください。

2 VPFS スケジューラデーモンは、少なくとも 1 つの機能が有効になった後、自動的に起動します。VPFS スケジューラを手動で開始するには、次のコマンドを実行します。

```
/usr/openv/pdde/vpfs/bin/vpfs_sched start
```

3 VPFS スケジューラデーモンの次のパラメータを構成します。

`VpfsScheduler.vpfsSchedInterval`	操作の各ループ間の間隔 (秒)。
`VpfsScheduler.vpfsSchedLogLevel`	最小ログレベル。 指定可能な値: error、warning、information、debug。

ユニバーサル共有の同時ダンプ制御を構成するには

1 ユニバーサル共有の同時ダンプ制御を有効にします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action setVpfsConfigValue
--key enableShareDumpThrottling --value true
```

2 ユニバーサル共有の同時ダンプ制御の次のパラメータを構成します。

`enableShareDumpThrottling`	共有ダンプのスロットル機能を有効にするかどうかを指定します。false の場合、共有の同時性は適用されません。
`VpfsScheduler.maxConcurrentActiveClientHostSharePairs`	同時にアクティブにできる最大の「クライアントホストと共有のペア」 この制限に達すると、新しい「クライアントホストと共有のペア」に属する要求されたダンプはキューに登録されます。これらは、他の「クライアントホストと共有のペア」が非アクティブに設定されている場合にアクティブになります。 値を大きくすると、同時に発生するダンプが増えます。同時に発生するダンプが多いと合計スループットが高くならず、特定のシステムに対して同時処理を調整することが必要になる場合があります。
`VpfsScheduler.shareDumpsInactiveThreshold`	VPFS スケジューラデーモンが待機する共有内の最後の IO 操作以降の最小時間 (秒)。指定した時間が経過すると、「クライアントホストと共有のペア」は非アクティブになります。 たとえば、この値を 300 に設定し、共有内で少なくとも 300 秒間 IO 操作が検出されない場合、「クライアントホストと共有のペア」はアクティブリストから削除されます。
`VpfsScheduler.enableShareDumpThrottlingReporting`	スロットルテーブル内に「クライアントホストと共有のペア」の変化を記録するかどうかを指定します。 変化には、キューに登録された、アクティブになった、または非アクティブになった「クライアントホストと共有のペア」が含まれます。

3 この機能を有効にする前に作成された既存の共有にダンプスクリプトをコピーします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action syncShareScript
```

4 ダンプ開始スクリプトを作業負荷の開始に追加し、作業負荷の最後に dump_end スクリプトを使用します。

次に例を示します。

- Windows バッチダンプスクリプト

```
¥¥hostname¥ushare-smb1¥.share-builtin-scripts¥dump_start.bat
--dump-id <dump_id>

Existing workload dumping data to universal share

¥¥hostname¥ushare-smb1¥.share-builtin-scripts¥dump_start.bat
--dump-id <dump_id>
```

- Linux bash ダンプスクリプト

```
/mnt/ushare_smb1/.share-builtin-scripts/dump_start.sh
--dump-id <dump_id>

Existing workload dumping data to universal share

/mnt/ushare_smb1/.share-builtin-scripts/dump_end.sh
--dump-id <dump_id>
```

メモ: dump_id を指定する必要があります。ランダムに生成した ID が推奨されますが、同じクライアントホストと共有のペアで使用されている他のダンプスクリプトとは異なっている必要があります。SQL Server の場合は、dump_id にジョブ ID を使用することをお勧めします。

- 既存のユニバーサルダンプのスロットルテーブルを表示します。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions -a dumpThrottleTable
```

ユニバーサル共有の自動バックアップを構成するには

1 ユニバーサル共有の自動バックアップを有効にします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action setVpfsConfigValue
--key VpfsScheduler.autoUShareBackupEnabled --value true
```

2 ユニバーサル共有の自動バックアップについて次のパラメータを構成します。

`VpfsScheduler.autoUShareBackupEnabled`	ユニバーサル共有の自動バックアップ機能を有効にします。
`VpfsScheduler.autoUShareBackupCheckInterval`	ユニバーサル共有のタッチファイルを確認する間隔。
`VpfsScheduler.autoUShareBackupJobCheckInterval`	この機能によってトリガされるユニバーサル共有のバックアップジョブの実行状態を確認する間隔。
`VpfsScheduler.autoUShareBackupPolicyFile`	ファイルシステムに設定されているポリシーファイルの場所。
`VpfsScheduler.autoUShareBackupOutputFile`	ファイルシステム内の出力ファイルの場所。完了したユニバーサル共有のバックアップジョブの詳細がファイルに書き込まれます。

3 ユニバーサル共有の自動バックアップによってトリガされるようにユニバーサル共有のバックアップポリシーを構成します。

トリガする必要があるユニバーサル共有ポリシーのリストから構成されるポリシーファイルを構成します。ポリシーファイルの場所は、`vpfs_actions` コマンドを使用して構成できる構成可能なパス `VpfsScheduler.autoUShareBackupPolicyFile` です。

ポリシー構成の各エントリは、ポリシー名、クライアント名、およびマーカーファイルの場所で構成されます。

例:

```
pl-ushare-nfs-1,host.domain.com,/mnt/vpfs_shares/
usha/ushare-nfs-1/backup
pl-ushare-nfs-2,host.domain.com,/mnt/vpfs_shares/usha/ushare
-nfs-2/backup
```

ポリシーファイルが変更されると、ポリシー構成が自動的に再ロードされます。

4 バックアップスケジュールのローテーションを構成します。

バックアップスケジュールは、キーと値のペアで構成されます。キーは平日 (月曜日から日曜日) で、値はユニバーサル共有のバックアップ形式のリストです。デフォルトの構成は、FULL、INCR、CINC、月曜日から日曜日までの毎日です。

次のバックアップ形式がサポートされます。

- FULL: 完全バックアップ
- INCR: 差分増分バックアップ
- CINC: 累積増分バックアップ

5 ユニバーサル共有の構成場所にマーカーファイルを作成します。ポリシーファイル `VpfsScheduler.autoUShareBackupPolicyFile` にマーケットファイルパスを構成した後、指定した場所にマーカーファイルを作成してバックアップをトリガします。

マーカーには、次の形式で名前を付ける必要があります。

`BACKUP_SUCCESS_<XXXX>_touch_<Date>` or `BACKUP_SUCCESS_<XXXX>_touch_<Date>_<Timestamp>`

`<XXXX>` は省略可能で、空白以外の任意の文字列を指定できます。`<Date>` は YYYYMMDD 形式にする必要があります。`<Timestamp>` は、毎回一意のタイムスタンプ (HHmmSS など) である必要があります。

データとタイムスタンプは平日に変換されます。その後、バックアップスケジュールを決定するために使用されます。

ユニバーサル共有のバックアップは、5 分より古い作成タイムスタンプを持つ新しいマーカーファイルを見つけるとトリガされます。

6 バックアップの正常に実行されたことを確認します。

バックアップジョブの状態を確認するには、NetBackup Web UI を参照してください。バックアップが成功すると、ジョブ情報はファイル (`VpfsScheduler.autoUShareBackupOutputFile` で構成可能) にも保存されます。

出力の形式は次のとおりです。

```
<job_id>,<schedule>,<state>,<status>,<total_size_kb>KB,<start_time>,
<end_time>,<client>,<policy>,<ushare_mount>
```

ユニバーサル共有に関連する問題のトラブルシューティング

このセクションでは、ユニバーサル共有の使用中に発生する可能性のある問題のトラブルシューティングについて説明します。

ユニバーサル共有の構成に関する問題をトラブルシューティングする

失敗したインストールまたは構成をトラブルシューティングする方法

ユニバーサル共有を構成するには、ストレージサーバーでインスタントアクセスが有効になっていることを確認します。インスタントアクセスについて詳しくは、次のマニュアルを参照してください。

- 『NetBackup for VMware 管理者ガイド』
- 『NetBackup for Microsoft SQL 管理者ガイド』

ストレージサーバーでインスタントアクセスが有効になっていることを確認するには

1. ストレージサーバーにログオンして、次のコマンドを実行します (BYO (Build Your Own) のみ)。

   ```
   /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
   ```

2. 前提条件の確認結果と構成結果を確認します。

   `/var/log/vps/ia_byo_precheck.log` (BYO のみ)

   `/usr/openv/pdde/vpfs/vpfs-config.log` (BYO とアプライアンス構成)

   次の例では、必要ないくつかのサービスが実行されていません。

   ```
   [root@rhelnbu06 ~]# /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
   Mon Apr 13 12:42:14 EDT 2020 Try to get storagepath
   Mon Apr 13 12:42:14 EDT 2020 Storage ContentRouter config path
   is
      /msdp/etc/puredisk/contentrouter.cfg
   Mon Apr 13 12:42:14 EDT 2020 Storagepath is /msdp
   Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp is
      ext2/ext3
   Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp/data

      is ext2/ext3
   Mon Apr 13 12:42:14 EDT 2020 **** Hardware Virtualization not
      supported, Instant Access browse may be slow ****
   Mon Apr 13 12:42:14 EDT 2020 **** system memory support 50 vpfs
      livemounts ****
   Mon Apr 13 12:42:14 EDT 2020 **** nginx service required by
      Instant Access is not running ****
   Mon Apr 13 12:42:14 EDT 2020 **** smb service required by
      Instant Access is not running ****
   Mon Apr 13 12:42:14 EDT 2020 **** docker service required by
      VMware Instant Access is not running ****
   ```

3. ログに示されている問題を解決します。たとえば、インスタントアクセスに必要なすべてのサービスを再起動します。

ユニバーサル共有機能を確認する方法

ストレージサーバーがユニバーサル共有機能を備えていることを確認するには

1. ストレージサービスが NetBackup 8.3 以降を実行していることを確認します。
2. ストレージサーバーにログオンして、次のコマンドを実行します。

   ```
   nbdevquery -liststs -U
   ```

   コマンドの出力に InstantAcess フラグが表示されていることを確認します。

   このフラグが表示されない場合は、前述のいずれかのガイドを参照して、ストレージサーバーでインスタントアクセスを有効にします。
3. 次のコマンドを実行します。

   ```
   nbdevconfig -getconfig -stype PureDisk -storage_server
   storage_server_name
   ```

   コマンドの出力に UNIVERSAL_SHARE_STORAGE フラグが表示されていることを確認します。

   このフラグが表示されない場合は、ストレージサーバーでユニバーサル共有を作成します。

   p.572 の「ユニバーサル共有の作成」を参照してください。

ユニバーサル共有を開始または停止する方法

ユニバーサル共有は、NetBackup サービスを使用して開始、再起動、または停止できます。

- ユニバーサル共有を開始または再起動するには、次のコマンドを使用します。

  ```
  netbackup start
  ```
- ユニバーサル共有を終了するには、次のコマンドを使用します。

  ```
  netbackup stop
  ```

NetBackup Web UI でユニバーサル共有が作成されるたびに、マウントポイントもストレージサーバーに作成されます。

次に例を示します。

```
[root@rsvlmvc01vm309 vpfs.mnt]# mount | grep vpfs
vpfsd on /mnt/vpfs type fuse.vpfsd
(rw,nosuid,nodev,relatime,user_id=0,
   group_id=0,default_permissions,allow_other)
vpfsd on /mnt/vpfs_shares/aa7e/aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e
   type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,group_id=0,
   default_permissions,allow_other)
```

この例では aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e がユニバーサル共有の ID です。この ID は、NetBackup Web UI のユニバーサル共有の詳細ページにあります。左側で[ストレージ (Storage)]、[ディスクストレージ (Disk storage)]、[ユニバーサル共有 (Universal Shares)]の順に選択し、ユニバーサル共有を選択して、その詳細を表示します。

ユニバーサル共有 VPFS インスタンスのログ記録とレポート

VPFS 操作に関して追加のレポートとログが生成されます。この情報は、パフォーマンスの分析とトラブルシューティングに使用できます。VPFS 書き込み統計は、JSON 形式で vpfsd 履歴に保存されます。

このファイルは、<msdp_vol>/history/vpfsd-report の場所に vpfsX_YYYY-MM-DD 形式で格納されます。たとえば、/msdp/vol/history/vpfsd-report/vpfs0_2023-05-01 などです。

サンプルファイル:

```
{"timestamp":1682906052.752,"threadId":140498966533888,"UID":"ushare
-1","UpdateCounter:":4846,"SegmentNumber":39148,"DedupeRate":0.00,"AvgDedupe
TimePerSegment(ms)":0.534,"AvgSegmentSize":128792.79,"AvgWriteTimePerSegment(
ms)":0.003,"TotalWriteSize":5041984256}
```

VPSF インスタンスのログ記録とレポートを構成するには

1 履歴レポートを CVS ファイルにエクスポートします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action getVpfsHistoryStat
--exportPath <export-path> [--targetDate <date> | --targetDateFrom
<start-date> --targetDateTo <end-date>]
```

2 レポートの間隔を変更します。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action setVpfsConfigValue
--key vpfsdReportInterval --value <newInterval>
```

レポートの間隔はデフォルトでは 3,600 秒です。VPSF インスタンスのログ記録とレポートを無効にするには、0 に設定します。

ユニバーサル共有でのファイルシステム操作のための vpfsd ログ

vpfsd ログレポートでは、予想より長い時間がかかったファイルシステム操作のログを記録できます。vpfsd ログレポートを有効にするには 2 つの構成があります。どちらの構成もデフォルトでは無効になっています。

ファイルシステム操作の vpfsd ログ記録を有効にするには

1 ファイルシステム操作のログ記録を有効にします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action setVpfsConfigValue
--key enableVpfsdLogReporting --value true
```

vpfsd ログ記録は、次のファイルシステム操作で有効になります。

- getattr
- rename
- open
- read
- write
- fsync
- truncate
- getDataCacheNodeForWrite

2 拡張されたファイルシステム操作のログ記録を有効にします。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action setVpfsConfigValue
--key enableVpfsdLogReportingExtended --value true
```

vpfsd ログ記録は、すべてのファイルシステム操作に対して有効になります。

3 ファイル内のメッセージを検索します。

```
cat /msdp/vol/log/vpfs/vpfsd/vpfs0_vpfsd.log | grep
"WARNING.*exceeded configured threshold"
```

4 (オプション) ログ記録のしきい値を変更します。

```
/usr/openv/pdde/vpfs/bin/vpfs_actions --action setVpfsConfigValue
--key logReportWriteTimeThreshold --value
```

vpfsd サービスを使用したプライマリサーバーへのイベントの通知

vpfsd サービスは、ファイル破損、チェックポイントエラー、ユニバーサル共有を保護するように設定された NetBackup ポリシーがないなどの問題を検出すると、NetBackup プライマリサーバーに重大なイベントを送信します。

ファイル破損イベントの場合、ユニバーサル共有は次を検出するとイベントを送信します。

- ファイルのメタデータが破損しているか不整合です。
- データコンテナが破損しているか損失しています。

例:

```
File path: <Corrupted file path>
```

```
Share name: <Universal share name>

Storage server: <The storage server for universal share>

Share type: VPFS
```

チェックポイントエラーはデータの一貫性に影響する可能性があり、チェックポイントが繰り返し失敗するとイベントがトリガされます。

ユニバーサル共有を保護するため、NetBackupUniversal-Share ポリシーを構成することをお勧めします。ユニバーサル共有が保護されていない場合、または指定した期間 (デフォルトでは過去 24 時間) に正常なバックアップがない場合、イベントが NetBackup プライマリサーバーに送信されます。

vpfsd サービスを使用したデータ整合性チェックとリカバリ

vpfsd サービスは、データの変更に応じてバックグラウンドでデータ整合性チェックを実行します。メタデータとデータ破損 (自動プロセス) を含むファイル破損が検出されると、イベントが NetBackup プライマリに送信されます。

破損したファイルは次の場所に移動されます。

```
/mnt/vpfs_share/<share dir>/<share ID>/.vpfs_corrupted
```

ファイルの syslog と履歴ログが作成されます。ユニバーサル共有のバックアップでは、問題があるファイルがスキップされます。

自動プロセスとは別に、vpfsck コマンドを使用してファイル破損を手動で確認して検出し、破損したファイルを次の場所に移動できます。

```
/mnt/vpfs_share/<share dir>/<share ID>/.vpfs_corrupted
```

ローカル VPFS のみがサポートされます。

例:

```
--verify_data  --share_id <share id>
 [--t <file creation time older than (int) hours>]
 --check_so    --share_id <share id>
 [--so <so fp, find files that contain this so>]
 [--file_path <check single file or folder,
 path relative to /mnt/vpfs/<share_id<0:4>>/<share_id>>]
 --verbose  optional
```

--share_id 後のすべてのオプションは省略可能です。

処理は <storage>/log/vpfs/vpfsd/vpfsck.log に記録され、オプション --verbose によって vpfsck のデバッグログが有効になります。

15

分離リカバリ環境 (IRE) の構成

この章では以下の項目について説明しています。

要件

プルモデルで IRE (分離リカバリ環境) を構成するための要件を次に示します。

- WORM ストレージサーバー: 17.0 以降 (Flex Appliance: 2.1.1 以降)
- NetBackup BYO メディアサーバー: 10.1 以降
- NetBackup Flex Scale: 3.2 以降
- Access Appliance: 8.2 以降

表 15-1に、分離リカバリ環境の MSDP ソースとターゲットのサポート対象の構成を一覧表示します。

表 15-1 MSDP ソースとターゲットのサポート対象構成

ソース	ターゲット	配備モデル	NetBackup のバージョン	WORM バージョン	レプリケーション - OptDup モデル
MSDP、WORM	WORM	Flex 2.1	10.0	16.0	プッシュモデル

ソース	ターゲット	配備モデル	NetBackup のバージョン	WORM バージョン	レプリケーション - OptDup モデル
MSDP、WORM	MSDP、WORM	BYO、Flex 2.1.1	10.1	17.0	プルモデル
MSDP、WORM	MSDP、WORM	BYO、Flex	10.1.1	17.1	プルモデル、IRE ホストに対する IPv6 + 混合 CA のサポート
MSDP、WORM、MSDP Scaleout	MSDP、WORM、MSDP Scaleout	BYO、Flex、Flex Scale	10.2	18.0	プルモデル
MSDP、WORM、MSDP Scaleout	MSDP、WORM、MSDP Scaleout	BYO、Flex、Flex Scale	10.3	19.0	Web UI

メモ: NetBackup 10.0 および WORM 16.0 の場合、ベリタスダウンロードセンターから、IRE の Flex Appliance 用に Hotfix `VRTSflex-HF3-2.1.0-0.x86_64.rpm` をダウンロードし、WORM ストレージサーバーアプリケーション用に NetBackup EEB `VRTSflex-msdp_EEB_ET4067891-16.0-3.x86_64.rpm` をダウンロードします。

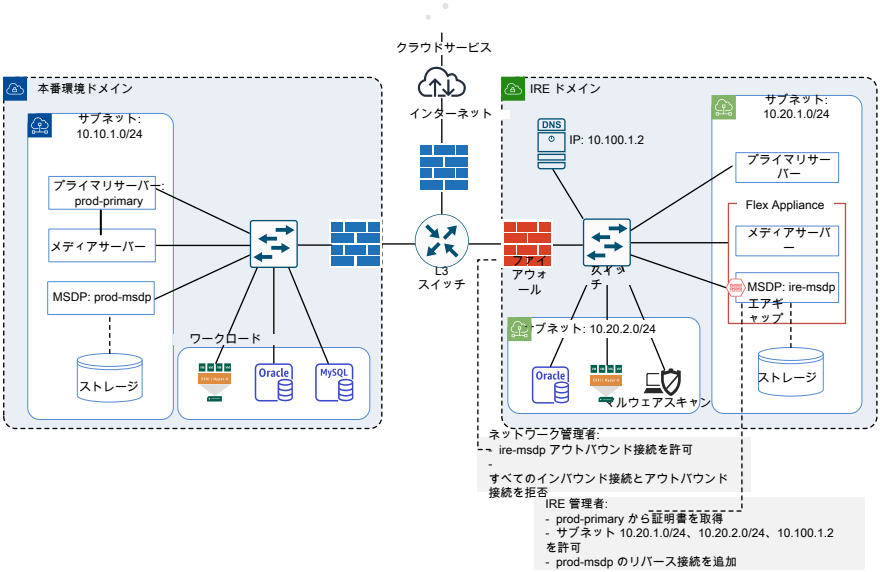
メモ: ソースドメインとターゲットドメインの両方がソフトウェアの最小バージョン要件を満たす必要があります。

10.3.0.1 より前の NetBackup リリースでは、分離リカバリ環境機能は Red Hat Enterprise Linux BYO でのみサポートされています。NetBackup 10.3.0.1 以降、SUSE Linux Enterprise Server BYO でも分離リカバリ環境がサポートされます。

ネットワーク分離の構成

IRE の AIR をサポートするには、IRE MSDP ストレージサーバーから実稼働 MSDP ストレージサーバーへのネットワーク通信が必要です。IRE MSDP ストレージサーバーがネットワーク接続を開始します。AIR を使用した IRE は、実稼動 MSDP サーバーが IRE MSDP サーバーへのネットワークアクセスがない場合でも機能します。

図 15-1 ネットワーク分離の例



ファイアウォールでのネットワーク分離の構成

すべてのインバウンド接続とアウトバウンド接続を拒否するように IRE ドメインでファイアウォールを構成します。これは、IREドメインのすべてのホストをサイバー攻撃から保護するのに役立ちます。IRE MSDP サーバーのアウトバウンド接続を許可する必要があります。IRE レプリケーションの場合、IRE MSDP サーバーは、ポート 10082 と 10102 を介して実稼働 MSDP サーバーにネットワークアクセスできる必要があります。IRE MSDP サーバーには、ポート 1556 を使用して実稼働プライマリサーバーへのネットワークアクセスも必要です。

ファイアウォールで単方向のネットワークアクセス (アウトバウンド接続のみ許可) を許可できない場合、IRE MSDP サーバーに対して双方向ネットワークを許可できます。IRE MSDP サーバーの IRE エアギャップは、引き続きすべてのインバウンド接続を拒否します。

IRE MSDP サーバーの IRE エアギャップの構成

IRE MSDP サーバーのエアギャップは次のように機能します。

- IRE ドメイン内のサーバーからのネットワーク接続を許可します。MSDP サーバーを機能させるためには、MSDP サーバーと NetBackup プライマリサーバーまたはメディアサーバーの間の接続が必要です。
  IREドメインのサブネットまたは IP アドレスを、許可するサブネットリストに追加します。サブネットリストの IP アドレスには、MSDP サーバーへの直接ネットワークアクセスがあります。

たとえば、Flex WORM の場合は、次のコマンドを使用します。

```
setting ire-network-control allow-subnets
subnets=<subnet1>,<subnet2>,<ip address>,etc
```

メモ: リストには、少なくとも IRE ドメインのプライマリサーバー、メディアサーバー、DNS サーバーが必要です。

IRE ドメイン外のドメインからサブネットまたは IP アドレスを追加しないでください。

- IRE エアギャップの時間帯に、単方向のネットワークアクセス (IRE MSDP サーバーから他のドメインへのアウトバウンド接続を許可) を有効にします。デフォルトでは、時間帯は 1 日あたり 24 時間です。

許可するサブネットリストにないすべてのインバウンド接続は拒否されます。

Web UI を使用した分離リカバリ環境の構成

次の手順を実行して、NetBackup Web UI を使用して分離リカバリ環境を構成します。

メモ: また、重複排除シェルから IRE を構成および管理することもできます。詳しくは、『NetBackup 重複排除ガイド』を参照してください。

IRE Web UI は、IRE MSDP ストレージサーバーのストレージプラットフォーム Web サービス (spws) に依存します。IRE MSDP ストレージサーバーを BYO メディアサーバーで実行する場合は、spws サービスが構成され、実行されていることを確認します。spws サービスを構成する前に、NGINX がインストールされ、起動されていることを確認します。

spws サービスを構成するために、p.740 の「ストレージプラットフォーム Web サービス (spws) が起動しない」を参照してください。

表 15-2 NetBackup Web UI を使用した IRE の構成

手順	作業	説明
1.	サブネット内のホストのみがストレージサーバーにアクセスできるように、許可されるサブネットを構成します。	p.634 の「許可されるサブネットの構成」を参照してください。
2.	分離されたリカバリ環境内にないストレージサーバーからのバックアップイメージのレプリケートをサポートするために、リバース接続を構成します。	p.634 の「リバース接続の構成」を参照してください。

手順	作業	説明
3.	(オプション) リバースレプリケーションスケジュールを構成して、特定の時間帯でのネットワークアクティビティを許可します。	p.636 の「リバースレプリケーションスケジュールの構成」を参照してください。
4.	稼働中の環境からバックアップイメージをレプリケートするために SLP を構成します。	p.637 の「実稼働プライマリサーバーの SLP へのレプリケーション操作の追加」を参照してください。

許可されるサブネットの構成

許可されるサブネットはファイアウォールのようなものです。許可されたサブネット内に存在しないホストは、IRE MSDP サーバーにアクセスできません。IRE プライマリサーバーが許可されたサブネットにあることを確認します。そうしないと、Web UI から IRE MSDP サーバーを制御できなくなります。IRE の構成に使用するコンピュータも、許可されたサブネット内に存在する必要があります。

メモ: Flex Scale の場合、許可されたサブネットは、ノード、NetBackup サーバー、MSDP エンジンを含むクラスタ全体を保護します。クラスタにアクセスする必要があるすべてのサブネットが、許可されたサブネットにあることを確認します。

許可されるサブネットを構成する方法

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. [ストレージサーバー (Storage servers)]タブをクリックします。
3. 構成する MSDP ストレージサーバーをクリックします。
4. [分離リカバリ環境 (Isolated Recovery Environment)]、[許可されたサブネット (Allowed subnets)]で、[サブネットの追加 (Add subnet)]をクリックします。
5. IPv4 または IPv6 を選択し、サブネットの IP アドレスを入力して[リストに追加 (Add to list)]をクリックします。
6. MSDP サーバーへのアクセスに必要な IRE ドメイン内のすべてのサブネットを追加し、[保存 (Save)]をクリックします。

リバース接続の構成

IRE ストレージサーバーから稼働中のストレージサーバーへのリバース接続を追加する前に、NBCA または ECA が本番ドメインの IRE ストレージサーバーで構成されていることを確認します。

BYO メディアサーバーの場合は、「稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするための A.I.R. の構成」のトピックの手順 1 を参照してください。

p.647 の「稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするための A.I.R. の構成」を参照してください。

WORM ストレージサーバー、Flex Scale、および Access Appliance の場合は、「稼動中の環境と IRE WORM ストレージサーバー間のデータ伝送の構成」のトピックの手順 2 を参照してください。

p.657 の「稼働中の環境と IRE WORM ストレージサーバー間のデータ送信の構成」を参照してください。

リバース接続を構成する方法

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. [ストレージサーバー (Storage servers)]タブをクリックします。
3. 構成する MSDP ストレージサーバーをクリックします。
4. [分離リカバリ環境 (Isolated Recovery Environment)]、[リバース接続 (Reverse connections)]で、[リバース接続の追加 (Add reverse connection)]をクリックします。
5. [リバース接続の追加 (Add reverse connection)]ページで、実稼働プライマリサーバー名を指定します。
6. 既存のログインクレデンシャルを選択するか、新しいクレデンシャルを追加して[次へ (Next)]をクリックします。
   - [既存のクレデンシャルの選択 (Select existing credential)]: 既存のクレデンシャルを選択します。
   - [新しいクレデンシャルの追加 (Add a new credential)]: 実稼働プライマリサーバーの新しいクレデンシャルを追加します。[クレデンシャル形式 (Credential type)]で、[Username Password 認証 (Username Password authentication)]または[API キーを使用 (Use API key)]を選択します。

   メモ: 実稼働プライマリサーバーのユーザーには、デフォルトの IRE SLP 管理者の役割の権限が必要です。
7. [接続 (Connect)]をクリックします。

8 次のページで、[リモート MSDP ストレージサーバー (Remote MSDP storage server)]を選択します。

本番ドメインから MSDP ストレージサーバーを選択できます。MSDP ストレージサーバーに複数のネットワークインターフェースが構成されており、リバース接続が必要な場合は、ストレージサーバー名ではなく別のインターフェースを使用します。稼働中の MSDP ストレージサーバーのネットワークインターフェースの FQDN を入力できます。

9 [ローカルインターフェース (Local interface)]フィールドで、データ伝送用のローカルストレージサーバーインターフェース名を指定します。

IRE MSDP サーバーに複数のインターフェースがあり、IRE MSDP サーバーが特定のインターフェースを使用して稼働中の MSDP ストレージサーバーに接続する場合は、IRE MSDP ストレージサーバーのネットワークインターフェースの FQDN を入力します。

[ローカルインターフェース (Local interface)]フィールドに何も指定されていない場合、IRE MSDP サーバーはデフォルトのネットワークインターフェースを使用して稼働中のストレージサーバーに接続します。

10 [追加 (Add)]をクリックします。

IRE MSDP サーバーから稼働中の MSDP サーバーへのリバース接続が構成されます。

リバースレプリケーションスケジュールの構成

デフォルトでは、IRE MSDP ストレージサーバーは、稼働中のストレージサーバーへのリバース接続を長い時間帯 (24 時間× 7 日間) にわたって許可します。セキュリティ上の理由から、管理者は短い時間帯にわたってリバース接続を作成する必要がある場合があります。

許可されるサブネットを構成する方法

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 [ストレージサーバー (Storage servers)]タブをクリックします。

3 構成する MSDP ストレージサーバーをクリックします。

4 [分離されたリカバリ環境 (Isolated Recovery Environment)]、[リバースレプリケーションスケジュール (Reverse replication schedule)]の順に選択して、[スケジュールの設定 (Configure schedule)]をクリックします。

5 リバース接続を許可するように各平日の時間帯を構成します。時間帯をデフォルトに戻すには、[デフォルトの 24 時間 365 日のスケジュールにリセット (Reset to default 24/7 schedule)]をクリックします。

6 [保存 (Save)]をクリックします。

実稼働プライマリサーバーの SLP へのレプリケーション操作の追加

リバース接続を構成する方法

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. [ストレージサーバー (Storage servers)]タブをクリックします。
3. 構成する MSDP ストレージサーバーをクリックします。
4. [分離リカバリ環境 (Isolated Recovery Environment)]で、[リモートプライマリサーバーの SLP の変更 (Modify SLP on the remote primary server)]をクリックします。
5. [リモートプライマリサーバーの SLP の変更 (Modify SLP on the remote primary server)]ページで、実稼働プライマリサーバー名を指定します。
6. 既存のログインクレデンシャルを選択するか、新しいクレデンシャルを追加して[次へ (Next)]をクリックします。
   - [既存のクレデンシャルの選択 (Select existing credential)]: 既存のクレデンシャルを選択します。
   - [新しいクレデンシャルの追加 (Add a new credential)]: 実稼働プライマリサーバーの新しいクレデンシャルを追加します。[クレデンシャル形式 (Credential type)]で、[Username Password 認証 (Username Password authentication)]または[API キーを使用 (Use API key)]を選択します。

     メモ: 実稼働プライマリサーバーのユーザーには、デフォルトの IRE SLP 管理者の役割の権限が必要です。
7. [接続 (Connect)]をクリックします。
8. IRE MSDP ストレージサーバーにレプリケーション操作を追加する SLP を選択し、[次へ (Next)]をクリックします。
9. 操作の後に、IRE MSDP ストレージサーバーにレプリケートする操作を選択し、[次へ (Next)]をクリックします。
10. レプリケーションの完了後にイメージのインポート用に IRE ドメインの SLP を選択します。

11 [時間帯 (Window)]タブで、レプリケーション操作の SLP 時間帯を構成します。新しい SLP 時間帯を作成するか、既存の SLP 時間帯を選択します。

SLP 時間帯を調整するときは、SLP 時間帯が IRE スケジュールに含まれていることを確認してください。IRE スケジュール外でレプリケーションがトリガされると、リバース接続は行われず、レプリケーションジョブは失敗します。

[リバース接続スケジュールとの同期 (Synchronize with the reverse connection schedule)]を使用すると、現在の SLP 時間帯を IRE スケジュールに置き換えることができます。IRE スケジュールに基づいて SLP 時間帯を調整できます。

ページに表示される日時は、IRE プライマリサーバーのタイムゾーンに基づいています。実稼働プライマリサーバーと IRE プライマリサーバーが異なるタイムゾーンにある場合、時差が計算され、実稼働プライマリサーバーの SLP 時間帯が自動的に変換されます。

[完了 (Finish)]をクリックします。

12 [保存 (Save)]をクリックします。

MSDP ストレージサーバーのレプリケーションターゲット、SLP 時間帯、SLP のレプリケーション操作を含むすべての構成が実稼働プライマリサーバーに適用されます。

コマンドラインを使用した分離リカバリ環境の構成

次のトピックを参照して、コマンドラインを使用して分離リカバリ環境を構成します。

表 15-3 コマンドラインを使用した IRE 構成

タスク	説明
NetBackup BYO メディアサーバーで分離リカバリ環境を構成します。	p.639 の「NetBackup BYO メディアサーバーでの分離リカバリ環境の構成」を参照してください。
NetBackup BYO メディアサーバーで分離リカバリ環境を管理します。	p.643 の「NetBackup BYO メディアサーバーでの分離リカバリ環境の管理」を参照してください。
稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするために AIR を構成します。	p.647 の「稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするための A.I.R. の構成」を参照してください。
WORM ストレージサーバーで分離リカバリ環境を構成します。	p.651 の「 WORM ストレージサーバーでの分離リカバリ環境の構成 」を参照してください。
WORM ストレージサーバーで分離リカバリ環境を管理します。	p.654 の「 WORM ストレージサーバーでの分離リカバリ環境の管理 」を参照してください。

タスク	説明
稼働中の環境と IRE WORM ストレージサーバー間でデータ伝送を構成します。	p.657 の「稼働中の環境と IRE WORM ストレージサーバー間のデータ送信の構成」を参照してください。

NetBackup BYO メディアサーバーでの分離リカバリ環境の構成

NetBackup BYO メディアサーバー上に分離リカバリ環境 (IRE) を構成して、稼働中の環境と保護データのコピーとの間にエアギャップを生み出すことができます。エアギャップは、常に IRE 環境へのネットワークアクセスを制限します。この機能は、ランサムウェアやマルウェアからの保護に役立ちます。IRE を構成するには、稼働中の NetBackup 環境と、BYO メディアサーバーに MSDP サーバーを構成した NetBackup IRE 環境が必要です。稼働中の環境では、この機能についての追加の手順は必要ありません。

BYO メディアサーバーに IRE を構成するには、次の手順を使用します。

BYO メディアサーバーに IRE を構成するには

1. この手順が適用されるのは NetBackup 10.1 以降にのみです。

   メディアサーバーにログインします。

2. この手順は省略可能です。この手順は、次のいずれかの場合に使用してください。

   - 既存のシステムで IRE を有効にする場合。
   - AIR SLP がすでに構成されている場合。
   - 既存の SLP 時間帯に基づいて、手順 4 で IRE スケジュールを構成する場合。

   次のコマンドを実行して、プライマリサーバーからメディアサーバーの MSDP ストレージに対するレプリケーションの SLP 時間帯を表示します。

   ```
   /usr/openv/pdde/shell/bin/show_slp_windows
   --production_primary_server production primary server name
   --production_primary_server_username production primary server
   username --ire_primary_server target primary server name
   --ire_primary_server_username target primary server username
   ```

   以下はその説明です。

   - *production primary server name* は、稼働中の環境のプライマリサーバーの完全修飾ドメイン名 (FQDN) です。
   - *production primary server username* は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。*production primary server username* は、Windows の `domain_name¥user_name` 形式である必要があります。

- *target primary server name* は、IRE のプライマリサーバーの FQDN です。稼働中の環境で SLP を構成するのに使用したのと同じホスト名を使用してください。
- *target primary server username* は、IRE 環境の SLP とストレージユニットを一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。
  target primary server username は、Windows の `domain_name¥user_name` 形式である必要があります。

例:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

コマンドの出力例を次に示します。

```
EveryDayAtNoon: SLPs: SLP1 Sunday start: 12:00:00 duration:
00:59:59
Monday start: 12:00:00 duration: 00:59:59 Tuesday start: 12:00:00

duration: 00:59:59 Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59 Friday start: 12:00:00

duration: 00:59:59 Saturday start: 12:00:00 duration: 00:59:59
WeeklyWindow: SLPs: SLP2 Sunday start: 10:00:00 duration: 01:59:59

Monday NONE Tuesday NONE Wednesday NONE Thursday NONE Friday NONE

Saturday start: 10:00:00 duration: 01:59:59
```

この例は、2 つの SLP 時間帯を示しています。

- 正午から 1 時間の日単位の時間帯。
- 午前 10 時から 2 時間の週単位の時間帯。

メモ: SLP 時間帯が 24 時間を超えると、`show-slp-windows` が期間を正しく表示しなくなることがあります。

---

3 ご使用の環境の出力に基づいて、SLP 時間帯に対応する日次スケジュールを判断し、それを書き留めます。前の例では、午前 10 時から午後 12 時の日単位のスケジュールが両方の SLP 時間帯に対応しています。

このコマンドの出力の開始時刻は、IRE サーバーのタイムゾーンにあります。

メモ: 稼働中のプライマリサーバーのタイムゾーンが変更された場合は、NetBackup サービスを再起動する必要があります。

---

4 次のコマンドを実行して、メディアサーバーへのアクセスが許可されているサブネットと IP アドレスを構成します。

```
/usr/openv/pdde/shell/bin/ire_network_control allow-subnets
--subnets CIDR subnets or IP addresses
```

CIDR subnets or IP addresses フィールドは、許可されている CIDR 表記の IP アドレスとサブネットのカンマ区切りリストです。

例:

```
/usr/openv/pdde/shell/bin/ire_network_control allow-subnets
--subnets 10.10.100.200,10.80.40.0/20
```

メモ: IRE 環境の IRE プライマリサーバー、IRE メディアサーバー、および DNS サーバーが許可リストに含まれている必要があります。これらのサーバーがすべて同じサブネットにある場合、サブネットのみが許可リストに含まれる必要があります。

メモ: ネットワーク環境がデュアルスタックの場合、IPv4 サブネットと IPv6 サブネットの両方と、IRE ドメインの IP アドレスが、許可されたサブネット内に構成されていることを確認します。たとえば、許可されたサブネット内に IPv6 サブネットのみを指定した場合、すべての IPv4 アドレスは、IRE ストレージサーバーへのアクセスを許可されません。

---

5 次のコマンドを実行して、日単位のエアギャップスケジュールを設定します。

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time time --duration duration [--weekday 0-6]
```

weekday は省略可能です。日曜日から始まります。特定の平日には、異なるネットワークや、時間帯のオープンまたはクローズを構成できます。指定しない場合、IRE スケジュールは毎日同じです。

例:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 10:00:00 --duration 03:00:00
```

メモ: 稼働中のドメインの SLP レプリケーション時間帯は、IRE スケジュールと同時に開くように構成する必要があります。IRE スケジュール時間帯は、平日については異なる場合があります。特定の平日に時間帯を構成できます。

例:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 11:00:00 --duration 10:00:00 --weekday 0
```

メモ: 稼働中の環境と IRE 環境のタイムゾーンが異なる場合、スケジュールはどちらのタイムゾーンでも 1 日に 1 回のみ開始する必要があります。

たとえば、ある環境のタイムゾーンが Asia/Kolkata でもう一方のタイムゾーンが America/New_York の場合、Kolkata では、火曜日の 22:00:00 と水曜日の 03:00:00 に開始するスケジュールはサポートされません。これらの開始時刻がニューヨークのタイムゾーンに変換されると、これらの開始時刻は火曜日の 12:30:00 と火曜日の 17:30:00 になり、これはサポートされません。

メモ: 終日 24 時間エアギャップネットワークを開く場合、IRE スケジュールを構成する必要はありません。ただし IRE メディアサーバーは、エアギャップが許可する、サブネット内に構成されていないホストからのネットワークアクセスを制限します。

NetBackup BYO メディアサーバーでの分離リカバリ環境の管理

分離リカバリ環境を NetBackup BYO メディアサーバーで構成すると、メディアサーバーから管理できます。

次のコマンドを使用します。

プライマリサーバーから WORM インスタンスへの SLP 時間帯を表示するには

◆ `/usr/openv/pdde/shell/bin/show_slp_windows --production_primary_server` *`production primary server name`* `--production_primary_server_username` *`production primary server username`* `--ire_primary_server` *`target primary server name`* `--ire_primary_server_username` *`target primary server username`*

以下はその説明です。

- *production primary server name* は、稼働中の環境のプライマリサーバーの完全修飾ドメイン名 (FQDN) です。
- *production primary server username* は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。
  production primary server username は、Windows の `domain_name¥user_name` 形式である必要があります。
- *target primary server name* は、IRE のプライマリサーバーの FQDN です。稼働中の環境で SLP を構成するのに使用したのと同じホスト名を使用してください。
- *target primary server username* は、IRE 環境の SLP とストレージユニットを一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。
  例:
  target primary server username は、Windows の `domain_name¥user_name` 形式である必要があります。

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

許可された IP アドレスとサブネットを表示するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control show-allows
```

IP アドレスとサブネットを許可リストに表示するには

- 次のコマンドを実行します。

  ```
  /usr/openv/pdde/shell/bin/ire_network_control allow-subnets
  --subnets CIDR subnets or IP addresses
  ```

  CIDR subnets or IP addresses フィールドは、許可されている CIDR 表記の IP アドレスとサブネットのカンマ区切りリストです。

  例:

  ```
  /usr/openv/pdde/shell/bin/ire_network_control allow-subnets
  --subnets 10.60.120.208,10.74.48.0/20
  ```

  メモ: IRE 環境の IRE プライマリサーバー、IRE メディアサーバー、および DNS サーバーが許可リストに含まれている必要があります。これらのサーバーがすべて同じサブネットにある場合、サブネットのみが許可リストに含まれる必要があります。

  メモ: ネットワーク環境がデュアルスタックの場合、IPv4 サブネットと IPv6 サブネットの両方と、IRE ドメインの IP アドレスが、許可されたサブネット内に構成されていることを確認します。たとえば、IPv6 サブネットのみを許可されたサブネット内に指定した場合、すべての IPv4 アドレスは、IRE ストレージサーバーへのアクセスを許可されません。

IP アドレスとサブネットを許可リストから削除するには

- 次のコマンドを実行します。

  ```
  /usr/openv/pdde/shell/bin/ire_network_control allow-subnets
  --subnets
  ```

日次エアギャップのスケジュールを表示するには

- 次のコマンドを実行します。

  ```
  /usr/openv/pdde/shell/bin/ire_network_control show-schedule
  ```

エアギャップのスケジュールを変更するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time time --duration duration [--weekday weekday in 0-6]
```

例:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 10:00:00 --duration 03:00:00
```

メモ: 稼働中のドメインの SLP レプリケーション時間帯は、IRE スケジュールと同時に開くように構成する必要があります。

エアギャップのスケジュールを停止するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control delete-schedule
[--weekday weekday in 0-6]
```

メモ: 特定の平日についての IRE 時間帯を削除できます。

現在のネットワーク状態を表示し、外部ネットワークが開いているか閉じているかを確認するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control
external-network-status
```

手動で外部ネットワークを開くには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control
external-network-open
```

手動で外部ネットワークを閉じてエアギャップのスケジュールを再開するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control resume-schedule
```

MSDP リバース接続を追加するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control reverse-connection
--add source msdp server [--remote_primary source primary server]
[--local_addr local msdp server]
```

MSDP リバース接続を削除するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control reverse-connection
--remove source msdp server
```

構成済みの MSDP リバース接続を一覧表示するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control reverse-connection
--list
```

特定のリバース接続が機能するかどうかを検証するには

◆ 次のコマンドを実行します。

```
/usr/openv/pdde/shell/bin/ire_network_control reverse-connection
--validate source msdp server
```

稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするための A.I.R. の構成

IRE の構成が完了すると、稼働中の NetBackup ホストは IRE MSDP ストレージサーバーにアクセスできなくなります。稼働中の MSDP サーバーと IRE MSDP サーバー間のデータ転送を許可するには、MSDP リバース接続を有効にする必要があります。

メモ: A.I.R. の構成操作は、外部ネットワークが IRE エアギャップによって開かれている場合にのみ実行できます。指定した操作はすべて IRE MSDP サーバーで実行されます。

前提条件

稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするために A.I.R. を構成する前に、次の点を確認してください。

- NetBackup 認証局 (CA) の場合は、稼働中のプライマリサーバーから IRE MSDP ストレージサーバーの CA 証明書とホスト証明書を取得します。
- 稼働中のプライマリサーバーでトークンを作成します。

稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするために A.I.R. を構成するには

1. 次のコマンドを実行します。
   - NetBackup 証明書:

     ```
     /usr/openv/netbackup/bin/nbcertcmd -getCACertificate -server
     <production primary server>
     /usr/openv/netbackup/bin/nbcertcmd -getCertificate -server
     <production primary server> -token <token>
     ```

   - 外部証明書:

     ```
     /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -server
     <production primary server>
     ```

2. 次のコマンドを実行して、MSDP リバース接続を有効にします。

   ```
   /usr/openv/pdde/shell/bin/ire_network_control reverse_connection
   --add production msdp server
   ```

3 IRE スケジュールを構成していない場合、この手順は必要ありません。IRE スケジュールが構成されていない場合は MSDP リバース接続が 24 時間有効になるためです。稼働中のプライマリサーバーは、任意の SLP 時間帯で SLP レプリケーション操作を構成できます。

MSDP リバース接続を構成したら、SLP 時間帯として NetBackup 本番ドメインに IRE スケジュールをコピーします。次のコマンドを使用します。

```
/usr/openv/pdde/shell/bin/sync_ire_window
--production_primary_server production primary server name
--production_primary_server_username production primary server
username [--slp_window_name slp_window_name ]
```

以下はその説明です。

production primary server name は、稼働中の環境のプライマリサーバーの完全修飾ドメイン名 (FQDN) です。

production primary server username は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。

production primary server username は、Windows の `domain_name¥user_name` 形式である必要があります。

slp_window_name は、IRE 時間帯と同期する SLP 時間帯の名前です。これは、省略可能なパラメータです。SLP 時間帯が指定されていない場合は、`IRE_DEFAULT_WINDOW` という名前の SLP 時間帯が稼働中のプライマリサーバーに作成されます。

4 その後、IRE MSDP ストレージサーバーを稼働中の NetBackup ドメインのレプリケーションターゲットとして追加できます。次に、次のコマンドを使用してレプリケーション操作を既存の SLP に追加し、稼働中の NetBackup ドメインから IRE MSDP ストレージサーバーにレプリケートします。

```
/usr/openv/pdde/shell/bin/add_replication_op
--production_primary_server production primary server name
--production_primary_server_username production primary server
username --source_slp_name source slp name
--target_import_slp_name target import slp name
--production_storage_server production storage server name
--ire_primary_server_username ire primary server username
--target_storage_server target storage server name
--target_storage_server_username target storage server username
--production_storage_unit msdp storage unit name used in source
SLP [--slp_window_name slp window name]
```

以下はその説明です。

production primary server name は、稼働中の環境のプライマリサーバーの完全修飾ドメイン名 (FQDN) です。

production primary server username は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。

production primary server username は、Windows の `domain_name¥user_name` 形式である必要があります。

production storage server name は、稼働中の環境にある稼働中のストレージサーバーの完全修飾ドメイン名 (FQDN) です。

ire primary server username は、IRE プライマリサーバーの管理者ユーザーのユーザー名です。

ire primary server username は、Windows の `domain_name¥user_name` 形式である必要があります。

source slp name は、レプリケーション操作を追加する稼働中のプライマリサーバーの SLP 名です。

target import slp name は、IRE プライマリサーバーのインポート SLP 名です。

target storage server name は、ターゲットの MSDP ストレージサーバーの完全修飾ドメイン名 (FQDN) です。

target storage server username は、ターゲットの MSDP ストレージサーバーのユーザー名です。

slp_window_name は、IRE 時間帯と同期する SLP 時間帯の名前です。または、操作の前に稼働中のプライマリサーバー上に作成されます。これは、省略可能なパ

ラメータです。SLP 時間帯を指定しない場合、操作の前に sync_ire_window コマンドを使用して作成する必要がある IRE_DEFAULT_WINDOW という名前の SLP 時間帯が使用されます。

production_storage_unit は、ソース SLP で使用されている PureDisk 形式のストレージユニット名です。

メモ: 操作の前に、ソース SLP とターゲットのインポート SLP を作成する必要があります。

WORM ストレージサーバーでの分離リカバリ環境の構成

WORM ストレージサーバー上に分離リカバリ環境 (IRE) を構成して、稼働中の環境と保護データのコピーとの間にエアギャップを生み出すことができます。エアギャップは、データレプリケーションが発生する時間枠を除いて、データへのネットワークアクセスを制限します。この機能は、ランサムウェアやマルウェアからの保護に役立ちます。

IRE を構成するには、稼働中の NetBackup 環境と、サポート対象の Cohesity アプライアンス上のターゲット WORM ストレージサーバーが必要です。互換性については、アプライアンスのマニュアルを確認してください。

稼働中の環境では、この機能についての追加の手順は必要ありません。重複排除シェルからターゲット WORM ストレージサーバーに IRE を構成するには、次の手順を実行します。

IRE を構成するには

1 A.I.R. が本番ドメインで構成されていない場合は、次の手順に進みます。

A.I.R. が本番ドメインですでに構成されている場合は、msdpadm ユーザーとして重複排除シェルにログインします。次のコマンドを実行して、プライマリサーバーから WORM サーバーへの、レプリケーションの SLP 時間帯を表示します。

```
setting ire-network-control show-slp-windows
production_primary_server=<production domain>
production_primary_server_username=<production username>
ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
username>
```

以下はその説明です。

- *<production domain>* は、稼働中の環境のプライマリサーバーの FQDN (完全修飾ドメイン名) です。
- *<production username>* は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。Windows ユーザー

の場合は、ユーザー名を *<domain name>¥<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。

- *<IRE domain>* は IRE のプライマリサーバーの FQDN です。稼働中の環境で SLP を構成したときにターゲットプライマリサーバーに使用したのと同じホスト名を使用してください。
- *<IRE username>* は、IRE の SLP とストレージユニットを一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。Windows ユーザーの場合は、ユーザー名を *<domain name>¥<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。

例:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

コマンドの出力例を次に示します。

```
EveryDayAtNoon:
SLPs: SLP1
Sunday start: 12:00:00 duration: 00:59:59
Monday start: 12:00:00 duration: 00:59:59
Tuesday start: 12:00:00 duration: 00:59:59
Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59
Friday start: 12:00:00 duration: 00:59:59
Saturday start: 12:00:00 duration: 00:59:59

WeeklyWindow:
SLPs: SLP2
Sunday start: 10:00:00 duration: 01:59:59
Monday NONE
Tuesday NONE
Wednesday NONE
Thursday NONE
Friday NONE
Saturday start: 10:00:00 duration: 01:59:59
```

この例は、2 つの SLP 時間帯を示しています。

- 正午から 1 時間の日単位の時間帯。

- 午前 10 時から 2 時間の週単位の時間帯。

2 ご使用の環境の要件に基づいて、スケジュールを決定して書き留めます。既存の A.I.R. 環境の場合、スケジュールは前の手順で表示した SLP 時間帯に対応する必要があります。

毎日同じ時間に開かれる日次スケジュールを設定することも、曜日ごとに異なるスケジュールを設定することもできます。

前の例では、次のいずれかで両方の SLP 時間帯に対応できます。

- 午前 10 時から午後 1 時までの日次スケジュール
- 月曜日から金曜日の午後 12 時から午後 1 時までと、土曜日と日曜日の午前 10 時から午後 1 時までのスケジュール

メモ: 稼働中の環境と IRE のタイムゾーンが異なる場合、スケジュールはどちらのタイムゾーンでも 1 日に 1 回のみ開始する必要があります。たとえば、ある環境のタイムゾーンが Asia/Kolkata でもう一方のタイムゾーンが America/New_York の場合、Kolkata では、火曜日の 22:00:00 と水曜日の 03:00:00 に開始するスケジュールはサポートされません。これらの開始時刻がニューヨークのタイムゾーンに変換されると、これらの開始時刻は火曜日の 12:30:00 と火曜日の 17:30:00 になり、これはサポートされません。

---

3 次のコマンドを実行して、WORM ストレージサーバーへのアクセスが許可されるサブネットと IP アドレスを構成します。

```
setting ire-network-control allow-subnets subnets=<CIDR subnets
or IP addresses>
```

<CIDR subnets or IP addresses> は、許可されている CIDR 表記の IP アドレスとサブネットのカンマ区切りリストです。

例:

```
setting ire-network-control allow-subnets
subnets=10.80.120.208,10.84.48.0/20
```

メモ: IRE プライマリサーバー、IRE メディアサーバー、および IRE の DNS サーバーが許可リストに含まれている必要があります。これらのサーバーがすべて同じサブネットにある場合、サブネットのみが許可リストに含まれる必要があります。デュアルスタック IPv4-IPv6 ネットワークを使用している場合は、IPv4 アドレスと IPv6 アドレスの両方が許可リストに追加されていることを確認します。

---

4 次のコマンドを実行して、日単位のエアギャップスケジュールを設定します。

```
setting ire-network-control set-schedule start_time=<time>
duration=<duration> [weekday=<0-6>]
```

[weekday=<*0-6*>] は、異なる曜日に異なるスケジュールを設定する必要がある場合に曜日を示す省略可能なパラメータです。0 は日曜日で、1 は月曜日です。

例:

```
setting ire-network-control set-schedule start_time=10:00:00
duration=03:00:00 weekday=0
```

5 本番ドメインと IRE ストレージサーバー間でデータを送信するには、MSDP 逆接続を追加してレプリケーション操作を追加する必要があります。

p.657 の「稼働中の環境と IRE WORM ストレージサーバー間のデータ送信の構成」を参照してください。

WORM ストレージサーバーでの分離リカバリ環境の管理

分離リカバリ環境 (IRE) を WORM ストレージサーバーで構成すると、msdpadm ユーザーとして重複排除シェルから管理できます。次のコマンドを使用します。

- プライマリサーバーから WORM サーバーへの SLP 時間帯を表示するには

  ```
  setting ire-network-control show-slp-windows
  production_primary_server=<production domain>
  production_primary_server_username=<production username>
  ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
  username>
  ```

  以下はその説明です。

  - *<production domain>* は、稼働中の環境のプライマリサーバーの FQDN (完全修飾ドメイン名) です。
  - *<production username>* は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。Windows ユーザーの場合は、ユーザー名を *<domain name>*¥*<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。
  - *<IRE domain>* は IRE のプライマリサーバーの FQDN です。稼働中の環境で SLP を構成したときにターゲットプライマリサーバーに使用したのと同じホスト名を使用してください。
  - *<IRE username>* は、IRE の SLP とストレージユニットを一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。Windows ユーザーの場合は、ユーザー名を *<domain name>*¥*<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。

  例:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

メモ: 稼働中のドメインの SLP レプリケーション時間帯は、IRE スケジュールと同時に開くように構成する必要があります。

- MSDP リバース接続を一覧表示するには
  `setting ire-network-control list-reverse-connections`
- MSDP リバース接続を追加するには
  `setting ire-network-control add-reverse-connection`
  `remote_storage_server=<production MSDP server>`
  `[remote_primary_server=<production primary server>]`
  `[local_storage_server=<IRE network interface>]`
  以下はその説明です。
  - *<production MSDP server>* は稼動中の環境にある MSDP サーバーの FQDN です。
  - [remote_primary_server=*<production primary server>*] は、稼働中の環境にあるプライマリサーバーの FQDN のオプションパラメータです。このパラメータは、IRE ドメインが代替名を使用して実稼働プライマリサーバーにアクセスする場合に必要です。このシナリオは、通常、実稼働プライマリサーバーが複数のネットワークで複数のホスト名で実行されている場合に発生します。
  - [local_storage_server=*<IRE network interface>*] は、IRE ストレージサーバーでのイメージレプリケーションに使用するネットワークインターフェースのホスト名のオプションパラメータです。このパラメータは、レプリケーションのネットワークインターフェースが IRE ストレージサーバー名と異なる場合に必要です。
- リバース接続が機能することを確認するには
  `setting ire-network-control validate-reverse-connection`
  `remote_storage_server=<production MSDP server>`
  `[remote_primary_server=<production primary server>]`
  `[local_storage_server=<IRE network interface>]`
- MSDP リバース接続を削除するには
  `setting ire-network-control remove-reverse-connection`
  `remote_storage_server=<production MSDP server>`
- 許可された IP アドレスとサブネットを表示するには
  `setting ire-network-control show-allows`

- IP アドレスとサブネットを許可リストに追加するには

  `setting ire-network-control allow-subnets subnets=<CIDR subnets or IP addresses>`

  <CIDR subnets or IP addresses> は、許可されている CIDR 表記の IP アドレスとサブネットのカンマ区切りリストです。

  例:

  ```
  setting ire-network-control allow-subnets
  subnets=10.80.120.208,10.84.48.0/20
  ```

  メモ: IRE プライマリサーバー、IRE メディアサーバー、および IRE の DNS サーバーが許可リストに含まれている必要があります。これらのサーバーがすべて同じサブネットにある場合、サブネットのみが許可リストに含まれる必要があります。デュアルスタック IPv4-IPv6 ネットワークを使用している場合は、IPv4 アドレスと IPv6 アドレスの両方が許可リストに追加されていることを確認します。

- IP アドレスとサブネットを許可リストから削除するには

  `setting ire-network-control allow-subnets subnets=,`

- 日次エアギャップのスケジュールを表示するには

  `setting ire-network-control show-schedule`

- エアギャップのスケジュールを変更するには

  `setting ire-network-control set-schedule start_time=<time> duration=<duration>`

  例:

  ```
  setting ire-network-control set-schedule start_time=10:00:00
  duration=03:00:00
  ```

  メモ: 稼働中の環境と IRE のタイムゾーンが異なる場合、スケジュールはどちらのタイムゾーンでも 1 日に 1 回のみ開始する必要があります。たとえば、ある環境のタイムゾーンが Asia/Kolkata でもう一方のタイムゾーンが America/New_York の場合、Kolkata では、火曜日の 22:00:00 と水曜日の 03:00:00 に開始するスケジュールはサポートされません。これらの開始時刻がニューヨークのタイムゾーンに変換されると、これらの開始時刻は火曜日の 12:30:00 と火曜日の 17:30:00 になり、これはサポートされません。

- エアギャップのスケジュールを停止するには

  `setting ire-network-control delete-schedule`

- 現在のネットワーク状態を表示し、外部ネットワークが開いているか閉じているかを確認するには

```
setting ire-network-control external-network-status
```

- 手動で外部ネットワークを開くには
  ```
  setting ire-network-control external-network-open
  ```
- 手動で外部ネットワークを閉じてエアギャップのスケジュールを再開するには
  ```
  setting ire-network-control resume-schedule
  ```

稼働中の環境と IRE WORM ストレージサーバー間のデータ送信の構成

IRE (分離リカバリ環境) の構成が完了すると、稼働中の NetBackup ホストは WORM ストレージサーバーにアクセスできなくなります。稼働中の MSDP ストレージサーバーと IRE WORM ストレージサーバー間のデータ伝送を許可するには、MSDP リバース接続を追加する必要があります。その後、レプリケーション操作を追加できます。

稼働中の環境と IRE 間のデータ伝送を構成するには

1. IRE WORM ストレージサーバーへの SSH セッションを開きます。次のコマンドを実行して、外部ネットワークが開いているかどうかを判断します。

   ```
   setting ire-network-control external-network-status
   ```

   開いていない場合は、次のコマンドを実行します。

   ```
   setting ire-network-control external-network-open
   ```

2. ホストの通信に使用する認証局の種類に応じて、次のいずれかを実行します。

   - NetBackup 認証局を使用する場合は、次のコマンドを実行して本番ドメインの証明書を要求します。

     ```
     setting certificate get-CA-certificate
     primary_server=<production primary server>
     setting certificate get-certificate primary_server=<production
     primary server> token=<token>
     ```

   - 外部の認証局を使用する場合は、次のコマンドを実行して本番ドメインに証明書を登録します。

     ```
     setting certificate enroll-external-certificates
     server=<production primary server>
     ```

3. 次のコマンドを実行して、MSDP リバース接続を追加します。

   ```
   setting ire-network-control add-reverse-connection
   remote_storage_server=<production MSDP server>
   [remote_primary_server=<production primary server>]
   [local_storage_server=<IRE network interface>]
   ```

   以下はその説明です。

- *<production MSDP server>* は稼動中の環境にある MSDP サーバーの FQDN (完全修飾ドメイン名) です。
- [remote_primary_server=*<production primary server>*] は、稼働中の環境にあるプライマリサーバーの FQDN のオプションパラメータです。このパラメータは、IRE ドメインが代替名を使用して実稼働プライマリサーバーにアクセスする場合に必要です。このシナリオは、通常、実稼働プライマリサーバーが複数のネットワークで複数のホスト名で実行されている場合に発生します。
- [local_storage_server=*<IRE network interface>*] は、IRE ストレージサーバーでのイメージレプリケーションに使用するネットワークインターフェースのホスト名のオプションパラメータです。このパラメータは、レプリケーションのネットワークインターフェースが IRE ストレージサーバー名と異なる場合に必要です。

4 必要に応じて、前の手順を繰り返して MSDP の逆接続を追加します。

5 AIR (自動イメージレプリケーション) が本番ドメインでまだ構成されていない場合は、次のコマンドを実行して、SLP (ストレージライフサイクルポリシー) の時間帯として本番ドメインに IRE スケジュールをコピーします。

```
setting ire-network-control sync-ire-window
production_primary_server=<production primary server>
production_primary_server_username=<production username>
[slp_window_name=<SLP window name>]
```

以下はその説明です。

- *<production primary server>* は稼動中の環境にあるプライマリサーバーの FQDN です。
- *<production username>* は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。Windows ユーザーの場合は、ユーザー名を *<domain name>*¥*<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。
- [slp_window_name=*<SLP window name>*] は、SLP 時間帯の名前を指定する省略可能なパラメータです。このパラメータを指定しない場合、SLP 時間帯の名前は `IRE_DEFAULT_WINDOW` になります。

6 まだ作成していない場合は、稼動中のプライマリサーバーにソース SLP を作成し、IRE プライマリサーバーにターゲットインポート SLP を作成します。詳しくは、『NetBackup 重複排除ガイド』の「ストレージライフサイクルポリシーの作成」セクションを参照してください。

メモ: SLP を作成するときに、NetBackup からレプリケーション操作を追加することはできません。次の手順に進み、レプリケーション操作を追加します。

---

7 次のコマンドを実行して、IRE WORM ストレージサーバーを稼動中の NetBackup ドメインのレプリケーションターゲットとして追加し、SLP にレプリケーション操作を追加します。

```
setting ire-network-control add-replication-op
production_primary_server=<production primary server>
production_primary_server_username=<production username>
production_storage_server=<production storage server>
ire_primary_server_username=<IRE username>
source_slp_name=<production SLP name> target_import_slp_name=<IRE
SLP name> target_storage_server=<target storage server>
target_storage_server_username=<target storage server username>
production_storage_unit=<MSDP storage unit> [slp_window_name=<slp
window name>]
```

以下はその説明です。

- *<production primary server>* は稼動中の環境にあるプライマリサーバーの FQDN です。
- *<production username>* は、稼働中の環境で SLP と SLP 時間帯を一覧表示する権限を持つ NetBackup ユーザーのユーザー名です。Windows ユーザーの場合は、ユーザー名を *<domain name>¥<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。
- *<production storage server>* は、稼働中の環境にある稼働中のストレージサーバーの FQDN です。
- *<IRE username>* は、IRE プライマリサーバーの管理者のユーザー名です。Windows ユーザーの場合は、ユーザー名を *<domain name>¥<username>* の形式で入力します。他のユーザーの場合は、ユーザー名のみを入力します。
- *<source SLP name>* は、レプリケーション操作を追加する稼働中のプライマリサーバーの SLP 名です。
- *<target SLP name>* は、IRE プライマリサーバーのインポート SLP 名です。
- *<target storage server>* は、IRE 環境のターゲット WORM ストレージサーバーの FQDN です。
- *<target storage server username>* は、ターゲット WORM ストレージサーバーのストレージクレデンシャルに対するユーザー名です。このユーザー名は、インスタンスを作成したときに入力したストレージのユーザー名と同じです。
- *<MSDP storage unit>* はソース SLP のレプリケーションソースである MSDP ストレージユニットの名前です。
- [slp_window_name=<*SLP window name*>] は、IRE スケジュールと同期した SLP 時間帯の名前の省略可能なパラメータです。このパラメータは、前の手順

の SLP 時間帯名と一致する必要があります (該当する場合)。このパラメータを指定しない場合は、デフォルト名が使用されます。

8 この手順の開始時に外部ネットワークを開いた場合は、次のコマンドを実行して閉じ、エアギャップスケジュールを再開します。

```
setting ire-network-control resume-schedule
```

IREドメインから本番環境ドメインへのバックアップイメージのレプリケート

何らかの理由で本番環境ドメインのバックアップイメージが失われた場合、IREドメインから本番環境ドメインにバックアップイメージをレプリケートして戻す必要がある場合があります。これらのバックアップイメージを新しいドメインにレプリケートすることもできます。

IRE ドメインから本番環境ドメインにバックアップイメージをレプリケートするには

1 NBCA (NetBackup 認証局) または ECA (外部認証局) が、IRE ストレージサーバーで構成されていることを確認します。

- BYO メディアサーバーの場合は、「稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするための A.I.R. の構成」のトピックの手順 1 を参照してください。
  p.647 の「稼働中の環境から IRE BYO 環境にバックアップイメージをレプリケートするための A.I.R. の構成」を参照してください。
- WORM ストレージサーバー、Flex Scale、および Access Appliance の場合は、「稼動中の環境と IRE WORM ストレージサーバー間のデータ伝送の構成」のトピックの手順 2 を参照してください。
  p.657 の「 稼働中の環境と IRE WORM ストレージサーバー間のデータ送信の構成 」を参照してください。

2 IRE プライマリサーバーで、コマンドラインを使用してレプリケーションターゲットを構成します。

- 次の情報を使用して、レプリケーションターゲットを追加するための構成ファイルを作成します。

`V7.5 "operation" " " string`	新しいレプリケーションターゲットを追加するには、値は `set-replication` である必要があります。
`V7.5 " rephostname" " " string`	レプリケーションターゲットのホスト名を指定します。
`V7.5 "replogin" " " string`	レプリケーションターゲットのストレージサーバーのユーザー名を指定します。

V7.5 "reppasswd" " " string	レプリケーションターゲットのストレージサーバーのパスワードを指定します。
V7.5 "repsourcevolume" " " string	レプリケーションソースのボリューム名を指定します。
V7.5 "reptargetvolume" " " string	レプリケーションターゲットのボリューム名を指定します。

- 次のコマンドを実行して、構成ファイルを適用してレプリケーションターゲットを追加します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
  -storage_server <IRE storage server name> -stype PureDisk
  -configlist <config file name>
  ```

- プライマリサーバーで、次のコマンドを実行してディスクプール情報を更新します。

  ```
  /usr/openv/netbackup/bin/admincmd/nbdevconfig -updatedp -stype
  PureDisk -dp <IRE disk pool name>
  ```

サンプル:

```
[admin@ire-primary ~]# cat add-replication.txt
V7.5 "operation" "set-replication" string
V7.5 "rephostname" "msdp-prod.example.com" string
V7.5 "replogin" "pduser" string
V7.5 "reppasswd" "pdpass" string
V7.5 "repsourcevolume" "PureDiskVolume" string
V7.5 "reptargetvolume" "PureDiskVolume" string
[admin@ire-primary ~]#
/usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig
-storage_server msdp-ire.example.com -stype PureDisk -configlist
 add-replication.txt
Storage server msdp-ire.example.com has been successfully updated
[admin@ire-primary ~]#
/usr/openv/netbackup/bin/admincmd/nbdevconfig -updatedp -stype
PureDisk -dp dp-ire
The following replication properties have been added to the disk
 pool : ReplicationSource
Replication sources and/or targets have changed for disk volumes:
 PureDiskVolume
Update of disk pool replication properties succeeded
```

3 実稼働プライマリサーバーに、関連する MSDP ストレージユニットをターゲットとする 1 つのインポート SLP があることを確認します。存在しない場合は作成します。

4 IRE プライマリサーバーで次のコマンドを実行して、バックアップイメージを本番環境ドメインに手動でレプリケートします。

```
/usr/openv/netbackup/bin/admincmd/nbreplicate -backupid <backup
id> -cn <local copy number> -rcn <copy number plus 101> -slp_name
reverse-air -target_sts <production MSDP storage server name>
```

例:

```
/usr/openv/netbackup/bin/admincmd/nbreplicate -backupid
client1_1234567890 -cn 1 -rcn 102 -slp_name reverse-air
-target_sts msdp-prod.example.com
```

メモ: レプリケーションを開始する前に、同じバックアップ ID のバックアップイメージが、本番環境ドメインに存在しないことを確認します。存在する場合は、まず本番環境ドメインでイメージを期限切れにする必要があります。そうしないと、レプリケートされた新しいイメージは、実稼働プライマリサーバーでインポート SLP によって自動的にはインポートされません。

16

NetBackup 重複排除シェルの使用

この章では以下の項目について説明しています。

NetBackup 重複排除シェルについて

NetBackup 重複排除シェルを使用して、次の製品の WORM および MSDP ストレージサーバーの設定を管理できます。

- Flex Appliance: WORM をサポート
- Access Appliance: WORM をサポート
- NetBackup Flex Scale: WORM と通常の MSDP をサポート
- Azure Kubernetes Services (AKS) での NetBackup: 通常の MSDP をサポート
- Amazon Elastic Kubernetes Service (EKS) での NetBackup: 通常の MSDP をサポート

インターフェースには、タブ補完のコマンドオプションが用意されています。

コマンドの主なカテゴリは次のとおりです。

- `dedupe`
  このコマンドを使用すると、重複排除サービスを管理できます。
- `retention`
  このコマンドを使用すると、イメージの保持を管理できます。このコマンドは WORM ストレージサーバーでのみ利用可能です。
- `setting`
  このコマンドを使用すると、重複排除とシステム構成の設定を管理できます。
- `support`
  このコマンドを使用すると、トラブルシューティングのために、関連するログと構成ファイルにアクセスしてアップロードできます。

重複排除シェルにアクセスするには、ストレージサーバーへの SSH セッションを開きます。初めてログインする場合は、次のクレデンシャルを使用します。

- NetBackup Flex Scale: アプライアンス管理者の役割を持つアプライアンスユーザー
- その他のすべての製品:
  - ユーザー名: msdpadm

- パスワード: P@ssw0rd

初回ログイン時にパスワードを変更する必要があります。

重複排除シェルからのユーザーの管理

WORM または MSDP ストレージサーバーを構成した後、重複排除シェルを使用して、ユーザーを追加および管理できます。

次の種類のユーザーがサポートされています。

- ローカルユーザー
  ストレージサーバーのローカルユーザーは、製品の重複排除シェルから管理されます (NetBackup Flex Scale の場合を除く)。NetBackup Flex Scale の場合は、NetBackup Flex Scale 管理コンソールを使用します。アプライアンス管理者役割を持つすべてのユーザーには、重複排除シェルへのアクセス権があります。
  p.665 の「重複排除シェルからのローカルユーザーの追加と削除」を参照してください。
- MSDP ユーザー
  p.666 の「重複排除シェルからの MSDP ユーザーの追加」を参照してください。
- Active Directory (AD) ユーザー (ユニバーサル共有とインスタントアクセス用)
  p.668 の「ユニバーサル共有とインスタントアクセスのための WORM または MSDP ストレージサーバーへの Active Directory ドメインの接続」を参照してください。

重複排除シェルからのローカルユーザーの追加と削除

ストレージサーバーのローカルユーザーは、製品の重複排除シェルから管理されます (NetBackup Flex Scale の場合を除く)。NetBackup Flex Scale の場合は、NetBackup Flex Scale 管理コンソールを使用します。アプライアンス管理者役割を持つすべてのユーザーには、重複排除シェルへのアクセス権があります。

重複排除シェルからローカルユーザーの追加や削除を行うには、次の手順を使用します。

ローカルユーザーの追加

ローカルユーザーを追加するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開きます。
2. (オプション) 新しいユーザーにランダムなパスワードを使用する場合は、次のコマンドを使用してランダムなパスワードを生成します。

```
setting user random-password
```

3 次のコマンドを実行します。

```
setting user add-user username=<username> password=<password>
```

ここで *<username>* は追加するユーザーのユーザー名、*<password>* はそのユーザーのパスワードです。

パスワードは 15 文字から 32 文字までにし、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字 (_.+~@={}?!) を含める必要があります。

4 次のコマンドを実行して新しいユーザーを表示します。

- `setting user show-user username=<username>`
  このコマンドは新しいユーザーについての情報を表示します。
- `setting user list-users`
  このコマンドはすべてのローカルユーザーのリストを表示します。

ローカルユーザーの削除

ローカルユーザーを削除するには

1 msdpadm ユーザーとしてサーバーへの SSH セッションを開きます。

2 次のコマンドを実行します。

```
setting user delete-user username=<username>
```

ここで *<username>* は削除するユーザーのユーザー名です。

メモ: msdpadm ユーザーを削除することはできません。

重複排除シェルからの MSDP ユーザーの追加

NetBackup では、MSDP ユーザーは重複排除ストレージに接続する必要があります。ストレージサーバーを構成する際は、1 名の MSDP ユーザーが必要です。WORM インスタンスで複数の NetBackup ドメインを使用する場合は、インスタンスの作成後に、NetBackup ドメインごとに MSDP ユーザーを追加する必要があります。

重複排除シェルから MSDP ユーザーを追加するには、次の手順を使用します。

MSDP ユーザーを追加するには

1 msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。

2 (オプション) 新しいユーザーにランダムなパスワードを使用する場合は、次のコマンドを使用してランダムなパスワードを生成します。

```
setting MSDP-user random-password
```

3 次のコマンドを実行します。NetBackup Flex Scale で、このコマンドをプライマリノードで実行します。

```
setting MSDP-user add-MSDP-user username=<username>
password=<password>
```

ここで *<username>* は追加するユーザーのユーザー名、*<password>* はそのユーザーのパスワードです。

ユーザー名には、4 文字から 30 文字までの文字と数字を含めることができます。

パスワードは 15 文字から 32 文字までにし、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字 (_.+~={}?!) を含める必要があります。

4 次のコマンドを実行して新しいユーザーを表示します。NetBackup Flex Scale で、このコマンドをプライマリノードで実行します。

- `setting MSDP-user verify-user username=<username>`
  このコマンドは新しいユーザーのユーザー名とパスワードを検証します。
- `setting MSDP-user list`
  このコマンドはすべての MSDP ユーザーのリストを表示します。

重複排除シェルからの MSDP 管理エイリアスユーザーの追加

MVG (MSDP ボリュームグループ) に MSDP サーバーのディスクボリュームを追加するには、MSDP サーバーで MSDP のデフォルトユーザーのエイリアスを作成する必要がある場合があります。MVG サーバーは、独自のクレデンシャルを使用して MSDP サーバーと通信します。これらのクレデンシャルがディスクボリュームが存在する MSDP サーバーのクレデンシャルと一致しない場合は、MSDP サーバーでエイリアス MSDP ユーザーを作成する必要があります。エイリアスユーザーのクレデンシャルは MVG サーバーのクレデンシャルと一致する必要があります。

MSDP エイリアスユーザーを追加するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。NetBackup Flex Scale で、このコマンドをプライマリノードで実行します。

   ```
   setting MSDP-user add-MSDP-admin-alias username=<username>
   password=<password> owner=<owner>
   ```

   ここで *<username>* と *<password>* は MVG サーバー上の MSDP ユーザーのユーザー名とパスワードで、<owner> は MSDP サーバー上の MSDP 管理者ユーザーのユーザー名です。

   MSDP コンテナがバージョン 20.5 以前の場合、このコマンドは重複排除シェルではサポートされません。
3. 次のコマンドを実行してエイリアスユーザーを確認します。ユーザーのリストに新しいエイリアスユーザーが含まれており、エイリアスユーザーのデータ選択 ID が MSDP サーバーの管理者ユーザーと同じであることを確認します。

   ```
   setting MSDP-user list
   ```

メモ: コンテナで操作を直接実行するには、root ユーザーで MSDP コンテナにアクセスする必要があります。p.241 の「クレデンシャルが異なる場合の MVG サーバーが使用する MSDP サーバーの構成」を参照してください。

ユニバーサル共有とインスタントアクセスのための WORM または MSDP ストレージサーバーへの Active Directory ドメインの接続

ユニバーサル共有とインスタントアクセスのため、WORM または MSDP ストレージサーバーに Active Directory (AD) ユーザードメインを接続できます。

メモ: AD ドメインは、ユニバーサル共有とインスタントアクセスにのみ使用されます。AD ユーザーは現在、重複排除シェルではサポートされていません。

重複排除シェルから AD ユーザードメインを接続するには、次の手順を使用します。

AD ユーザードメインを接続するには

1. ストレージサーバーが AD ドメインと同じネットワークにあることを確認します。そうでない場合は、サーバーがドメインにアクセスできるように設定を編集します。
2. ストレージサーバーとリモートホストとの間で次のポートを開きます (まだ開いていない場合)。
   - 139

- 445

3 msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。

4 次のコマンドを実行します。

```
setting ActiveDirectory configure ad_server=<server name>
domain=<domain name> domain_admin=<username>
```

ここで *<server name>* は AD サーバー名、*<domain name>* は接続するドメイン、*<username>* はそのドメインの管理者ユーザーのユーザー名です。

5 プロンプトが表示されたら、ドメイン管理者ユーザーのパスワードを入力します。

重複排除シェルからの Active Directory ドメインの接続の切断

重複排除シェルから Active Directory (AD) ユーザードメインの接続を切断するには、次の手順を使用します。

AD ユーザードメインの接続を切断するには

1 msdpadm ユーザーとしてストレージサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。

2 次のコマンドを実行します。

```
setting ActiveDirectory unconfigure ad_server=<server name>
domain=<domain name> domain_admin=<username>
```

ここで *<server name>* は AD サーバー名、*<domain name>* は接続を切断するドメイン、*<username>* はそのドメインの管理者ユーザーのユーザー名です。

3 プロンプトが表示されたら、ドメイン管理者ユーザーのパスワードを入力します。

重複排除シェルからのユーザーパスワードの変更

重複排除シェルからローカルユーザーまたは MSDP ユーザーのパスワードを変更するには、次の手順を使用します。

メモ: リモートディレクトリユーザーのパスワードをシェルから変更することはできません。これらは、所属するサーバーから変更する必要があります。

ローカルユーザーのパスワードの変更

ローカルユーザーまたはデフォルトの msdpadm ユーザーのパスワードを変更するには、次の手順を使用します。

ローカルユーザーのパスワードを変更するには

1. パスワードを変更するユーザーとして、サーバーへの SSH セッションを開きます。msdpadm ユーザーとして、または NetBackup Flex Scale の場合はアプライアンス管理者としてログインすることもできます。
2. (オプション) ランダムなパスワードを使用する場合は、次のコマンドを使用してランダムなパスワードを生成します。

   ```
   setting user random-password
   ```

3. 次のコマンドを実行します。

   ```
   setting user change-password username=<username>
   ```

   ここで *<username>* は、パスワードを変更するユーザーのユーザー名です。
4. プロンプトに従ってパスワードを変更します。

   パスワードは 15 文字から 32 文字までにし、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字 (_.+~@={}?!) を含める必要があります。
5. (オプション) デフォルトでは、パスワードの有効期限はありません。パスワードの有効期限を指定するには、次のコマンドを実行します。

   ```
   setting user set-password-exp-date username=<username>
   password_exp_date=<date>
   ```

   ここで *<date>* は YYYY-MM-DD 形式の有効期限です。

   有効期限を設定すると、次のコマンドを使用して表示できます。

   ```
   setting user show-password-exp-date username=<username>
   ```

MSDP ユーザーのパスワードの変更

MSDP ユーザーのパスワードを変更するには、次の手順を使用します。

MSDP ユーザーのパスワードを変更するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. (オプション) ランダムなパスワードを使用する場合は、次のコマンドを使用してランダムなパスワードを生成します。

   ```
   setting MSDP-user random-password
   ```

3. 次のコマンドのいずれかを実行します。
   - パスワードをリセットする:

     ```
     setting MSDP-user reset-password username=<username>
     ```

     プロンプトに従って新しいパスワードを入力します。
   - NetBackup Flex Scale でパスワードを検証して変更する:

```
setting MSDP-user change-password username=<username>
```

既存のパスワードを入力し、新しいパスワードを入力します。

パスワードは 15 文字から 32 文字までにし、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字 (_.+~={}?!) を含める必要があります。

重複排除シェルからの VLAN インターフェースの管理

WORM または MSDP ストレージサーバーで複数の NetBackup ドメインを使用する場合は、サーバーの VLAN インターフェースを追加して他のドメインに接続できます。VLAN インターフェースを管理するには、次の手順を使用します。

VLAN インターフェースの追加

VLAN インターフェースを追加するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting MSDP-VLAN add interface=<VLAN IP address>
```

VLAN インターフェースの削除

VLAN インターフェースを削除するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting MSDP-VLAN remove interface=<VLAN IP address>
```

VLAN インターフェースの表示

VLAN インターフェースを表示するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting MSDP-VLAN list
```

WORM ストレージサーバーでの保持ポリシーの管理

WORM 保持ポリシーは、変更不可と削除不可によって WORM ストレージサーバーに保存されているデータを保護する期間を定義します。初期保持ポリシーは、サーバーの

構成時に決定されます。重複排除シェルからポリシーを表示または変更するには、次の手順を使用します。

保持ポリシーの表示

保持ポリシーを表示するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting WORM status
```

保持ポリシーの変更

保持ポリシーを変更するには、次の手順を使用します。新しい保持ポリシーは、今後のバックアップに適用されます。変更を行う前に取得したバックアップには適用されません。

保持ポリシーを変更するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行し、ストレージを変更不可および削除不可に保つ最小期間を指定します。

```
setting WORM set-min worm_min=<duration in seconds>
```

3. 次のコマンドを実行し、ストレージを変更不可および削除不可に保つ最大期間を指定します。

```
setting WORM set-max worm_max=<duration in seconds>
```

メモ: この操作は、マルチパーソン認証をサポートします。p.711 の「重複排除シェルコマンドのマルチパーソン認証」を参照してください。

WORM ストレージサーバーでの保持ロックを使用したイメージの管理

WORM ストレージサーバーのバックアップイメージには、保持ポリシーに基づく保持ロックがあります。保持ロックによって、イメージが変更または削除されることを防止できます。重複排除シェルから保持ロックを使用してバックアップイメージを管理するには、次の手順を使用します。

メモ: シェルで `catdbutil` コマンドを実行してイメージを管理することもできます。このコマンドはシェルメニューには表示されませんが、直接実行できます。ただし、コマンドの引数にパスの区切り記号 (/) を含めることはできません。p.221 の「変更不可および削除不可のデータを構成するための NetBackup コマンドラインオプションについて」を参照してください。

保持ロックを使用したバックアップイメージの表示

保持ロックを使用してバックアップイメージを表示するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

   ```
   retention policy list
   ```

バックアップイメージの保持ロックの無効化

アプライアンスがエンタープライズモードの場合は、バックアップイメージの保持ロックを無効にできます。アプライアンスがコンプライアンスモードの場合は、ロックを無効にできません。

保持ロックを無効にするには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドのいずれかを実行します。

   - 単一のバックアップイメージの保持ロックを無効化するには

     ```
     retention policy disable backup_ID="<ID>" copynumber=<number>
     ```

   - 同じコピー番号を持つ複数のバックアップイメージの保持ロックを無効化するには

     ```
     retention policy batch-disable
     backupids="<backupid1,backupid2,backupid3,...,backupidn>"
     copynumber=<number>
     ```

   `retention policy list` コマンドの出力で、バックアップ ID とコピー番号を確認します。

メモ: この操作は、マルチパーソン認証をサポートします。p.711 の「重複排除シェルコマンドのマルチパーソン認証」を参照してください。

WORM の保持に関する変更の監査

保持ポリシーやバックアップイメージの変更など、WORM 構成に対する変更の完全な履歴を表示するには、次の手順を使用します。

メモ: シェルで `catdbutil` コマンドを実行することで、保持に関する変更を管理することもできます。このコマンドはシェルメニューには表示されませんが、直接実行できます。ただし、コマンドの引数にパスの区切り記号 (/) を含めることはできません。p.221 の「変更不可および削除不可のデータを構成するための NetBackup コマンドラインオプションについて」を参照してください。

保持に関する変更を監査するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
retention policy audit
```

重複排除シェルからの MSDP カタログの保護

デフォルトでは、WORM ストレージサーバーは、専用のカタログボリューム (`/mnt/msdpcat`) で利用可能な元のコピーに加えて、ディレクトリ `/mnt/msdp/vol0` に MSDP カタログのコピーを格納します。

MSDP が単一ボリューム (Flex メディア、BYO、Cloud Scale) で最初に構成され、最初のボリュームが失われた場合、MSDP カタログのコピーも失われ、リカバリできません。現在は、新しいデータボリュームが追加されると、専用のカタログボリュームがない場合、カタログコピーは新しいデータボリュームに自動的に追加されます。カタログのシャドウコピーは新しいデータボリュームで利用可能で、最初のボリュームが失われたときにリカバリできます。

カタログの保護を強化する場合は、追加のコピーを構成できます。重複排除シェルから MSDP カタログコピーを管理するには、次の手順を使用します。

カタログコピーを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
cacontrol --catalog listshadowcopies
```

追加コピーを構成するには

1 サーバーへの SSH セッションを開きます。

2 次のコマンドを実行して、/mnt/msdp ディレクトリに存在するボリュームを判断します。

```
df -h
```

vol0 以外のボリュームの 1 つを選択します。

メモ: 追加のカタログコピーを構成するには、vol0 以外の 1 つ以上のボリュームが /mnt/msdp ディレクトリに存在する必要があります。

---

3 次のコマンドを実行します。

```
cacontrol --catalog addshadowcopy /mnt/msdp/<ボリューム名>
```

ここで <*ボリューム名*> は、前の手順で選択したボリュームです。

例:

```
cacontrol --catalog addshadowcopy /mnt/msdp/vol1
```

外部 MSDP カタログバックアップについて

外部 MSDP カタログバックアップユーティリティを使用して、コンテナ化された MSDP (Flex WORM、Flex Scale、Cloud Scale) の外部ストレージサーバーに MSDP カタログをバックアップします。他のプラットフォームで MSDP カタログを保護するには、次のトピックを参照してください。

p.197 の「MSDP カタログの保護について」を参照してください。

構成後、ユーティリティは MSDP カタログのバックアップを取得し、SLP を使用して NetBackup にインポートします。インポートされた MSDP カタログバックアップイメージを別のストレージサーバーに複製するには、最初に SLP を構成する必要があります。

バックアップ対象のデフォルトのカタログパスは次のとおりです。

- /database_path/databases/catalogshadow
- /storage_path/etc
- /database_path/databases/spa
- /storage_path/var
- /usr/openv/lib/ost-plugins/pd.conf
- /usr/openv/lib/ost-plugins/mtstrm.conf

- /database_path/databases/datacheck

重複排除シェルからの外部 MSDP カタログバックアップの構成

重複排除シェルで cacontrol ユーティリティを使用して、外部 MSDP カタログバックアップを構成および変更します。このユーティリティは /usr/openv/pdde/pdcr/bin にあります。外部 MSDP カタログバックアップを構成するには、MSDP ユーザーをアプリの役割で作成する必要があります。アプリの役割を持ち、新しい MSDP ユーザーを作成できる既存のユーザーを使用するか、新しいクレデンシャルを指定できます。

外部 MSDP カタログバックアップを設定する方法

1. NetBackup Web UI で、インポート操作を使用して SLP を作成します。

   MSDP ローカル LSU ストレージユニットとして宛先ストレージを選択します。

   保持形式が[ターゲットの保持 (Target retention)]に設定されていることを確認します。

2. SLP に子ルールを追加します。

   [複製 (Duplication)]操作を選択し、MSDP カタログバックアップを格納するために必要な外部ストレージサーバーに宛先ストレージを設定します。

   複製ストレージサーバーは、手順 1 で指定した MSDP ストレージサーバーと同じにすることはできません。保持形式が[固定 (Fixed)]に設定されていることを確認し、必要に応じて保持期間を設定します。

3. MSDP サーバーへの SSH セッションを開きます。

4. MSDP サーバーで、必要なユーザー名とパスワードを使用して、アプリの役割を持つ MSDP ユーザーを作成します。MSDP アプリユーザーがすでに存在する場合は、この手順をスキップできます。

   ```
   /usr/openv/pdde/pdcr/bin/spauser -a -u <app-username> -p
   <app-password> --role app
   ```

5. MSDP カタログバックアップを設定するには、MSDP サーバーで次のコマンドを実行します。

   ```
   cacontrol --catalog setupexternalcopy <username> <password>
   <frequency in minutes> <slp_name>
   ```

   - frequency: MSDP カタログバックアップをキャプチャする間隔 (分単位) です (1,440 = 毎日、10,080 = 毎週)。
   - slp_name: 手順 1 で作成された SLP の名前です。
   - username/password: 必要な権限を持った NetBackup ユーザーまたは管理者のユーザー名とパスワード。

これは、<STORAGE>/etc/puredisk/cat_backup.cfg の場所で MSDP データボリューム内の構成ファイルを作成します。構成ファイルは手動では変更できません。ログファイルとディレクトリは <STORAGE>/log/spad/ の場所に作成されます。

構成を表示する方法

1. MSDP サーバーへの SSH セッションを開きます。
2. MSDP カタログバックアップの構成設定を表示するには、次のコマンドを実行します。

```
cacontrol --catalog getexternalcopyconfig
```

バックアップ間隔を変更する方法

1. MSDP サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行してバックアップ間隔を変更します。

```
cacontrol --catalog editexternalcopyfrequency <frequency in
minutes>
```

バックアップ間隔は、外部 MSDP カタログバックアップの設定後にのみ変更します。

インポート SLP 名を変更する方法

1. NetBackup Web UI で、インポート操作を使用して SLP を作成します。

   MSDP ローカル LSU ストレージユニットとして宛先ストレージを選択します。

   保持形式が[ターゲットの保持 (Target retention)]に設定されていることを確認します。

2. SLP に子ルールを追加します。

   [複製 (Duplication)]操作を選択し、MSDP カタログバックアップを格納するために必要な外部ストレージサーバーに宛先ストレージを設定します。

   複製ストレージサーバーは、手順 1 で指定した MSDP ストレージサーバーと同じにすることはできません。保持形式が[固定 (Fixed)]に設定されていることを確認し、必要に応じて保持期間を設定します。

3. MSDP サーバーへの SSH セッションを開きます。
4. 次のコマンドを実行して、MSDP カタログバックアップイメージを NetBackup にインポートするために使用される SLP 名を変更します。

```
cacontrol --catalog editexternalcopyslpname <slp_name>
```

SLP 名は、外部 MSDP カタログバックアップの設定後にのみ変更します。

外部 MSDP カタログバックアップからのリストア

MSDP インスタンスには NetBackup クライアントがないため、破損した MSDP インスタンスにカタログイメージを直接リストアすることはできません。代わりに、MSDP カタログバックアップを最初に任意の NetBackup メディアサーバーにリストアする必要があります。その後、メディアサーバーから MSDP インスタンスにコピーできます。

p.536 の「MSDP カタログのリカバリについて」を参照してください。

外部 MSDP カタログバックアップのトラブルシューティング

SLP インポート操作が MSDP ストレージサーバーと一致するように正しく構成されていない場合、バックアップジョブはポリシー名 SLP_No_Target_SLP でインポートされ、複製はトリガされません。

この問題を修正するには、Web UI で SLP に移動し、SLP インポート操作を編集します。宛先ストレージをローカル LSU MSDP ストレージユニットに変更します。

重複排除シェルからの証明書の管理

NetBackup ホストを認証するため、NetBackup は認証局 (CA) が発行するセキュリティ証明書を使用します。NetBackup ストレージサーバーは、NetBackup CA または外部 CA のいずれかを使用できます。CA は、サーバーを構成するときに最初に構成されます。構成後は、重複排除シェルを使用して CA 証明書を管理できます。

NetBackup による証明書の使用について詳しくは、『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。

重複排除シェルからの証明書の詳細の表示

証明書の詳細を表示するには、msdpadm ユーザーとして、または NetBackup Flex Scale の場合はアプライアンス管理者として重複排除シェルにログインします。

現在の証明書構成の詳細を表示するには、次のコマンドを使用します。

- `setting certificate list-certificates`
  サーバーで利用可能なすべてのホスト証明書の詳細を表示します
- `setting certificate list-CA-cert-details`
  サーバーで利用可能なすべての CA 証明書の詳細を表示します
- `setting certificate show-CA-cert-detail`
  現在使用しているプライマリサーバーの NetBackup CA 証明書の詳細を表示します
- `setting certificate show-external-CA-cert-detail`
  現在使用しているプライマリサーバーの外部 CA 証明書の詳細を表示します

- `setting certificate list-enrollment-status`
  関連付けられたプライマリサーバーの登録状態を、ローカル証明書ストアから取得します
- `setting certificate show-CRL-check-level`
  外部証明書の失効確認レベルを表示します

証明書の状態を確認するには、次のコマンドを使用します。

- `setting certificate host-self-check`
  サーバーのホスト証明書が証明書失効リスト (CRL) に含まれているかどうかを確認します
- `setting certificate external-CA-health-check`
  外部証明書、RSA キー、トラストストアを検証します

重複排除シェルからの証明書のインポート

重複排除シェルから NetBackup 証明書または外部証明書をインポートするには、次の手順を使用します。

NetBackup 証明書のインポート

NetBackup 証明書をインポートするには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - プライマリサーバーから NetBackup CA 証明書を要求するには
     `setting certificate get-CA-certificate`
     デフォルトでは、このコマンドは NetBackup 構成ファイル内の最初のプライマリサーバーエントリを使用します。`primary_server` パラメータを使用して代替のプライマリサーバーを指定できます。例:
     `setting certificate get-CA-certificate primary_server=<alternate primary server hostname>`
   - プライマリサーバーからホスト証明書を要求するには
     `setting certificate get-certificate [force=true]`
     [force=true] はオプションのパラメータで、既存の証明書がすでに存在する場合はそれを上書きします。
     デフォルトでは、このコマンドは NetBackup 構成ファイル内の最初のプライマリサーバーエントリを使用します。`primary_server` パラメータを使用して代替のプライマリサーバーを指定できます。例:
     `setting certificate get-certificate primary_server=<alternate primary server hostname>`

プライマリサーバーのセキュリティレベルによっては、認証またはトークンの再発行がホストで必要になる場合があります。要求にトークンが必要であることを求めるメッセージが表示されたら、ホスト ID ベースの証明書のトークンを指定したコマンドを再入力します。例:

```
setting certificate get-certificate primary_server=<alternate primary server hostname> token=<certificate token> force=true
```

外部証明書のインポート

外部証明書をインポートするには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - 外部 CA 証明書とホスト証明書の両方をダウンロードしてインストールするには

     ```
     setting certificate install-external-certificates cacert=<trust store> cert=<host certificate> private_key=<key> [passphrase=<passphrase>] scp_host=<host> scp_port=<port>
     ```

     以下はその説明です。
     - *<trust store>* は PEM 形式のトラストストアです。
     - *<host certificate>* は、PEM 形式のホストの X.509 証明書です。
     - *<key>* は PEM 形式の RSA 秘密鍵です。
     - [passphrase=*<passphrase>*] は秘密鍵のパスフレーズの省略可能なパラメータです。このパラメータは、鍵が暗号化されている場合に必要になります。
     - *<host>* は、外部証明書を格納するホストのホスト名です。
     - *<port>* はリモートホストの接続先ポートです。
   - 外部 CA 証明書をダウンロードしてインストールするには

     ```
     setting certificate get-external-CA-certificate cacert=<trust store> scp_host=<host> scp_port=<port>
     ```

     以下はその説明です。
     - *<trust store>* は PEM 形式のトラストストアです。
     - *<host>* は、外部証明書を格納するホストのホスト名です。
     - *<port>* はリモートホストの接続先ポートです。
   - 外部ホスト証明書をダウンロードしてインストールするには

```
setting certificate get-external-certificates cert=<host
certificate> private_key=<key> [passphrase=<passphrase>]
scp_host=<host> scp_port=<port>
```

以下はその説明です。

- *<host certificate>* は、PEM 形式のホストの X.509 証明書です。
- *<key>* は PEM 形式の RSA 秘密鍵です。
- [passphrase=*<passphrase>*] は秘密鍵のパスフレーズの省略可能なパラメータです。このパラメータは、鍵が暗号化されている場合に必要になります。
- *<host>* は、外部証明書を格納するホストのホスト名です。
- *<port>* はリモートホストの接続先ポートです。

メモ: 外部ホスト証明書がサーバーにすでに存在する場合、その証明書は上書きされます。

3 (オプション) 次のコマンドを実行して、外部証明書の失効の確認レベルを指定します。

```
setting certificate set-CRL-check-level check_level=<DISABLE,
LEAF, or CHAIN>
```

確認レベルは次のとおりです。

- DISABLE: 失効の確認を無効にします。ホストとの通信時に、CRL で証明書の失効状態は検証されません。
- LEAF: CRL でリーフ証明書の失効状態が検証されます。デフォルト値は LEAF です。
- CHAIN: CRL で証明書チェーンの証明書すべての失効状態が検証されます。

重複排除シェルからの証明書の削除

重複排除シェルから NetBackup 証明書または外部証明書を削除するには、次の手順を使用します。

警告: 既存の証明書を削除し、新しい証明書をインストールしていない場合、WORM サーバーはプライマリサーバーと通信できなくなります。認証局 (CA) をある種類から別の種類に切り替えるには、既存の証明書を削除する前に、新しい NetBackup 証明書または外部証明書をインストールします。

NetBackup 証明書を削除するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting certificate disable-CA
```

外部証明書を削除するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting certificate remove-enrollment
```

重複排除シェルからの FIPS モードの管理

FIPS (Federal Information Process Standards) 140-2 に準拠するように、WORM または MSDP ストレージサーバーでは FIPS モードを使用できます。FIPS モードを管理するには、次の手順を使用します。

FIPS モードの表示

FIPS モードが有効または無効のどちらになっているかを確認するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting FIPS status
```

FIPS モードの有効化

FIPS モードを有効にするには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting FIPS enable
```

FIPS モードの無効化

FIPS モードを無効にするには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

```
setting FIPS disable
```

重複排除シェルからの PQC (ポスト量子暗号化) モードの管理

WORM ストレージサーバーで PQC (ポスト量子暗号化) モードを有効にして、TLS 1.3 Hybrid Key Exchange の PQC アルゴリズムの使用を有効にできます。PQC モードは FIPS モードが無効になっている場合にのみ有効にできます。

NetBackup での PQC サポートについて詳しくは、『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。

注意: NetBackup は OQS プロバイダを使用して、セキュアな通信のために PQC (ポスト量子暗号化) をサポートします。OQS プロバイダは耐量子の未来への準備に向けた重要なステップですが、現在は実験環境や研究環境で広く使用されています。Cohesity では、PQC モードを有効にする前に、関連するすべてのリスクを徹底して評価し、その使用状況が組織のセキュリティポリシーおよびコンプライアンス要件と一致していることを確認することをお勧めします。

PQC モードを管理するには、次の手順を使用します。

PQC モードの状態の表示

PQC モードが有効または無効のどちらになっているかを確認するには

1. msdpadm ユーザーとしてサーバーで SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting PQC status
```

PQC モードの有効化

PQC モードを有効にするには

1. msdpadm ユーザーとしてサーバーで SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting PQC enable
```

PQC モードの無効化

PQC モードを無効にするには

1. msdpadm ユーザーとしてサーバーで SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting PQC disable
   ```

重複排除シェルからのバックアップの暗号化

WORM または MSDP ストレージサーバーでバックアップを暗号化するには、KMS (Key Management Service) を有効または無効にして MSDP 暗号化を構成できます。

重複排除シェルからバックアップの暗号化を構成するには、次の手順を使用します。

KMS を使用して MSDP 暗号化を構成するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting encryption enable-kms kms_server=<server> key_group=<key group>
   ```

   ここで *<server>* は外部 KMS サーバーのホスト名、*<key group>* は KMS サーバーのキーグループ名です。
3. KMS 暗号化の状態を確認するには、`setting encryption kms-status` コマンドを実行します。

KMS を使用せずに MSDP 暗号化を構成するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting encryption enable
   ```

3. MSDP 暗号化の状態を確認するには、`setting encryption status` コマンドを実行します。

レガシー KMS の KEK (キー暗号化キー) への変換

`convert-legacy-kms` コマンドは、レガシーインデックスベースの KMS を KEK ベースの KMS に移行します。この移行では、レガシー KMS キーを使用して SO レコードの暗号化が解除され、アクティブな KEK を使用して SO レコードが再暗号化されます。

KEK 暗号化のキーをローテーションするには:

- rotate-kektag コマンドを使用して新しい KEK を作成し、新しい 3 階層 KMS システムを使用して SO レコードを新しい KEK にローテーションします。このシステムでは、KMS キーが KEK を暗号化し、それによって SO を暗号化するようになりました。
- rotate-kms-keys コマンドは、新しい KMS システムで KMS キーをローテーションします。KMS プロキシデータベースに格納されている KEK は、対応する KMS キーを使用して暗号化解除され、アクティブな KMS キーを使用して再暗号化されます。

重複排除シェルからの MSDP 構成の調整

デフォルトの MSDP 構成は、ほとんどのインストール環境で機能します。ただし、調整する必要がある場合は、次のコマンドを使用してパラメータを設定または表示します。

パラメータ	説明	コマンド
AllocationUnitSize	サーバー上のデータの割り当てユニットサイズ	パラメータを設定するには: setting set-MSDP-param allocation-unit-size value=*<number of MiB>* パラメータを表示するには: setting get-MSDP-param allocation-unit-size
DataCheckDays	データの一貫性を検査する日数	パラメータを設定するには: setting set-MSDP-param data-check-days value=*<number of days>* パラメータを表示するには: setting get-MSDP-param data-check-days
LogRetention	ログを保持する期間	パラメータを設定するには: setting set-MSDP-param log-retention value=*<number of days>* パラメータを表示するには: setting get-MSDP-param log-retention
MaxCacheSize	NetBackup 重複排除エンジン (spoold) の指紋キャッシュの最大サイズ	パラメータを設定するには: setting set-MSDP-param max-cache-size value=*<number of GB>* パラメータを表示するには: setting get-MSDP-param max-cache-size

パラメータ	説明	コマンド
MaxRetryCount	失敗した伝送を再試行する最大回数	パラメータを設定するには: `setting set-MSDP-param max-retry-count value=<number of retry times>` パラメータを表示するには: `setting get-MSDP-param max-retry-count`
SpadLogging	NetBackup 重複排除マネージャ (spad) のログレベル	パラメータを設定するには: `setting set-MSDP-param spad-logging log_level=<value>` p.690 の「重複排除シェルからの MSDP ログレベルの設定」を参照してください。 パラメータを表示するには: `setting get-MSDP-param spad-logging`
SpooldLogging	NetBackup 重複排除エンジン (spoold) のログレベル	パラメータを設定するには: `setting set-MSDP-param spoold-logging log_level=<value>` p.690 の「重複排除シェルからの MSDP ログレベルの設定」を参照してください。 パラメータを表示するには: `setting get-MSDP-param spoold-logging`
WriteThreadNum	データをデータコンテナに並列で書き込むためのスレッドの数	パラメータを設定するには: `setting set-MSDP-param write-thread-num value=<number of threads>` パラメータを表示するには: `setting get-MSDP-param write-thread-num`

CloudDataCacheSize	クラウド LSU を追加するときのデフォルトのデータキャッシュサイズ。十分な空き容量が利用できない場合は、この値を小さくします。	パラメータを設定するには:
		`setting set-MSDP-param cloud-data-cache-size value=<number>`
		パラメータを表示するには:
		`setting get-MSDP-param cloud-data-cache-size`

パラメータ	説明	コマンド

CloudMapCacheSize	クラウド LSU を追加するときのデフォルトのマップキャッシュサイズ。十分な空き容量が利用できない場合は、この値を小さくします。	パラメータを設定するには:
		`setting set-MSDP-param cloud-map-cache-size value=<number>`
		パラメータを表示するには:
		`setting get-MSDP-param cloud-map-cache-size`

CloudMetaCacheSize	クラウド LSU を追加するときのデフォルトのメタキャッシュサイズ。十分な空き容量が利用できない場合は、この値を小さくします。	パラメータを設定するには:
		`setting set-MSDP-param cloud-meta-cache-size value=<number>`
		パラメータを表示するには:
		`setting get-MSDP-param cloud-meta-cache-size`

CloudUploadCacheSize	クラウド LSU を追加するときのデフォルトのアップロードキャッシュサイズ。最小値は 12 GiB です。	パラメータを設定するには:
		`setting set-MSDP-param cloud-upload-cache-size value=<number>`
		パラメータを表示するには:
		`setting get-MSDP-param cloud-upload-cache-size`

EnableLocalPredictive SamplingCache	ローカルの予測サンプリングキャッシュを有効または無効にするパラメータ。spoold および spad の両方にこのパラメータがあり、それらの間で同期する必要があります。	パラメータを設定するには:
		`setting set-MSDP-param enable-local-predictive-sampling-cache value=<true/false>`
		パラメータを表示するには:
		`setting get-MSDP-param enable-local-predictive-sampling-cache`

パラメータ	説明	コマンド

MaxPredictiveCacheSize	spoold 予測キャッシュの最大サイズ。	パラメータを設定するには:
		`setting set-MSDP-param max-predictive-cache-size value=<number of bytes/%>`
		パラメータを表示するには:
		`setting get-MSDP-param max-predictive-cache-size`

MaxSamplingCacheSize	spoold サンプリングキャッシュの最大サイズ。	パラメータを設定するには:
		`setting set-MSDP-param max-sampling-cache-size value=<number of bytes/%>`
		パラメータを表示するには:
		`setting get-MSDP-param max-sampling-cache-size`

UsableMemoryLimit	spoold の利用可能な最大メモリサイズ。	パラメータを設定するには:
		`setting set-MSDP-param usable-memory-limit value=<number of bytes/%>`
		パラメータを表示するには:
		`setting get-MSDP-param usable-memory-limit`

MaxCacheSize(Cluster)	クラスタ内のすべてのノードの spoold 指紋キャッシュの最大サイズ。	パラメータを設定するには:
		`setting set-MSDP-param max-cache-size-cluster value=<number>`
		パラメータを表示するには:
		`setting get-MSDP-param max-cache-size-cluster`

パラメータ	説明	コマンド
MaxPredictiveCacheSize (Cluster)	クラスタ内のすべてのノードの spoold 予測キャッシュの最大サイズ。	パラメータを設定するには: setting set-MSDP-param max-predictive-cache-size-cluster value=<number of bytes> パラメータを表示するには: setting get-MSDP-param max-predictive-cache-size-cluster
MaxSamplingCacheSize (Cluster)	クラスタ内のすべてのノードの spoold サンプリングキャッシュの最大サイズ。	パラメータを設定するには: setting set-MSDP-param max-sampling-cache-size-cluster value=<number of bytes> パラメータを表示するには: setting get-MSDP-param max-sampling-cache-size-cluster
UsableMemoryLimit(Cluster)	クラスタ内のすべてのノードの spoold で使用可能な最大メモリサイズ。	パラメータを設定するには: setting set-MSDP-param usable-memory-limit-cluster value=<number> パラメータを表示するには: setting get-MSDP-param usable-memory-limit-cluster
EnableLocalPredictiveSampling Cache(Cluster)	クラスタ内のすべてのノードのローカルの予測サンプリングキャッシュを有効または無効にするパラメータ。spoold および spad の両方にこのパラメータがあり、それらの間で同期する必要があります。	パラメータを設定するには: setting set-MSDP-param enable-local-predictive-sampling-cache-cluster value=<true/false> パラメータを表示するには: setting get-MSDP-param enable-local-predictive-sampling-cache-cluster

パラメータ	説明	コマンド

VpfsCloudFPIndexRemoval Threshold (cluster)	クラスタ内のすべてのノードの、クラウドフィンガープリントインデックスファイルを削除するためのしきい値。フィンガープリントインデックスファイルに含まれる、削除されたデータコンテナの数がしきい値を超えると、フィンガープリントインデックスファイルが削除されます。	パラメータを設定するには:
		`setting set-MSDP-param vpfs-cloud-fpindex-removal-threshold value=<%>`
		パラメータを表示するには:
		`setting get-MSDP-param vpfs-cloud-fpindex-removal-threshold`

VpfsPCacheReloadThreshold (cluster)	置き換えられた pcache のフィンガープリントに基づいてフィンガープリントインデックスファイルからフィンガープリントを再ロードするための spoold のしきい値。これはクラスタ内のすべてのノードに適用されます。	パラメータを設定するには:
		`setting set-MSDP-param vpfs-pcache-reload-threshold-cluster value=<%>`
		パラメータを表示するには:
		`setting get-MSDP-param vpfs-pcache-reload-threshold-cluster`

重複排除シェルからの MSDP ログレベルの設定

次の MSDP サービスの WORM または MSDP ストレージサーバーのログレベルを設定できます。

- NetBackup 重複排除マネージャ (spad)
- NetBackup 重複排除エンジン (spoold)

ログレベルを設定するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - `setting set-MSDP-param spad-logging log_level=<value>,[thread],[date],[timing],[silent]`
   - `setting set-MSDP-param spoold-logging log_level=<value>,[thread],[date],[timing],[silent]`

   以下はその説明です。
   - *<value>* は次のいずれかです。
     - minimal: 重要、エラー、承認、およびバグのログを有効にします。
     - short: minimal のログをすべて有効にし、警告ログを追加します。

- long: short のログをすべて有効にし、情報ログを追加します。
- verbose: long のログをすべて有効にし、通知ログを追加します。
- full: verbose のログをすべて有効にし、トレースメッセージを追加します (すべての利用可能なログ)
- none: ログを無効にします。

- [thread] は、スレッド ID のログ記録を有効にするオプションのパラメータです。
- [date] は、各ログイベントの先頭に日付を含めるためのオプションのパラメータです。
- [timing] は、高解像度のタイムスタンプを有効にするオプションのパラメータです。
- [silent] は、コンソールまたは画面へのログの出力を停止するオプションのパラメータです。

例:

```
setting set-MSDP-param spoold-logging log_level=full,thread
```

重複排除シェルからの NetBackup サービスの管理

次の NetBackup サービスを重複排除シェルから管理できます。

- 巡回冗長検査 (CRC) サービス
  p.692 の「巡回冗長検査 (CRC) サービスの管理」を参照してください。
- コンテンツルーターのキュー処理 (CRQP) サービス
  p.693 の「コンテンツルーターのキュー処理 (CRQP) サービスの管理」を参照してください。
- オンラインチェックサービス
  p.694 の「オンラインチェックサービスの管理」を参照してください。
- 圧縮サービス
  p.694 の「圧縮サービスの管理」を参照してください。
- 重複排除 (MSDP) サービス
  p.695 の「重複排除 (MSDP) サービスの管理」を参照してください。
- ストレージプラットフォーム Web サービス (SPWS)
  p.696 の「ストレージプラットフォーム Web サービス (SPWS) の管理」を参照してください。
- Cohesity プロビジョニングファイルシステム (VPFS)
  p.698 の「Cohesity プロビジョニングファイルシステム (VPFS) 構成パラメータの管理」を参照してください。

p.699 の「Cohesity プロビジョニングファイルシステム (VPFS) マウントの管理」を参照してください。

- NGINX サービス
  p.700 の「NGINX サービスの管理」を参照してください。
- SMB サービス
  p.701 の「SMB サービスの管理」を参照してください。
- 次の重複排除ユーティリティがあります。
  - 重複排除マネージャユーティリティ (`cacontrol`)
    p.44 の「Oracle ストリームハンドラ」を参照してください。
  - 重複排除エンジンユーティリティ (`crcontrol`)
    p.488 の「MSDP コンテナファイル内のストレージ使用状況の表示」を参照してください。

メモ: これらのコマンドはシェルメニューには表示されませんが、直接実行できます。これらのコマンドの引数にパスの区切り記号 (/) を含めることはできません。

巡回冗長検査 (CRC) サービスの管理

巡回冗長検査 (CRC) サービスはデータ整合性チェックです。重複排除シェルから CRC サービスを管理するには、次の手順を使用します。

CRC サービスの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - CRC サービスの一般的な状態を表示するには
     ```
     dedupe CRC state
     ```
   - CRC サービスで修正モードの状態を表示するには
     ```
     dedupe CRC fixmode-state
     ```

CRC サービスを有効にするか、別の CRC モードを有効にするには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - CRC サービスを有効にするには
     ```
     dedupe CRC enable
     ```
   - コンテナ 64 から検査を開始し、コンテナの検査間でスリープ状態にならない高速検査を有効にするには

```
dedupe CRC fast
```

高速 CRC が終了すると、CRC の動作は高速検査が呼び出される前の動作に復帰します。

- 検査を実行し、不整合なメタデータの修正を試みる修正モードを有効にするには

```
dedupe CRC enable-fixmode
```

CRC サービスまたは修正モードを無効にするには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - CRC サービスを無効にするには

     ```
     dedupe CRC disable
     ```

   - 修正モードを無効にするには

     ```
     dedupe CRC disable-fixmode
     ```

コンテンツルーターのキュー処理 (CRQP) サービスの管理

コンテンツルーターのキュー処理 (CRQP) サービスは、内部データベースがストレージと同期していることを確認します。重複排除シェルから CRQP サービスを管理するには、次の手順を使用します。

CRQP サービスの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - `dedupe CRQP status`
     このコマンドは CRQP サービスが最後に実行された時点からの状態を示します。
   - `dedupe CRQP info`
     このコマンドは CRQP サービスの現在のアクティビティについての情報を示します。

CRQP サービスを開始するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
dedupe CRQP start
```

オンラインチェックサービスの管理

オンラインチェックサービスはデータ整合性チェックです。オンラインチェックサービスを管理するには、次の手順を使用します。

オンラインチェックサービスを開始するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
dedupe online-check start
```

オンラインチェックサービスの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
dedupe online-check status
```

オンラインチェックサービスを有効化または無効化するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。

```
dedupe online-check enable

dedupe online-check disable
```

圧縮サービスの管理

圧縮サービスはMSDPカタログから不要なデータを削除します。圧縮サービスを管理するには、次の手順を使用します。

圧縮サービスの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
dedupe compaction state
```

圧縮サービスを有効化または無効化するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。

```
dedupe compaction enable

dedupe compaction disable
```

システムスケジュール以外で圧縮サービスを開始するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
dedupe compaction start
```

重複排除 (MSDP) サービスの管理

重複排除サービスは、ストレージサーバーのメディアサーバー重複排除プール (MSDP) ストレージを操作します。MSDP サービスを管理するには、次の手順を使用します。

MSDP サービスの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
dedupe MSDP status
```

MSDP サービスを停止するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを使用して、健全性監視の状態を確認します。

```
setting health status
```

3. 健全性監視が有効になっている場合は、次のコマンドを使用して監視を停止します。

```
setting health disable
```

4. 健全性監視を無効にしたら、次のコマンドを使用して MSDP サービスを停止します。

```
dedupe MSDP stop
```

MSDP サービスを起動するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを使用して MSDP サービスを起動します。

```
dedupe MSDP start
```

3. 次のコマンドを使用して健全性監視を開始します。

```
setting health enable
```

クラスタ全体の MSDP サービスの管理

重複排除サービスは、ストレージサーバーの MSDP (メディアサーバー重複排除プール) ストレージを操作します。クラスタの MSDP サービスを管理するには、次の手順を使用します。

MSDP サービスの状態を表示するには

1. クラスタ内の任意の MSDP エンジンへの SSH セッションを開きます。
2. 次のコマンドを実行して、クラスタの MSDP サービスの状態を表示します。

   ```
   dedupe MSDP-cluster status
   ```

   vpfsd の状態も表示されます。

MSDP サービスを停止するには

1. クラスタ内の任意の MSDP エンジンへの SSH セッションを開きます。
2. 次のコマンドを実行して、クラスタの MSDP サービスを停止します。

   ```
   dedupe MSDP-cluster stop
   ```

   vpfsd サービスも停止されます。

MSDP サービスを起動するには

1. クラスタ内の任意の MSDP エンジンへの SSH セッションを開きます。
2. 次のコマンドを実行して、クラスタの MSDP サービスを開始します。

   ```
   dedupe MSDP-cluster start
   ```

   vpfsd サービスも開始されます。

ストレージプラットフォーム Web サービス (SPWS) の管理

ストレージプラットフォーム Web サービス (SPWS) は、インスタントアクセスとユニバーサル共有のサービスです。SPWS を管理するには、次の手順を使用します。

SPWS の状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   dedupe spws status
   ```

SPWS を停止または起動するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。

   ```
   dedupe SPWS stop
   ```

   ```
   dedupe SPWS start
   ```

SPWS 構成パラメータを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting spws-config get-spws-param spws_configkey=<parameter>
   ```

   ここで <parameter> は表示するパラメータです。

SPWS 構成パラメータを変更するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting spws-config set-spws-param spws_configsection=<section>
   spws_configkey=<parameter> spws_configvalue=<value>
   ```

   ここで、<section> は Samba 構成セクション、<parameter> は変更するパラメータ、<value> はそのパラメータの変更後の値です。次に例を示します。

   ```
   setting spws-config set-spws-param spws_configsection=Livemount
   spws_configkey=maxallowedusharebackupjobs spws_configvalue=5
   ```

接続エラーのトラブルシューティング

SPWS への永続的な接続エラーが発生した場合は、次の手順を使用して SPWS からプライマリ NetBackup Web サービスに証明書をプッシュします。

証明書をプッシュするには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   dedupe spws push-spws-certificate
   ```

   メモ: クラスタ環境で、カタログエンジンからこのコマンドを実行する必要があります。他のエンジンからは実行できません。

Open Cloud Storage デーモンの管理

Open Cloud Storage デーモン (ocsd) は、クラウドと対話するサービスです。

OCSD の状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   dedupe ocsd status
   ```

OCSD を停止または起動するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。

```
dedupe ocsd stop
```

```
dedupe ocsd start
```

Cohesity プロビジョニングファイルシステム (VPFS) 構成パラメータの管理

Cohesity プロビジョニングファイルシステム (VPFS) は、インスタントアクセスとユニバーサル共有のサービスです。ほとんどの環境では、デフォルトの VPFS 構成で動作します。ただし、必要に応じてパラメータを調整できます。パフォーマンスに影響する可能性があるパラメータの一部を次に示します。

- `numOfInstance`
  このパラメータは `vpfsd` インスタンスの数を指定します。ユニバーサル共有は、デフォルトで 1 つの `vpfsd` インスタンスを使用します。ほとんどの場合、1 つのインスタンスで十分です。`vpfsd` インスタンスの数を増やすと、ユニバーサル共有のパフォーマンスが向上する可能性がありますが、必要な CPU とメモリも増えます。`vpfsd` インスタンスの数は 1 から最大 16 まで増やすことができ、共有はすべての `vpfsd` インスタンスに分散できます。
- `CloudCacheSize`
  このパラメータはローカルディスクのキャッシュサイズを指定します。このオプションは、オブジェクトストアを使用したユニバーサル共有と、オブジェクトストアを使用したインスタントアクセスにのみ適用されます。

VPFS 構成パラメータを管理するには、次の手順を使用します。

VPFS 構成パラメータを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting vpfs-config get-vpfs-param vpfs_configkey=<parameter>
```

ここで *<parameter>* は表示するパラメータです。

VPFS 構成パラメータを変更するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting vpfs-config set-vpfs-param vpfs_configkey=<parameter>
   vpfs_configvalue=<value>
   ```

   ここで *<parameter>* は変更するパラメータであり、*<value>* はそのパラメータの変更後の値です。例:

   ```
   setting vpfs-config set-vpfs-param vpfs_configkey=numOfInstance
   vpfs_configvalue=2
   ```

VPFS 共有のログレベルを一時的に変更するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting vpfs-config set-log-level vpfs_loglevel=<level>
   vpfs_shareid=<share ID>
   ```

   ここで *<level>* は、`debug`、`information`、または `error` で、*<share ID>* はログレベルを変更する共有の ID です。次に例を示します。

   ```
   setting vpfs-config set-log-level vpfs_loglevel=debug
   vpfs_shareid=my-db-share
   ```

メモ: このコマンドは短いデバッグセッション用であり、インスタンスを再起動すると変更は保持されません。ログレベルを永続的に変更するには、次のコマンドを使用します。

```
setting vpfs-config set-vpfs-param vpfs_configkey=logLevel
vpfs_configvalue=<level>
```

デフォルトのログレベルは `information` です。

Cohesity プロビジョニングファイルシステム (VPFS) マウントの管理

Cohesity プロビジョニングファイルシステム (VPFS) は、インスタントアクセスとユニバーサル共有のサービスです。VPFS マウントを管理するには、次の手順を使用します。

VPFS マウントの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   dedupe vpfs status
   ```

VPFS マウントを停止または開始するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。

   `dedupe vpfs stop`

   `dedupe vpfs force-stop` (このコマンドは、`dedupe vpfs stop` コマンドが機能しないか停止した場合にのみ使用します。)

   `dedupe vpfs start`

VPFS 共有のリストを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   `dedupe vpfs list-shares`

NGINX サービスの管理

NGINX サービスは、ストレージプラットフォーム Web サービス (SPWS) のゲートウェイです。NGINX サービスを管理するには、次の手順を使用します。

NGINX サービスの状態を表示するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

   `setting nginx status`

NGINX サービスを起動または停止するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドのいずれかを実行します。

   `setting nginx stop`

   `setting nginx start`

NGINX 証明書の構成

NGINX 証明書を使用すると、NGINX は NetBackup プライマリサーバーと通信できます。証明書に問題がある場合は、次の手順を使用して構成を管理します。

NGINX 証明書を構成するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting nginx config-cert
   ```

3. 次のコマンドを使用して、NGINX 証明書の詳細を表示できます。

   ```
   setting nginx show-cert
   ```

SMB サービスの管理

SMB サービスには、インスタントアクセス用とユニバーサル共有用の SMB ユーザーが含まれます。SMB サービスを管理するには、次の手順を使用します。

SMB サービスの状態を表示するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting smb status
   ```

SMB サービスを停止または開始する方法

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. 次のコマンドのいずれかを実行します。

   ```
   setting smb stop
   ```

   ```
   setting smb start
   ```

SMB 構成パラメータを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting smb get-smb-param smb_configkey=<parameter>
   ```

   ここで <parameter> は表示するパラメータです。

SMB 構成パラメータを変更するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting smb set-smb-param smb_configsection=<section>
smb_configkey=<parameter> smb_configvalue=<value>
```

ここで、<section> は Samba 構成セクション、<parameter> は変更するパラメータ、<value> はそのパラメータの変更後の値です。次に例を示します。

```
setting smb set-smb-param smb_configsection="global"
smb_configkey="server signing" smb_configvalue="mandatory"
```

重複排除シェルからの NetBackup サービスの監視およびトラブルシューティング

次のコマンドを使用して、WORM または MSDP ストレージサーバーの NetBackup サービスを監視およびトラブルシューティングできます。

- `setting health` コマンド
  このコマンドは、アプリケーションの高可用性の状態を監視するサーバーの健全性モニターを管理します。
  p.703 の「健全性モニターの管理」を参照してください。
- `support` コマンド
  このコマンドを使用すると、トラブルシューティングのためにログと構成ファイルにアクセスできます。
  p.703 の「システムについての情報の表示」を参照してください。
  p.704 の「重複排除 (MSDP) の履歴または構成ファイルの表示」を参照してください。
  p.706 の「ログファイルの表示」を参照してください。
  p.708 の「トラブルシューティングファイルの収集と転送」を参照してください。
- `setting kernel` コマンド
  このコマンドを使用すると、カーネルパラメータのキーワードを検索できます。
  p.703 の「システムについての情報の表示」を参照してください。
- `crstats` コマンドと `dcscan` コマンド

メモ: これらのコマンドはシェルメニューには表示されませんが、直接実行できます。これらのコマンドの引数にパスの区切り記号 (/) を含めることはできません。

p.286 の「クラウドサポートのツールの更新について」を参照してください。

- `msdpimgutil` コマンド
  このコマンドを使用すると、ストレージサーバーの重複排除プールの暗号化の状態またはイメージの暗号化の状態を確認できます。
  p.490 の「イメージの暗号化状態の確認」を参照してください。

健全性モニターの管理

アプリケーションの高可用性の状態を監視するため、健全性モニターはデフォルトで有効になっています。重複排除シェルから健全性モニターを管理するには、次の手順を使用します。

健全性モニターの状態を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting health status
```

健全性モニターを有効または無効にするには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。

```
setting health enable
```

```
setting health disable
```

システムについての情報の表示

重複排除シェルからシステムに関する情報を表示するには、次のコマンドを使用します。

ハードウェアに関する情報を表示するには

- `support hardware cpumem` または `support process htop`: CPU とメモリの情報を表示します

ソフトウェアに関する情報を表示するには

- `support software show-MSDP-version`: メディアサーバー重複排除プール (MSDP) のバージョンを表示します
- `support software show-OS-version`: Linux オペレーティングシステムのバージョンを表示します

システムプロセスに関する情報を表示するには

- `support process MSDP-process`: MSDP プロセスを表示します
- `support process pidstat`: オペレーティングシステムプロセス (PID) を表示します

システムパフォーマンスに関する情報を表示するには

- `support diskio iostat`: ディスク I/O についての情報を表示します
- `support diskio vmstat`: ディスク I/O での待機についての情報を表示します
- `support diskio nmon`: ディスク I/O、ネットワーク I/O、CPU 使用率を監視する監視システムに関する情報を表示します。
- `support diskio disk-volume`: ディスクボリュームについての情報を表示します
- `support process memory-usage`: 空きメモリと使用済みメモリを表示します
- `support process atop`: オペレーティングシステムとプロセスアクティビティに関する詳細情報を表示します

カーネルパラメータを検索するには

- `setting kernel search-param keyword=<keyword>`
  ここで ***<keyword>*** は検索する単語です。

ネットワーク設定を表示するには:

- `setting network ifconfig`: インターネット構成を表示します
- `setting network ping ip=<ip_address>`: ターゲット IP アドレスに ping を実行します
- `setting network route route=<route>`: ネットワークルーティング情報を表示します
- `setting network netstat`: ネットワークの状態とプロトコルの統計を表示します

重複排除 (MSDP) の履歴または構成ファイルの表示

重複排除サービスは、ストレージサーバーのメディアサーバー重複排除プール (MSDP) ストレージを操作します。MSDP サービスから次のファイルを表示できます。

- MSDP 履歴ファイル
- MSDP 構成ファイル

重複排除シェルからこれらのファイルを表示または検索するには、次の手順を使用します。

ファイルに関する情報を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - `support MSDP-history ls [dir=<directory>]`
   - `support MSDP-config ls [dir=<directory>]`

ここで、[dir=<*directory*>] は、ファイルを表示するディレクトリを指定するオプションのパラメータです。例:

```
support MSDP-config ls dir=config
```

ファイルを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のいずれかを実行します。
   - ファイル全体を表示するには、次のコマンドのいずれかを実行します。
     - `support MSDP-history cat file=<file>`
     - `support MSDP-config cat file=<file>`

     ここで ***<file>*** は、表示するファイルのファイル名です。
   - ファイルの末尾 10 行を表示するには、次のコマンドのいずれかを実行します。
     - `support MSDP-history tail file=<file>`
     - `support MSDP-config tail file=<file>`

     ここで ***<file>*** は、表示するファイルのファイル名です。

ファイルを検索するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - `support MSDP-history grep file=<file> pattern=<keyword>`
   - `support MSDP-config grep file=<file> pattern=<keyword>`

   ここで `<file>` は、検索するファイルのファイル名で、`<keyword>` は検索する名前のパターンです。例:

   ```
   support MSDP-config grep file=spa.cfg pattern=address
   ```

pseudo-file システムでのプロセス情報の表示

/proc/ ディレクトリからファイルを表示または検索するには、次の手順を使用します。

ファイルに関する情報を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   support proc ls [dir=<directory>]
   ```

   - ここで、`[dir=<directory>]` は、ファイルを表示するディレクトリを指定するオプションのパラメータです。次に例を示します。

     ```
     support proc ls dir=config
     ```

ファイルを表示するには

1 サーバーへの SSH セッションを開きます。

2 次のいずれかを実行します。

- ファイル全体を表示するには、次のコマンドを実行します。
  `support proc cat file=<file>`
  ここで `<file>` は、表示するファイルのファイル名です。
- ファイルの末尾 10 行を表示するには、次のコマンドを実行します。
  `support proc tail file=<file>`
  ここで `<file>` は、表示するファイルのファイル名です。

ファイルを検索するには

1 サーバーへの SSH セッションを開きます。

2 次のコマンドを実行します。

```
support proc grep file=<file> pattern=<keyword>
```

ここで `<file>` は、検索するファイルのファイル名で、`<keyword>` は検索する名前のパターンです。例:

```
support proc grep file=spa.cfg pattern=address
```

VPFS (Veritas provisioning file service) 共有の重複排除率の表示

VPFS (Veritas provisioning file service) 共有の重複排除率を表示するには、次の手順を使用します。

重複排除率を表示するには

1 サーバーへの SSH セッションを開きます。

2 次のコマンドを実行します。

```
dedupe vpfs meta-dump vpfs_metakind=dedupe vpfs_shareid=<share ID>
```

ここで、*<share ID>* は重複排除率を表示する共有の ID です。

ログファイルの表示

WORM ストレージサーバーでは、次のログを利用できます。

- メディアサーバー重複排除プール (MSDP) のログ
  これらのファイルには、`spad`、`spoold`、`ocsd`、および `vpfsd` サービスのログが含まれます。
- システムログ

これらのファイルには /mnt/nblogs ディレクトリのログが含まれます。これには、インスタンス管理と証明書に関連するログが含まれます。

重複排除シェルからログファイルを表示または検索するには、次の手順を使用します。

ファイルに関する情報を表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - `support MSDP-log ls [dir=<directory>]`
   - `support syslogs ls [dir=<directory>]`

   ここで、[dir=<*directory*>] は、ファイルを表示するディレクトリを指定するオプションのパラメータです。例:

   ```
   support MSDP-log ls dir=spoold
   ```

ファイルを表示するには

1. サーバーへの SSH セッションを開きます。
2. 次のいずれかを実行します。
   - ファイル全体を表示するには、次のコマンドのいずれかを実行します。
     - `support MSDP-log cat file=<file>`
     - `support syslogs cat file=<file>`

     ここで ***<file>*** は、表示するファイルのファイル名です。
   - ファイルの末尾 10 行を表示するには、次のコマンドのいずれかを実行します。
     - `support MSDP-log tail file=<file>`
     - `support syslogs tail file=<file>`

     ここで ***<file>*** は、表示するファイルのファイル名です。

ファイルを検索するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドのいずれかを実行します。
   - `support MSDP-log grep file=<file> pattern=<keyword>`
   - `support syslogs grep file=<file> pattern=<keyword>`

   ここで <file> は、検索するファイルのファイル名で、<keyword> は検索する名前のパターンです。例:

   ```
   support MSDP-log grep file=spad* pattern=sessionStartAgent
   ```

トラブルシューティングファイルの収集と転送

次のカテゴリからファイルを収集し、表示しやすくするために別のホストに転送できます。

- メディアサーバー重複排除プール (MSDP) の履歴ファイル
- MSDP 構成ファイル
- MSDP ログファイル
- システムログファイル

重複排除シェルからこれらのファイルを収集して転送するには、次の手順を使用します。

ファイルを収集して転送するには

1. msdpadm ユーザーとしてサーバーへの SSH セッションを開くか、NetBackup Flex Scale の場合はアプライアンス管理者としてセッションを開きます。
2. サイズの大きいログファイルを収集して転送する場合は、SSH 接続がタイムアウトするまでの時間を増やすことが必要になる場合があります。デフォルトは 10 分です。時間を長くするには、次の手順を使用します。
   - 次のコマンドを実行します。
     `setting ssh set-ssh-timeout ssh_timeout=<number of seconds>`
   - 次のコマンドを実行して変更を確認します。
     `setting ssh show-ssh-timeout`
   - 現在の SSH セッションを閉じ、新しい SSH セッションを開きます。
3. 次のコマンドを実行して、目的のカテゴリから対象のファイルを収集します。
   - `support MSDP-history collect`
   - `support MSDP-config collect`
   - `support MSDP-log collect`
   - `support syslogs collect`

   次のオプションパラメータを使用することもできます。
   - `pattern=<keyword>`
     このパラメータはファイル内のキーワードを検索します。
   - `mmin="<minutes, +minutes, or -minutes>"`
     このパラメータは、ファイルを収集する時間枠を分単位で指定します。x 分前からのファイルを収集するには、`mmin="x"` を入力します。x 分前より前のファイルを収集するには、`mmin="-x"` を入力します。x 分前より後のファイルを収集するには、`mmin="+x"` を入力します。
   - `mtime="<days, +days, or -days>"`

このパラメータは、ファイルを収集する時間枠を日単位で指定します。x 日前からのファイルを収集するには、mtime="x" を入力します。x 日前より前のファイルを収集するには、mtime="-x" を入力します。x 日前より後のファイルを収集するには、mtime="+x" を入力します。

例:

```
support MSDP-log collect pattern=spoold* mmin="+2"
```

4 任意のカテゴリから scp コマンドを実行して、以前に収集された (全カテゴリの) すべてのファイルの tarball を作成し、scp プロトコルを使用してターゲットホストに tarball を転送します。例:

```
support MSDP-config scp scp_target=user@example.com:/tmp
```

5 必要に応じ、次のコマンドを実行して SSH のタイムアウトをデフォルトに戻します。

```
setting ssh set-ssh-timeout ssh_timeout=600
```

setting ssh show-ssh-timeout コマンドを使用して変更を確認します。

重複排除シェルからの S3 サービスの管理

Flex アプライアンスの MSDP WORM ストレージサーバーを構成した後、重複排除シェルを使用して、S3 サービスを構成および管理できます。

- S3 サービスを構成します。
p.709 の「S3 サービスの構成」を参照してください。
- root ユーザーのクレデンシャルを作成またはリセットします。
p.710 の「root クレデンシャルの作成またはリセット」を参照してください。
- S3 サービス証明書を変更します。
p.710 の「S3 サービス証明書の変更」を参照してください。
- S3 サービスの状態を管理します。
p.710 の「S3 サービスの管理 」を参照してください。

S3 サービスの構成

MSDP に S3 インターフェースを使用するには、MSDP WORM ストレージサーバーインスタンスで S3 サービスを構成します。

S3 サービスを構成するには

1 サーバーへの SSH セッションを開きます。

2 次のコマンドを実行します。

```
setting s3srv s3srv-config s3srv_ca_type=<ca type>
[s3srv_loglevel=<log level>] [s3srv_port=<s3 port>]
```

- s3srv_ca_type: 認証局のタイプ。NBCA: 1、ECA: 2。
- s3srv_loglevel: S3 サーバーのログレベル。
  なし: 0
  エラー: 1
  警告: 2
  情報: 3 (デフォルト)
  デバッグ: 4
- s3srv_port: S3 サーバーポート。デフォルトのポートは 8443 です。

root クレデンシャルの作成またはリセット

MSDP の S3 インターフェースを構成した後、root ユーザーのクレデンシャルを作成して、S3 クレデンシャルを管理できます。

S3 サービスの root クレデンシャルを作成またはリセットするには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting s3srv s3srv-reset-iam
```

S3 サービス証明書の変更

S3 サーバーの HTTPS 証明書の期限が切れたら、手動で更新する必要があります。

S3 サービス証明書を変更するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

```
setting s3srv s3srv-change-ca s3srv_ca_type=<ca type>
```

- s3srv_ca_type: 認証局のタイプ。NBCA: 1、ECA: 2

S3 サービスの管理

S3 サービスの状態を管理するには、次の手順を実行します。

S3 サービスを管理するには

1. サーバーへの SSH セッションを開きます。
2. S3 サービスの状態を表示します。

   ```
   setting s3srv status
   ```

3. S3 サービスを停止します。

   ```
   setting s3srv stop
   ```

4. S3 サービスを起動します。

   ```
   setting s3srv start
   ```

S3 サービスログレベルの変更

S3 サービスログレベルを管理するには、次の手順を実行します。

S3 サービスログレベルを変更するには

1. サーバーへの SSH セッションを開きます。
2. 次のコマンドを実行します。

   ```
   setting s3srv s3srv-change-loglevel s3srv_loglevel=<level>

   s3srv_loglevel: None: 0, Error: 1, Warning: 2, Info: 3, Debug: 4
   ```

重複排除シェルコマンドのマルチパーソン認証

NetBackup Web UI で、セキュリティ管理者は、重要な MSDP 操作に対してマルチパーソン認証を構成できます。マルチパーソン認証について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』にある「マルチパーソン認証の構成」の章を参照してください。

マルチパーソン認証が操作に対して構成されている場合、その操作を実行するには承認者からの承認が必要です。MSDP 管理者が重複排除シェルを使用して操作コマンドを実行すると、確認用のマルチパーソン認証チケットが作成されます。チケットが承認者によって承認された後にのみ、MSDP 管理者は操作を実行できます。

たとえば、MSDP WORM 構成の変更にはマルチパーソン認証が必要です。MSDP 管理者が、WORM 保持ロックの最大期間を変更する `setting WORM set-max` コマンドを実行すると、確認用のチケットが作成されます。

```
[msdp shell] > setting WORM set-max worm_max=1900000
Multi-person authorization is enforced. This operation requires
authorization from the primary server: primary.example.com.
Create a ticket for approval (y/n)? y
Ticket comment: enlarge the WORM lock duration.
Ticket 7 is created. Please wait for an approval and run the command
```

```
 again.
Operation failed
```

チケットが承認者によって確認され、承認されると、MSDP 管理者はコマンドを実行して WORM 構成の変更を実行できます。

```
[msdp shell] > setting WORM set-max worm_max=1900000
Multi-person authorization is enforced. This operation requires
authorization from the primary server: primary.example.com.
Ticket 7 for this operation is approved.
Operation completed successfully
```

チケットがまだ承認待ちで、MSDP 管理者がコマンドを再実行する場合、重複排除シェルは管理者に承認を待つよう求めます。

```
[msdp shell] > setting WORM set-max worm_max=1900000
Multi-person authorization is enforced. This operation requires
authorization from the primary server: primary.example.com.
The ticket 7 for this operation is still under review. Please wait
for an approval and run the command again.
Operation failed
```

Flex Scale と Cloud Scale でのクラウド LSU の管理

重複排除シェルを使用して、クラウド LSU (論理ストレージユニット) の設定を管理および構成します。

Flex Scale と Cloud Scale でクラウド WORM LSU を管理するには

1. クラスタ内の任意の MSDP エンジンへの SSH セッションを開きます。
2. クラウド WORM LSU を一覧表示します。

   ```
   setting WORM-Cloud list-lsu
   ```

3. WORM の構成を再ロードします。

   ```
   setting WORM-Cloud reload-config lsu_name=<lsu_name>
   ```

クラウド LSU について詳しくは、「MSDP クラウドのサポート」の章を参照してください。

MSDP コンテナの NFS バージョン 3 サーバーサービスの管理

NetBackup 重複排除シェルを使用して、Flex Scale で MSDP コンテナの NFS バージョン 3 サーバーサービスを管理できます。

NetBackup Flex Scale 3.5 では、NFS バージョン 3 はデフォルトでは無効になっています。

MSDP コンテナの NFS バージョン 3 サーバーサービスを管理するには

1. NetBackup Flex Scale のアプライアンス管理者としてサーバーへの SSH セッションを開きます。
2. 現在のカーネル構成でサポートされている NFS サーバーのバージョンを表示します。

   ```
   setting NFS get-nfs-versions
   ```

3. MSDP コンテナの NFS バージョン 3 サーバーサービスを有効にします。

   ```
   setting NFS enable-nfsv3
   ```

4. MSDP コンテナの NFS バージョン 3 サーバーサービスを無効にします。

   ```
   setting NFS disable-nfsv3
   ```

MSDP コンテナに割り当てられた NetBackup RBAC の役割の表示

MSDP コンテナでは、NetBackup API を正常に呼び出すには、任意の MSDP コンテナの役割が必要です。ユーザーが NetBackup プライマリサーバーの構成に、必要な `MSDP_SERVER` エントリを追加できなかったり、エントリが構成から削除されていたりすることがあります。

このようなケースで、問題を迅速にトラブルシューティングして解決することが困難な場合があります。新しい制限付きシェルコマンドを使用すると、適切な NetBackup RBAC の役割が MSDP コンテナに割り当てられているかどうかを迅速に判断できます。

MSDP コンテナに割り当てられた NetBackup RBAC の役割を表示する方法

1. 次のコマンドを実行します。

   ```
   setting certificate show-nb-web-token-roles
   ```

2. ［任意の MSDP コンテナ (Any MSDP Container)］というテキストの出力を確認します。

   このテキストが表示されない場合は、`MSDP_SERVER` エントリが NetBackup プライマリサーバー構成に存在せず、追加する必要があることを示します。

17

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

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.717 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 17-1　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'

フィールド名	形式	説明	例
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
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

フィールド名	形式	説明	例
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 17-2 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 17-3 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

項目	例
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`

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。

MSDP 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、次の URL にある『NetBackup ログリファレンスガイド』を参照してください。

http://www.veritas.com/docs/DOC5332

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 MSDP ログファイル

NetBackup の重複排除コンポーネントは各種のログファイルに情報を書き込みます。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。他の処理では、Veritas Unified Logging (VxUL) ログファイルが使用されます。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。オリジネータ ID (OID) で、ログメッセージを書き込む処理が識別されます。

p.719 の「レガシーログについて」を参照してください。

p.714 の「統合ログについて」を参照してください。

VxUL ログでは、`sts` で始まるメッセージは、重複排除プラグインとの通信に関連します。ほとんどの通信は NetBackup メディアサーバーで発生します。VxUL のログファイルを表示および管理するには、NetBackup のログコマンドを使用する必要があります。NetBackup サーバーのログの使用方法および管理方法については、『NetBackup ログ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。

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 17-4 に示すように構成ファイルでログレベルを設定します。

表 17-4 に、各コンポーネントのログファイルを示します。

表 17-4 NetBackup MSDP アクティビティのログ

コンポーネント	VxUL OID	説明
バックアップおよびリストア	117	nbjm(Job Manager)
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)。ログファイルへのパスは次のとおりです。 UNIX の場合: /usr/openv/netbackup/logs/bpbrm Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥bpbrm ■ bpdbm(Database Manager)。ログファイルへのパスは次のとおりです。 UNIX の場合: /usr/openv/netbackup/logs/bpdbm Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥bpdbm ■ bptm (Tape Manager) の I/O 処理。ログファイルへのパスは次のとおりです。 UNIX の場合: /usr/openv/netbackup/logs/bptm Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥bptm
カタログシャドウコピー	該当なし	MSDP カタログのシャドウコピープロセスは、次のログファイルとディレクトリにメッセージを書き込みます。 UNIX の場合: /*storage_path*/log/spad/spad.log /*storage_path*/log/spad/sched_CatalogBackup.log /*storage_path*/log/spad/*client_name*/ Windows の場合: *storage_path*¥log¥spad¥spad.log *storage_path*¥log¥spad¥sched_CatalogBackup.log *storage_path*¥log¥spad¥*client_name*¥

コンポーネント	VxUL OID	説明
クライアント重複排除のプロキシプラグイン	該当なし	メディアサーバー上のクライアント重複排除プロキシプラグインは bptm、bpstsinfo、および bpbrm プロセスで実行されます。プロキシプラグインアクティビティについては、それらのプロセスのログファイルを調べます。ログメッセージに埋め込まれた文字列 proxy または ProxyServer でプロキシサーバーのアクティビティを識別します。 ログファイルは次のディレクトリに書き込まれます。 ■ bptm: UNIX の場合: /usr/openv/netbackup/logs/bptm Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥bptm ■ bpstsinfo: Windows の場合: /usr/openv/netbackup/logs/admin UNIX の場合: /usr/openv/netbackup/logs/bpstsinfo Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥admin Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥stsinfo ■ bpbrm: UNIX の場合: /usr/openv/netbackup/logs/bpbrm Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥bpbrm
クライアント重複排除のプロキシサーバー	該当なし	クライアント上の重複排除プロキシサーバー nbostpxy は、次のようにディレクトリ内のファイルにメッセージを書き込みます。 UNIX の場合: /usr/openv/netbackup/logs/nbostpxy Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥nbostpxy.
重複排除構成スクリプト	該当なし	次は重複排除構成スクリプトのログファイルのパス名です。 ■ UNIX の場合: *storage_path*/log/pdde-config.log ■ Windows の場合: *storage_path*¥log¥pdde-config.log NetBackup は構成処理時にこのログファイルを作成します。構成が正常に実行された場合は、ログファイルを調べる必要はありません。ログファイルを見る唯一の理由は構成が失敗したらです。ストレージディレクトリの作成と入力後に構成処理に失敗した場合は、このログファイルによっていつ構成に失敗したかを識別します。

コンポーネント	VxUL OID	説明
重複排除プラグイン	該当なし	DEBUGLOGファイルのLOGLEVELエントリおよびLOGLEVELファイルで重複排除プラグインのログの場所およびレベルが決まります。ログファイルのデフォルトの場所は次のとおりです。 ■ UNIX の場合: /var/log/puredisk/pdplugin.log ■ Windows の場合: C:¥pdplugin.log ログファイルの場所と名前およびログレベルを構成できます。そのためには、pd.conf ファイルの DEBUGLOG エントリと LOGLEVEL エントリを編集します。 p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。 p.175 の「MSDP pd.conf ファイルの編集」を参照してください。
デバイス構成と監視	111	nbemm の処理
デバイス構成と監視	178	Enterprise Media Manager (EMM) プロセスで実行される Disk Service Manager プロセス。
デバイス構成と監視	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。
デバイス構成と監視	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。
drcontrol ユーティリティ	該当なし	drcontrol ユーティリティは MSDP ストレージサーバーホストで実行する必要があります。コマンドを実行するには管理者権限が必要です。 ユーティリティはログファイルを作成し、コマンド出力のパス名を表示します。ユーティリティはオペレーティングシステムに応じて次のディレクトリにログファイルを書き込みます。 UNIX の場合: /[storage_path]/log/drcontrol/policy_admin /*storage_path*/log/drcontrol/dedupe_catalog_DR Windows の場合: *storage_path*¥log¥drcontrol¥policy_admin *storage_path*¥log¥drcontrol¥dedupe_catalog_DR p.197 の「MSDP カタログの保護について」を参照してください。 p.536 の「MSDP カタログのリカバリについて」を参照してください。

コンポーネント	VxUL OID	説明
インストール	該当なし	NetBackup インストール処理により、次のディレクトリのログファイルに重複排除コンポーネントのインストールについての情報が書き込まれます。 ■ UNIX の場合: /var/log/puredisk ■ Windows の場合: %ALLUSERSPROFILE%¥Symantec¥NetBackup¥InstallLogs
NetBackup 重複排除エンジン	該当なし	NetBackup 重複排除エンジンは次のように複数のログファイルを書き込みます。 ■ *storage_path*/log/spoold ディレクトリ内のログファイルは次のとおりです。 ■ spoold.log ファイルはメインログファイルです ■ storaged.log ファイルはキュー処理に使用されます。 ■ storaged_<dsid>.log ファイルはクラウド LSU のキュー処理に使用されます。 ■ エンジンへの各接続のログファイルはストレージのパスの spoold ディレクトリに保存されます。次に示すのは接続用のログファイルのパス名です。 *hostname/application/TaskName/MMDDYY*.log たとえば、次に示すのは Linux システム上の crcontrol 接続ログパス名の例です。 /*storage_path*/log/spoold/serverexample.com/crcontrol/Control/010112.log 通常、これらの接続ログファイルは Cohesity のサポート担当者に依頼された場合にのみ調べます。 ■ NetBackup がポーリングから受信するイベントとエラーの VxUL ログファイル。重複排除エンジンのオリジネータ ID は 364 です。
NetBackup 重複排除エンジン	364	重複排除ストレージサーバー上で実行される NetBackup 重複排除エンジン。

コンポーネント	VxUL OID	説明
NetBackup 重複排除マネージャ	該当なし	ログファイルは、次のように /*storage_path*/log/spad ディレクトリにあります。 ■ spad.log ■ sched_QueueProcess.log ■ SchedClass.log ■ Manager への各接続のログファイルはストレージのパスの spad ディレクトリに保存されます。次に示すのは接続用のログファイルのパス名です。 *hostname/application/TaskName/MMDDYY*.log たとえば、次に示すのは Linux システム上の bpstsinfo 接続ログパス名の例です。 /*storage_path*/log/spoold/serverexample.com/bpstsinfo/spad/010112.log 通常、これらの接続ログファイルは Cohesity のサポート担当者に依頼された場合にのみ調べます。 [ストレージサーバーの変更 (Change Storage Server)]ダイアログボックスの[プロパティ (Properties)]タブで、ログレベルと保持期間を設定できます。 p.497 の「MSDP ストレージサーバーのプロパティの変更」を参照してください。
最適化複製とレプリケーション	該当なし	最適化複製および自動イメージレプリケーションの場合、次のログファイルが情報を提供します。 ■ NetBackup bptm Tape Manager の I/O 処理。ログファイルへのパスは次のとおりです。 UNIX の場合: /usr/openv/netbackup/logs/bptm Windows の場合: *install_path*¥Veritas¥NetBackup¥logs¥bptm ■ MSDP レプリケーションログファイルのパス名は次のとおりです。 /storage_path/*log/spad/replication.log*
耐障害性が高いネットワーク接続	387	Remote Network Transport Service (nbrntd) は耐障害性が高いネットワーク接続ソケットを管理します。これは、プライマリサーバー上、メディアサーバー上、クライアント上で動作します。VxUL オリジネータ ID 387 を使用して、NetBackup が使用するソケット接続についての情報を表示します。 **メモ:** 複数のバックアップストリームを同時に動作する場合、Remote Network Transport Service は多量の情報をログファイルに書き込みます。このようなシナリオの場合、Cohesityでは、OID 387 のログレベルを 2 以下に設定することをお勧めします。統合ログを構成するには、『NetBackup ログリファレンスガイド』を参照してください。

コンポーネント	VxUL OID	説明
耐障害性が高いネットワーク接続	該当なし	重複排除プラグインは、接続の維持に関する情報をログに記録します。 重複排除プラグインのログファイルについての詳細は、この表の「重複排除プラグイン」を参照してください。 pd.confファイルFILE_KEEP_ALIVE_INTERVALパラメータは接続存続間隔を制御します。 p.175 の「MSDP pd.conf 構成ファイルについて」を参照してください。 p.175 の「MSDP pd.conf ファイルの編集」を参照してください。
CRC 通知	該当なし	CRC 健全性チェックのデバッグログは次の場所に保存されます。 /<storage_path>/log/spad/sched_CRCHealthCheck.log

MSDP 構成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.720 の「NetBackup MSDP ログファイル」を参照してください。

p.726 の「MSDP ストレージサーバーの構成の失敗」を参照してください。

p.727 の「MSDP データベースのシステムエラー (220)」を参照してください。

p.727 の「MSDP の[サーバーが見つかりませんでした (Server not found)]エラー」を参照してください。

p.728 の「MSDP 構成中のライセンス情報エラー」を参照してください。

p.729 の「ディスクプールウィザードで MSDP ボリュームが表示されない」を参照してください。

MSDP ストレージサーバーの構成の失敗

ストレージサーバーの構成に失敗した場合は、[ストレージサーバーの構成ウィザード (Storage Server Configuration Wizard)] によって報告された問題を最初に解決します。次に、ストレージサーバーの構成を再試行する前に、重複排除ホストの構成ファイルを削除します。

NetBackup はストレージサーバーがすでに存在しているホストにストレージサーバーを構成できません。構成済みストレージサーバーを示す目安の 1 つが重複排除ホストの構成ファイルです。したがって、失敗後にストレージサーバーの構成を試みる前にそれを削除する必要があります。

p.196 の「MSDP ホストの構成ファイルの削除」を参照してください。

MSDP データベースのシステムエラー (220)

データベースのシステムエラーはエラーがストレージ初期設定で起きたことを示します。

エラーメッセージ　`ioctl() error, Database system error (220)`

例　`RDSM has encountered an STS error:`

```
Failed to update storage server ssname, database
system error
```

診断　`PDDE_initConfig` スクリプトは呼び出されましたが、エラーがストレージ初期設定の間に起きました。

最初に、関連のあるサーバー名の重複排除構成スクリプトログファイルを検査します。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

次に、サーバー名のクレデンシャルの作成について `tpconfig` コマンドのログファイルのエラーを検査します。`tpconfig` コマンドは標準の NetBackup 管理者コマンドログディレクトリに書き込みます。

MSDP の[サーバーが見つかりませんでした (Server not found)]エラー

次の情報は構成の間に発生することがある[サーバーが見つかりませんでした (Server not found)]エラーメッセージを解決するのに役立つことがあります。

エラーメッセージ　`Server not found, invalid command parameter`

例

```
RDSM has encountered an issue with STS where
  the server was not found:  getStorageServerInfo

   Failed to create storage server ssname, invalid
   command parameter
```

診断　　考えられる根本的原因:

- ストレージサーバーを構成したときに、サポート外のオペレーティングシステムを実行するメディアサーバーを選択しました。環境のすべてのメディアサーバーは[ストレージサーバーの構成ウィザード (Storage Server Configuration Wizard)]に表示されます。サポート対象のオペレーティングシステムを実行するメディアサーバーのみ選択することを忘れないでいてください。
- ストレージサーバーを設定するために nbdevconfig コマンドを使った場合、ホスト名を不正確に入力していることがあります。また、ストレージサーバー形式では大文字と小文字が区別されます。したがってストレージサーバー形式に PureDisk を使うようにしてください。

MSDP 構成中のライセンス情報エラー

ライセンス情報エラーについての構成エラーメッセージは、NetBackup サーバーが互いに通信できないことを示します。

重複排除ストレージサーバーまたは負荷分散サーバーを構成できない場合は、ネットワーク環境が DNS の名前の逆引き参照用に構成されていない可能性があります。

重複排除に使うメディアサーバー上の hosts ファイルを編集できます。または、名前の逆引き参照を使用しないように NetBackup を構成できます。

NetBackup Web UI を使用してホスト名の逆引き参照を禁止する方法

1. NetBackup Web UI を開きます。
2. 左側で、[ホスト (Host)]、[ホストプロパティ (Host Properties)]の順に選択します。
3. 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。
4. [ネットワーク設定 (Network settings)]をクリックします。
5. 次のいずれかのオプションを選択します。
   - 許可 (Allowed)
   - 制限あり (Restricted)
   - 禁止 (Prohibited)

   これらのオプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

bpsetconfig コマンドを使用してホスト名の逆引き参照を禁止する方法

- 重複排除に使う各メディアサーバーで次のコマンドを入力します。

  echo REVERSE_NAME_LOOKUP = PROHIBITED | bpsetconfig -h *host_name*

  bpsetconfig コマンドは、次のディレクトリに存在します。

  UNIX の場合: /usr/openv/netbackup/bin/admincmd

  Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥admincmd

ディスクプールウィザードで MSDP ボリュームが表示されない

［ディスクプールの構成ウィザード (Disk Pool Configuration Wizard)］には、重複排除ストレージサーバーのディスクボリュームは表示されません。

最初に、NetBackup のデーモンまたはサービスをすべて再起動します。この手順により、NetBackup Deduplication Engine が起動し、要求に応答できるようになります。

次に、NetBackup Web UI を更新します。この手順により、ディスクボリュームの表示に失敗したときにキャッシュされた情報が消去されます。

MSDP 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.730 の「MSDP サーバーに十分なメモリがあることを確認する」を参照してください。

p.730 の「MSDP バックアップまたは複製ジョブの失敗」を参照してください。

p.732 の「MSDP クライアントの重複排除が失敗する」を参照してください。

p.732 の「ボリュームのマウントが解除されると MSDP ボリュームが停止状態になる」を参照してください。

p.733 の「MSDP のエラー、遅延応答、ハングアップ」を参照してください。

p.734 の「MSDP ディスクプールを削除できない」を参照してください。

p.735 の「MSDP メディアのオープンエラー (83)」を参照してください。

p.737 の「MSDP メディアの書き込みエラー (84)」を参照してください。

p.738 の「MSDP 正常に処理されたイメージはありませんでした (191)」を参照してください。

p.739 の「MSDP ストレージの空きのない状態」を参照してください。

p.739 の「MSDP カタログバックアップのトラブルシューティング」を参照してください。

MSDP サーバーに十分なメモリがあることを確認する

ストレージサーバーのメモリが不十分な場合、操作上の問題が発生する可能性があります。操作上の問題が発生した場合は、ストレージサーバーに十分なメモリがあることを確認する必要があります。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

NetBackup 重複排除処理が Red Hat Linux で開始されない場合は、少なくとも 128 MB (`SHMMAX=128MB`) の共有メモリを構成してください。

MSDP バックアップまたは複製ジョブの失敗

次のサブセクションでは、バックアップまたは重複排除ジョブの可能性のある失敗とそれらを解決する方法を説明します。

- 「ディスクボリュームが停止しています (Disk Volume is Down)」
- 「ストレージサーバーはダウンしているか、利用できません。」
- 「バックアップジョブ: システムエラーが発生しました (174) (Backup job: System error occurred) (174)」
- 「ストレージパスを開く、または CRQP トランザクションを準備できませんでした」

ディスクボリュームが停止しています (Disk Volume is Down)

次のようなメッセージがジョブの詳細に表示されます。

```
Error 800: Disk Volume is Down
```

ディスクのエラーログを調べて、ボリュームが停止 (DOWN) としてマークされた理由を判断します。

ストレージサーバーは、ジョブでビジー状態の場合、プライマリサーバーのディスクポーリング要求に適時に応答しないことがあります。ビジー状態の負荷分散サーバーでもこのエラーが発生することがあります。その結果、問い合わせがタイムアウトし、プライマリサーバーはボリュームを DOWN とマーク付けします。

最適化複製ジョブのエラーが発生した場合は、ソースストレージサーバーがターゲットストレージサーバーの負荷分散サーバーとして構成されていることを確認します。また、ターゲットストレージサーバーがソースストレージサーバーの負荷分散サーバーとして構成されていることを確認します。

p.741 の「MSDP ディスクのエラーとイベントの表示」を参照してください。

ストレージサーバーはダウンしているか、利用できません。

Windows サーバーのみ。

次のようなメッセージがジョブの詳細に表示されます。

```
Error nbjm(pid=6384) NBU status: 2106, EMM status: Storage Server is
down or unavailable Disk storage server is down(2106)
```

NetBackup Deduplication Manager (spad.exe) と NetBackup Deduplication Engine (spoold.exe) の共有メモリ構成値が異なっています。この問題は、これらの 2 つのコンポーネントの一方の共有メモリ値だけを変更するコマンドを使った場合に発生することがあります。

問題を解決するためには、構成ファイルに次の共有メモリ値を指定します。

```
SharedMemoryEnabled=1
```

次に、両方のコンポーネントを再起動します。他の 2 つの共有メモリパラメータの値を変更しないでください。

SharedMemoryEnabled パラメータは次のファイルに格納されています。

storage_path¥etc¥puredisk¥agent.cfg

バックアップジョブ: システムエラーが発生しました (174) (Backup job: System error occurred) (174)

次のようなメッセージがジョブの詳細に表示されます。

```
media manager - system error occurred (174)
```

ジョブの詳細に、次のようなエラーも含まれている場合、イメージのクリーンアップジョブが失敗したことを示しています。

```
Critical bpdm (pid=610364) sts_delete_image
 failed: error 2060018 file not found
Critical bpdm (pid=610364) image delete
 failed: error 2060018: file not found
```

このエラーは、重複排除バックアップジョブが、バックアップの一部をメディアサーバー重複排除プールに書き込んだ後に失敗した場合に発生します。NetBackup はイメージクリーンアップジョブを開始しますが、イメージのクリーンアップの実行に必要なデータがメディアサーバー重複排除プールに書き込まれていないため、そのジョブが失敗します。

重複排除キュー処理はイメージオブジェクトをクリーンアップするため、修正措置を適用する必要はありません。ただし、ジョブログと重複排除ログを調べて、バックアップジョブが失敗した理由を判断してください。

p.517 の「MSDP キュー処理について」を参照してください。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

ストレージパスを開く、または CRQP トランザクションを準備できませんでした

次に似たエラーメッセージは、NetBackup Deduplication Engine (spoold) ログファイルの 1 つに記録されます。

```
RefDBEngine::write_prepare fail to open
/storage_path/databases/refdb/prepare/64.ref.prepare
```

```
RefDBManager::write_prepare fail to prepare CRQP transaction for
refdb 64
```

p.720 の「NetBackup MSDP ログファイル」を参照してください。

このエラーは、*/storage_path*/databases/refdb/prepare ディレクトリが削除されている場合に起きます。

この問題を解決するには、次のいずれかの操作を実行します。

- 見つからないディレクトリを手動で作成します。
- NetBackup Deduplication Engine (spoold) を再起動します。最初に、メディアサーバーのストレージユニットでバックアップが実行中でないこと確認してください。

メモ: RefDBEngine および refdb はオープンソースの RefDB 参照データベースおよび文献目録ツールを参照せず、またこれらに関連していません。

MSDP クライアントの重複排除が失敗する

NetBackup のクライアント側のエージェント (クライアントの重複排除を含む) は NetBackup サーバー名のホスト名の逆引き参照によって決まります。逆に、通常のバックアップは前方ホスト名解決によって決まります。したがって、クライアントの通常のバックアップは成功することがありますが、自身のデータを複製するクライアントのバックアップは失敗することがあります。

クライアント側の重複排除バックアップが失敗したら、ドメインネームサーバーがストレージサーバー名のすべての置換を含んでいること検証します。

また、Cohesity は NetBackup 環境に完全修飾ドメイン名を使用することをお勧めします。

p.49 の「完全修飾ドメイン名を使用する」を参照してください。

ボリュームのマウントが解除されると MSDP ボリュームが停止状態になる

ボリュームのマウントが解除されると、NetBackup によってボリュームが停止状態に変更されます。そのボリュームを必要とする NetBackup ジョブは失敗します。

ボリュームの状態を判断する方法

- プライマリサーバー上、または重複排除ストレージサーバーとして機能するメディアサーバー上で、次のコマンドを起動します。

  UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype PureDisk -U`

  Windows の場合: *install_path*`¥NetBackup¥bin¥admincmd¥nbdevquery -listdv -stype PureDisk -U`

  次の出力例は、`DiskPoolVolume` が起動状態であることを示しています。

```
Disk Pool Name      : PD_Disk_Pool
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
Disk Media ID       : @aaaab
Total Capacity (GB) : 49.98
Free Space (GB)     : 43.66
Use%                : 12
Status              : UP
Flag                : ReadOnWrite
Flag                : AdminUp
Flag                : InternalUp
Num Read Mounts     : 0
Num Write Mounts    : 1
Cur Read Streams    : 0
Cur Write Streams   : 0
Num Repl Sources    : 0
Num Repl Targets    : 0
WORM Lock Min Time  : 0
WORM Lock Max Time  : 0
```

ボリュームを起動状態に変更する方法

1. ファイルシステムをマウントします。

   しばらくすると、ボリュームは起動状態 (UP) になります。これ以外の操作は必要ありません。

2. ボリュームの状態が変わらない場合は、手動で変更します。

   p.514 の「MSDP ディスクボリュームの状態の変更」を参照してください。

MSDP のエラー、遅延応答、ハングアップ

メモリまたはホストの機能が不十分な場合、複数のエラー、遅延応答およびハングアップが発生することがあります。

p.34 の「MSDP サーバーの必要条件について」を参照してください。

仮想マシンでは、Cohesity は次のように設定することをお勧めします。

- ホストの物理メモリの 2 倍になるように各仮想マシンのメモリサイズを設定します。
- 各仮想マシンの最小値と最大値を同じ値 (ホストの物理メモリの 2 倍) に設定します。これらのメモリ設定により、仮想メモリは縮小または拡大しないため、ディスクでフラグメント化されません。

これらの推奨事項は、すべての仮想マシンに最適な構成であるとはかぎりません。ただし、パフォーマンス上の問題をトラブルシューティングするときは、Cohesity はこの解決策を最初に試みることをお勧めします。

MSDP ディスクプールを削除できない

有効なバックアップイメージを含んでいないと判断されるディスクプールを削除できない場合、次の情報は問題のトラブルシューティングを行うのに役立つことがあります。

- 「期限切れのフラグメントが MSDP ディスクに残る」
- 「不完全な SLP 複製ジョブ」

期限切れのフラグメントが MSDP ディスクに残る

ある状況下では、期限切れのバックアップイメージを構成するフラグメントはイメージが期限切れになったのにディスクに残ることがあります。たとえば、ストレージサーバーがクラッシュすると、通常のクリーンアップ処理は動作しないことがあります。それらの状況では、イメージフラグメントレコードがまだ存在するのでディスクプールを削除できません。エラーメッセージは次に類似することがあります。

```
DSM has found that one or more volumes in the disk pool diskpoolname
has image fragments.
```

ディスクプールを削除するには、最初にイメージフラグメントを削除してください。nbdelete コマンドは期限切れになったイメージフラグメントをディスクボリュームから削除します。

期限切れイメージのフラグメントを削除する方法

◆ 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/netbackup/bin/admincmd/nbdelete -allvolumes -force`

Windows の場合: `install_path¥NetBackup¥bin¥admincmd¥nbdelete -allvolumes -force`

`-allvolumes` オプションは期限切れになったイメージフラグメントを含んでいるすべてのボリュームからそれらを削除します。

-force オプションはフラグメントの削除が失敗してもイメージフラグメントのデータベースエントリを削除します。

不完全な SLP 複製ジョブ

ストレージライフサイクルポリシーの不完全な複製ジョブはディスクプールの削除を妨げることがあります。不完全なジョブが存在するかどうかを判断し、次にそれらを取り消します。

ストレージライフサイクルポリシーの複製ジョブを取り消す方法

1. プライマリサーバーで次のコマンドを実行することによって、不完全な SLP 複製ジョブが存在するかを判断します。

   UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbstlutil stlilist -image_incomplete`

   Windows の場合: *install_path*¥NetBackup¥bin¥admincmd¥nbstlutil stlilist -image_incomplete

2. 前のコマンドによって戻される各々のバックアップ ID に対して次のコマンド (*xxxxx* はバックアップ ID を表します) を実行することによって不完全なジョブを取り消します。

   UNIX の場合: `/usr/openv/netbackup/bin/admincmd/nbstlutil cancel -backupid xxxxx`

   Windows の場合: *install_path*¥NetBackup¥bin¥admincmd¥nbstlutil cancel -backupid *xxxxx*

MSDP メディアのオープンエラー (83)

media open error (83) メッセージは複製の一般エラーです。エラーは[アクティビティモニター (Activity Monitor)]に表示されます。

多くの場合、NetBackup 重複排除エンジン (spoold) または NetBackup 重複排除マネージャ (spad) は、余りにもビジーで重複排除の処理を適時に応答できません。外的要因によって重複排除エンジンまたは重複排除マネージャが応答できない場合も考えられます。それらは一時的にビジー状態 (キューの処理が進行中であったなど) でしたか? 余りにも多くのジョブが同時に動作しますか?

必ずしもそうではありませんが、通常は NetBackup の bpdm ログは状態 83 についての追加情報を提供します。

それに続くサブセクションには、エラー 83 を生成したユースケースが記述されます。

SQL Server クライアント側のバックアップの失敗

SQL Server データベースのクライアント側のバックアップは次の状況で失敗することがあります。

- [IPv4 と IPv6 の両方 (Both IPv4 and IPv6)]オプションが NetBackup 重複排除エンジンおよびクライアントをホストするメディアサーバーであるプライマリサーバー用に有効になっている。[IPv4 と IPv6 の両方 (Both IPv4 and IPv6)]オプションは[ネットワーク設定 (Network settings)]ホストプロパティで設定されます。
- NetBackup 重複排除エンジンおよびクライアントをホストするメディアサーバーであるプライマリサーバー用の優先のネットワークとして、IPv6 ネットワークが設定されている。優先ネットワークの[一致 (通信には上記のネットワークが優先されます) (Match (Above network will be preferred for communication))]プロパティも有効になっている。優先ネットワークは[優先ネットワーク (Preferred networks)]ホストプロパティで構成されます。
- IPv6 ネットワークがバックアップのために選択されている。

bpbrmログファイルを検査して、次に示すエラーと類似するものを探してください。

```
probe_ost_plugin: sts_get_server_prop_byname failed: error 2060057
```

エラーメッセージが存在する場合、NetBackup ホスト名のキャッシュには正しいホスト名のマッピング情報が含まれないかもしれません。ネットワーク環境の DNS の変更が環境全体に完全に反映されなかった場合、キャッシュの同期は行われない可能性があります。DNS の変更がネットワーク環境全体に反映されるのは時間がかかります。

問題を解決するには、MSDP ストレージサーバー上の NetBackup プライマリサーバーで次の操作を行います。

1. NetBackup サービスを停止します。
2. 次のコマンドを実行します。

   UNIX の場合: `/usr/openv/netbackup/bin/bpclntcmd -clearhostcache`

   Windows の場合: *install_path*¥NetBackup¥bin¥bpclntcmd.exe -clearhostcache
3. NetBackup サービスを起動します。

クライアント重複排除のログ記録について詳しくは、「MSDP ログファイル」トピックにある「クライアント重複排除プロキシプラグイン」を参照してください。

p.720 の「NetBackup MSDP ログファイル」を参照してください。

リストアまたは複製の失敗

media open error (83) のメッセージは[アクティビティモニター (Activity Monitor)]に表示されます。

「表 17-5」には、表示される可能性のあるその他のメッセージが記載されています。

表 17-5　大文字と小文字の区別をするエラーメッセージ

操作	アクティビティモニターに表示されるジョブの詳細	bpdm および bptm のログファイルの状態
リストア	`Image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`
複製 (MSDP ソース)	`Image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`
レプリケーション (MSDP ソース)	`get image properties failed: error 2060013: no more entries`	`rpl_add_image_set: rpl_get_image_info() failed, error 2060013`

このメッセージは MSDP 環境のクライアント名の大文字と小文字の区別による問題を示す場合があります。

MSDP メディアの書き込みエラー (84)

表 17-6は、[メディアサーバー重複排除プール (Media Server Deduplication Pool)]のバックアップ、複製、レプリケーションの間に生じるかもしれないメディア書き込みエラーに対する解決方法について説明します。

また、より複雑な解決方法の説明は、次のサブセクションを参照してください。

- 「ホスト名解決の問題」

表 17-6　メディア書き込みエラーの原因

NetBackup 重複排除エンジン (spoold) はビジー状態のため応答できませんでした。	PureDisk という名前を含むエラーについては[ディスクのログ (Disk Logs)]レポートを確認してください。詳しくは、重複排除プラグインのディスクの監視サービスのログファイルを検査します。
データ削除が動作しています。	データの削除とバックアップは同時にはできません。 p.517 の「MSDP キュー処理について」を参照してください。
ユーザーはストレージを改変しました。	ユーザーはストレージにファイルを追加、ストレージのファイルを変更、ストレージのファイルを削除、またはストレージのファイルアクセス許可を変更してはなりません。ファイルが追加された場合は、それを削除します。

ストレージ容量が増やされました。	ストレージを増やしたら、新しい容量が認識されるようにストレージサーバーで NetBackup サービスを再起動してください。
ストレージに空きがありません。	可能な場合は、ストレージ容量を増やします。 p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。
重複排除プールが停止しています。	状態を起動に変更します。
ファイアウォールのポートが開いていません。	ポート 10082 と 10102 が重複排除ホスト間の任意のファイアウォールで開いていることを確認します。

ホスト名解決の問題

クライアント側の重複排除はクライアントがサーバーのホスト名を解決できなければ失敗する場合があります。具体的には、ストレージサーバーが短い名前で構成されている場合にクライアントが完全修飾ドメイン名を解決することを試みると、エラーが発生することがあります。

クライアントがストレージサーバーに使用する名前を判断するには、クライアントの重複排除ホストの構成ファイルを検査します。

p.195 の「MSDP ホストの構成ファイルについて」を参照してください。

この問題を修正するには、ストレージサーバー名のすべての置換が解決するようにネットワーク環境を構成します。

Cohesity は完全修飾ドメイン名を使うことを推奨します。

p.49 の「完全修飾ドメイン名を使用する」を参照してください。

MSDP 正常に処理されたイメージはありませんでした (191)

`no images successfully processed (191)` のメッセージは[アクティビティモニター (Activity Monitor)]に表示されます。

「表 17-7」には、表示される可能性のあるその他のメッセージが記載されています。

表 17-7　大文字と小文字の区別をするエラーメッセージ

操作	アクティビティモニターに表示されるジョブの詳細	bpdm および bptm のログファイルの状態
検証	`image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`

メッセージは MSDP 環境のクライアント名の大文字と小文字の区別による問題を示す場合があります。

MSDP ストレージの空きのない状態

UNIX の df コマンドのようなオペレーティングシステムのツールは重複排除ディスクの使用状況を正確に報告しません。オペレーティングシステムのコマンドはストレージに空きがある場合に空きがないと報告することがあります。NetBackup ツールを使用すると、ストレージの容量と使用状況をより正確に監視できます。

p.485 の「MSDP ストレージの容量と使用状況のレポートについて」を参照してください。

p.487 の「MSDP コンテナファイルについて」を参照してください。

p.488 の「MSDP コンテナファイル内のストレージ使用状況の表示」を参照してください。

[ディスクのログ (Disk Logs)]レポートでしきい値の警告の有無を検査することで、ストレージに空きがない状態がいつ起きる可能性があるかを知ることができます。

NetBackup がどのようにメンテナンスを実行するかは、ストレージがいつ解放されて使えるようになるかに影響します。

p.517 の「MSDP キュー処理について」を参照してください。

p.527 の「MSDP のデータ削除処理について」を参照してください。

推奨はされていませんが、空き領域を手動で再利用できます。

p.517 の「MSDP トランザクションキューの手動処理」を参照してください。

MSDP カタログバックアップのトラブルシューティング

次のサブセクションでは MSDP カタログのバックアップとリカバリについての情報を提供します。

カタログバックアップ

表 17-8 はカタログバックアップポリシーを作成または更新するときに起きることがあるエラーメッセージを記述します。メッセージは drcontrol ユーティリティを実行したシェルウィンドウに表示されます。また、ユーティリティはメッセージをログファイルに書き込みます。

表 17-8 MSDP drcontrol のコードとメッセージ

コードまたはメッセージ	説明
1	drcontrol ユーティリティによって呼び出される、オペレーティングシステムまたは重複排除コマンドの致命的なエラー。

コードまたはメッセージ	説明
110	コマンドは必要な NetBackup の構成情報を見つけることができません。
140	コマンドを呼び出したユーザーに管理者権限がありません。
144	コマンドオプションまたは引数が必要です。
226	指定したポリシー名はすでに存在しています。
227	このエラーコードは NetBackup `bplist` コマンドから渡されます。指定した MSDP カタログバックアップポリシーが存在しないか、指定したポリシー名に対するバックアップが存在しません。
255	`drcontrol` ユーティリティの致命的なエラー。

状態コードとエラーメッセージについて詳しくは、次を参照してください。

- NetBackup 管理コンソールのトラブルシュータ。
- NetBackup 状態コードリファレンスガイド

シャドーコピーからのカタログリカバリ

NetBackup で MSDP カタログに破損が検出されると、重複排除マネージャはカタログを最新のシャドーコピーから自動的にリカバリします。このリカバリ処理では、リカバリした MSDP カタログが最新になるようにトランザクションログも使います。

シャドーコピーのリカバリ処理は自動的に実行されますが、シャドーコピーから手動でリカバリする必要がある場合はリカバリ手順を利用できます。

p.537 の「シャドーコピーからの MSDP カタログのリストア」を参照してください。

ストレージプラットフォーム Web サービス (spws) が起動しない

`bp.start_all` を実行したときに、ストレージプラットフォーム Web サービス (`spws`) が起動しません。

回避方法:

`bp.start_all` の実行時に `spws` が起動しない場合は、次のコマンドを実行して `vpfs` と `spws` を再構成します。

```
vpfs_config.sh --configure_byo
```

ディスクボリューム API またはコマンドラインオプションが機能しない

8.3 より前のバージョンの NetBackup が MSDP ストレージサーバーにインストールされていて、暗号化と KMS の詳細が有効になっていません。新しいディスクボリューム更新

API を使用してローカルボリュームの暗号化と KMS の詳細を更新しようとすると、API 操作は正常に実行されます。ただし、実際の値は更新されません。

この問題は、API とコマンドラインの両方のオプションで発生します。

MSDP ディスクのエラーとイベントの表示

次に示すように、複数の方法でディスクのエラーとイベントを表示できます。

- ［ディスクのログ (Disk Logs)］レポート
- -disk オプションを指定して NetBackup の bperror コマンドを実行すると、ディスクのエラーが報告されます。このコマンドは、次のディレクトリに存在します。
  UNIX の場合: /usr/openv/netbackup/bin/admincmd
  Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥admincmd

MSDP イベントのコードとメッセージ

次の表は重複排除イベントコードとメッセージを示したものです。イベントコードは bperror コマンドの -disk 出力と NetBackup 管理コンソールのディスクのレポートに表示されます。

表 17-9 MSDP イベントのコードとメッセージ

イベント番号	イベントの重大度	NetBackup の重大度	メッセージの例
1000	2	エラー	Operation configload/reload failed on server PureDisk:server1.example.com on host server1.example.com.
1001	2	エラー	Operation configload/reload failed on server PureDisk:server1.example.com on host server1.example.com.
1002	4	警告 (Warning)	The open file limit exceeded in server PureDisk:server1.example.com on host server1.example.com. Will attempt to continue further.
1003	2	エラー	A connection request was denied on the server PureDisk:server1.example.com on host server1.example.com.
1004	1	重要 (Critical)	Network failure occurred in server PureDisk:server1.example.com on host server1.example.com.
1008	2	エラー	Task Aborted; An unexpected error occurred during communication with remote system in server PureDisk:server1.example.com on host server1.example.com.

イベント番号	イベントの重大度	NetBackup の重大度	メッセージの例
1009	8	認可	Authorization request from <IP> for user <USER> denied (<REASON>).
1010	2	エラー	Task initialization on server PureDisk:server1.example.com on host server1.example.com got an unexpected error.
1011	16	情報 (Info)	Task ended on server PureDisk:server1.example.com on host server1.example.com.
1013	1	重要 (Critical)	Task session start request on server PureDisk:server1.example.com on host server1.example.com got an unexpected error.
1012	2	エラー	A request for agent task was denied on server PureDisk:server1.example.com on host server1.example.com.
1014	1	重要 (Critical)	Task session start request on server PureDisk:server1.example.com on host server1.example.com got an unexpected error.
1015	1	重要 (Critical)	Task creation failed, could not initialize task class on server PureDisk:server1.example.com on host server1.example.com.
1017	1	重要 (Critical)	Service Cohesity DeduplicationEngine exit on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error. The application has terminated.
1018	16	情報 (Info)	Startup of Cohesity Deduplication Engine completed successfully on server1.example.com.
1019	1	重要 (Critical)	Service Cohesity DeduplicationEngine restart on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error. The application has restarted.
1020	1	重要 (Critical)	Service Cohesity Deduplication Engine connection manager restart failed on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error.The application has failed to restart.

イベント番号	イベントの重大度	NetBackup の重大度	メッセージの例
1028	1	重要 (Critical)	Service Cohesity DeduplicationEngine abort on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error.The application has caught an unexpected signal.
1029	1	重要 (Critical)	Double backend initialization failure; Could not initialize storage backend or cache failure detected on host PureDisk:server1.example.com in server server1.example.com.
1030	1	重要 (Critical)	Operation Storage Database Initialization failed on server PureDisk:server1.example.com on host server1.example.com.
1031	1	重要 (Critical)	Operation Content router context initialization failed on server PureDisk:server1.example.com on host server1.example.com.
1032	1	重要 (Critical)	Operation log path creation/print failed on server PureDisk:server1.example.com on host server1.example.com.
1036	4	警告 (Warning)	Operation a transaction failed on server PureDisk:server1.example.com on host server1.example.com.
1037	4	警告 (Warning)	Transaction failed on server PureDisk:server1.example.com on host server1.example.com. Transaction will be retried.
1040	2	エラー	Operation Database recovery failed on server PureDisk:server1.example.com on host server1.example.com.
1043	2	エラー	Operation Storage recovery failed on server PureDisk:server1.example.com on host server1.example.com.
1044	複数	複数	The usage of one or more system resources has exceeded a warning level. Operations will or could be suspended. Please take action immediately to remedy this situation.
1057			A data corruption has been detected.データー貫性検査がメディアサーバー重複排除プール (MSDP) でデータ損失またはデータの破損を検出して影響のあるバックアップを報告しました。 バックアップ ID とポリシー名は NetBackup ディスクのログレポートとストレージサーバーの *storage_path*/log/spoold/storaged.log ファイルに表示されます。
2000		エラー (Error)	Low space threshold exceeded on the partition containing the storage database on server PureDisk:server1.example.com on host server1.example.com.

p.485 の「MSDP ストレージの容量と使用状況のレポートについて」を参照してください。

p.729 の「MSDP 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。

Windows OS が搭載された AWS EC2 インスタンスを使用するための管理者パスワードを取得できない

このエラーは、自動ディザスタリカバリを使用して変換した AMI からインスタンスを起動した後に発生します。

次のエラーが表示されます。

```
Password is not available. This instance was launched from a custom AMI, or the default password has changed. A password cannot be retrieved for this instance. If you have forgotten your password, you can reset it using the Amazon EC2 configuration service. For more information, see Passwords for a Windows Server Instance.
```

詳しくは、次の記事を参照してください。

- Amazon Elastic Compute Cloud の一般的なメッセージ
- ADMT を使用して AWS の管理対象 Microsoft AD にオンプレミスドメインを移行する方法

複数ドメインの問題のトラブルシューティング

以降のセクションでは、NetBackup の複数ドメインのシナリオに関する問題のトラブルシューティングに役立つ情報を示します。

p.744 の「別のドメインから OpenStorage サーバーを構成できない」を参照してください。

p.745 の「OpenStorage サーバーを構成すると MSDP ストレージサーバーが停止する」を参照してください。

別のドメインから OpenStorage サーバーを構成できない

別のドメインから OpenStorage サーバーを構成しようとしたときにエラー「サーバー xxx のログインクレデンシャルの検証に失敗しました (`Login credentials verification failed for server xxxxxx`)」が表示された場合は、次の手順を実行して根本原因を特定します。

- ユーザー名とパスワードが正しいかどうかを確認します。

- OpenStorage サーバーの構成に使用されるメディアサーバーに、NetBackup 証明書が配備されているかどうかを確認します。証明書が正しく配備されていない場合、pdplugin ログで次のエラーログが見つかります。

```
[ERROR] PDSTS: pd_register: PdvfsRegisterOST(egsuse1) failed
(30000:Unknown error 30000
[ERROR] PDSTS: get_agent_cfg_file_path_for_mount: pd_register()
failed for configuration file:</openv/lib/ost-plugins/egsuse1.cfg>
(2060401:UNKNOWN STS ERROR CODE)
```

  複数ドメインに NetBackup 証明書を配備するための nbcertcmd コマンドの使用について詳しくは、「p.211 の「MSDP のマルチドメインのサポートについて」を参照してください。」を参照してください。

OpenStorage サーバーを構成すると MSDP ストレージサーバーが停止する

別のドメインから OpenStorage サーバーを構成した後、MSDP ストレージサーバーが停止しているか応答しない場合は、次の手順を実行して根本原因を特定します。

- 2 つ以上の NetBackup ドメインで同じ MSDP ユーザーが使用されていないかどうかを確認します。
- spad.log に次のようなログエントリがあるかどうかを確認します。

```
ERR [44] [140589294249728]: 25000: spaProcessing(), It's found
that same
msdp user "user1" is used by multiple NBU domains. This is wrong
MultiDomain configuration which will cause potential data loss
issue.
Now other NBU domains cannot use msdp user "user1" to access MSDP

services in this server.
```

  エラーログがある場合、問題は、複数ドメインでサポートされていない 1 台の MSDP ストレージサーバーに、異なる NetBackup ドメインが同じ MSDP ユーザーを使用してアクセスしていることです。

- バックアップジョブまたはリストアジョブが失敗すると、ジョブの詳細に次のエラーメッセージが表示されます。

```
Critical bptm (pid=140303) sts_open_server failed: error 2060405
Wrong MSDP multi-domain configuration is detected. This NBU domain

should use a different MSDP user to access the MSDP storage server.
```

```
See NetBackup Deduplication Guide for details.
```

この問題を解決するには

1. MSDP ストレージサーバーに新しい MSDP ユーザーを作成します。

   p.211 の「MSDP のマルチドメインのサポートについて」を参照してください。

   MSDP ストレージサーバーが NetBackup WORM ストレージサーバーまたは NetBackup Flex Scale ストレージサーバーの場合は、次の NetBackup 重複排除シェルコマンドを実行して MSDP ユーザーを作成します。

   ```
   setting MSDP-user add-MSDP-user username=<user_name> role=admin
   ```

2. 2 つの NetBackup ドメインが同じ MSDP ユーザーを使用して MSDP サーバーにアクセスする場合は、2 番目の NetBackup ドメインで MSDP ストレージサーバーのクレデンシャルを更新します。2 番目の NetBackup ドメインは、新しい MSDP ユーザーを使用して MSDP ストレージサーバーにアクセスする必要があります。2 番目の NetBackup ドメインにある MSDP ストレージサーバーのすべての負荷分散サーバーで、次のコマンドを実行します。

   ```
   tpconfig -update -stype PureDisk -storage_server
   <msdp_storage_server> -sts_user_id <user_name> -password
   <password>
   ```

3. 次のコマンドを実行して、MSDP ストレージサーバーで spad サービスを再起動します。

   ```
   /usr/openv/pdde/pdconfigure/pdde spad stop
   ```

   ```
   /usr/openv/pdde/pdconfigure/pdde spad start
   ```

   MSDP ストレージサーバーが NetBackup WORM ストレージサーバーまたは NetBackup Flex Scale ストレージサーバーの場合は、次の NetBackup 重複排除シェルコマンドを実行して MSDP サービスを再起動します。

   ```
   dedupe MSDP stop
   ```

   ```
   dedupe MSDP start
   ```

MSDP サーバーが複数の NetBackup ドメインで使用されている場合に過負荷になる

MSDP サーバーが複数の NetBackup ドメインによって使用され、MSDP サーバーの負荷が高い場合は、次の手順を実行して、異なるドメインから作業負荷を確認します。

1. 次のコマンドを実行して、現在のタスクの状態を取得します。

   UNIX の場合:

```
/usr/openv/pdde/pdcr/bin/crcontrol --taskstat
```

Windows の場合:

<*install_path*>¥Veritas¥pdde¥crcontrol.exe --taskstat

2. NetBackup ドメインに属しているクライアントの一覧で[クライアント (client)]列を確認し、1 つのドメインのクライアントの作業負荷を特定したら、次のドメインの作業負荷を特定します。
3. 1 つの NetBackup ドメインで `bpplclients` コマンドを実行すると、そのドメインのすべてのクライアントが一覧表示されます。

クラウド圧縮エラーメッセージのトラブルシューティング

クラウド圧縮に関する次のエラーメッセージをトラブルシューティングします。

- spoold は、次のエラーメッセージがあると開始できません。
  `Failed to recover from single container compaction.`
  spoold はクラウドから何も取得できません。OCSD に問題がある可能性があります。クラウドへの接続が機能していることを確認します。
- クラウド圧縮は、次のエラーメッセージがあると機能しません。
  `ingleDCCompactRecover: Call dcOutPlaceUpdateReplay_Cloud failed (...)`
  クラウドジャーナルフォルダ内のコンテナを `/data/compact_journal/*` からダウンロードできません。
  クラウドジャーナルフォルダのデータコンテナオブジェクトをダウンロードできることを確認します。

msdpcmdrun の問題のトラブルシューティング

次の表に、`msdpcmdrun` の問題とそのトラブルシューティング方法を示します。

表 17-10 msdpcmdrun の問題

問題	解決方法
次のエラーメッセージが表示されます。 [msdpcmdrun コマンドを実行するには、オペレーティングシステムのユーザーが重複排除管理者グループに所属する必要があります。(The operating system user must be part of the deduplication administrator group to run msdpcmdrun command.)]	msdpcmdrun コマンドを実行しようとしているユーザーが、重複排除管理者グループに含まれていません。 管理者は pdadmin グループにユーザーを追加する必要があります。 p.226 の「msdpcmdrun を使用して MSDP コマンドを実行するための root 以外のユーザーの構成」を参照してください。

次のエラーメッセージが表示されます。
[msdpcmdrun が管理者サービスへの接続に失敗しました。(msdpcmdrun failed to connect to the admin service.)]
	msdpcmdrun が PDPAS (PureDisk 特権アクセスサービス) サービスと通信できません。次の理由で発生する場合があります。
	■ PDPAS サービスが実行されていません。
	■ pdadmin グループに新しいユーザーが追加されましたが、PDPAS サービスにアクセスできません。
	この問題を解決するには
	1 実行されていない場合は、PDPAS サービスを開始します。
	`/usr/openv/pdde/pdconfigure/pdde pdpas start`
	2 PDPAS サービスがすでに実行中の場合は、再起動します。
	`/usr/openv/pdde/pdconfigure/pdde pdpas stop`
	`ps -ef | grep pdpas`
	`/usr/openv/pdde/pdconfigure/pdde pdpas start`

問題	解決方法
PDPAS サービスは、bp.kill_all コマンドを使用すると停止に失敗します。	PDPAS サービスを停止しようとすると、bp.kill_all コマンドが失敗し、サービスが実行されたままになる場合があります。 この問題を解決するには 1 次のコマンドを使用して PDPAS サービスを停止します。 /usr/openv/pdde/pdconfigure/pdde pdpas stop 2 プロセスが停止しない場合は、PID (PDPAS プロセス ID) を特定し、手動で強制終了します。 ■ 実行中の PDPAS サービスの PID を特定します。 ps -ef | grep pdpas ■ プロセスを強制終了します。 kill -9 <PDPAS_PID> ■ プロセスが実行中でなくなったことを確認します。 ps -ef | grep pdpas
停止した後、PDPAS サービスが再び実行されます。	cron ジョブは、PDPAS を監視するために 5 分ごとに実行されます。実行されていない場合、PDPAS サービスは自動的に開始されます。 PDPAS サービスの自動起動を停止する場合は、PDPAS サービスを監視する cron ユーティリティを無効にするか cron ファイルを削除します。 ■ cron ユーティリティを無効にするには、オペレーティングシステム固有のコマンドを使用して cron サービスを停止します。たとえば、RHEL 8 の場合は、次のコマンドを使用します。 systemctl status crond.service ■ cron ファイルを削除するには、次のコマンドを実行します。 rm /etc/cron.d/pdpas_monitor.cron

問題	解決方法

msdpcmdrunコマンドの出力の先頭に、次のエラーメッセージのいずれかまたは両方が表示されます。
■ ［管理サービスからの応答の受信に失敗しました。(Failed to receive a response from the admin service.)］
■ ［エラー: -1: recvmsg が失敗しました: 88 (Error: -1: recvmsg failed: 88)］
	msdpcmdrun は PDPAS サービスと正常に通信できますが、場合によっては、オペレーティングシステムの競合状態により、コマンド出力の先頭にエラーメッセージが表示されることがあります。
	この問題を解決するには、PDPAS サービスを再起動します。
	`/usr/openv/pdde/pdconfigure/pdde pdpas stop`
	`ps -ef | grep pdpas`
	`/usr/openv/pdde/pdconfigure/pdde pdpas start`

メモ: msdpcmdrun の実行中に予期しないエラーが発生した場合は、PDPAS サービスを再起動します。

A

MSDP ストレージへの移行

この付録では以下の項目について説明しています。

別のストレージ形式から MSDP への移行

別の NetBackup のストレージ形式から重複排除ストレージに移行する場合、Cohesity は他のストレージ上のバックアップイメージを期限切れになるまでエージングすることをお勧めします。Cohesityでは、ディスクストレージまたはテープストレージから移行する場合は、バックアップイメージをエージングすることをお勧めします。

AdvancedDisk などの他のストレージに使用しているディスクストレージは、NetBackup の重複排除に使用しないでください。各形式はストレージの管理方法が異なり、排他的に利用できるストレージを必要とします。また、NetBackup Deduplication Engine は、別の NetBackup のストレージ形式が作成したバックアップイメージを読み込むことができません。このため、ストレージハードウェアを再利用する前に、データの期限が切れるようにデータの経過時間を指定する必要があります。そのデータが期限切れになるまで、2 つのストレージの宛先 (メディアサーバーの重複排除プールとその他のストレージ) が存在します。他のストレージ上のイメージが期限切れになって削除された後、他のストレージのニーズに合わせてそのストレージを再利用できます。

表 A-1 NetBackup の MSDP への移行

手順	作業	手順詳細
手順 1	NetBackup の重複排除を構成します	p.62 の「NetBackup でのメディアサーバー重複排除の構成」を参照してください。

手順	作業	手順詳細
手順 2	バックアップジョブをリダイレクトします	メディアサーバー重複排除プールのストレージユニットにバックアップジョブをリダイレクトします。そのためには、バックアップポリシーのストレージの宛先を重複排除プールのストレージユニットに変更します。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 http://www.veritas.com/docs/DOC5332
手順 3	ストレージを再利用します	ストレージに関連付けられているバックアップイメージすべての期限が切れた後で、そのストレージを再利用します。 ディスクストレージの場合は、既存のメディアサーバー重複排除プールにそのストレージを追加できません。別の新しい重複排除ノードのストレージとして使用できます。

B

Cloud Catalyst から MSDP ダイレクトクラウド階層化への移行

この付録では以下の項目について説明しています。

Cloud Catalyst から MSDP ダイレクトクラウド階層化への移行について

メモ: この付録の手順は、バージョン 10.0.0.1 から 10.2.0.1 を実行している MSDP サーバーで実行する必要があります。マスターサーバーで新しいバージョンが実行されている可能性がありますが、`nbdecommission -migrate_cloudcatalyst` コマンドを実行する MSDP サーバーは、これらのバージョンのいずれかを実行している必要があります。

NetBackup 8.3 以降のリリースには、MSDP ダイレクトクラウド階層化のサポートが含まれます。この新しい技術は、パフォーマンス、信頼性、操作性、柔軟性の改善により以前の Cloud Catalyst 製品よりも優れています。これらの改善点と今後の機能強化の活用のため、MSDP ダイレクトクラウド階層化への移行をお勧めします。

Cloud Catalyst の使用を継続する場合は、NetBackup 9.0 以降と互換性がある、NetBackup バージョン 8.1 から 8.3.0.2 を実行しているサーバーで引き続き使用できます。これらの古いバージョンは、バージョン 9.0 以降の NetBackup プライマリサーバーインストールの旧バージョンサーバーとしてサポートされます。NetBackup プライマリサーバーを 9.0 以降のバージョンにアップグレードした後は、コマンドラインを使用して Cloud Catalyst サーバーを構成する必要があります。NetBackup 9.0 以降では、Cloud Catalyst の構成に Web UI を使用できません。

Cloud Catalyst サーバーがバージョン 9.0 以降にアップグレードされるのを防ぐため、NetBackup のインストールプロセスに `nbcheck` ユーティリティテストが追加されました。サーバーで Cloud Catalyst が検出されると、インストールが停止します。アップグレードが停止した後もサーバーは変更されないまま、現在インストール済みのバージョンの NetBackup が引き続き実行されます。

Cloud Catalyst の移行戦略について

Cloud Catalyst から MSDP ダイレクトクラウド階層化への移行には複数の戦略があります。インストールの最適な戦略は、クラウドストレージの種類 (パブリックまたはプライベート、標準ストレージクラスまたはコールドストレージクラス) やデータ保持要件などの要因によって異なります。

Cloud Catalyst から MSDP ダイレクトクラウド階層化への移行の 4 つの戦略を次に示します。このうち 3 つの戦略は NetBackup 8.3 以降のリリースで導入でき、4 つ目の直接移行はリリース 10.0 以降で利用できます。4 つの戦略すべてについて、ご使用の環境に最適な選択をするために確認する必要がある利点と欠点が記載されています。

Cloud Catalyst から MSDP ダイレクトクラウド階層化への移行の 4 つの戦略:

- 「自然失効戦略」- NetBackup リリース 8.3 以降で利用可能
- 「イメージ複製戦略」- NetBackup リリース 8.3 以降で利用可能
- 「組み合わせ戦略」- NetBackup リリース 8.3 以降で利用可能
- 「直接移行戦略」- NetBackup リリース 10.0 以降で利用可能

自然失効戦略

この戦略は、すべての環境で機能します。この戦略を使用するには、まず NetBackup 8.3 以降の新しい MSDP ダイレクトクラウド階層ストレージサーバーを構成する必要があります。または、MSDP ダイレクトクラウド階層ディスクプールとストレージユニットを既存の NetBackup 8.3 以降の MSDP ストレージサーバーに追加します (サーバー容量を確認してください)。次に、新しい MSDP ダイレクトクラウド階層ストレージを使用するため、

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変更します。すべての新しい複製ジョブまたはバックアップジョブが新しい MSDP ダイレクトクラウド階層ストレージに書き込むと、古い Cloud Catalyst ストレージのイメージが徐々に期限切れになります。これらのイメージがすべて期限切れになった後、Cloud Catalyst サーバーを破棄、またはその用途を変更できます。

自然失効戦略の利点は次のとおりです。

- NetBackup バージョン 8.3 以降で利用できます。この戦略により、MSDP ダイレクトクラウド階層のパフォーマンス、信頼性、操作性、柔軟性が向上します。NetBackup 10.0 にアップグレードしなくても使用できます。
- Cloud Catalyst ストレージサーバーを引き続き使用しながら、新しい MSDP クラウドストレージサーバーを使用して徐々に実装できます。
- パブリッククラウドのコールドストレージ (AWS Glacier や AWS Glacier Deep Archive など) を含むすべての環境で使用できます。
- Cloud Catalyst よりも効率的にクラウドストレージを使用する MSDP ダイレクトクラウド階層化を使用して、すべての新しいデータがアップロードされます。クラウドストレージの長期的な合計使用量とコストを削減できる場合があります。

自然失効戦略の欠点は次のとおりです。

- すべての古い Cloud Catalyst イメージが期限切れになり削除されるまで、クラウドストレージのデータが一部重複します。この重複は、古い Cloud Catalyst イメージと新しい MSDP ダイレクトクラウド階層イメージの間で発生する場合があります。パブリッククラウド環境を使用する場合、追加のストレージコストが発生する可能性があります。
- 個別のサーバーが必要です。
- Cloud Catalyst サーバーからアップロードされたイメージが期限切れになるか、不要になるまで、Cloud Catalyst サーバーを維持する必要があります。

イメージ複製戦略

この戦略は、パブリッククラウドのコールドストレージ (AWS Glacier や AWS Glacier Deep Archive など) を使用する環境を除く、ほとんどの環境で機能します。この戦略を使用するには、まず NetBackup 8.3 以降の新しい MSDP ダイレクトクラウド階層ストレージサーバーを構成する必要があります。または、MSDP ダイレクトクラウド階層ディスクプールとストレージユニットを既存の NetBackup 8.3 以降の MSDP ストレージサーバーに追加します (サーバー容量を確認してください)。次に、新しい MSDP ダイレクトクラウド階層ストレージを使用するため、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変更します。すべての新しい複製ジョブまたはバックアップジョブが新しい MSDP ダイレクトクラウド階層ストレージに書き込むと、古い Cloud Catalyst ストレージに既存のイメージが移動されます。これらのイメージは、手動で開始する `bpduplicate` コマンドを使用して、新しい MSDP ダイレクトクラウド階層ストレージに移動されます。すべての既存のイメージが古い Cloud Catalyst ストレージから新しい MSDP ダイレクトクラウド階層ス

トレージに移動された後、Cloud Catalyst サーバーを破棄、またはその用途を変更できます。

イメージ複製戦略の利点は次のとおりです。

- NetBackup バージョン 8.3 以降で利用できます。この戦略により、MSDP ダイレクトクラウド階層のパフォーマンス、信頼性、操作性、柔軟性が向上します。NetBackup 10.0 にアップグレードしなくても使用できます。
- Cloud Catalyst ストレージサーバーを引き続き使用しながら、新しい MSDP クラウドストレージサーバーを使用して徐々に実装できます。
- Cloud Catalyst よりも効率的にクラウドストレージを使用する MSDP ダイレクトクラウド階層化を使用して、Cloud Catalyst のすべての新しいデータと古いデータがアップロードされます。クラウドストレージの長期的な合計使用量とコストを削減できる場合があります。

イメージ複製戦略の欠点は次のとおりです。

- パブリッククラウドのコールドストレージ環境 (AWS Glacier や AWS Glacier Deep Archive など) では、クラウドからのリストアはサポートされていますが、クラウドからの複製はサポートされていないため、この戦略は使用できません。
- パブリッククラウドストレージを使用している場合、新しい MSDP クラウドストレージに複製するために古い Cloud Catalyst イメージを読み取る際、高額なデータ取り出し料が請求される可能性があります。
- 古い Cloud Catalyst イメージを新しい MSDP ダイレクトクラウド階層ストレージに複製する際、クラウドとの間で追加のネットワークトラフィックが発生します。
- すべての古い Cloud Catalyst イメージが MSDP ダイレクトクラウド階層ストレージに移動されるまで、クラウドストレージのデータが一部重複します。この重複は、古い Cloud Catalyst イメージと新しい MSDP ダイレクトクラウド階層イメージの間で発生する場合があります。パブリッククラウド環境を使用する場合、追加のコストが発生する可能性があります。
- 個別のサーバーが必要です。
- Cloud Catalyst サーバーからアップロードされたイメージが新しい MSDP ダイレクトクラウド階層ストレージにすべて移動されるか、不要になるまで、Cloud Catalyst サーバーを維持する必要があります。

組み合わせ戦略

この戦略は、パブリッククラウドのコールドストレージ (AWS Glacier や AWS Glacier Deep Archive など) を使用する環境を除く、ほとんどの環境で機能します。この戦略は、前述の 2 つの方法を組み合わせたものです。この戦略を使用するには、まず NetBackup 8.3 以降の新しい MSDP ダイレクトクラウド階層ストレージサーバーを構成する必要があります。または、MSDP ダイレクトクラウド階層ディスクプールとストレージユニットを既存の NetBackup 8.3 以降の MSDP ストレージサーバーに追加します (サーバー容量を確

認してください)。次に、新しい MSDP ダイレクトクラウド階層ストレージを使用するため、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変更します。すべての新しい複製ジョブまたはバックアップジョブが新しい MSDP ダイレクトクラウド階層ストレージに書き込むと、Cloud Catalyst ストレージの最も古いイメージから徐々に期限切れになります。古い Cloud Catalyst ストレージの期限切れになっていない残りのイメージ数が指定したしきい値を下回ると、残りのイメージが移動されます。これらのイメージは、手動で開始する `bpduplicate` コマンドを使用して、新しい MSDP ダイレクトクラウド階層ストレージに移動されます。すべての残りのイメージが古い Cloud Catalyst ストレージから新しい MSDP ダイレクトクラウド階層ストレージに移動された後、Cloud Catalyst サーバーを破棄、またはその用途を変更できます。

組み合わせ戦略の利点は次のとおりです。

- NetBackup バージョン 8.3 以降で利用できます。この戦略により、MSDP ダイレクトクラウド階層のパフォーマンス、信頼性、操作性、柔軟性が向上します。NetBackup 10.0 にアップグレードしなくても使用できます。
- Cloud Catalyst ストレージサーバーを引き続き使用しながら、新しい MSDP ダイレクトクラウド階層ストレージサーバーを使用して徐々に実装できます。
- Cloud Catalyst よりも効率的にクラウドストレージを使用する MSDP ダイレクトクラウド階層化を使用して、Cloud Catalyst のすべての新しいデータと古いデータがアップロードされます。クラウドストレージの長期的な合計使用量とコストを削減できる場合があります。
- 古い Cloud Catalyst サーバーのイメージがすべて期限切れになる前に、それらのサーバーを破棄できます。

組み合わせ戦略の欠点は次のとおりです。

- パブリッククラウドのコールドストレージ環境 (AWS Glacier や AWS Glacier Deep Archive など) では、クラウドからのリストアはサポートされていますが、クラウドからの複製はサポートされていないため、この戦略は使用できません。
- パブリッククラウドストレージを使用している場合、高額なデータ取り出し料が請求される可能性があります。この問題は、古い Cloud Catalyst イメージを読み取って新しい MSDP ダイレクトクラウド階層ストレージに複製するときに発生する場合があります。
- 古い Cloud Catalyst イメージを新しい MSDP ダイレクトクラウド階層ストレージに複製する際、クラウドとの間で追加のネットワークトラフィックが発生します。
- すべての Cloud Catalyst イメージが期限切れになるか、MSDP ダイレクトクラウド階層ストレージに移動されるまで、クラウドストレージのデータが一部重複します。この重複は、古い Cloud Catalyst イメージと新しい MSDP ダイレクトクラウド階層イメージの間で発生する場合があります。したがって、パブリッククラウド環境を使用している場合は追加のコストが発生することがあります。
- 個別のサーバーが必要です。

- Cloud Catalyst サーバーからアップロードされたイメージがすべて期限切れになるか、新しい MSDP ダイレクトクラウド階層に移動されるか、不要になるまで、Cloud Catalyst サーバーを維持する必要があります。

直接移行戦略

この戦略は NetBackup 10.0 以降のリリースで利用でき、任意の環境で機能します。この戦略を使用するには、まず最新のリリースを使用して新しい MSDP ダイレクトクラウド階層ストレージサーバーを構成する必要があります。または、最新リリースを使用して、既存の Cloud Catalyst サーバーを新しい MSDP ダイレクトクラウド階層ストレージサーバーとして再イメージ化して再インストールできます。既存のサーバーを使用する場合、そのサーバーを使用するための最小要件を満たす必要があります。

p.23 の「MSDP の配置計画」を参照してください。

この操作はアップグレードではない点に注意してください。その代わり、削除と再インストールの操作になります。新しい MSDP ダイレクトクラウド階層ストレージサーバーが利用可能になると、`nbdecommission -migrate_cloudcatalyst` ユーティリティを使用して新しい MSDP ダイレクトクラウド階層が作成されます。この新しいストレージは、以前 Cloud Catalyst によってクラウドストレージにアップロードされたデータを参照できます。移行プロセスが完了してユーティリティが実行されると、新しい MSDP ダイレクトクラウド階層を新しいバックアップ操作と複製操作に使用できます。この新しいストレージは、古い Cloud Catalyst イメージのリストア操作に使用できます。

`nbdecommission` 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。

直接移行戦略の利点は次のとおりです。

- パブリッククラウドのコールドストレージ (AWS Glacier や AWS Glacier Deep Archive など) を含むすべての環境で使用できます。
- Cloud Catalyst サーバーを MSDP ダイレクトクラウド階層サーバーとして再イメージ化して移行に使用できるため、個別のサーバーは不要です。

直接移行戦略の欠点は次のとおりです。

- Cloud Catalyst ストレージサーバーを新しいバックアップジョブまたは複製ジョブに引き続き使用しながら、新しい MSDP ダイレクトクラウド階層ストレージサーバーを使用して徐々に実装できません。移行プロセスの実行中は、古い Cloud Catalyst ストレージサーバーを新しいバックアップジョブまたは複製ジョブに使用できません。
- Cloud Catalyst は、MSDP ダイレクトクラウド階層よりも非効率的にクラウドストレージを使用します。この問題は、NetBackup 8.2 より前のバージョンの Cloud Catalyst に特に該当します。この戦略では、既存の Cloud Catalyst オブジェクトを新しい MSDP ダイレクトクラウド階層イメージに引き続き使用します。MSDP ダイレクトクラウド階層で得られるクラウドストレージの効率性の一部は実現されません。
- 新しい MSDP サーバーが必要なため、既存の MSDP サーバーは使用できず、いずれの Cloud Catalyst サーバーの統合も不可能です。

p.760 の「直接移行の開始について」を参照してください。

Cloud Catalyst から MSDP ダイレクトクラウド階層化への直接移行について

このセクションでは、Cloud Catalyst サーバーから MSDP ダイレクトクラウド階層ストレージサーバーにイメージを移動する直接移行戦略について説明します。このセクションでは次の 5 つの領域について説明します。

- p.759 の「新しい MSDP ダイレクトクラウド階層ストレージサーバーの要件について」を参照してください。
- p.760 の「直接移行の開始について」を参照してください。
- p.761 の「Cloud Catalyst サーバーを一貫性がある状態にする」を参照してください。
- p.763 の「新しい MSDP ダイレクトクラウド階層サーバーのインストールと構成について」を参照してください。
- p.765 の「新しい MSDP ダイレクトクラウド階層サーバーへの移行の実行」を参照してください。

新しい MSDP ダイレクトクラウド階層ストレージサーバーの要件について

移行では、新しい MSDP ダイレクトクラウド階層ストレージサーバーとして、既存のディスクプールがない新しい MSDP サーバーを使用する必要があります。新しい MSDP ダイレクトクラウド階層サーバーとして、Cloud Catalyst サーバーを再インストールして再利用できます。ただし、新しいハードウェアで新しい MSDP サーバーを使用して、既存の Cloud Catalyst サーバーはそのまま維持する方が良い場合があります。移行プロセス中に予期しないエラーが発生した場合に備え、既存の Cloud Catalyst サーバーをフェールセーフとして維持できます。

空きディスク容量が少ないシステムにも移行できますが、新しい MSDP サーバーを作成した後と Cloud Catalyst の移行を実行する前に追加の手順が必要になります。この追加の手順では、`contentrouter.cfg` ファイルで `CloudDataCacheSize` と `CloudMetaCacheSize` のデフォルト値を変更します。

`CloudDataCacheSize`、`CloudMetaCacheSize`、`contentrouter.cfg` ファイルについて詳しくは、次を参照してください。

p.278 の「cloud.json、contentrouter.cfg、spa.cfg 内の構成項目について」を参照してください。

新しい MSDP サーバーで移行機能をサポートする最新バージョンの NetBackup (10.0 以降) を実行している必要があります。そのためには、プライマリサーバーも NetBackup 10.0 以降を実行している必要があります。

直接移行の開始について

移行プロセスの間、既存の Cloud Catalyst サーバーと新しい MSDP サーバーをオフラインにできるメンテナンスウィンドウを決定します。ほとんどの環境で、このプロセスにかかる時間は 1 日未満です。一部の非常に大規模な環境や、クラウドへのアップロードに利用可能な帯域幅が狭い環境では、プロセスに時間がかかる場合があります。

直接移行を始める前に、次の情報を収集します。

- Cloud Catalyst サーバー名 (Cloud Catalyst アプライアンスまたは BYO サーバーのホスト名)。
- Cloud Catalyst サーバーの `root` のログオンクレデンシャル。Cloud Catalyst サーバーがアプライアンスの場合は、アプライアンスにログオンしてメンテナンスモードに昇格するためのクレデンシャル。
- Cloud Catalyst ストレージサーバー名 (Cloud Catalyst 用に使用される NetBackup Cloud Storage Server)。
- Cloud Catalyst バケットまたはコンテナ名。
- KMS 構成、特に KMS キーグループ名 (KMS が構成されている場合のみ)。
  - Cloud Catalyst ストレージサーバーの形式が `_cryptd` で終わる場合は KMS が有効で、`<Cloud Catalyst` **ストレージサーバー名**`>:<`**バケット/コンテナ名**`>` が KMS キーグループ名です。
  - Cloud Catalyst ストレージサーバーの形式が `_rawd` で終わる場合は、Cloud Catalyst サーバーで `contentrouter.cfg` の `KMSOptions` セクションを確認します。KMS が有効になっているか確認し、KMS キーグループ名を見つけます。`KMSOptions` セクションが存在しない場合、KMS は無効です。`KMSOptions` セクションがあり、有効な場合は `KMSEnable` エントリが `True`、無効な場合は `False` です。
  - Cloud Catalyst サーバーで `/usr/openv/pdde/pdcr/bin/keydictutil --list` コマンドを使用して、これらの KMS 設定を表示できます (Cloud Catalyst バージョン 8.2 以降)。
  - NetBackup プライマリサーバーで `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkgs` コマンドを使用して、KMS キーグループ名を一覧表示できます。収集した KMS キーグループ名が存在し、正しいことを確認します。
- 移行した MSDP ダイレクトクラウド階層ストレージサーバーの新しいディスクボリュームに使用される名前。
- 移行した MSDP ダイレクトクラウド階層ストレージサーバーの新しいディスクプールに使用される名前。

- 任意のクラウドクレデンシャル (AWS IAM ロールを使用する場合は、アクセスキー dummy とシークレットアクセスキー dummy を使用するようにします)。
- その他すべてのクラウド固有の構成情報。
- 現在 Cloud Catalyst ストレージサーバーに書き込んでいる、すべての NetBackup ポリシーと SLP のリスト。

上記の情報のリストを収集した後、Cohesity ダウンロードセンターから sync_to_cloud ユーティリティをダウンロードし、Cloud Catalyst サーバーで移行前の手順に利用できるようにします。

Cloud Catalyst に使用される MSDP DSID (データ選択 ID) が 2 であることを確認します。<Cloud Catalyst キャッシュディレクトリ>/storage/databases/catalog ディレクトリの内容を確認します。名前が 2 のサブディレクトリが 1 つあるはずです。サブディレクトリがそれより多い場合、またはサブディレクトリ 2 が存在しない場合は、続行する前にこの問題を修正する必要があります。Cohesity のサポートにお問い合わせください。

プライマリサーバーで、カタログバックアップポリシー (ポリシー形式: NBU-Catalog) が存在し、そのポリシーストレージの宛先が移行する Cloud Catalyst ストレージサーバー以外であることを確認します。失敗した移行からのロールバックリカバリを可能にするため、移行プロセスの特定の時点で、このカタログバックアップポリシーの手動バックアップが開始されます。Cloud Catalyst サーバー以外のストレージにカタログバックアップが存在しない場合は、失敗した移行からのリカバリが困難または不可能になる場合があります。

Cloud Catalyst サーバーを一貫性がある状態にする

データの整合性と一貫性を維持するには、Cloud Catalyst サーバーを使用する実行中のジョブが移行時にないことが重要です。移行プロセスを開始する前に、次の手順を実行してすべてのジョブを停止し、Cloud Catalyst サーバーを一貫性がある安定した状態にします。

メモ: 最終的な移行を開始する前に、次の手順で確認したすべてのエラーに対処する必要があります。お使いの環境でこのプロセスを開始する前に、手順全体と手順に続くテキストをお読みください。

Cloud Catalyst サーバーを一貫性がある状態にするには

1. Cloud Catalyst ストレージサーバーに書き込むバックアップポリシーをすべて無効にします。
2. Cloud Catalyst ストレージサーバーに書き込むストレージライフサイクルポリシーをすべて無効にします。
3. Cloud Catalyst ストレージサーバーを使用する実行中のジョブがすべて停止していることを確認します。

4 bpimage -cleanup コマンドを使用してプライマリサーバーでカタログクリーンアップを実行します。

場所: /usr/openv/netbackup/bin/admincmd/bpimage -cleanup -allclients -prunetir

5 カタログクリーンアップが完了したら、crcontrol --processqueue コマンドを使用して Cloud Catalyst サーバーで MSDP トランザクションキューを手動で処理し、処理が完了するまで待機します。

場所: /usr/openv/pdde/pdcr/bin/crcontrol --processqueue

p.517 の「MSDP トランザクションキューの手動処理」を参照してください。

6 手順 5 を繰り返して、すべてのイメージが処理されたことを確認します。

7 Cloud Catalyst サーバーで /usr/openv/netbackup/logs/esfs_storage ログを少なくとも 15 分間監視し、すべての削除要求が処理されたことを確認します。

8 Cloud Catalyst サーバーで、/usr/openv/pdde/pdcr/bin/cacontrol --catalog recover all_missing コマンドを実行します。

警告: この手順でエラーが報告された場合は、次の手順に進む前にそれらのエラーに対処する必要があります。エラーの対処にサポートが必要な場合は、Cohesity のサポートにお問い合わせください。

---

9 Cloud Catalyst サーバーで /usr/openv/pdde/pdcr/bin/catdbutil --list コマンドを実行し、出力を一時ファイルにリダイレクトします。

このファイルでエラーを監視し、エラーが報告された場合は Cohesity テクニカルサポートにお問い合わせください。

10 前の手順がエラーなしで完了したら、sync_to_cloud ユーティリティを実行し、完了するまで待機します。環境によっては、このユーティリティの実行に時間がかかる場合があります。

p.760 の「直接移行の開始について」を参照してください。

11 sync_to_cloud が正常に完了したら、Cloud Catalyst サーバーでサービスを停止します。

Cloud Catalyst サーバーでサービスを停止したままにしてもかまいません。または、別の MSDP サーバーを使用して Cloud Catalyst を移行する場合は、<Cloud Catalyst キャッシュディレクトリ>/cache/etc/esfs.json の Readonly フィールドを 1 に変更できます。その後、Cloud Catalyst サーバーでサービスを再起動します。移行時に Cloud Catalyst サーバーでサービスが実行されている場合は、クラウドバケット名などの特定の構成項目が自動的に決定されます。決定されない場合は、次のセクションで収集した構成項目を入力する必要があります。

p.760 の「直接移行の開始について」を参照してください。

12 カタログバックアップポリシー (ポリシー形式: NBU-Catalog) の手動バックアップを実行します。

この手動バックアップの実行は非常に重要なため、この手順をスキップしないでください。このバックアップによって、移行が正常に完了しなかった場合に、戻る時点を確立します。

可能な場合は、新しい MSDP ダイレクトクラウド階層サーバーを移行に使用してください。新しいサーバーを使用すると、移行が予期せず失敗した場合に、既存の Cloud Catalyst サーバーはそのまま維持され使用できます。Cloud Catalyst サーバーを新しい MSDP ダイレクトクラウド階層サーバーとして再利用する場合は、この時点でサーバーをアンインストールまたは再イメージ化する必要があります。すべての NetBackup と Cloud Catalyst キャッシュディレクトリの内容を削除してください。Cloud Catalyst アプライアンスを再利用する場合は、Cloud Catalyst のキャッシュを削除するためにストレージのリセットが必要な場合があります。詳しくは、アプライアンスのマニュアルを参照してください。

p.23 の「MSDP の配置計画」を参照してください。

メモ: 通常は非推奨ですが、一部の特別な状況では、Cloud Catalyst がプライマリサーバーで実行されています。プライマリサーバーはアンインストールまたは再イメージ化できず、構成済みの Cloud Catalyst を使用してアップグレードできないため、/usr/openv/esfs/script/esfs_cleanup.sh スクリプトを実行して Cloud Catalyst を削除する必要があります。その後、プライマリサーバーをアップグレードし、移行を続行できます。

新しい MSDP ダイレクトクラウド階層サーバーのインストールと構成について

Cloud Catalyst の移行には、既存のディスクプールがない新しい MSDP ダイレクトクラウド階層サーバーが必要です。このセクションでは、移行をサポートする最新バージョンの NetBackup (10.0 以降) にプライマリサーバーがアップグレード済みであると想定しま

す。また、このセクションでは、移行に使用するメディアサーバーまたはアプライアンスに最新バージョンの NetBackup (10.0 以降) がインストール済みであると想定します。

移行に使用するメディアサーバーで MSDP ダイレクトクラウド階層サーバーを構成します。そのストレージサーバーにはディスクプールを構成しないでください。Cloud Catalyst で使用した KMS 設定と同じ設定を使用して、新しい MSDP ダイレクトクラウド階層サーバーを構成する必要があります。Cloud Catalyst ストレージサーバーの形式が `_cryptd` で終わる場合は (例: `PureDisk_amazon_cryptd`)、KMS を有効にする必要があります。Cloud Catalyst ストレージサーバーの形式が `_rawd` で終わる場合は (例: `PureDisk_azure_rawd`)、KMS を有効にする必要がある場合とない場合があります。この情報は、「直接移行の開始について」セクションに記載されているとおり、移行前にコンパイルする必要があります。

メモ: KMS を有効にする必要がある場合は、Web UI の MSDP サーバー構成画面にある KMS 関連の 3 つのチェックボックスすべてにチェックマークを付ける必要があります。また、Cloud Catalyst の KMS キーグループ名を入力する必要があります。KMS 設定が一致しない場合、Cloud Catalyst がアップロードしたいずれかのデータへのアクセスを試行すると問題が発生する可能性があります。すべての KMS 関連情報が一致することを確認する必要があります。

新しい MSDP ダイレクトクラウド階層サーバーには、少なくとも 1 TB の空きディスク容量が必要です。空きディスク容量が少ないシステムにも移行できますが、新しい MSDP ダイレクトクラウド階層サーバーを作成した後と Cloud Catalyst の移行を実行する前に追加の手順が必要になります。この追加の手順では、`contentrouter.cfg` ファイルで `CloudDataCacheSize` と `CloudMetaCacheSize` のデフォルト値を変更します。

p.278 の「cloud.json、contentrouter.cfg、spa.cfg 内の構成項目について」を参照してください。

NTP サーバーを使用して、新しい MSDP サーバーを正しい時刻に設定する必要があります。MSDP サーバーの時刻が正しくない場合、一部のクラウドプロバイダがエラー (`Request Time Too Skewed` など) を報告し、アップロードやダウンロードの要求に失敗することがあります。詳しくは特定のクラウドベンダーのマニュアルを参照してください。

メモ: 新しい MSDP サーバーを構成した後、続行する前に、カタログバックアップポリシー (ポリシー形式 NBU-Catalog) の手動バックアップを実行します。この手動バックアップの実行は非常に重要なため、この手順をスキップしないでください。このバックアップによって、移行が正常に完了しなかった場合に、戻る時点を確立します。

---

p.760 の「直接移行の開始について」を参照してください。

新しい MSDP ダイレクトクラウド階層サーバーへの移行の実行

新しい MSDP ダイレクトクラウド階層サーバーのインストールと構成のプロセスを続行する前に、ログの設定をお勧めします。インストール中に問題が発生した場合、ログは移行中に発生する可能性のあるエラーの診断に役立ちます。推奨項目を次に示します。

- nbdecommission コマンドを実行する前に、/usr/openv/netbackup/logs/admin ディレクトリが存在することを確認します。
- bp.conf ファイルでログレベルを VERBOSE=5 に設定します。
- /etc/pdregistry.cfg で OpenCloudStorageDaemon に loglevel=3 を設定します。
- contentrouter.cfg ファイルで Logging=full を設定します。

移行を実行するには、MSDP ダイレクトクラウド階層サーバーでコマンドプロンプトに移動して、次を実行します。

```
/usr/openv/netbackup/bin/admincmd/nbdecommission
-migrate_cloudcatalyst
```

メモ: このユーティリティは、数時間以上実行してもタイムアウトしたり閉じたりしないウィンドウで実行する必要があります。アプライアンスで移行を実行する場合は、メンテナンスシェルにアクセスできる必要があります。移行の実行中はシェルがロック解除されたままにする必要があります。数時間以上実行した場合でも、メンテナンスシェルは有効なままにする必要があります。

移行する Cloud Catalyst ストレージサーバーを選択し、nbdecommission ユーティリティのプロンプトに従って情報を入力します。

移行中に表示される可能性がある例を次に示します。

```
# /usr/openv/netbackup/bin/admincmd/nbdecommission
-migrate_cloudcatalyst
MSDP storage server to use for migrated CloudCatalyst:
myserver.test.com

Generating list of configured CloudCatalyst storage servers.
This may take a few minutes for some environments, please wait.

Cloud Storage Server Cloud Bucket CloudCatalyst Server Storage Server
 Type
1) amazon.com         my-bucket    myserver.test.com
PureDisk_amazon_rawd

Enter line number of CloudCatalyst server to migrate: 1
```

```
MSDP KMS encryption is enabled for amazon.com.
Please confirm that CloudCatalyst was configured using
KMSKeyGroupName amazon.com:testkey

Continue? (y/n) [n]: y

Enter new disk volume name for migrated CloudCatalyst server: newdv
Enter new disk pool name for migrated CloudCatalyst server: newdp
Enter cloud account username or access key:  AAAABBBBBCCCCCDDDDD
Enter cloud account password or
secret access key: aaaabbbbccccddddeeeeffffggg

You want to migrate amazon.com (bucket my-bucket) to
newmsdpserver.test.com (volume newdv, pool newdp).
Is that correct? (y/n) [n]: y

To fully decommission myserver.test.com after
CloudCatalyst migration is complete,run the
following command on the primary server:
/usr/openv/netbackup/bin/admincmd/nbdecommission
-oldserver myserver.test.com

Administrative Pause set for machine myserver.test.com

Migrating CloudCatalyst will include moving the images to server
newmsdpserver.test.com deleting the old disk pool, storage unit, and

storage server, deactivating policies that reference the old storage

unit, and restarting MSDP on server newmsdpserver.test.com.

Before proceeding further, please make sure that no jobs are running
 on
media server myserver.test.com or media server newmsdpserver.test.com.
This command may not be able to migrate CloudCatalyst
with active jobs on either of those servers.

To avoid potential data loss caused by conflicts between the
old CloudCatalyst server and the migrated MSDP server, stop the
NetBackup services on myserver.test.com if they are running.

It is recommended to make one or both of the following changes
```

```
on myserver.test.com to prevent future data loss caused by
inadvertently starting NetBackup services.
1) Rename /usr/openv/esfs/bin/vxesfsd to
/usr/openv/esfs/bin/vxesfsd.off
2) Change "ReadOnly" to "1" in the esfs.json configuration file
See the documentation for more information about esfs.json.

It is also recommended to perform a catalog cleanup and backup prior

to migration so that the catalog can be restored to its original
state in the event that migration is not completed.

Continue? (y/n) [n]: y

Successfully cloned storage server: amazon.com to:
newmsdpserver.test.com_newdv

Storage server newmsdpserver.test.com has been successfully updated

The next step is to list the objects in the cloud and migrate
the MSDP catalog. The duration of this step depends on how much data

was uploaded by CloudCatalyst.
It may take several hours or longer, so please be patient.

You may reduce the duration by not migrating the
CloudCatalyst image sharing information if you are certain that
you do not use the image sharing feature.

Do you wish to skip migrating CloudCatalyst image
sharing information? (y/n) [n]:

Jun 24 15:37:11 List CloudCatalyst objects in cloud
Jun 24 15:37:13 List CloudCatalyst objects in cloud
Jun 24 15:37:18 List CloudCatalyst objects in cloud
Jun 24 15:37:26 MSDP catalog migrated successfully from CloudCatalyst

Disk pool newdp has been successfully created with 1 volumes

Moved CloudCatalyst images from myserver.test.com to
newmsdpserver.test.com

Disk pool awsdp (PureDisk_amazon_rawd) is referenced by the following
```

```
storage units:
    awsdp-stu

Storage unit awsdp-stu: host myserver.test.com
Deactivating policies using storage unit awsdp-stu
Storage unit awsdp-stu is referenced by policy testaws
Deactivated policy testaws
Deleting storage unit awsdp-stu on host _STU_NO_DEV_HOST_
Deleted storage unit awsdp-stu
Deleted PureDisk_amazon_rawd disk pool awsdp
Deleted PureDisk_amazon_rawd storage server amazon.com

Stopping ocsd and spoold and spad
Checking for PureDisk ContentRouter
spoold (pid  55723) is running...
Checking for PDDE Mini SPA                                  [  OK  ]
spad (pid  55283) is running...
Checking for Open Cloud Storage Daemon                      [  OK  ]
ocsd (pid 55150) is running...
Stopping PureDisk Services
ocsd is stopped

Run MSDP utility to prepare for online checking.
This may take some time, please wait.

Starting ocsd and spoold and spad
Checking for Open Cloud Storage Daemon
ocsd is stopped
Starting Open Cloud Storage Daemon: ocsd Checking for PDDE Mini SPA
spad is stopped
spad (pid  56856) is running...                            [  OK  ]
Checking for PureDisk ContentRouter
spoold is stopped
spoold (pid  57013) is running...spoold                     [  OK  ]
Starting PureDisk Services
spoold (pid  57013) is running...

Enabling data integrity check.
Starting data integrity check.
Waiting for data integrity check to finish.
Processing the queue.
CloudCatalyst server myserver.test.com has been successfully
```

```
migrated to newmsdpserver.test.com.
To avoid potential data loss caused by conflicts between the
old CloudCatalyst server and the
migrated MSDP server, stop the NetBackup daemons (or services)
on myserver.test.com if they are running.
```

nbdecommission コマンドの出力でエラーを監視します。アクティビティと潜在的なエラーを監視するためのその他のログは、storage_path/log/ ディレクトリにあります。cacontrol コマンドの問題については、ocsd_storage、spad、spoold ログを監視してください。

エラーが発生して、そのエラーを修正できた場合は、nbdecommission コマンドの出力に示されるとおり start_with オプションを使用して、その時点から移行を再開できます。エラーについて質問がある場合は、移行を再開する前に Cohesity のサポートにお問い合わせください。

移行中のプロンプトについて

移行を実行すると、移行中に複数のプロンプトが表示されます。必要に応じて、コマンドラインオプションを使用してこれらのプロンプトに対する回答を入力できます。Cohesity では、コマンドラインオプションを使用した場合よりも移行が簡単になりエラーが発生しにくくなるため、対話形式のプロンプトを使用するようお勧めします。コマンドラインを使用する場合は、『NetBackup コマンドリファレンスガイド』にオプションが記載されています。

移行プロセス中のプロンプトの多くは自明であり、プロンプトの数と種類は変化する場合があります。プロンプトの数と種類は次によって異なります。

- 移行時に使用されている Cloud Catalyst のバージョン
- 移行時に Cloud Catalyst サーバーが実行されている場合
- Cloud Catalyst サーバーで KMS が有効になっている場合

表 B-1 では、いくつかのプロンプトに関する追加情報について説明します。

表 B-1　　移行のプロンプト

プロンプト	説明

`No MSDP storage server found on myserver.test.com.`
 	
`Please create the MSDP storage server before running this utility.`
	この出力は、MSDP ストレージサーバーが構成されていないメディアサーバーで nbdecommission -migrate_cloudcatalyst コマンドを実行すると表示されます。
	
	p.763 の「新しい MSDP ダイレクトクラウド階層サーバーのインストールと構成について」を参照してください。

プロンプト	説明

`Disk pools exist for storage server PureDisk myserver.test.com.`
 	
`CloudCatalyst migration requires a new storage server with no configured disk pools.`
	このサンプル出力は、MSDP ストレージサーバーが構成されておらず、既存のディスクプールが構成されているメディアサーバーで `nbdecommission -migrate_cloudcatalyst` コマンドを実行すると表示されます。Cloud Catalyst の移行は、既存のディスクプールがない新しい MSDP クラウド階層サーバーでのみ実行できます。

`Enter cloud bucket name:`	移行時に Cloud Catalyst サーバーが実行されていない場合は、既存の Cloud Catalyst バケットまたはコンテナ名を手動で入力する必要があります。この情報が移行に使用されます。
`Enter CloudCatalyst server hostname:`	移行時に Cloud Catalyst サーバーが実行されていない場合は、移行する既存の Cloud Catalyst サーバーのサーバーホスト名を手動で入力する必要があります。
`Is MSDP KMS encryption enabled for amazon.com? (y/n) [n]:`	移行時に Cloud Catalyst サーバーが実行されていない場合は、既存の Cloud Catalyst サーバーの KMS 設定を手動で入力する必要がある場合があります。
`Enter new disk volume name for migrated CloudCatalyst server:`	新しい MSDP クラウド階層サーバーで作成する MSDP クラウドディスクボリュームの名前を入力します。この名前は、移行する Cloud Catalyst データ用に使用されます。
`Enter new disk pool name for migrated CloudCatalyst server:`	新しい MSDP サーバーに作成し、移行する Cloud Catalyst データ用に使用する MSDP クラウドディスクプールの名前を入力します。

`Enter cloud account username or access key:`
 	
`Enter cloud account password or secret access key:`
	移行する Cloud Catalyst データにアクセスするために使用するクラウドアカウントのクレデンシャルを入力します。AWS IAM ロールを使用してデータにアクセスする場合は、アクセスキーとシークレットアクセスキーの両方に `dummy` と入力してください。

移行後の構成とクリーンアップについて

移行が正常に完了すると、MSDP クラウド階層の新しいディスクプールが作成されます。新しい保護計画、ポリシー、または複製ジョブの宛先としてこの新しい MSDP クラウド階層サーバーを使用する場合は、新しいストレージユニットを作成します。NetBackup Web UI またはストレージ API を使用して、この新しいディスクプール用に新しいストレージユニットを作成する必要があります。ストレージユニットは、移行プロセスで自動的には作成されません。

保護計画、ポリシー、SLP の宛先として新しいストレージユニットを使用します。既存のポリシーや SLP は移行プロセスで無効にされるため、移行した Cloud Catalyst サーバーに以前書き込んでいた既存のポリシーと SLP を有効にする必要があります。

移行が正常に完了したら、Cloud Catalyst が作成した古いオブジェクトのクリーンアップが必要になる場合があります。これを行うと、MSDP クラウド階層サーバーで不要になった、比較的少量のクラウド領域を解放できます。Cohesity は、移行が正常に完了したことを確認するまで、`cacontrol --catalog cleanupcloudcatalystobjects` コマンドの実行を数日または数週間待つことをお勧めします。このコマンドを実行すると、データにアクセスするために Cloud Catalyst に復帰できる可能性はなくなります。この手順は省略可能で、実行しない場合も機能に影響はありません。

古いオブジェクトをクリーンアップするには、次のコマンドを実行します。

```
/usr/openv/pdde/pdcr/bin/cacontrol --catalog
cleanupcloudcatalystobjects <lsuname>
```

イメージ共有への影響について

移行中、`nbdecommission` コマンドは次の質問を表示します。

```
Do you wish to skip migrating CloudCatalyst
image sharing information? (y/n) [n]:
```

ご使用の NetBackup 環境でイメージ共有機能を使用しない場合は、この質問に `y` と回答できます。

他のすべての状況で、またはご使用の環境でイメージ共有が使用されていないか不明な場合は、デフォルトの回答の `n` を残す必要があります。

Cloud Catalyst によってクラウドにアップロードされたイメージにアクセスできるようにするには、イメージ共有サーバーで追加のコマンドを実行する必要があります。このコマンドは、イメージ共有を使用する場合にのみ実行する必要があります。イメージ共有サーバーで次のコマンドを実行します。

```
/usr/openv/pdde/pdcr/bin/cacontrol
--catalog buildcloudcatalystobjects <lsuname>
```

`cacontrol --catalog buildcloudcatalystobjects <lsuname>` コマンドを実行した後、イメージ共有サーバーで NetBackup サービスを再起動します。

NetBackup アクセラレータへの影響について

バックアップが Cloud Catalyst サーバーに直接書き込まれ、ポリシーで NetBackup アクセラレータオプションを有効にしている場合、Cloud Catalyst の移行に関する特別な考慮事項があります。アクセラレータオプションは最適化にストレージサーバー名を使用しますが、そのストレージサーバー名は移行によって変更されます。したがって、移行した MSDP クラウド階層サーバーに書き込まれる最初のバックアップジョブにアクセラレータの最適化は行われません。また、移行した MSDP クラウド階層サーバーに直接書き込

む、アクセラレータが有効な複数ストリームのポリシーの場合、最初のバックアップジョブの重複排除率はゼロになる場合があります。以降のバックアップジョブでは、通常のアクセラレータの最適化率と重複排除率に戻ります。

NetBackup アクセラレータが有効なポリシーが MSDP に書き込み、次に複製ジョブを使用して Cloud Catalyst に書き込む場合、移行はそれらのポリシーに影響しません。

MachineState 設定への影響について

nbdecommission コマンドは、一部のサーバーで MachineState を administrative pause (13) に設定します。サーバーで MachineState が administrative pause (13) に設定されている場合、ジョブは実行されず、サーバーが停止しているように見える場合があります。

次のコマンドで MachineState を表示できます。

```
/usr/openv/netbackup/bin/admincmd/nbemmcmd -listhosts
-display_server -machinename myserver.test.com
-machinetype media -verbose
```

サーバーで administrative pauseMachineState を消去する必要がある場合は、次のコマンドを実行します。

```
/usr/openv/netbackup/bin/admincmd/nbemmcmd -updatehost
-machinename myserver.test.com -machinetype media
-machinestateop clr_admin_pause -masterserver mymaster.test.com
```

Cloud Catalyst の移行の -dryrun オプションについて

-dryrun オプションは nbdecommission -migrate_cloudcatalyst コマンドに追加できます。-dryrun は、移行のテスト実行として一部の環境で役立つ場合があります。-dryrun オプションでは一部の移行手順が実行されないため、このオプションを使用した実行が成功しても、実際の移行を試行した場合に成功するとはかぎりません。このオプションは、実際の移行の前に対処できるエラーを識別するのに役立ちます。

-dryrun オプションは、新しい MSDP クラウド階層サーバーを作成し、Cloud Catalyst データを移行します。その後、環境が以前の状態に戻る前に、新しく追加した MSDP クラウド階層サーバーを削除します。

メモ: -dryrun オプションでは、イメージを新しい MSDP クラウド階層サーバーに移動するためにプライマリサーバーのカタログエントリを変更しません。したがって、-dryrun オプションを使用する場合は、テストリストアや他の操作を実行してデータにアクセスできません。

-dryrun オプションを使用した後は、クラウドコンソールまたはその他のインターフェースを使用して、クラウドストレージ (AWS、Azure、その他のクラウドベンダーなど) に新しく追加されたクラウドボリュームを手動で削除する必要があります。この新しいボリュームを削除しない場合、その後の移行操作に影響します。

Cloud Catalyst の移行の cacontrol オプションについて

NetBackup には、イメージのクリーンアップと Cloud Catalyst の正常な移行に役立つ複数の cacontrol オプションがあります。

メモ: nbdecommision コマンドを実行すると cacontrol オプションが有効になるため、複数の cacontrol コマンドオプションを直接実行することは意図されていません。表 B-2 のすべてのオプションを慎重に確認してください。

表 B-2 に、Cloud Catalyst の移行中に使用できる cacontrol コマンドオプションと、その使用方法を示します。

表 B-2 cacontrol オプション

cacontrol オプション	説明
buildcloudcatalystobjects	場所: /usr/openv/pdde/pdcr/bin/cacontrol --catalog buildcloudcatalystobjects <lsuname> <lsuname> = Name of the MSDP Cloud LSU that was migrated from CloudCatalyst. このオプションは、MSDP クラウド階層への正常な移行の後に、イメージ共有用のルックアップテーブルを作成します。移行後、このコマンドをイメージ共有サーバーで実行してから、そのサーバーのサービスを再起動する必要があります。

cacontrol オプション	説明
cleanupcloudcatalystobjects	場所: /usr/openv/pdde/pdcr/bin/cacontrol --catalog cleanupcloudcatalystobjects <lsuname> <lsuname> = Name of the MSDP Cloud LSU that was migrated from CloudCatalyst. このオプションは、MSDP クラウド階層サーバーへの正常な移行の後に、未使用の Cloud Catalyst オブジェクトをクラウドから削除します。このコマンドは、移行後数日または数週間後に実行できる省略可能な手順です。このオプションは、新しい MSDP クラウド階層サーバーに不要な Cloud Catalyst オブジェクトをクリーンアップします。このコマンドを実行すると Cloud Catalyst に復帰してデータにアクセスできなくなるため、移行が確実に成功した場合のみ実行してください。
migratecloudcatalyst	場所: /usr/openv/pdde/pdcr/bin/cacontrol --catalog migratecloudcatalyst <lsuname> <cloudcatalystmaster> <cloudcatalystmedia> [skipimagesharing] [start_with] <lsuname> = Name of the MSDP Cloud LSU to be migrated from CloudCatalyst. <cloudcatalystmaster> = Master server name. <cloudcatalystmedia> = Media server hostname of the CloudCatalyst server to be migrated. [skipimagesharing] = Flag which indicates to skip migrating the image sharing data from CloudCatalyst to the new MSDP Cloud LSU. [start_with] = Indicates the point at which to resume a failed migration after the cause of the failure has been addressed. nbdecommission -migrate_cloudcatalyst コマンドが必要に応じてこの cacontrol コマンドを呼び出します。この cacontrol は直接実行しないでください。代わりに、nbdecommission -migrate_cloudcatalyst コマンドを使用して移行を実行してください。

cacontrol オプション	説明
migratecloudcatalyststatus	場所: /usr/openv/pdde/pdcr/bin/cacontrol --catalog migratecloudcatalyststatus <lsuname> <lsuname> = Name of the MSDP Cloud LSU being migrated from CloudCatalyst. nbdecommission -migrate_cloudcatalyst コマンドが必要に応じてこの cacontrol コマンドを呼び出します。この cacontrol は直接実行しないでください。代わりに、nbdecommission -migrate_cloudcatalyst コマンドを使用して移行を実行してください。

正常な移行から Cloud Catalyst への復帰

Cloud Catalyst に戻す (復帰) 処理では、nbdecommission -migrate_cloudcatalyst コマンドを実行する前に、プライマリサーバーカタログに対して NetBackup カタログバックアップが実行されたと想定します。そのような NetBackup カタログバックアップイメージがない場合、移行プロセスによって NetBackup カタログが変更されるため、Cloud Catalyst に復帰できません。

また、復帰処理では、移行した MSDP クラウド階層サーバーでコマンド /usr/openv/pdde/pdcr/bin/cacontrol --catalog cleanupcloudcatalystobjects が実行されていないと想定します。これは、そのコマンドを一度実行すると、Cloud Catalyst に復帰できないためです。

Cloud Catalyst が書き込んだイメージと、移行の完了後に期限切れになったイメージは、クラウドストレージから削除されています。これらのデータは存在しないため、Cloud Catalyst に復帰しても、これらのイメージはリストアに利用できません。

NetBackup プライマリサーバーのカタログリカバリを実行する場合のすべての注意事項と制限事項が適用されます。詳しくは、『NetBackup 管理者ガイド』でカタログリカバリの詳細について説明されているセクションを参照してください。具体的には、カタログバックアップイメージが作成された時点以降は、MSDP サーバーまたは他のストレージサーバーにデータは書き込まれず、利用できません。NetBackup プライマリサーバーのカタログリカバリが実行された後は、データをリストアに利用できません。

次のいずれかの手順を使用して、Cloud Catalyst に復帰できます。

- 「サーバーの状態が移行の実行時と同じである場合の Cloud Catalyst への復帰」
- 「移行の実行時にサーバーが再利用または再インストールされた場合の Cloud Catalyst への復帰」

次の手順では、Cloud Catalyst サーバーが移行時と同じ状態で、すべてのサービスが停止されていると想定しています。

サーバーの状態が移行の実行時と同じである場合の Cloud Catalyst への復帰

1. 新しい MSDP クラウド階層サーバーで NetBackup サービスを停止します。
2. NetBackup Web UI を開きます。
3. [リカバリ (Recovery)]をクリックします。次に、[NetBackup カタログリカバリ (NetBackup catalog recovery)]をクリックします。
4. Cloud Catalyst を MSDP クラウド階層サーバーに移行する `nbdecommission -migrate_cloudcatalyst` コマンドを実行する前に作成した、カタログバックアップイメージを選択します。
5. ウィザードのすべての手順を完了して、NetBackup カタログをリカバリします。
6. プライマリサーバーで NetBackup サービスを停止して再起動します。
7. Cloud Catalyst サーバーの `esfs.json` ファイルで、`ReadOnly` が `0` に設定されていることを確認します。

   リストアのみを実行する必要があり、Cloud Catalyst に対して新しいバックアップジョブまたは複製ジョブを実行しない場合は、`ReadOnly` を `1` に設定します。
8. Cloud Catalyst サーバーで NetBackup サービスを開始します。
9. Cloud Catalyst ストレージサーバーがオンラインになったら、リストアジョブ、バックアップジョブ、最適化複製ジョブを続行できます。

   バックアップジョブまたは最適化複製ジョブは、`esfs.json` ファイルで `ReadOnly` を `0` に設定する必要があります。
10. 8.2 より前のバージョンの Cloud Catalyst (8.1、8.1.1、8.1.2 など) を実行している場合は、メディアサーバーに新しいホスト名ベースの証明書の配備が必要な場合があります。プライマリサーバーで次のコマンドを実行して、証明書を配備できます。

    ```
    /usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert
    <CloudCatalyst host-name>
    ```

    Cloud Catalyst サーバーで NetBackup サービスを再起動する必要があります。

11 Cloud Catalyst でクラウドストレージのバケットからの読み取りを許可するには、次のコマンドの実行が必要な場合があります。

```
/usr/openv/esfs/bin/setlsu_ioctl
<cachedir>/storage/proc/cloud.lsu <bucketname>
```

このコマンドが不要な場合に実行しても、問題はありません。このコマンドを実行すると、次の出力が表示されます。

```
return code: -1

File exists.
```

12 (オプション) 無駄な領域を防ぎ、今後 MSDP クラウド階層サーバーに移行する際に問題が発生しないようにするため、クラウドストレージで MSDP クラウドのサブバケットフォルダ全体を削除します。

次の手順では、Cloud Catalyst サーバーが MSDP クラウド階層サーバーとして再利用または再インストールされたか、他の何らかの理由で利用できない場合を想定しています。

移行の実行時にサーバーが再利用または再インストールされた場合の Cloud Catalyst への復帰

1 新しい MSDP クラウド階層サーバーで NetBackup サービスを停止します。

2 NetBackup Web UI を開きます。

3 [リカバリ (Recovery)]をクリックします。次に、[NetBackup カタログリカバリ (NetBackup catalog recovery)]をクリックします。

4 Cloud Catalyst を MSDP クラウド階層サーバーに移行する `nbdecommission -migrate_cloudcatalyst` コマンドを実行する前に作成した、カタログバックアップイメージを選択します。

5 ウィザードのすべての手順を完了して、NetBackup カタログをリカバリします。

6 プライマリサーバーで NetBackup サービスを停止して再起動します。

7 移行時に有効だった NetBackup バージョンと EEB バンドルを使用して、Cloud Catalyst サーバーを再インストールします。

8 その後、Cohesity テクニカルサポートに問い合わせて、rebuild_esfs プロセスを使用してクラウドストレージ内のデータからその Cloud Catalyst サーバーをリカバリします。(rebuild_esfs プロセスは Cloud Catalyst サーバーをリカバリするための方法で、古い drcontrol メソッドよりも優先されます。drcontrol メソッドは非推奨です。)

9 (オプション) 無駄な領域を防ぎ、今後 MSDP クラウド階層サーバーに移行する際に問題が発生しないようにするため、クラウドストレージで MSDP クラウドのサブバケットフォルダ全体を削除します。

失敗した移行から Cloud Catalyst への復帰

正常な移行と失敗した移行の試行の両方で Cloud Catalyst に復帰する最も安全な方法は、NetBackup プライマリサーバーカタログをリカバリすることです。ただし、プライマリサーバーカタログをリカバリせずに、失敗した移行の試行から Cloud Catalyst に復帰できる場合があります。

次のメッセージが表示される前にエラーが発生して nbdecommission コマンドが終了した場合は、プライマリサーバーカタログをリカバリせずに Cloud Catalyst に復帰できる可能性があります。コマンドの出力または nbdecommission コマンドの admin ログファイルに、次のメッセージが表示されます。

```
Disk pool <new disk pool name> has been successfully
created with 1 volumes
```

Disk pool メッセージが表示された後に移行エラーが発生した場合、Cloud Catalyst に復帰するにはプライマリサーバーカタログのリカバリが必要です。

プライマリサーバーカタログをリカバリしない場合は、新しいディスクプール、ディスクボリューム、クラウドストレージサーバー、MSDP クラウド階層サーバーを手動で削除する必要があります。Cloud Catalyst に復帰した後にこれらを削除する必要があります。

次の手順では、Disk pool メッセージが出力される前に移行が失敗すると想定しています。また、この手順では、移行時に Cloud Catalyst サーバーを MSDP クラウド階層サーバーとして再利用しないと想定しています。

失敗した移行の後の Cloud Catalyst への復帰

1 新しい MSDP クラウド階層サーバーで NetBackup サービスを停止します。

2 Cloud Catalyst サーバーの esfs.json ファイルので、ReadOnly が 0 に設定されていることを確認します。

リストアのみを実行する必要があり、Cloud Catalyst に対して新しいバックアップジョブまたは複製ジョブを実行しない場合は、ReadOnly を 1 に設定します。

3 Cloud Catalyst サーバーで NetBackup サービスを開始します。

4 Cloud Catalyst ストレージサーバーがオンラインになったら、リストアジョブ、バックアップジョブ、最適化複製ジョブを続行できます。

バックアップジョブまたは最適化複製ジョブは、esfs.json ファイルで ReadOnly を 0 に設定する必要があります。

5 8.2 以前のバージョンの Cloud Catalyst を実行している場合は、メディアサーバーに新しいホスト名ベースの証明書の配備が必要な場合があります。プライマリサーバーで次のコマンドを実行して、証明書を配備できます。

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert
<CloudCatalyst host-name>
```

Cloud Catalyst サーバーで NetBackup サービスを再起動する必要があります。

6 Cloud Catalyst でクラウドストレージのバケットからの読み取りを許可するには、次のコマンドの実行が必要な場合があります。

```
/usr/openv/esfs/bin/setlsu_ioctl
<cachedir>/storage/proc/cloud.lsu <bucketname>
```

このコマンドが不要な場合に実行しても、問題はありません。このコマンドを実行すると、次の出力が表示されます。

```
return code: -1

File exists.
```

7 (オプション) 無駄な領域を防ぎ、今後 MSDP クラウド階層サーバーに移行する際に問題が発生しないようにするため、クラウドストレージで MSDP クラウドのサブバケットフォルダ全体を削除します。

次の手順では、MSDP クラウド階層サーバーとして再利用または再インストールされた Cloud Catalyst サーバーで移行が失敗した場合を想定しています。

Cloud Catalyst サーバーが再利用された場合の失敗した移行の後の Cloud Catalyst への復帰

1 新しい MSDP クラウド階層サーバーで NetBackup サービスを停止します。

2 移行時に有効だった NetBackup バージョンと EEB バンドルを使用して、Cloud Catalyst サーバーを再インストールします。

3 その後、Cohesity テクニカルサポートに問い合わせて、`rebuild_esfs` プロセスを使用してクラウドストレージ内のデータからその Cloud Catalyst サーバーをリカバリします。(`rebuild_esfs` プロセスは Cloud Catalyst サーバーをリカバリするための方法で、古い `drcontrol` メソッドよりも優先されます。`drcontrol` メソッドは非推奨です。)

4 (オプション) 無駄な領域を防ぎ、今後 MSDP クラウド階層サーバーに移行する際に問題が発生しないようにするため、クラウドストレージで MSDP クラウドのサブバケットフォルダ全体を削除します。

C

Encryption Crawler

この付録では以下の項目について説明しています。

Encryption Crawler について

Encryption Crawler は、暗号化されていないデータがないかどうかを確認するため、すべての MSDP プールを検索します。既存のデータコンテナをすべて走査し、暗号化されていないデータセグメントを見つけると、そのセグメントを AES-256-CTR アルゴリズムで暗号化します。KMS が有効な場合、Encryption Crawler は、KMS 自動変換プロセスが処理しなかったデータセグメントの暗号化キーを暗号化します。KMS 自動変換プロセスでは、既存のすべての暗号化データの暗号化キーが暗号化されます。

p.111 の「NetBackup Key Management Server サービスを使用した MSDP 暗号化について」を参照してください。

ユーザーがすべてのデータを暗号化しようとしても、いくつかの条件が重なることで、暗号化されていないデータセグメントが MSDP プールに残る場合があります。

- プールが構成されている場合、暗号化は有効になりません。暗号化は、バックアップデータがプールに取り込まれた後にのみ有効になります。

- encrypt キーワードは、MSDP の contentrouter.cfg の ServerOptions オプションには追加されません。この場合、MSDP ホスト、負荷分散メディアサーバー、独自の (BYO) サーバー、および NetBackup Client Direct に存在する可能性があるすべての pd.conf では暗号化は有効になりません。

遅延したバックアップが、暗号化されていないデータを参照したり、古いイメージの期限が切れても処理を終了しない場合があります。Encryption Crawler は、MSDP プールに存在する、これまで暗号化されていないすべての既存データを暗号化するために使用されます。

Encryption Crawler では、暗号化が正しく構成されている必要があります。encrypt キーワードは、MSDP の contentrouter.cfg の ServerOptions オプションに追加する必要があります。インスタントアクセスまたはユニバーサル共有が構成されている場合、Encryption Crawler では、暗号化が VpFS に対して有効になっている必要があります。さらに、暗号化を有効にした後、既存のすべての VpFS 共有についてチェックポイントを作成する必要があります。環境が NetBackup 8.1 より前のリリースからアップグレードされる場合、Encryption Crawler はすべてのローリングデータ変換プロセスを完了している必要があります。

Encryption Crawler の 2 つのモードについて

Encryption Crawler はデフォルトではオンになりません。crcontrol コマンドを使用して明示的に有効にする必要があります。Encryption Crawler には、グレースフルモードとアグレッシブモードの 2 つのモードがあります。これらの 2 つのモードは、特定のジョブがどのように実行されるかに影響します。以下の情報を確認して、お使いの環境に適したモードを選択してください。

グレースフルモード

ユーザーが crcontrol --encconvertlevel コマンドを使用して別のモードを指定しないかぎり、Encryption Crawler のデフォルトのモードはグレースフルです。このモードでは、MSDP プールが比較的アイドル状態であり、圧縮ジョブまたは CRQP ジョブが実行中でない場合にのみ Encryption Crawler が実行されます。通常、MSDP プールがアイドル状態のときは、MSDP プールでバックアップ、リストア、複製、またはレプリケーションのジョブが実行中でないことを意味します。システムが過負荷にならないようにするため、Encryption Crawler は継続的には実行されません。Encryption Crawler がグレースフルモードの場合、完了までに時間がかかることがあります。

グレースフルモードは、MSDP プールが比較的アイドル状態かどうかを確認します。各データコンテナを処理する前に、MSDP プールの I/O 統計情報を計算してプールの状態を確認し、圧縮ジョブまたは CRQP ジョブが実行中でないことを確認します。MSDP プールがアイドル状態ではなく、圧縮ジョブや CRQP ジョブが実行中である場合は一時停止します。多くの場合、バックアップ、リストア、複製、またはレプリケーションのジョブが MSDP プールで実行中になっていると、グレースフルモードは一時停止します。

実行中の NetBackup ジョブのデータ重複排除率が高い場合、I/O 操作率が低く、MSDP プールが比較的アイドル状態になる傾向があります。この場合、実行中の圧縮ジョブや CRQP ジョブがないと、グレースフルモードが実行されることがあります。

MSDP 指紋キャッシュのロードが進行中の場合、MSDP プールの I/O 操作率は低くはありません。この場合、グレースフルモードは一時停止し、指紋キャッシュのロードが完了するまで待機することがあります。Encryption Crawler は spoold ログを監視し、ThreadMain: Data Store nodes have completed cache loading で始まるメッセージを待機してから処理を再開します。spoold ログは *storage_path*/log/spoold/spoold.log にあります。圧縮ジョブまたは CRQP ジョブが実行中かどうかを確認するには、crcontrol --processqueueinfo または crcontrol --compactstate コマンドを実行します。

グレースフルモードをより速く実行するには、詳細オプションの CheckSysLoad、BatchSize、および SleepSeconds を使用して、グレースフルモードの動作とパフォーマンスをチューニングします。BatchSize の値を大きくし、SleepSeconds の値を小さくすると、グレースフルモードはより継続的に実行されます。

CheckSysLoad をオフにすると、バックアップ、リストア、複製、レプリケーション、圧縮、または CRQP のジョブが実行中であってもグレースフルモードが実行されます。このような変更は、グレースフルモードをよりアクティブにできますが、アグレッシブモードほどアクティブにはなりません。

アグレッシブモード

このモードでは、Encryption Crawler は CRC チェックと圧縮を無効にします。バックアップ、リストア、複製、レプリケーション、または CRQP のジョブの実行中に Encryption Crawler が実行されます。

アグレッシブモードは、バックアップ、リストア、複製、レプリケーションのジョブのパフォーマンスに影響します。影響を最小限に抑えるには、グレースフルモードを使用します。これを選択すると、システムがビジー状態のときに暗号化プロセスが一時停止し、このプロセスの速度が低下する可能性があります。アグレッシブモードは、システムの状態に関係なく、プロセスのアクティブ状態を維持し、継続的に実行します。

次に示すのは、アグレッシブモードが有効な場合に考慮する必要のある事項です。

- ユーザー入力と前回までの進捗は、MSDP の再起動時に保持されます。リカバリするためにコマンドを再実行する必要はありません。Encryption Crawler によって自動的にリカバリされ、前回までに進んだ箇所から続行されます。
- MSDP の contentrouter.cfg ファイルにある ServerOptions オプションの encrypt キーワードを使用して暗号化を適用する必要があります。また、Encryption Crawler を有効にする前に MSDP を再起動する必要があります。そうしないと、Encryption Crawler は有効と表示されません。

- NetBackup 8.1 より前のリリースから環境をアップグレードした場合は、Encryption Crawler を有効にする前に、ローリングデータ変換が完了するまで待機する必要があります。待機しないと、Encryption Crawler は有効と表示されません。
- Encryption Crawler プロセスが完了した後に同じ処理を繰り返すことはできません。暗号化を有効にする前に存在したデータのみが非暗号化されます。新しいデータはすべてインラインで暗号化され、スキャンとクロールは必要ありません。
- Encryption Crawler プロセスの完了後に暗号化の適用を無効にすると、Encryption Crawler の状態はリセットされます。暗号化が再度適用されたときに、Encryption Crawler プロセスを再起動できます。完了に必要な時間は、次の項目によって異なります。
  - 暗号化されていない新しいデータを取り込む量。
  - MSDP プールに存在するデータの量。

グレースフルモードとアグレッシブモードのリソース使用率

メモリ: Encryption Crawler は、MSDP パーティションごとに 1 GB の追加メモリを消費する場合があります。グレースフルモードは、アグレッシブモードより少ないメモリを消費します。

CPU: Encryption Crawler は、AES-256-CTR アルゴリズムを使用したデータの暗号化に主に CPU を使用します。CPU 使用率は、同じ量のデータをバックアップするよりも少なくなります。処理中は、指紋の取得や、コンポーネント間またはノード間のデータ転送は行われません。

ディスク I/O: Encryption Crawler は、特にアグレッシブモードで I/O を集中的に行います。アグレッシブモードは、I/O で実行中のジョブと大きく競合し、バックアップジョブより多くの I/O をコミットする可能性があります。

Encryption Crawler の管理

Encryption Crawler を管理するには、`crcontrol` コマンドを使用します。次の表に、Encryption Crawler の動作を管理するために使用するオプションを示します。

表 C-1 `crcontrol` コマンドオプション

オプション	説明
`--encconverton`	Encryption Crawler プロセスを有効にして開始するには、`--encconverton [num]` を使用します。 *num* 変数は省略可能で、パーティションインデックスの数 (1 から開始) を示します。このパラメータにより、指定した MSDP パーティションに対して Encryption Crawler が有効になります。 *num* を指定しない場合、すべての MSDP パーティションに対して有効になります。 `/etc/nbapp-release` ファイル (Linux) または `c:¥etc¥nbapp-release` ファイル (Windows) がない場合、*num* 変数は BYO 設定でサポートされません。BYO 設定で、複数のボリュームのサポートを有効にするファイルを作成すると、*num* 変数がサポートされます。 例: `[root@vrawebsrv4663 ~]# /usr/openv/pdde/pdcr/bin/crcontrol --encconverton Encryption conversion turned on for all partitions` p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。
`--encconvertoff`	Encryption Crawler プロセスを無効にして停止するには、`--encconvertoff [num]` を使用します。 *num* 変数は省略可能で、パーティションインデックスの数 (1 から開始) を示します。このパラメータにより、指定した MSDP パーティションに対して Encryption Crawler が有効になります。 *num* を指定しない場合、すべての MSDP パーティションに対して無効になります。 `/etc/nbapp-release` ファイル (Linux) または `c:¥etc¥nbapp-release` ファイル (Windows) がない場合、*num* 変数は BYO 設定でサポートされません。BYO 設定で、複数のボリュームのサポートを有効にするファイルを作成すると、*num* 変数がサポートされます。 p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。

オプション	説明

`--encconvertlevel`	グレースフルモードとアグレッシブモードを切り替えるには、`--encconvertlevel level` を使用します。
	
	level は必須です。
	
	■ *level* 変数の値 1 は、グレースフルモードのデフォルト値です。
	例:
	`/usr/openv/pdde/pdcr/bin/crcontrol --encconvertlevel 1`
	■ *level* 変数の値が 2 から 4 の場合は、アグレッシブモードが有効であることを示します。数値が大きいほど、Encryption Crawler がよりアグレッシブになることを示します。
	例:
	`/usr/openv/pdde/pdcr/bin/crcontrol --encconvertlevel 2`

`--encconvertstate`	Encryption Crawler プロセスのモードと進捗状況を決定するには、`--encconvertstate [verbose]` を使用します。 必要に応じ、このオプションには詳細レベル (0 から 2) を指定できます。 ■ 0 はデフォルトの詳細レベルで、全体の簡単な概要情報を示します。 ■ 1 は、全体の概要情報と各パーティションの詳細情報を示します。 ■ 2 は、全体の概要情報と各パーティションの詳細情報を示します。パーティションに対するプロセスが終了しても、パーティションの詳細情報が表示されます。 `/etc/nbapp-release` ファイル (Linux) または `c:¥etc¥nbapp-release` ファイル (Windows) がない場合、`verbose` パラメータは BYO 設定でサポートされません。BYO 設定で、複数のボリュームのサポートを有効にするファイルを作成すると、*num* 変数がサポートされます。 例: `/usr/openv/pdde/pdcr/bin/crcontrol --encconvertstate 2` p.56 の「MSDP 用のストレージのプロビジョニングについて」を参照してください。

Encryption Crawler を有効にすると、`crcontrol --encconvertstate` コマンドを使用して、状態、モード、進捗状況を監視できます。

表 C-2 Encryption Crawler モニター

項目	説明
状態 (Status)	Encryption Crawler の状態 (オン、オフ、完了) を示します。
レベル (Level)	Encryption Crawler のレベルとモードを示します。値は「モード (レベル)」の形式で表されます (例: グレースフル (1))。
ビジー (Busy)	Encryption Crawler がビジー状態かどうかを示します。
最大グループ ID (Max Group ID)	Encryption Crawler がオンの場合に処理するコンテナグループ ID の最大値。これはデータ境界であり、Encryption Crawler がオンになると変更されることはありません。
現在のグループ ID (Current Group ID)	現在処理しているグループ ID を示します。
現在のコンテナ ID (Current Container ID)	現在処理しているコンテナ ID を示します。
コンテナの推定数 (Containers Estimated)	Encryption Crawler が処理する必要がある、MSDP プール内のデータコンテナの推定数。これは統計情報であり、パフォーマンス上の理由により正確でない場合があります。この値は、Encryption Crawler をオンにした後は更新されません。
スキャンされたコンテナの数 (Containers Scanned)	Encryption Crawler が処理する必要があるデータコンテナの数。
変換されたコンテナの数 (Containers Converted)	Encryption Crawler のプロセスで暗号化されたコンテナの数。
スキップされたコンテナの数 (Containers Skipped)	Encryption Crawler がスキップしたデータコンテナの数。理由はさまざまであり、「「スキップされたデータコンテナについて」」で説明されています。 スキップされたデータコンテナがある場合は、Encryption Crawler ログまたは履歴ログで詳細を確認できます。`encryption_reporting` ツールは、Encryption Crawler プロセスの完了後、個々のコンテナをレポートして暗号化するのに役立ちます。この `encryption_reporting` ツールの詳細情報が利用可能です。 p.794 の「データの暗号化」を参照してください。 p.795 の「コマンドの使用の出力例」を参照してください。
スキャンされたデータのサイズ (Data Size Scanned)	[スキャンされたコンテナの数 (Containers Scanned)]のスキャン済みデータコンテナのデータサイズの合計。

項目	説明
変換されたデータのサイズ (Data Size Converted)	[変換されたコンテナの数 (Containers Converted)]の変換済みデータコンテナのデータサイズの合計。
進捗状況 (Progress)	Encryption Crawler がスキャンしたデータコンテナの推定合計数の割合。 進捗状況 = スキャンされたコンテナの数 / コンテナの推定数
変換率 (Conversion Ratio)	Encryption Crawler が変換した、スキャン済みデータのサイズの割合。 変換率 = 変換されたデータのサイズ / スキャンされたデータのサイズ
マウントポイントの情報 (Mount Points Information)	各マウントポイントの状態。 `--encconvertstate` オプションに詳細度を示す値 1 を指定すると、未完了のマウントポイントの詳細が出力されます。 `--encconvertstate` オプションに詳細度を示す値 2 を指定すると、完了状態に関係なく、すべてのマウントポイントの詳細が出力されます。

ログの進捗状況行を使用すると、Encryption Crawler の所要時間を推定できます。たとえば、プールの 3.3% が 24 時間で完了している場合、プロセスの完了には約 30 日かかります。

メモ: Encryption Crawler は、新しいものから順にデータコンテナを処理します。

暗号化の適用後に新しいデータをバックアップすることは可能ですが、Encryption Crawler を有効にする前に行ってください。この場合、新しいデータコンテナの[変換率 (Conversion Ratio)]が最初は 99% 未満になることがあります。プロセスの実行中は、[変換率 (Conversion Ratio)]の値が高くなることがあります。これは、暗号化されていないデータが、古いデータコンテナの方に多く存在する可能性があるためです。このような場合、[変換率 (Conversion Ratio)]、[変換されたコンテナの数 (Containers Converted)]、[コンテナの推定数 (Containers Estimated)]を参照すると、これらのデータコンテナの処理にかかる時間を推定するのに役立ちます。

Encryption Crawler が有効なときに[変換率 (Conversion Ratio)]の変化を監視すると、暗号化されていないデータの割合がわかることがあります。

メモ: 暗号化プロセスの間、進捗状況は MSDP が再起動しても続きます。

スキップされたデータコンテナについて

[スキップされたコンテナの数 (Containers Skipped)]が示すように Encryption Crawler が一部のデータコンテナをスキップするのは、次のような理由からです。

- データコンテナが期限切れになるがまだ削除されていない場合、そのデータコンテナはスキップされます。
- データコンテナにデータ整合性の問題の可能性がある場合、そのデータコンテナはスキップされます。Encryption Crawler はコンテナを CRC チェックプロセスに伝えてコンテナを識別し、場合によってはコンテナを修正します。
- インスタントアクセスまたはユニバーサル共有が構成されており、Encryption Crawler プロセスの前に一部の共有にチェックポイントが作成されていない場合、その共有が、排他的な権限付きでデータコンテナをいくつか保持することがあります。このようなデータコンテナはスキップされます。Cohesity では、Encryption Crawler プロセスをオンにする前に、インスタントアクセスまたはユニバーサル共有のすべての共有について、チェックポイントを作成することをお勧めしています。そうすることで、VpFS はこれらのデータコンテナの排他的な権限を解放し、spoold と Encryption Crawler で処理できるようになります。
- 3.1.2 リリース以降のアプライアンスは、インスタントアクセスまたはユニバーサル共有が構成されている場合でも、VpFS root 共有 vpfs0 が予約する空のデータコンテナを所有する場合があります。この状況は、インスタントアクセスまたはユニバーサル共有が構成されている BYO 設定でも発生する可能性があります。通常、VpFS はこのようなデータコンテナの排他的な権限を解放しません。このようなデータコンテナはスキップされます。スキップされたこれらのコンテナは無視できます。

  スキップされたデータコンテナが空かどうか、および VpFS root 共有 vpfs0 がそれらを所有しているかどうかを確認する方法は次のとおりです。VpFS が所有する他のデータコンテナも同様の方法で確認できます。

  - VpFS が所有していると判定され、スキップされたデータコンテナは、Encryption Crawler ログの次の箇所で見つけることができます。

    ```
    n152-h21:/home/maintenance # grep VpFS
    /msdp/data/dp1/pdvol/log/spoold/enccrawler.log
    February 04 05:13:14 WARNING [139931343951616]: -1:
    __getDcidListFromOneGroup: 1 containers owned by VpFS in group
    7 were skipped. min DC ID 7168, max DC ID 7168
    ```

  - VpFS root 共有 vpfs0 がデータコンテナを所有しているかどうかを確認します。

    ```
    n152-h21:/home/maintenance # cat /msdp/data/dp1/4pdvol/7/.shareid
    vpfs0
    106627568
    ```

- VpFS root 共有 vpfs0 が所有するデータコンテナは空です。

```
n152-h21:/home/maintenance # ls -Al /msdp/data/dp1/4pdvol/7
total 24
-rw-r--r-- 1 root root 64 Feb 1 02:40 7168.bhd
-rw-r--r-- 1 root root 0 Feb 1 02:40 7168.bin
-rw------- 1 root root 12 Feb 1 02:40 .dcidboundary
-rw-r----- 1 root root 15 Feb 1 02:40 .shareid
drwxr-xr-x 3 root root 96 Feb 4 15:37 var
n152-h21:/home/maintenance # /usr/openv/pdde/pdcr/bin/dcscan 7168
Path = /msdp/data/dp1/4pdvol/7/7168.[bhd, bin]
*** Header for container 7168 ***
version : 1
flags : 0x4000(DC_ENTRY_SHA256)
data file last position : 0
header file last position : 64
source id : 0
retention : 0
file size : 0
delete space : 0
active records : 0
total records : 0
deleted records : 0
crc32 : 0x1d74009d
```

詳細オプション

contentrouter.cfg の EncCrawler セクションに表示されるオプションを指定して、Encryption Crawler のデフォルトの動作を変更できます。オプションはグレースフルモードにのみ影響します。また、これらのオプションはデフォルトでは存在しません。必要に応じて追加する必要があります。

これらの値のいずれかを変更した後、変更を有効にするには、Encryption Crawler プロセスを再起動する必要があります。crcontrol コマンド、および --encconvertoff オプションと --encconverton オプションを使用して、Encryption Crawler プロセスを再起動します。MSDP サービスを再起動する必要はありません。

初期チューニングの後、実行中のジョブの進捗状況やシステムへの影響を確認できます。必要に応じて、いつでもプロセスの途中でさらにチューニングできます。

表 C-3 詳細オプション

オプション	値	説明
SleepSeconds	型: 整数 範囲: 1-86400 デフォルト: 5	このオプションは、データコンテナのバッチを処理した後のグレースフルモードのアイドル時間です。デフォルト設定は 5 秒で、範囲は 1 から 86400 秒です。
BatchSize	型: 整数 範囲: 1-INT_MAX デフォルト: 20	このオプションは、アイドル時間にグレースフルモードがバッチとして処理するデータコンテナの数です。デフォルト設定は 20 です。
CheckSysLoad	型: ブール値 範囲: yes または no デフォルト: yes	実行中のバックアップ、リストア、複製、レプリケーション、圧縮、または CRQP のジョブが検出された場合、グレースフルモードは実行されません。 このオプションを no に設定した場合、グレースフルモードはチェックを実行しません。代わりに、いくつかの BatchSize データコンテナを処理し、SleepSeconds で指定した秒数の間スリープしてから別のバッチを処理し、再びスリープします。このプロセスが、完了するまで続きます。

チューニングオプション

グレースフルモードのチューニング

グレースフルモードを高速化するには、CheckSysLoad、BatchSize、SleepSeconds の各オプションを活用して、グレースフルモードの動作とパフォーマンスをチューニングします。

p.790 の「詳細オプション」を参照してください。

BatchSize の値を大きくし、SleepSeconds の値を小さくすると、グレースフルモードはより継続的に実行されます。CheckSysLoad をオフにすると、バックアップ、リストア、複製、レプリケーション、圧縮、または CRQP のジョブが実行中であっても、グレースフルモードのままになります。このような変更は、グレースフルモードをよりアグレッシブにはできますが、アグレッシブモードほどにはなりません。利点は、チューニングされたグレースフルモードが、バックアップ、リストア、複製、レプリケーションのジョブのアグレッシブモードより、システムパフォーマンスに与える影響が少ないことです。影響は、最も低いレベル 2 のアグレッシブモードより少なくなります。代わりに、特に CheckSysLoad が無効な場合は、準アグレッシブになります。これは、実行中のジョブのシステムパフォーマンスに影響する可能性があり、CRC チェック、CRQP 処理、または圧縮の実行と完了にかかる時間が長くなります。

アグレッシブモードのチューニング

アグレッシブモードには 3 つのレベル (2 から 4) があります。レベルが高いほどアグレッシブになり、通常は Encryption Crawler のパフォーマンスが向上します。また、バックアップ、リストア、複製、レプリケーションのジョブのシステムパフォーマンスへの影響が大きくなります。

Encryption Crawler で最適なパフォーマンスを実現するには、システムへの日常的な負荷に応じて、アグレッシブモードのレベル 2 から 4 を使用します。それ以外の場合は、グレースフルモードのレベル 1 を使用します。高レベルのアグレッシブモードを使用しても、Encryption Crawler と実行中のジョブの両方でシステムパフォーマンスが全体的に向上するわけではないことに注意してください。アグレッシブモードがグレースフルモードより優れたパフォーマンスを発揮するわけでもありません。最適なレベルを見極めるには、Encryption Crawler の進捗状況と、実行中のジョブがシステムに与える影響の監視が必要な場合があります。

半日から数日にかけて、アグレッシブモードとグレースフルモードを動的に切り替えることも検討してください。変更は、毎日のシステム負荷や実行中のジョブのパターンに基づいて行ってください。動的な切り替えにより、どちらのモードがお使いの環境に適しているかを判断しやすくなります。

p.784 の「Encryption Crawler の管理」を参照してください。

p.782 の「Encryption Crawler の 2 つのモードについて」を参照してください。

システムへの影響を軽減するため、一部の MSDP パーティションに対して Encryption Crawler をオンにする

アグレッシブモードは、バックアップ、リストア、複製、レプリケーションのジョブのパフォーマンスに影響します。アグレッシブモードほどの影響はありませんが、チューニングしたグレースフルモードも同様です。システムへの影響を軽減するため、一部の MSDP パーティションに対して Encryption Crawler を選択的に同時にオンにできます。

MSDP パーティションに対して DataStore への書き込みを選択的に無効にして、システムへの影響を軽減する

アグレッシブモードは、バックアップ、リストア、複製、レプリケーションのジョブのパフォーマンスに影響します。アグレッシブモードほどの影響はありませんが、チューニングしたグレースフルモードも同様です。システムへの影響を軽減するため、Encryption Crawler を実行する MSDP パーティションに対して DataStore への書き込みを選択的に無効にできます。これは、BYO 設定用の `crcontrol --dswriteoff` コマンドを使用することで実行できます。NetBackup Appliance の場合は、CLISH を介してコマンドを実行する必要があります。そうしない場合、NetBackup Appliance はしばらくしてから自動的に状態をリセットします。

パーティションに新しいバックアップデータを取り込むには、プロセスの完了時に DataStore への書き込み状態をリセットする必要があります。

Encryption Crawler のチューニングに関する推奨事項

表 C-4　チューニングに関する推奨事項

処理	説明
デフォルト設定を使用して、グレースフルモードで Encryption Crawler をオンにする。	Cohesity では、指紋キャッシュのロードが完了するまで待機してから、バックアップを実行したり、Encryption Crawler をオンにしたりすることをお勧めしています。起動タイミングは、spoold ログを監視し、ThreadMain: Data Store nodes have completed cache loading で始まるメッセージが表示されるまで待機してから決定してください。 Encryption Crawler は、デフォルトでは起動時にグレースフルモードになっています。Encryption Crawler の起動後、通常のバックアップ、複製、レプリケーションのジョブで 24 時間から 48 時間実行します。この時間が経過すると、Encryption Crawler の進捗状況を crcontrol --encconvertstate コマンドで確認できます。 Encryption Crawler プロセスを確認したら、まずは[進捗状況 (Progress)]項目で Encryption Crawler の進捗状況を確認します。進捗がない、または予測した速さで進捗していない場合は、プロセスを高速化するために変更を加える必要があります。[進捗状況 (Progress)]項目を使用すると、Encryption Crawler の所要時間を推定できます。たとえば、プールの 3.3% が 24 時間で完了している場合、プロセスの完了には約 30 日かかります。 進捗が想定より遅い場合は、このプロセスで示すように、Encryption Crawler の処理速度が速くなるように調整します。Encryption Crawler は新しいものから順にデータコンテナを処理する点に注意してください。暗号化の適用後に新しいデータをバックアップすることは可能ですが、Encryption Crawler を有効にする前に行ってください。この場合、新しいデータコンテナの[変換率 (Conversion Ratio)]が最初は 99% 未満になることがあります。プロセスが実行中の場合は、[変換率 (Conversion Ratio)]の値が高くなることがあります。これは、暗号化されていないデータが、古いデータコンテナの方に多く存在する可能性があるためです。このような場合、[変換率 (Conversion Ratio)]、[変換されたコンテナの数 (Containers Converted)]、[コンテナの推定数 (Containers Estimated)]を参照すると、これらのデータコンテナの処理にかかる時間を推定するヒントが見つかる場合があります。Encryption Crawler が有効なときに[変換率 (Conversion Ratio)]の変化を監視すると、暗号化されていないデータの割合に関するヒントが見つかる場合があります。 p.784 の「Encryption Crawler の管理」を参照してください。

処理	説明
処理が速くなるようにグレースフルモードをチューニングする。	「「グレースフルモードのチューニング」」の情報を使用して、グレースフルモードの処理をスピードアップできます。初期チューニングの後、実行中のジョブの進捗状況やシステムへの影響の確認がときどき必要になる場合があります。必要に応じて、いつでもプロセスの途中でさらにチューニングできます。チューニングされたグレースフルモードが、実行中のジョブのシステムパフォーマンスに悪影響を与える場合は、一部の MSDP パーティションについて Encryption Crawler をオフにすることを検討してください。「「システムへの影響を軽減するため、一部の MSDP パーティションに対して Encryption Crawler をオンにする」」の推奨事項に従い、他のパーティションについては実行を継続し、システムへの影響を軽減できます。また、「「MSDP パーティションに対して DataStore への書き込みを選択的に無効にして、システムへの影響を軽減する」」にある推奨事項に従い、Encryption Crawler を実行している一部の MSDP パーティションについて DataStore への書き込み権限をオフにすることも検討してください。処理速度が期待どおりにならない場合は、お使いの環境でアグレッシブモードを活用できます。
アグレッシブモードをオンにする。	「「アグレッシブモードのチューニング」」の情報を使用して、Encryption Crawler に最適なパフォーマンスを実現できます。Cohesity では、最も低いレベル 2 から始め、徐々にレベルを上げることをお勧めしています。実行中のジョブの進捗状況やシステムへの影響の確認がときどき必要になる場合があります。必要に応じて、いつでもプロセスの途中でさらにチューニングできます。
プロセスの処理速度とシステムへの影響のバランスがとれたチューニングポイントを見つける。	Encryption Crawler の処理速度が速いということは、通常、実行中のジョブについてシステムへの影響が大きいことを意味します。チューニングオプションを組み合わせることで、両者の適度なバランスをとることができます。

データの暗号化

この手順では、すべての MSDP データを暗号化する方法を示します。手順 4 の `encryption_reporting` ツールはいつでも実行できます。これは、暗号化されていないデータを報告するために使用される独立したツールです。

すべての MSDP データの暗号化

1 MSDP に暗号化を適用します (適用されていない場合)。

`contentrouter.cfg` の `ServerOptions` オプションに `encrypt` キーワードを追加し、MSDP を再起動して暗号化を適用します。追加する前に、競合または重複するキーワードが存在しないことを確認してください。競合するキーワードは `noencrypt` です。暗号化の有効化または適用について詳しくは、次を参照してください。

p.106 の「MSDP の暗号化について」を参照してください。

インスタントアクセスまたはユニバーサル共有が構成されている場合は、`vpfsd_config.json` を変更し、VpFS を再起動して暗号化を個別に有効にする必要があります。さらに、暗号化を有効にした後、すべての VpFS 共有についてチェックポイントを作成する必要もあります。

2 ローリングデータ変換が進行中の場合は、完了するまで待機します。

3 Encryption Crawler プロセスを完了するまで実行します。

Encryption Crawler の実行、チューニング、および Encryption Crawler の進捗状況の監視に関する詳細情報を参照してください。

p.782 の「Encryption Crawler の 2 つのモードについて」を参照してください。

p.784 の「Encryption Crawler の管理」を参照してください。

p.791 の「チューニングオプション」を参照してください。

4 レポートツール `encryption_reporting` を実行して、暗号化されていないデータを持つ既存のデータコンテナがあるかどうかを確認します。

レポートツールの実行方法に関する詳細情報を参照してください。

p.795 の「コマンドの使用の出力例」を参照してください。

5 暗号化されていないデータが報告された場合は、`--encrypt` オプションを指定して `encryption_reporting` ツールを再実行し、完了するまで待機します。

このオプションを指定して `encryption_reporting` ツールを実行すると、見つかったデータコンテナがレポートプロセスによって暗号化されます。

オプション `--encrypt` を指定したツールにより、データコンテナの暗号化でエラーが報告された場合は、その理由をツールのログと MSDP ログで確認します。エラーを確認したら、必要に応じて手順 4 と手順 5 を繰り返します。

コマンドの使用の出力例

暗号化が適用されていない、またはローリングデータ変換が完了していない場合、`crcontrol` コマンドは Encryption Crawler 関連の操作を拒否します。次に、出力の例を示します。

```
[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/crcontrol --encconvertstate
CRControlEncConvertInfoGet failed : operation not supported
Please double check the server encryption settings
```

Encryption Crawlerプロセスの前に、データコンテナのデータ形式を確認します。次に、出力の例を示します。

```
[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan --so-data-format 3080|head -n
 15
Path = /MSDP/data/3/3080.[bhd, bin]
*** Header for container 3080 ***
version                     : 1
flags                       : 0xe000(DC_ENTRY_FULL|DC_ENTRY_SHA256|DC_ENTRY_BINHEADER)
data file last position     : 67001810
header file last position   : 55252
source id                   : 2505958
retention                   : 0
file size                   : 67001810
delete space                : 0
active records              : 511
total records               : 511
deleted records             : 0
crc32                       : 0x4fd80a49

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan --so-data-format 3080|tail -n
 15
type of record : SO
version        : 4
flags          : 0x2
backup session : 1670238781
fptype         : 3
size           : 131118
record crc     : 4164163489
data crc       : 1313121942
ctime          : 1642086781
offset         : 66870692
digest         : 7f7fd0c5d8fc64d9a7e25c7c079af86613b40d9feff9d316cdfc09c1eafb1690
KMS Enc        : NO
SO crc         : 85135236
data format    : [LZO Compressed Streamable, v2, window size 143360 bytes]

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan
--so-data-format 3080|grep "data format"|wc
    511    5621   38325
```

```
[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan
--so-data-format 3080|grep "data format"|tail -n 5
data format    : [LZO Compressed Streamable, v2, window size 143360 bytes]
data format    : [LZO Compressed Streamable, v2, window size 143360 bytes]
data format    : [LZO Compressed Streamable, v2, window size 143360 bytes]
data format    : [LZO Compressed Streamable, v2, window size 143360 bytes]
data format    : [LZO Compressed Streamable, v2, window size 143360 bytes]
[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan
--so-data-format 3080|grep "data format"|grep -i -e "AES" -e "Encrypted"
```

Encryption Crawlerプロセスの後で、データコンテナのデータ形式を確認します。次に、出力の例を示します。

```
[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan --so-data-format 3080|head -n
 15
Path = /MSDP/data/3/3080.[bhd, bin]
*** Header for container 3080 ***
version                    : 1
flags                      : 0xe000(DC_ENTRY_FULL|DC_ENTRY_SHA256|DC_ENTRY_BINHEADER)
data file last position    : 67009986
header file last position  : 55252
source id                  : 2505958
retention                  : 0
file size                  : 67009986
delete space               : 0
active records             : 511
total records              : 511
deleted records            : 0
crc32                      : 0x54380a69

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan --so-data-format 3080|tail -n
 15
type of record : SO
version        : 4
flags          : 0x2
backup session : 1670238781
fptype         : 3
size           : 131134
record crc     : 4210300849
data crc       : 1992124019
ctime          : 1642086781
offset         : 66878852
digest         : 7f7fd0c5d8fc64d9a7e25c7c079af86613b40d9feff9d316cdfc09c1eafb1690
KMS Enc        : NO
```

```
SO crc          : 85331847
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan
--so-data-format 3080|grep "data format"|wc
    511    8176   59276

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan
--so-data-format 3080|grep "data format"|tail -n 5
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan
--so-data-format 3080|grep "data format"|grep -i -e "AES" -e "Encrypted"
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]
data format     : [AES-256-CTR Encrypted archive 256bit key LZO Compressed Streamable,
v2, window size 143360 bytes]

[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan --so-is-encrypted 3080
1 of 1: unencrypted 0: container 3080: size 67009986
```

dcscan --so-is-encrypted を使用して、コンテナまたはコンテナのリストが暗号化されているかどうかを確認します。

状態メッセージ unencrypted 0 はすでに暗号化されていることを示します。unencrypted 1 は、暗号化されておらず、暗号化が必要であることを示します。次に、出力の例を示します。

```
[root@rsvlmvc01vm0771 /]# /usr/openv/pdde/pdcr/bin/dcscan --so-is-encrypted 3080
1 of 1: unencrypted 1: container 3080: size 67001810
```

レポートツールを使用して、暗号化されていない MSDP データについて報告する

Cohesity は、レポートツール encryption_reporting を使用して、MSDP プール内の暗号化されていないデータを報告することをお勧めします。

メモ: 暗号化レポートツールは、Flex WORM 設定ではサポートされません。

表 C-5

OS および Python の要件	詳細
Linux Red Hat インストールでの encryption_reporting に対する Python の要件。	NetBackup Red Hat インストールには Python が付属しており、Python を実行するための追加の手順はありません。
Windows および Linux SUSE BYO インストールでの encryption_reporting に対する Python の要件。	NetBackup 10.0 以降のバージョンでは、Python 3.6.8-3.9.16 をインストールする必要があります。現在、追加のソフトウェアパッケージをインストールする必要はありません。encryption_reporting を含むディレクトリに移動し (Windows の場合は ¥Veritas¥pdde、Linux SUSE の場合は /usr/openv/pdde/pdcr/bin)、Python スクリプトとして実行します。

デフォルトでは、レポートツールは 2 つのスレッドのスレッドプールを作成します。このツールは、これらのスレッドを使用して、暗号化されていないデータを検索するか、暗号化されていないデータを暗号化します。1 つのスレッドを使用して、1 つの MSDP マウントポイントが完了まで処理されます。マウントポイントの処理が完了すると、スレッドはスレッドプールに戻されます。その後、スレッドは、処理のためにキューに投入された追加のマウントポイントを処理するために使用されます。

スレッド数は、同時に処理できるマウントポイントの数と同じです。-n オプションを指定することで、スレッドプールのスレッド数を増減できます。スレッド数の最小値は 1 で、最大値は 20 です。

レポートツールは I/O を集中的に行います。MSDP マウントポイントの合計数までスレッド数を増やすと、通常は、レポートツールのパフォーマンスが向上します。また、システムに対する負荷が増え、バックアップ、リストア、重複排除、およびレプリケーションのジョブのパフォーマンスへの影響も大きくなります。マウントポイントよりも多いスレッドを使用しても、パフォーマンスの向上は見られません。

レポートツールを使用して暗号化されていないデータを検索すると、各スレッドは dcscan のインスタンスを 1 つ呼び出します。各 dcscan インスタンスは、約 N * 160 MB のメモリを使用します。この式で、N はサーバー上の MSDP マウントポイントの数を示します。合計で 12 個の MSDP マウントポイントがある場合、各 dcscan インスタンスは約 1.8 GB

のメモリを使用します。レポートツールで 4 つのスレッドが実行されている場合、レポートツールと dcscan プロセスは 7 GB を超えるメモリを消費します。

Windows BYO では、dcscan へのデフォルトパスは C:¥Program Files¥Veritas¥pdde です。他の場所に dcscan をインストールした場合は、-d オプションまたは --dcscan_dir オプションを使用して正しい場所を指定する必要があります。

encryption_reporting は、Encryption Crawler を使用して暗号化されたデータについては把握しません。以前に Encryption Crawler を実行してデータを暗号化し、メタデータファイルがある場合は、-c オプションを使用してメタデータファイルを消去する必要があります。その後、encryption_reporting を再実行して最新情報を取得します。

特定の状況では、データが「Encrypted needs KMS convert」と報告されることがあります。これは、データは暗号化されているが KMS は使用されていないことを意味します。このメッセージが表示された場合は、クローラコマンドの ./crcontrol -encconvertreset および ./crcontrol -encconverton を使用して、残りのデータを KMS で暗号化します。

Cohesity は、Encryption Crawler プロセスがアクティブなときにレポートツールを実行することはお勧めしません。

コマンドラインの一般的な使用方法

- ./encryption_reporting -h
  コマンドのヘルプの出力を表示します。
- ./encryption_reporting -n 4
  スクリプトのスキャンが完了したら、暗号化されていないデータと暗号化されたデータの量を報告します。-n オプションを使用して、スレッドプールのスレッド数を定義します。スレッドのデフォルト数は 2 です。
- ./encryption_reporting -r
  このコマンドは、以前のスキャン中に生成されたメタデータファイルから、暗号化されていないデータの量を報告します。スキャンは実行されません。
- ./encryption_reporting -e -n 4
  メタデータファイルを使用して、crcontrol を介してデータコンテナの暗号化コマンドを送信します。-n オプションを使用して、スレッドプールで使用されるスレッドの数を定義します。スレッドのデフォルト数は 2 です。
- ./encryption_reporting -c
  スキャン中に作成されたメタデータファイルを削除します。このコマンドは、前回のスキャンで生成されたすべてのメタデータファイルを削除することに注意してください。
- ./encryption_reporting
  スクリプトを実行して、メディアサーバー上の暗号化されたデータと暗号化されていないデータの量を確認します。

このコマンドは、unencrypted_metadata というディレクトリにある MSDP ログディレクトリに、各コンテナディレクトリのメタデータファイルを生成します。

スクリプトは /etc/pdregistry.cfg から configfilepath を読み取り、パスを解析して fstab.cfg からマウントポイントを読み取ります。fstab.cfg のすべてのマウントポイントを読み取ります。

暗号化されたデータと暗号化されていないデータの量を確認するには、次のような、太字で強調された行を探します。

```
2021-01-28 17:46:05,555 - root - CRITICAL - unencrypted bytes
58.53GB, encrypted bytes 14.46GB
```

KMS 構成の更新

セキュリティ上またはコンプライアンス上の理由により、KMS 構成に次の変更を加える必要がある場合があります。

- KMS 変換
  KMS 変換を使用して、インデックスベースの KMS データコンテナを KEK ベースの KMS データコンテナに変換します。KMS 暗号化が以前に有効になっていた場合は、NetBackup 10.2 以前のバージョンから NetBackup 10.5 にアップグレードした後で、レガシー KMS を変換できます。KMS 変換では、Encryption Crawler を使用して、KMS 暗号化が有効なデータストアのデータコンテナを更新します。
  p.802 の「レガシー KMS の KEK ベースの KMS への変換」を参照してください。
- KMS キーのローテーション
  KMS キーのローテーションを使用して、基になる既存の KEK を変更せずに、KEK の暗号化に使用する KMS キーを置き換えます。
  p.802 の「KMS キーのローテーションの実行」を参照してください。
- KMS KEK のローテーション
  KMS KEK のローテーションは、新しいアクティブな KMS KEK を生成し、新しいアクティブな KEK のタグを使用するようにデータコンテナを更新します。KEK が侵害された場合は、KMS KEK のローテーションを使用します。KMS KEK のローテーションでは、Encryption Crawler を使用して、KMS 暗号化が有効なデータストアのデータコンテナを更新します。
  p.803 の「KEK のローテーションの実行」を参照してください。
- KMS ベンダーの移行
  KMS ベンダーの移行では、NetBackup KMS からサードパーティの KMS ベンダーへの変更、サードパーティの KMS ベンダーから NetBackup KMS への変更、サードパーティの KMS ベンダー A からサードパーティの KMS ベンダー B への変更など、KMS サービスプロバイダを変更できます。KMS ベンダーの移行では、ユーザーは、KMS ベンダーの移行を使用する前に、追加の KMS サービスプロバイダを構成する必要があります。新しい KMS サービスの KMS キーグループ名は、現在の KMS サービスの KMS キーグループ名と一致する必要があります。

p.803 の「KMS ベンダーの移行」を参照してください。

レガシー KMS の KEK ベースの KMS への変換

NetBackup 10.2 以前のバージョンは、インデックスベースの KMS を使用します。レガシーのインデックスベースの KMS を使用して書き込まれたデータコンテナは、Encryption Crawler を使用して現在の KEK ベースの KMS に変換できます。この処理は、バックアップやリストアなどの通常の NetBackup 操作と同時に実行される場合があります。ベストプラクティスは、保守ウィンドウ中に KMS 変換を実行することです。変換時間は変換が必要なデータの量によって異なるため、変換が完了するまでに、非常に長い時間がかかる場合があります。

レガシー KMS を KEK ベースの KMS に変換するには

1. Encryption Crawler が以前に使用されていた場合は、それをリセットします。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --encconvertreset
   ```

2. 変換プロセスを MSDP で開始するには、次のコマンドを実行します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --legacykmsconverton
   ```

3. 変換の進行状況を監視します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --encconvertstate 2
   ```

KMS キーのローテーションの実行

この処理は、バックアップやリストアなどの通常の NetBackup 操作と同時に実行される場合があります。ただし、ベストプラクティスは、保守ウィンドウ中に KMS キーのローテーションを実行することです。KMS キーのローテーションはすぐに完了します。

KMS キーのローテーションを実行するには

1. MSDP を使用するように構成した KMS サービスで、新しい KMS キーを作成したことを確認します。

2. KMS キーのローテーションプロセスを MSDP で開始するには、次のコマンドを実行します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --kmskeyrotation
   ```

3. `kek_tag_reporting` ツールを使用して、新しい KMS キーが更新されたことを確認します。

   ```
   /usr/openv/pdde/pdcr/bin/kek_tag_reporting.py -r
   ```

   ```
   /usr/openv/netbackup/bin/nbkmscmd -listKeys -name nbkms
   ```

KEK のローテーションの実行

この処理は、バックアップやリストアなどの通常の NetBackup 操作と同時に実行される場合があります。ただし、ベストプラクティスは、保守ウィンドウ中に KEK のローテーションを実行することです。変換時間は KEK のローテーションが必要なデータの量によって異なるため、ローテーションが完了するまでに、非常に長い時間がかかる場合があります。

KEK のローテーションを実行するには

1. Encryption Crawler が以前に使用されていた場合は、それをリセットします。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --encconvertreset
   ```

2. KEK のローテーションプロセスを MSDP で開始するには、次のコマンドを実行します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --kekconverton
   ```

3. KEK のローテーションを監視します。

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --encconvertstate 2
   ```

KMS ベンダーの移行

ベストプラクティスは、保守ウィンドウ中に KMS ベンダーの移行を実行することです。

KMS ベンダーを移行するには

1. 現在の KMS サービスを一覧表示して、KMS サービスの優先度を判断します。

   ```
   /usr/openv/netbackup/bin/nbkmscmd -listKMSConfig
   ```

2. 現在の KMS サービスの優先度を 0 より大きい値に更新します。

   ```
   /usr/openv/netbackup/bin/nbkmscmd -updateKMSConfig -name
   configuration_name [-server primary_server_name] [-priority
   priority_of_KMS_server]
   ```

3. 現在の KMS サービスが使用しているキーグループ名と同じキーグループ名を使用して、新しい KMS サービスを設定します。

4. 新しい KMS サービスでアクティブな KMS キーを作成します。

5. 優先度を 0 にして、NetBackup で新しい KMS サービスを構成します。

6. NetBackup がプライマリサーバー上の両方の KMS サービスを報告することを確認します。

   ```
   /usr/openv/netbackup/bin/nbkmscmd -listKMSConfig
   ```

7 新しい KMS サービスの優先度を、以前の KMS サービスで設定されている優先度よりも高い優先度に更新します。

```
/usr/openv/netbackup/bin/nbkmscmd -updateKMSConfig -name
configuration_name [-server primary_server_name] [-priority
priority_of_KMS_server]
```

8 MSDP で KMS ベンダーの移行プロセスを開始します。

```
/usr/openv/pdde/pdcr/bin/crcontrol --migratekmsprovider
```

9 kek_tag_reporting ツールを使用して、最新のエントリの kms_key_tag が、新しい KMS サービスのアクティブなキーに関して nbkmscmd が報告する「キー ID」と一致することを確認します。

```
/usr/openv/pdde/pdcr/bin/kek_tag_reporting.py -r
```

```
/usr/openv/netbackup/bin/nbkmscmd -listKeys -name nbkms
```

索引

記号

A

B

C

D