NetBackup™ クラウドオブジェクトストア管理者ガイド

リリース 10.5

VERITAS™

NetBackup™ クラウドオブジェクトストア管理者ガイド

最終更新日: 2024-10-16

法的通知と登録商標

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

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

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

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

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

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

マニュアル

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

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

1

概要

この章では以下の項目について説明しています。

クラウドオブジェクトストアの NetBackup 保護の概要

NetBackup Web UI は、プライベートクラウドサービスとパブリッククラウドサービスの両方で、クラウドオブジェクトストアのバックアップとリストアの機能を提供します。オブジェクトストアと同じクラウドネットワークに NetBackup 環境を配備できます。または、オブジェクトストアサービスエンドポイントとバックアップホストまたはスケールアウトサーバーに HTTP(s) 接続を提供できます。ベンダーのクラウド外にも NetBackup を配備できます。

メモ: クラウドベンダーは、ネットワークからデータを移動するためのデータ取り出しに多額の料金がかかる場合があります。あるクラウドから別のクラウドリージョンまたはオンプレミスデータセンターにデータを転送するバックアップポリシーを構成する前に、クラウドプロバイダのデータ取り出しの価格設定を確認してください。

NetBackup は、Azure Blob Storage に加え、AWS S3、Google Cloud Storage (GCS)、Hitachi Cloud Platform オブジェクトストアなど、さまざまな S3 API 互換オブジェクトストアを保護できます。互換性のあるオブジェクトストアの完全なリストについては、NetBackup ハードウェア互換性リスト (HCL) を参照してください。

Azure Data Lake の保護対象オブジェクトは、基礎となるオブジェクトが BLOB 型であっても、ファイルおよびディレクトリと呼ばれます。

NetBackup クラウドオブジェクトストアの作業負荷サポートの機能

表 1-1 主な特長

機能	説明
NetBackup の RBAC (役割ベースのアクセス制御) との統合	NetBackup Web UI は、NetBackup でクラウドオブジェクトストア操作を管理できる NetBackup ユーザーを制御するために、RBAC の役割としてデフォルトのクラウドオブジェクトストア管理者を提供します。クラウドオブジェクトストアを管理するために NetBackup 管理者である必要はありません。
クラウドオブジェクトストアアカウントの管理	必要に応じて、異なるクラウドベンダー間で、複数のクラウドオブジェクトストアアカウントに対して単一の NetBackup プライマリサーバーを構成できます。
認証およびクレデンシャル	セキュリティに幅広く重点を置いています。単一の Azure Blob Storage アカウントを保護するため、ストレージアカウントとアクセスキーを指定する必要があります。Azure Blob Storage アカウントを保護するためにサポートされる認証メカニズムは、アクセスキー、サービスプリンシパル、および管理対象 ID です。すべての S3 API 対応クラウドベンダーで、アクセスキーとシークレットキーがサポートされます。Amazon S3 では、認証メカニズムとして、アクセスキー、IAM ロール、Assume ロール (クロス AWS アカウント用) がサポートされます。 完全なリストについては、NetBackup 互換性リストを参照してください。
バックアップポリシー	単一のバックアップポリシーで、1 つのクラウドオブジェクトストアアカウントの複数の S3 バケットまたは Azure Blob コンテナを保護できます。

機能	説明
クラウドオブジェクトのインテリジェントな選択	NetBackup では、単一のポリシー内でバケットまたはコンテナごとに異なるクエリーを柔軟に構成できます。一部のバケットまたはコンテナは、バケットまたはコンテナ内のすべてのオブジェクトをバックアップするように構成できます。また、次に基づいてオブジェクトを識別するためのインテリジェントなクエリーで一部のバケットとコンテナを構成することもできます。 ■ オブジェクト名の接頭辞 ■ オブジェクト名全体 ■ オブジェクトタグ ■ Azure Data Lake のファイルとディレクトリ
高速で最適化されたバックアップ	完全バックアップに加えて、NetBackup は高速バックアップのためにさまざまな形式の増分スケジュールもサポートしています。アクセラレータ機能は、クラウドオブジェクトストアポリシーでもサポートされています。 ポリシーの「チェックポイントから再開」機能を有効にすると、失敗したジョブまたは一時停止したジョブを、前回のチェックポイントから再開できます。ジョブの始めからデータ転送全体を繰り返す必要はありません。
個別リストア	NetBackup では、バケットまたはコンテナ内のすべてのオブジェクトを簡単にリストアできます。また、接頭辞、フォルダ、またはオブジェクトベースのビューを使用して、リストアするオブジェクトを選択することもできます。 日付と時間の範囲を指定して、NetBackup でのリストア対象のバックアップイメージを絞り込むことができます。

機能	説明
リストアオプション	NetBackup は、メタデータ、プロパティ、タグ、ACL、オブジェクトロックプロパティとともにオブジェクトストアデータをリストアします。 NetBackup では、リストア時にすべてのオブジェクトに任意の接頭辞を追加できます。その結果、元のオブジェクトとの衝突を避けることが望まれる場合は、区別しやすい名前でオブジェクトをリストアできます。ただし、Azure Data Lake のファイルとディレクトリには、接頭辞は必要ありません。代わりに、ファイルとディレクトリは指定した代替の場所にリストアされます。 デフォルトでは、NetBackup は、帯域幅とクラウドコストを節約するために、クラウドオブジェクトストアにすでにあるオブジェクトの上書きをスキップします。このデフォルトの動作は、[上書き (Overwrite)]オプションを使用して変更できます。これにより、リストアされたコピーでクラウドオブジェクトストアのコピーを上書きできます。
リストアの代替場所	オブジェクトのリストア先として次を選択できます。 ■ 同じバケットまたはコンテナ ■ 同じアカウントまたはサブスクリプションの別のバケットまたはコンテナ ■ 異なるアカウントまたはサブスクリプションの別のバケットまたはコンテナ
リカバリ前のマルウェアスキャンのサポート	Web UI からのリカバリフローの一部として、リカバリ対象として選択したファイルまたはフォルダのマルウェアスキャンを実行し、マルウェアスキャン結果に基づいてリカバリ処理を決定できます。
動的マルチストリーム	この機能により、単一のクライアントまたはバックアップ対象に対して複数のバックアップストリームを同時に実行できます。この機能により、大量のデータとオブジェクトを伴う作業負荷を、指定したバックアップ処理時間帯で処理できます。動的マルチストリームは、バックアップ対象のオブジェクトを複数のストリームに暗黙的に分散し、データ分散と並行してストリームの作成を自動化します。

機能	説明
バックアップホストの拡張性のサポート	NetBackup クラウドオブジェクトストア保護は、NetBackup Snapshot Manager を、メディアサーバーと共に、クラウド配備用の拡張性のあるバックアップホストとして構成することをサポートしています。環境内に既存の NetBackup Snapshot Manager 配備がある場合は、これをクラウドオブジェクトストアポリシーのバックアップホストとして使用できます。 NetBackup Snapshot Manager をバックアップホストとして使用すると、大規模なジョブのために複数のバックアップホストを構成したり、これらのバックアップホスト全体で負荷を分散するために複数のポリシーを作成したりする必要がありません。Snapshot Manager は、バックアップ操作中にデータムーバーコンテナの数を増やし、保護タスクが完了したときにそれらを削減できます。
オブジェクトロック	この機能を使用すると、元のオブジェクトロックプロパティを保持できます。また、オブジェクトロックプロパティをカスタマイズするオプションも使用できます。リストアされたオブジェクトにオブジェクトロックプロパティを使用すると、保持期間が終了するかリーガルホールドが解除されるまで、これらのオブジェクトを削除できません。オブジェクトロックと保持のプロパティは、ポリシーの作成やバックアップ中に構成することなく使用できます。

2

クラウドオブジェクトストア資産の管理

この章では以下の項目について説明しています。

クラウドオブジェクトストア資産の NetBackup 保護の計画

このセクションでは、クラウドオブジェクトストア資産の保護を目的として NetBackup を配備するために実行する必要があるタスクについて詳しく説明します。

表 2-1 NetBackup 配備の手順

手順	処理	説明
手順 1	オペレーティングシステムおよびプラットフォームの互換性を確認します。	NetBackup 互換性リストを参照してください。
手順 2	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。
手順 3	必要な権限とクレデンシャルを構成します。	p.14 の「クラウドオブジェクトストアアカウントの追加の前提条件」を参照してください。
手順 4	保護するバケットとコンテナを特定します。	NetBackup で保護するバケットとコンテナのリストを作成し、手順 5 で作成するクラウドオブジェクトストアアカウントに含めます。
手順 5	クラウドオブジェクトストアアカウントを作成します。	p.21 の「クラウドオブジェクトストアアカウントの追加」を参照してください。
手順 6	ポリシーを作成します。	p.46 の「バックアップポリシーの作成」を参照してください。

クラウドオブジェクトストアアカウントの追加の前提条件

クラウドオブジェクトストアアカウントの追加を開始する前に、次のものを収集します。

- クラウドプロバイダ、サービスホスト、および地域に関する情報を収集します。
  ここで、サービスホストは、クラウドプロバイダによって提供されるクラウドオブジェクトストレージ API エンドポイントのホスト名です。たとえば、AWS パブリック S3 エンドポイントの URL `https://s3.us-east-1.amazonaws.com` では、「`s3.us-east-1.amazonaws.com`」という部分がサービスホストです。
  プライベートクラウド設定の場合、URL は `https://s3.us-east-1.amazomaws.com/tenent123/` のようになります。サービスホストは `s3.us-east-1.amazomaws.com/tenent123/` です。
- クラウドサービスプロバイダでサポートされている認証形式を確認し、使用する認証形式を決定します。すべてのクラウドプロバイダは、アクセスクレデンシャルの認証形式をサポートします。その他のサポート対象の認証形式:
  - IAM ロール (EC2): Amazon および Amazon Gov の場合
  - 引き受け役割: Amazon および Amazon Gov の場合
  - 役割の引き受け (EC2): Amazon および Amazon Gov の場合
  - クレデンシャルブローカー: Amazon Gov の場合

- サービスプリンシパル: Azure の場合
- 管理対象 ID: Azure の場合

- クラウドエンドポイントとの通信にプロキシを使用する予定の場合は、プロキシサーバーの必要な詳細情報を収集します。
- クラウドアカウントのクレデンシャル、および認証形式に応じた追加の必須パラメータを取得します。これらのクレデンシャルの詳細情報には、NetBackup のマニュアルで推奨されている必須の権限が付与されている必要があります。
  p.16 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。
  p.17 の「Azure Blob ストレージに必要な権限」を参照してください。
  p.18 の「GCP に必要な権限」を参照してください。
- 必要なアウトバウンドポートが開かれていること、およびバックアップホストまたはスケールアウトサーバーからクラウドプロバイダエンドポイントへの REST API 呼び出しを使用した通信の構成が完了していることを確認してください。
  - バックアップホストで、S3 または Azure ストレージ URL エンドポイントは HTTPS のデフォルトポート 443 を使用します。プライベートクラウドプロバイダの場合、このポートはプライベートクラウドストレージに構成されている任意のカスタムポートにすることができます。
  - プロキシサーバーを使用してクラウドストレージに接続する場合は、そのポートを許可する必要があります。クラウドオブジェクトストアアカウントの作成時に、NetBackup でプロキシサーバー関連の詳細を指定できます。
  - 証明書失効状態の確認オプションは、通常 HTTP ポート 80 を使用する OCSP プロトコルを使用します。OCSP URL がバックアップホストから到達可能であることを確認します。

バックアップのバッファサイズの構成

読み取りまたは書き込みバッファのサイズは、クラウドオブジェクトストアでの NetBackup のパフォーマンスに影響します。

デフォルトでは、NetBackup は 4 MB のバッファを作成します。バケットまたはコンテナのほとんどのオブジェクトが 4 MB 未満の場合は、このデフォルトのバッファサイズを使用できます。バケットまたはコンテナに 4 MB を超える多数のオブジェクトがある場合は、バッファサイズを最大 64 MB に増やすことができます。

バッファサイズを構成するには

1 バックアップホストで /usr/openv/netbackup/bp.conf ファイルを開きます。

[クラウドオブジェクト (Cloud objects)]タブで、対応するポリシーからバックアップホストを識別できます。

2 このパラメータの値を MB 単位で *COS_SHM_BUFFER_SIZE =* に入力します。

例: *COS_SHM_BUFFER_SIZE = 16*

バッファ数の構成

デフォルトでは、NetBackup は読み込み操作または書き込み操作ごとに 7 個のバッファを作成します。バックアップホストのメモリの可用性に応じて、各ストリームのバッファ数を 4 から 16 に設定できます。バッファ数を増やすとバックアップが高速になりますが、バックアップホストのメモリ使用量が増加することがあります。

バッファ数を構成するには

1 バックアップホストで /usr/openv/netbackup/bp.conf ファイルを開きます。

2 このパラメータの値を MB 単位で *COS_NO_SHM_BUFFER =* に入力します。

例: *COS_NO_SHM_BUFFER = 12*

これらの設定はそのバックアップホストを使用するすべてのバックアップジョブに適用されることに注意してください。

Amazon S3 クラウドプロバイダのユーザーに必要な権限

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

- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketLocation
- s3:GetObject
- s3:PutObject
- s3:GetObjectTagging
- s3:GetObjectAcl
- s3:PutObjectAcl
- s3:PutObjectTagging

- s3:RestoreObject
- s3:PutObjectRetention
- s3:BypassGovernanceRetention
- s3:GetBucketObjectLockConfiguration
- s3:Getobjectretention

Azure Blob ストレージに必要な権限

Microsoft Azure オブジェクトストアの検出、バックアップ、リストア、認証に必要なカスタム役割定義 (JSON 形式) を次に示します。NetBackup ユーザーが Azure Blob と連携するために使用できる、これらの権限を持つカスタム役割を関連付ける必要があります。サービスプリンシパルまたはマネージド ID 認証を使用するには、次の権限を持つ役割が必要です。

```
{
    "properties": {
        "roleName": "cosp_minimal",
        "description": "minimal permission required for cos
protection.",
        "assignableScopes": [
            "/subscriptions/<Subsfription_ID>"
        ],
        "permissions": [
            {
                "actions": [

"Microsoft.Storage/storageAccounts/blobServices/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/write",
                    "Microsoft.ApiManagement/service/*",
                    "Microsoft.Authorization/*/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",
                  "Microsoft.Storage/storageAccounts/read"

                ],
                "notActions": [],
                "dataActions": [
```

```
"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/immutableStorage/runAsSuperUser/action",

                ],
                "notDataActions": []
            }
        ]
    }
}
```

GCP に必要な権限

GCP を NetBackup と連携させるには、次の権限が必要です。

```
storage.bucketOperations.cancel
storage.bucketOperations.get
storage.bucketOperations.list
storage.buckets.create
storage.buckets.createTagBinding
storage.buckets.delete
storage.buckets.deleteTagBinding
storage.buckets.enableObjectRetention
storage.buckets.get
storage.buckets.getIamPolicy
storage.buckets.getObjectInsights
storage.buckets.list
storage.buckets.listEffectiveTags
storage.buckets.listTagBindings
storage.buckets.restore
```

```
storage.buckets.setIamPolicy
storage.buckets.update
storage.multipartUploads.abort
storage.multipartUploads.create
storage.multipartUploads.list
storage.multipartUploads.listParts
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.getIamPolicy
storage.objects.list
storage.objects.restore
storage.objects.setIamPolicy
storage.objects.update
```

制限事項および考慮事項

クラウドオブジェクトストア作業負荷を保護するときは、次の点を考慮してください。

- NetBackup では、「/」で始まる接頭辞またはオブジェクト問い合わせは許可されません。例:

  ```
  prefix = /
  prefix = /folder1
  prefix = /object1
  prefix = folder1//
  object = /obj1
  ```

- 名前が <name>/ の形式のオブジェクトは NetBackup でバックアップされません

アップグレードシナリオに基づく制限事項

- 最新の NetBackup バージョンにバージョン 10.1 または 10.2 からアップグレードする場合は、次の制限事項が適用されます。
  - クラウドオブジェクトストアアカウントの作成には、バージョン 10.3 以降のバックアップホストまたはスケールアウトサーバーのみを使用できます。バージョン 10.3 より前のバックアップホストまたはスケールアウトサーバーで、NetBackup 10.3 以降で作成された既存のクラウドオブジェクトストアアカウントを更新できません。
  - ポリシーの作成には、バージョン 10.3 以降のバックアップホストまたはスケールアウトサーバーのみを使用できます。バージョン 10.3 より前のバックアップホストまたはスケールアウトサーバーで、NetBackup 10.3 以降で作成された既存のポリシーを更新できません。

- バージョン 10.3 より前のバックアップホストまたはスケールアウトサーバーでは、次のクレデンシャルタイプはサポートされません: Azure の場合: サービスプリンシパルと管理対象 ID。AWS の場合: 役割の引き受け (EC2)。
- オブジェクトロックプロパティを使用したリストアは、バージョン 10.3 以降のバックアップホストまたはスケールアウトサーバーでのみサポートされます。
- デフォルトの保持が有効になっているバケットのバックアップとリストアは、バージョン 10.3 以降のバックアップホストまたはスケールアウトサーバーでのみサポートされます。

- Azure で、バージョン 10.3 より前の NetBackup で作成されたポリシーを、バージョン 10.3 以降のバックアップホストまたはスケールアウトサーバーで更新すると、バックアップは失敗します。回避策として、既存のクエリーで指定された生成 ID の新しい形式を使用するようにすべてのバケットを更新します。この回避策を正常に実行するには、10.3 以降の NetBackup を使用して、関連付けられたクラウドオブジェクトストアアカウントをポリシー内に作成する必要があります。
- RHEL に配備された、NetBackup バージョン 10.3 以降で検出がサポートされます。サポート対象のホストが利用できない場合、どの構成済みクラウドストレージアカウントでも検出が開始されません。この場合、検出状態は利用できず、ポリシーの作成中にバケットリストを表示できません。検出が失敗した後にバケットを手動で追加した場合でも、バックアップが失敗することがあります。サポート対象のバックアップホストまたはスケールアウトサーバーを少なくとも 1 台アップグレードして、新しいポリシーを作成します。
- 10.3 より前の NetBackup バージョンで作成されたポリシーを更新する場合は、バックアップ後に次の点を考慮してください。
  - バックアップ後に、古い形式と新しい形式の 2 つのバージョンの同じバケットが表示される場合があります。古いデータをリストアする場合は、古い形式のバケットを選択します。新しいバックアップの場合は、新しい形式のバックアップを選択します。
  - 更新後の後続のバックアップは、ポリシーで構成されている内容に関係なく完全バックアップです。
- 10.3 にアップグレードすると、構成されたバックアップが増分バックアップの場合でも、最初の Azure Blob 高速バックアップでは、選択されているすべてのオブジェクトのバックアップが作成されます。この完全バックアップは、NetBackup バージョン 10.2 と 10.3 間で Azure Blob のメタデータプロパティを変更する場合に必要です。後続の増分バックアップでは、変更されたオブジェクトだけがバックアップされます。
- 10.3 より前のバージョンで作成されたクラウドオブジェクトストアアカウントを使用する場合、NetBackup は古い形式のバケットを検出します。この場合、uniqueName=bucketName です。

クラウドオブジェクトストアアカウントの追加

クラウドオブジェクトストアアカウントの追加は、作業負荷を保護するために最初に実行する手順です。NetBackup プライマリサーバーに 1 つ以上のアカウントを追加できます。ビジネスロジックに合わせて異なるクラウドオブジェクトストアアカウントを作成できます。たとえば、特定のクラウドサービスプロバイダのバケットのグループ化などです。AWS S3 と互換性のあるアカウントでは、バックアップとリストアに個別の RBAC アクセス権が必要です。バックアップとリストア用に個別のアカウントを作成して、アクセス権をより良く整理できます。

保護するバケットまたはコンテナに応じて、各クラウドサービスプロバイダに、地域ごとに少なくとも 1 つのクラウドオブジェクトストアアカウントを追加する必要があります。

同じクラウドサービスプロバイダと地域に対して、複数のクラウドオブジェクトストアアカウントを作成する必要がある場合があります。SSL、プロキシ、一連のバケットまたはコンテナに使用するクレデンシャルの種類などの設定をより良く整理するために、複数のアカウントを作成できます。

バックアップとリカバリに必要な権限は異なります。バックアップとリカバリ用に個別のアカウントを作成すると便利かどうかを確認してみてください。リカバリ時に別のクラウドオブジェクトストアアカウントにリストアするには、元のバケットオプション以外の何かを使用する必要があります。

メモ: クラウドオブジェクトストアアカウントは、クラウドストレージサーバーおよび MSDP-CLSU 名と名前空間を共有します。

クラウドオブジェクトストアアカウントのため、NetBackup は、AWS S3 と互換性のある API を使用して、Microsoft Azure 以外のさまざまなクラウドプロバイダ (Amazon、Google、Hitachi など) をサポートします。このようなプロバイダの場合、プロバイダのクレデンシャル (アクセスキー ID、シークレットアクセスキーなど) を追加するために、AWS S3 と互換性のあるアカウントのアクセス詳細を指定する必要があります。

クラウドオブジェクトストアアカウントの作成時に検証ホストを選択する必要があります。検証ホストは、クレデンシャルを検証する特定のバックアップホストです。検証ホストは、手動検出、定期的な検出、および既存のクラウドオブジェクトストアアカウントで手動検証が必要な場合に使用されます。検証ホストは、ポリシーで指定された実際のバックアップホストとは異なる場合があります。

クラウドオブジェクトストアアカウントを追加するには:

1. 左側で、[作業負荷 (Workloads)]の[クラウドオブジェクトストア (Cloud object store)]をクリックします。
2. [クラウドオブジェクトストアアカウント (Cloud object store account)]タブで、[追加 (Add)]をクリックします。[クラウドオブジェクトストア名 (Cloud object store name)]フィールドにアカウントの名前を入力し、[クラウドオブジェクトストアプロバイダの選択 (Select Cloud object store provider)]リストからプロバイダを選択します。
3. バックアップホストまたはスケールアウトサーバーを選択するには、[検証用ホストの選択 (Select host for validation)]をクリックします。RHEL メディアサーバー上のホストは、クラウドオブジェクトストアのクレデンシャルの検証、バックアップ、およびリカバリをサポートする NetBackup 10.1 以降にする必要があります。
   - バックアップホストを選択するには、[バックアップホスト (Backup host)]オプションを選択し、リストからホストを選択します。
   - スケールアウトサーバーを使用するには、[スケールアウトサーバー (Scale out server)]オプションを選択し、リストからサーバーを選択します。NetBackup Snapshot Manager サーバー 10.3 以降は、スケールアウトサーバーとして機能します。
     バケットの数が非常に多い場合は、NetBackup 10.3 以降のリリースのバックアップホストとして NetBackup Snapshot Manager を使用することもできます。[スケールアウトサーバー (Scale out server)]オプションを選択し、リストから NetBackup Snapshot Manager を選択します。

     メモ: 既存の NetBackup プライマリサーバーは、NetBackup Snapshot Manager のこのインスタンスで構成されている必要があります。
4. 利用可能な地域リストから地域を選択します。[地域 (Region)]テーブルの上の[追加 (Add)]をクリックして、新しい地域を追加します。

   p.30 の「新しい地域の追加」を参照してください。。一部のクラウドオブジェクトストアプロバイダでは、地域を利用できません。

   デュアル地域バケットをサポートする GCP の場合は、アカウントの作成時にベースの地域を選択します。たとえば、デュアル地域バケットが *US-CENTRAL1*、*US-WEST1* の地域にある場合、アカウントの作成時に地域として *US* を選択してバケットを一覧表示します。
5. [アクセス設定 (Access settings)]ページで、アカウントのアクセス方法の種類を選択します。
   - アクセスのクレデンシャル (Access credentials): この方法では、NetBackup はアクセスキー ID とシークレットアクセスキーを使用して、クラウドオブジェクトスト

アアカウントへのアクセスとセキュリティ保護を行います。この方法を選択した場合は、必要に応じて後続の手順 6 から 10 を実行してアカウントを作成します。

- IAM 役割 (EC2) (IAM role (EC2)): NetBackup は、EC2 インスタンスに関連付けられた IAM 役割名とクレデンシャルを取得します。選択したバックアップホストまたはスケールアウトサーバーは EC2 インスタンスでホストされている必要があります。EC2 インスタンスに関連付けられている IAM ロールに、クラウドオブジェクトストアの保護に必要なクラウドリソースにアクセスするためのアクセス権があることを確認します。このオプションを使用してクラウドオブジェクトストアアカウントを構成する際は、EC2 インスタンスに関連付けられた権限に応じて正しい地域を選択してください。このオプションを選択した場合は、必要に応じて任意の手順 7 と 8 を実行してから、手順 9 と 10 を実行します。
- 役割の引き受け (Assume role): NetBackup は指定されたキー、シークレットアクセスキー、役割 ARN を使用して、同じアカウントとクロスアカウント用の一時的なクレデンシャルを取得します。必要に応じて手順 6 から 10 を実行してアカウントを作成します。
  p.26 の「AWS でのクロスアカウントアクセスの作成 」を参照してください。
- 役割の引き受け (EC2)(Assume role (EC2)): NetBackup は、EC2 インスタンスでホストされている、選択したバックアップホストまたはスケールアウトサーバーに関連付けられている AWS IAM の役割のクレデンシャルを取得します。その後、NetBackup は、クラウドオブジェクトストアの保護に必要なクラウドリソースにアクセスするために、役割 ARN に指定された役割を引き受けます。
- クレデンシャルブローカー (Credentials broker): NetBackup はクラウドオブジェクトストアの保護に必要なクラウドリソースにアクセスするためのクレデンシャルを取得します。
- サービスプリンシパル (Service principal): NetBackup では、サービスプリンシパルに関連付けられているテナント ID、クライアント ID、およびクライアントシークレットを使用して、クラウドオブジェクトストア保護に必要なクラウドリソースにアクセスします。Azure でサポートされます。
- 管理対象 ID (Managed identity): NetBackup では、選択したバックアップホスト、スケールアウトサーバー、またはユーザーと関連付けられた管理対象 ID を使用して、Azure AD トークンを取得します。NetBackup は、これらの Azure AD トークンを使用して、クラウドオブジェクトストアの保護に必要なクラウドリソースにアクセスします。システムまたはユーザーによって割り当てられた管理対象 ID を使用できます。

6 既存のクレデンシャルを追加することも、アカウントの新しいクレデンシャルを作成することもできます。

- アカウントの既存のクレデンシャルを選択するには、[既存のクレデンシャルの選択 (Select existing credentials)]オプションを選択し、表から必要なクレデンシャルを選択して[次へ (Next)]をクリックします。

- Azure で管理対象 ID を使用するには、[システム割り当て (System assigned)] または[ユーザー割り当て (User assigned)]を選択します。ユーザー割り当ての方法の場合は、クラウドリソースにアクセスするためにユーザーに関連付けられているクライアント ID を入力します。
- アカウントの新しいクレデンシャルを追加するには、[新しいクレデンシャルを追加 (Add new credentials)]を選択します。新しいクレデンシャルの[クレデンシャル名 (Credential name)]、[タグ (Tag)]、[説明 (Description)]を入力します。AWS S3 と互換性のある API を介してサポートされるクラウドプロバイダの場合は、AWS S3 と互換性のあるクレデンシャルを使用します。[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。

  Microsoft Azure クラウドプロバイダの場合:

  - アクセスキーの方法では、ストレージアカウントのクレデンシャルを指定し、ストレージアカウントを指定します。
  - サービスプリンシパルの方法では、クライアント ID、テナント ID、シークレットキーを指定します。
- アクセス方法として[役割の引き受け (Assume role)]を使用する場合は、[役割 ARN (Role ARN)]フィールドで、アカウントに使用する役割の Amazon リソースネーム (ARN) を指定します。

7 (任意) NetBackup とクラウドストレージプロバイダの間のユーザー認証またはデータ転送に SSL (Secure Sockets Layer) プロトコルを使用する場合は、[SSL を使用する (Use SSL)]を選択します。

- [認証のみ (Authentication only)]: クラウドストレージにアクセスするときのユーザーの認証で SSL のみを使用する場合は、このオプションを選択します。
- [認証とデータ転送 (Authentication and data transfer)]: ユーザー認証にも、NetBackup からクラウドストレージへのデータ転送にも SSL を使用する場合は、このオプションを選択します。
- [証明書の失効を確認する (IPv6 はこのオプションのサポート対象外) (Check certificate revocation (IPv6 not supported for this option))]: すべてのクラウドプロバイダに対し、NetBackup は OCSP プロトコルを使用して SSL 証明書の失効状態を検証するための機能を提供します。OCSP プロトコルは、証明書の現在の失効状態を取得するために、証明書発行者に検証要求を送信します。SSL を有効にして証明書失効の確認オプションを有効にすると、OCSP 要求で自己署名以外の各 SSL 証明書が検証されます。証明書が無効である場合、NetBackup はクラウドプロバイダに接続しません。

メモ: NetBackup は、SSL モードでのクラウドストレージとの通信時に、認証局 (CA) によって署名された証明書のみをサポートします。クラウドサーバー (パブリックまたはプライベート) に CA による署名付き証明書があることを確認します。CA によって署名された証明書がない場合は、SSL モードでの NetBackup とクラウドプロバイダ間のデータ転送が失敗します。自己署名 SSL 証明書を使用する場合は、NetBackup のクラウドストレージ CA トラストストアに証明書を追加する必要があります。p.27 の「NetBackup クラウドの認証局 (CA) の管理 」を参照してください。

メモ: Amazon GovCloud クラウドプロバイダの FIPS リージョン (s3-fips-us-gov-west-1.amazonaws.com) では、セキュアモードの通信のみがサポートされます。このため、FIPS 領域を持つ Amazon GovCloud クラウドストレージを設定するときに[SSL を使用する (Use SSL)]オプションを無効にすると、設定は失敗します。

8 (任意) プロキシサーバーを使用する場合は、[プロキシサーバーを使用する (Use proxy server)]オプションを選択し、プロキシサーバーの設定を指定します。[プロキシサーバーを使用する (Use proxy server)]オプションを選択すると、次の詳細を指定できます。

- プロキシホスト (Proxy host): プロキシサーバーの IP アドレスまたは名前を指定します。
- プロキシポート (Proxy Port): プロキシサーバーのポート番号を指定します。
- プロキシの形式 (Proxy type): 次のプロキシの形式のいずれかを選択できます。
  - HTTP

    メモ: HTTP プロキシ形式のプロキシクレデンシャルを指定する必要があります。

  - SOCKS
  - SOCKS4
  - SOCKS5
  - SOCKS4A

HTTP プロキシ形式には、[プロキシのトンネリングを使用 (Use proxy tunneling)]を選択します。

[プロキシのトンネリングを使用 (Use Proxy Tunneling)]を有効にすると、HTTP CONNECT 要求がバックアップホストまたはリカバリホストから HTTP プロキシサーバーに送信されます。TCP 接続はクラウドバックエンドストレージに直接転送されま

す。データは、接続からヘッダーやデータを読み取ることなくプロキシサーバーを通過します。

HTTP プロキシ形式を使用する場合は、次のいずれかの認証形式を選択します。

- なし (None): 認証が有効になりません。ユーザー名とパスワードは要求されません。
- 基本 (Basic): ユーザー名とパスワードが必要です。
- NTLM: ユーザー名とパスワードが必要です。

ユーザー名 (Username): プロキシサーバーのユーザー名です。

パスワード (Password): 空にできます。最大 256 文字を使用できます。

9 [次へ (Next)]をクリックします。

10 [確認 (Review)]ページでアカウントの設定全体を確認し、[完了 (Finish)]をクリックしてアカウントを保存します。

NetBackup は、指定された接続情報に関連付けられたクレデンシャルを検証した後にのみ、クラウドオブジェクトストアアカウントを作成します。エラーが発生した場合は、エラーの詳細に従って設定を更新します。また、指定された接続情報とクレデンシャルが正しいかどうかを確認します。検証のために割り当てたバックアップホストまたはスケールアウトサーバーは、指定された情報を使用してクラウドプロバイダのエンドポイントに接続できます。

AWS でのクロスアカウントアクセスの作成

環境内に複数の AWS アカウントがあり、そのうちのいずれかのアカウントに NetBackup が配備されている場合、すべての AWS アカウントのデータを保護できます。アクセス方法として[役割の引き受け (Assume role)]または[役割の引き受け (EC2) (Assume role EC2)]を選択する前に、AWS ポータルでクロスアカウントデータアクセスを構成する必要があります。NetBackup には、アクセスキー、シークレットキー、役割 ARN のみが必要です。

クロスアカウントアクセスを作成するには、AWS のマニュアルに記載されたガイドラインに従ってください。簡単に説明すると、次の手順を実行する必要があります。

AWS クロスアカウントを構成するには:

1 AWS プロバイダポータルにログオンします。

2 保護するターゲット AWS アカウントで、新しい IAM ロールを作成します。

3 IAM ロール用の新しいポリシーを作成し、そのロールに、ターゲット AWS アカウントのバケットとオブジェクトにアクセスするために必要なアクセス権が割り当てられていることを確認します。p.16 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。

4 ソースとターゲットの AWS アカウント間で信頼関係を確立させます。

5 ソース AWS アカウントで、ソース AWS アカウントの IAM ロールがターゲット AWS アカウントの IAM ロールを引き受けられるようにするポリシーを作成します。

6 ソースアカウントユーザーにポリシーを設定し、このユーザーのアクセスキーとシークレットアクセスキーを、引き受けるロールに使用します。

証明書の失効の確認

NetBackup はすべてのクラウドプロバイダを対象に、OCSP (Online Certificate Status Protocol) を使用した、SSL 証明書の失効状態を検証する機能を提供しています。SSL と[証明書の失効を確認する (Check certificate revocation)]オプションの両方が有効になっている場合、NetBackup は各 SSL 証明書を検証します。検証のため、NetBackup は OCSP 要求を CA に送信し、SSL ハンドシェーク中に提示された証明書の失効状態を調べます。状態が失効と返された場合、または SSL 証明書に記載された OCSP エンドポイントへの接続に失敗した場合、NetBackup はクラウドプロバイダに接続しません。

検証を有効にするには、[クラウドオブジェクトストアアカウント (Cloud object store account)]ダイアログで、**[証明書の失効を確認する** `(Check certificate revocation)`**]** プロパティを更新します。

[証明書の失効を確認する (Check certificate revocation)]オプションを有効にするための要件

- OCSP エンドポイントは HTTP であるため、外部ネットワークへの HTTP (ポート 80) 接続を遮断するファイアウォールルールはすべてオフにします。例: http://ocsp.sca1b.amazontrust.com
- OCSP の URL は証明書から動的に取得されるため、不明な URL を遮断するファイアウォールルールはすべて無効にします。
- 通常、OCSP の URL のエンドポイントは IPV4 をサポートしています。IPV6 環境の場合、[証明書の失効を確認する (Check certificate revocation)]オプションは無効にします。
- プライベートクラウドには通常、自己署名証明書があります。そのため、プライベートクラウドでは証明書の失効の確認は必要ありません。アカウントの構成中にこのチェックを無効にしてください。無効にしないと、アカウントの作成が失敗します。
- CA の OSCP URL は、証明書の「Authority Information Access」拡張フィールドに記載されているはずです。

NetBackup クラウドの認証局 (CA) の管理

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

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

- Windows の場合:

  <installation-path>¥NetBackup¥var¥global¥cloud

- UNIX の場合:

  /usr/openv/var/global/cloud/

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

---

cacert.pem バンドルの CA を追加または削除できます。

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

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

CA を追加するには

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

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

   次の情報ブロックを追加します。

   ```
   Certificate Authority Name

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

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

   <Certificate content>

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

3. ファイルを保存します。

CA を削除するには

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

1 cacert.pem ファイルを開きます。

2 目的の CA を削除します。次の情報ブロックを削除します。

```
Certificate Authority Name

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

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

<Certificate content>

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

3 ファイルを保存します。

NetBackup によって承認されている CA のリスト

- Starfield Services Root Certificate Authority - G2
- Baltimore CyberTrust Root
- DigiCert Assured ID Root CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Global CA G2
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert High Assurance EV Root CA
- DigiCert Trusted Root G4
- D-Trust Root Class 3 CA 2 2009
- GlobalSign Root CA
- GlobalSign Root CA - R3
- COMODO RSA 認証局
- AAA 証明書サービス
- GoDaddy ルート認証局 - G2
- ISRG Root X1

新しい地域の追加

アカウントの作成時に、NetBackup で作成する特定のクラウドオブジェクトストアアカウントに新しい地域を追加できます。地域を追加すると、指定した地域にアクセスが制限されます。一部のクラウドオブジェクトストアプロバイダでは、地域の選択を実行できません。

新しい地域を追加するためのオプションは、Azure Data Lake Storage および Azure Data Lake Storage Government のプロバイダ形式では利用できません。

地域を追加するには:

1. 一意の地域名を入力します。[ロケーションの制約 (Location constraint)]に、関連付けられている地域のバケットまたはコンテナにアクセスするためにクラウドプロバイダサービスが使用するロケーション識別子を入力します。パブリッククラウドストレージの場合、クラウドプロバイダからロケーションの制約の詳細を取得する必要があります。

   AWS v4 署名をサポートするクラウドプロバイダの場合、[ロケーションの制約 (Location constraint)] フィールドの指定は必須です。該当するバケットで `getBucketLocation` API を使用して、ロケーションの制約の正しい値を取得できます。この API がロケーションの制約を空白として返す場合は、ロケーションの制約として「us-east-1」を使用します。

2. サービス URL を入力します。例: `hostname:port_number/service_path`
3. クラウドサービスプロバイダのエンドポイントのアクセススタイルを選択します。クラウドサービスプロバイダが URL の仮想ホスティングも追加でサポートする場合は、[仮想ホステッドスタイル (Virtual Hosted Style)]を選択します。それ以外の場合は、[パスの形式 (Path Style)]を選択します。
4. 地域に使用する HTTP ポートおよび HTTPS ポートを指定します。
5. [追加 (Add)]をクリックします。追加した地域は、[基本プロパティ (Basic properties)]ページの[地域 (Region)]テーブルに表示されます。

クラウドオブジェクトストアアカウントの管理

[クラウドオブジェクトストア (Cloud object store)]タブでは、クラウドオブジェクトストアアカウントを表示、追加、編集、および削除できます。また、このタブからクラウドオブジェクトストアアカウントのクレデンシャルを検証することもできます。

クラウドオブジェクトストアアカウントを表示するには

1. 左側で、[作業負荷 (Workloads)]、[クラウドオブジェクトストア (Cloud object store)]の順に選択します。
2. [クラウドオブジェクトストアアカウント (Cloud object store account)]タブに、利用可能なアカウントが表示されます。

保護対象の資産の手動検出

資産を手動で検出するには

1. 左側で、[作業負荷 (Workloads)]、[クラウドオブジェクトストア (Cloud object store)] の順に選択します。
2. 検出を実行するアカウントの行を選択し、上部にある[検出 (Discover)]をクリックします。または、アカウントの行にある省略記号メニュー (3 つのドット) をクリックし、[検出 (Discover)]をクリックします。

クラウドオブジェクトストアアカウントの編集

[編集 (Edit)]ページでは、プロバイダ、選択したサービスホスト、または地域を更新することはできません。

地域を変更するには、クラウドオブジェクトストアアカウントを削除して再作成する必要がある場合があります。アカウントがアクティブで、ジョブが関連付けられていない場合は、保守ウィンドウで実行できます。また、プライマリサーバーの[ホストプロパティ (Host Properties)]、[クラウドストレージ (Cloud storage)]で地域を更新することもできます。

クラウドオブジェクトストアアカウントを編集するには

1. 左側で、[作業負荷 (Workloads)]、[クラウドオブジェクトストア (Cloud object store)] の順に選択します。
2. 編集するアカウントを選択します。[編集 (Edit)]をクリックします。

   p.21 の「クラウドオブジェクトストアアカウントの追加」を参照してください。

クラウドオブジェクトストアアカウントのクレデンシャルの検証

クラウドオブジェクトストアアカウントのクレデンシャルを検証するには

1. 左側で、[作業負荷 (Workloads)]、[クラウドオブジェクトストア (Cloud object store)] の順に選択します。
2. 編集するアカウントを選択します。次に、[検証 (Validate)]をクリックします。

   検証プロセスの結果は、同じ列に表示されます。

クラウドオブジェクトストアアカウントの削除

クラウドオブジェクトストアアカウントを削除すると、NetBackup ではこのアカウントに関連付けられたポリシーは保護されなくなります。別のクラウドオブジェクトストアアカウントを使用して、既存のバックアップイメージをリカバリすることはできます。このクラウドオブジェクトストアアカウントに関連付けられているポリシーのバックアップは失敗します。

クラウドオブジェクトストアアカウントを削除するには

1. 左側で、[作業負荷 (Workloads)]、[クラウドオブジェクトストア (Cloud object store)]の順に選択します。
2. 編集するアカウントを選択します。それから[削除 (Delete)]をクリックします。
3. [削除 (Delete)]をクリックします。

マルウェアのスキャン

NetBackup バージョン 10.5 以降では、Cloud-Object-Store ポリシー形式を介して、クラウドオブジェクトストア資産のマルウェアスキャンをサポートしています。

マルウェアスキャンをトリガするには、スキャンホストを構成する必要があります。スキャンホストの構成について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「スキャンホストの構成」の章を参照してください。

バックアップイメージ

このセクションでは、クライアントバックアップイメージのポリシーでマルウェアをスキャンする手順について説明します。

クライアントバックアップイメージのポリシーでマルウェアをスキャンするには

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。
3. [検索基準 (Search by)]オプションで、[バックアップイメージ (Backup images)]を選択します。
4. 検索条件で、以下を確認して編集します。
   - ポリシー名 (Policy name): サポート対象のポリシー形式のみが一覧表示されます。
   - クライアント名 (Client name): サポート対象のポリシー形式のバックアップイメージを含むクライアントが表示されます。
   - ポリシー形式 (Policy type): ポリシー形式として Cloud-Object-Store を選択します。
   - バックアップ形式
   - コピー (Copies): 選択したコピーがインスタントアクセスをサポートしない場合、バックアップイメージのマルウェアスキャンはスキップされます。

- ディスクプール (Disk pool): MSDP (PureDisk)、OST (DataDomain)、AdvancedDisk ストレージ形式のディスクプールが一覧表示されます。
- ディスク形式 (Disk type): MSDP (PureDisk)、OST (DataDomain)、AdvancedDisk のディスク形式が一覧表示されます。
- マルウェアスキャンの状態 (Malware scan status)
- [バックアップの期間の選択 (Select the timeframe of backups)]で、日時の範囲を確認するか、更新します。

5 [検索 (Search)]をクリック: 検索条件を選択し、選択したスキャンホストがアクティブで利用可能であることを確認します。

6 [スキャンするバックアップの選択 (Select the backups to scan)]テーブルで、スキャンする 1 つ以上のイメージを選択します。

7 [マルウェアスキャナホストプールの選択 (Select a malware scanner host pool)]で、適切なホストプール名を選択します。

メモ: 選択したスキャンホストプールのスキャンホストは、NFS/SMB 共有形式で構成されているストレージサーバーで作成されたインスタントアクセスマウントにアクセスできる必要があります。

---

8 [マルウェアのスキャン (Scan for malware)]をクリックします。

9 スキャンが開始されると、[マルウェアのスキャン (Malware Scan)]の進捗が表示されます。

状態フィールドは次のとおりです。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)
  状態にカーソルを重ねると、スキャンが失敗した理由が表示されます。

  メモ: 検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートされるのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、ストレージに格納されたバックアップイメージのみです。

- 処理中 (In progress)
- 保留中 (Pending)

メモ: 1 つ以上の処理中および保留中のジョブのマルウェアスキャンをキャンセルできます。

ポリシー形式別の資産

NetBackup は、マルウェアスキャン向けの Cloud-Object-Store ポリシー形式もサポートします。

ポリシー形式でサポート対象の資産をスキャンするには、次の手順を実行します。

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。
3. [検索条件 (Search by)]オプションで、[ポリシー形式別の資産 (Assets by policy type)] (Cloud-Object-Store) を選択します。
4. [クライアント (Client)]または[資産 (Asset)]テーブルで、スキャンするクライアントまたは資産を選択します。
5. [次へ (Next)]をクリックします。

   前述の手順で選択したクライアントが複数のポリシー形式をサポートする場合、スキャンに単一のポリシー形式を選択できます。
6. [開始日付 / 時刻 (Start date/time)]と[終了日付 / 時刻 (End date/time)]で、日時の範囲を確認または更新します。

   スキャンは最大 100 個のイメージに対して開始されます。
7. [スキャナホストプール (Scanner host pool)]で、適切なホストプール名を選択します。
8. [マルウェアスキャンの現在の状態 (Current status of malware scan)]から、次のいずれかを選択します。
   - 未スキャン (Not scanned)
   - 感染なし (Not infected)
   - 感染 (Infected)
   - すべて (All)

9 ［マルウェアのスキャン (Scan for malware)］をクリックします。

警告: スキャンは 100 個までのイメージに制限されています。日付範囲を調整して再試行してください。

10 スキャンが開始されると、［マルウェアのスキャン (Malware Scan)］の進捗が表示されます。状態フィールドは次のとおりです。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

メモ: 状態にカーソルを重ねると、スキャンが失敗した理由が表示されます。

検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートされるのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、ストレージに格納されたバックアップイメージのみです。

- 保留中 (Pending)
- 処理中 (In progress)

マルウェアスキャン状態について詳しくは、『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。

3

クラウドオブジェクトストア資産の保護

この章では以下の項目について説明しています。

- クラウドオブジェクトストアポリシーの管理

アクセラレータのサポートについて

クラウドオブジェクトストア用の NetBackup アクセラレータは、バックアップを最適化します。バックアップホストまたはスケールアウトサーバーは、変更検出技術を使用して、クラウドオブジェクトストアのオブジェクトまたは BLOB の現在の状態を判断し、前回のバックアップ以降に発生した変更を特定します。バックアップホストまたはスケールアウトサーバーは、より効率のよいバックアップストリームによって、変更されたデータをメディアサーバーに送信します。メディアサーバーは、変更されたデータと、以前のバックアップで保存された残りのクラウドオブジェクトストアデータを結合します。オブジェクトまたは BLOB の一部がすでにストレージに存在し、かつ変更されていない場合、メディアサーバーはクライアントから同じ内容を読み込まず、代わりにストレージ内のコピーを使用します。アクセラレータバックアップには次の利点があります。

- クライアントの I/O と CPU のオーバーヘッドを削減できます。
- バックアップホストまたはスケールアウトサーバーとサーバー間で使用するネットワーク帯域幅が少ないコンパクトなバックアップストリームを作成します。
- 作成するバックアップイメージには、リストアに必要なすべてのデータが含まれています。

NetBackup アクセラレータとクラウドオブジェクトストアの連携方法

NetBackup アクセラレータは、バックアップストリームとバックアップイメージを次のように作成します。

- 指定されたポリシー、バケット、問い合わせのトラックログがバックアップホストまたはスケールアウトサーバーに存在しない場合、NetBackup は完全バックアップを実行し、トラックログを作成します。このトラックログには、次回のバックアップでの比較用に、問い合わせ条件に従ってバックアップされたオブジェクトまたは BLOB のデータに関する情報が含まれています。
- 次回のバックアップで、NetBackup は、前回のバックアップ以降変更されたデータまたはメタデータを識別します。この識別のために、NetBackup はバケットの問い合わせ条件に従って、オブジェクトまたは BLOB ごとにトラックログの情報とクラウドオブジェクトストアの情報を比較します。
- NetBackup バックアップホストまたはスケールアウトサーバーは、オブジェクトまたは BLOB で変更されたブロック、前回のバックアップ ID、変更されていないブロックのデータエクステント (ブロックオフセットとサイズ) のストリームをメディアサーバーに送信します。
- メディアサーバーは、オブジェクトまたは BLOB で変更されたブロック、バックアップ ID、変更されていないブロックのデータエクステントを受信します。メディアサーバー

は、バックアップ ID とオブジェクトまたは BLOB の記述子から、既存のバックアップにあるその他のオブジェクトまたは BLOB のデータの場所を特定します。

- メディアサーバーはストレージサーバーに対し、変更されたブロックを書き込み、それらのブロックと、ローカルに保存されているこれまで変更されていないブロックを組み合わせて、新しい完全イメージを作成するよう指示を出します。

アクセラレータの注意と要件

NetBackup アクセラレータについて次の点に注意してください。

- NetBackup アクセラレータが適切なライセンスを取得している必要があります。ライセンスの最新情報については、NetBackup 営業部門またはパートナー企業ご相談窓口までお問い合わせください。
- ディスクストレージユニットのみをサポートします。サポート対象のストレージは、メディアサーバー重複排除プール、NetBackup Appliance、クラウドストレージ、認定されたサードパーティの OST ストレージです。サポート対象のストレージ形式については、次の URL にある『NetBackup Enterprise Server and Server - Hardware and Cloud Storage Compatibility List』を参照してください。
http://www.netbackup.com/compatibility
- ストレージユニットグループは、グループでのストレージユニットの選択がフェールオーバーの場合にのみサポートされます。
- 完全バックアップと増分バックアップをサポートします。
- [アクセラレータを使用する (Use accelerator)]オプションを有効にするすべてのポリシーに対して、少なくとも次のバックアップスケジュールをお勧めします: [アクセラレータ強制再スキャン (Accelerator forced rescan)]オプションを有効にしている完全バックアップスケジュール。[アクセラレータ強制再スキャン (Accelerator forced rescan)]オプションを有効にしていない別の完全バックアップスケジュール。p.40 の「クラウドオブジェクトストアのアクセラレータ強制再スキャン (スケジュール属性)」を参照してください。
- バックアップホストまたはスケールアウトサーバーにポリシー、バケット、問い合わせの前回のバックアップ履歴がない場合、NetBackup は完全バックアップを行い、バックアップホストまたはスケールアウトサーバー上にトラックログを作成します。この初回バックアップは、通常の (加速なし) 完全バックアップの速度で実行されます。同じバックアップホストまたはスケールアウトサーバーを使用したそれ以後のアクセラレータバックアップでは、トラックログを使用してバックアップ速度を加速します。

メモ: 初めてポリシーを有効にしてアクセラレータを使用すると、次回のバックアップ (完全または増分) は実質的に完全バックアップとなります。これは、クラウドオブジェクトの問い合わせに対応するすべてのオブジェクトをバックアップします。そのバックアップが増分としてスケジュールされていると、バックアップ処理時間内に完了しない場合があります。

- NetBackup は、以降のアクセラレータバックアップのためにトラックログを保持します。問い合わせを追加すると、NetBackup はリストに追加された問い合わせに対して加速なしの完全バックアップを実行します。変更されていない問い合わせは、通常のアクセラレータバックアップとして処理されます。
- ポリシーを作成するとき、ポリシーに関連付けられるストレージユニットを検証できない場合は、後でバックアップジョブが始まるときストレージユニットが検証されます。アクセラレータがストレージユニットをサポートしない場合、バックアップは失敗します。bpbrm ログに、次のいずれかのようなメッセージが表示されます: ストレージサーバー %s、タイプ %s、イメージを含む場合はサポートされません (Storage server %s, type %s, does not support image include)。ストレージサーバー形式 %s、アクセラレータバックアップはサポートされません (Storage server type %s, does not support accelerator backup)。
- アクセラレータでは、ストレージの `OptimizedImage` 属性が有効になっている必要があります。
- [コピー後に期限切れにする (Expire after copy)]の保持を指定することにより、バックアップの実行中にイメージが期限切れになることがあります。新しい完全バックアップを合成するには、SLP ベースのアクセラレータバックアップで以前のバックアップが必要になります。
- メタデータの変更を検出するために、NetBackup はオブジェクトまたは BLOB ごとに 1 つ以上のクラウド API を使用します。そのため、変更検出時間は、処理対象のオブジェクトまたは BLOB の数に合わせて増加します。データの変更が少ないか、まったくない場合でもオブジェクト数が多い場合は、バックアップの実行が予想よりも長くなる場合があります。
- 環境内の特定のオブジェクトに対して、メタデータまたはタグは常にデータとともに変更 (追加、削除、更新) されます。パフォーマンスとコストの観点からアクセラレータありの増分ではなく、アクセラレータなしの増分を使用して評価します。
- 複数のタグベースの問い合わせでクラウドオブジェクトストアポリシーを作成するときに、アクセラレータで最適な効果を得るためにいくつかの単純なルールを使用できます。ポリシー作成ページで問い合わせビルダーを使用し、タグごとに 1 つの問い合わせを作成します。アクセラレータベースのポリシーは、この構成で最も高いパフォーマンスを発揮します。

クラウドオブジェクトストアのアクセラレータ強制再スキャン (スケジュール属性)

アクセラレータ強制再スキャンは、完全バックアップスケジュールのプロパティです。これは、クラウドオブジェクトストアポリシーには必要ありません。

クラウドオブジェクトストアポリシーでアクセラレータ強制再スキャンが有効な完全スケジュールを使用すると、変更検出ロジックはすべてのオブジェクトが変更されたと見なします。NetBackup は、データをダウンロードして指紋をとり、トラックログを使用して、データが変更されたかどうかを検出します。バックアップホストまたはスケールアウトサーバーとサーバー間では、使用するネットワーク帯域幅が少ないコンパクトなバックアップストリームが使用されます。

アクセラレータバックアップおよび NetBackup カタログ

アクセラレータを使用しても、NetBackup カタログのサイズに影響はありません。アクセラレータを使用する完全バックアップでは、アクセラレータなしで同じデータを完全バックアップする場合と同じカタログサイズになります。

これは、増分バックアップでも同様です。アクセラレータを使用するとき、アクセラレータなしの同じバックアップより大きいカタログ領域を必要としません。カタログに影響が生じる可能性は、完全バックアップでのアクセラレータの使用頻繁によって異なります。

アクセラレータを使用する完全バックアップは、通常の完全バックアップより高速に完了します。このため、増分バックアップの代わりにアクセラレータによる完全バックアップを使用するほうが有利に見えるかもしれません。

ただし、完全バックアップでは増分バックアップより大きなカタログ領域が必要なので、増分バックアップを完全バックアップに入れ替えるとカタログサイズが増えます。

NetBackup アクセラレータトラックログサイズの計算

アクセラレータトラックログには、オブジェクトのメタデータとファイル指紋が 128 KB セグメントに格納されます。トラックログはバックアップホストに格納されます。トラックログのサイズはバックアップするオブジェクトのサイズおよび数に比例します。トラックログは、ポリシー、バックアップ対象 (クラウドアカウントとバケット)、ストリームの組み合わせごとに個別に作成されます。

次に示すのはガイドラインのみで、特定の環境の要件は異なる可能性があります。データが頻繁に変更される環境では、より大きいトラックログサイズが必要になることがあります。

次の式を使用して、おおよそのトラックログサイズを計算できます。

```
Track log Size in Bytes = 2*( (Number of objects * 200) + ((Total
used disk space in KiB/128KiB) * 20))
```

たとえば、100 万個のオブジェクトを含む 1 TB のファイルシステムには、約 701 MB のトラックログが必要です。

アクセラレータが有効なポリシーのバックアップ対象またはストリーム数を変更した場合、NetBackup は新しいトラックログを作成することに注意してください。古いトラックログはバックアップホストに残ります。

増分バックアップについて

NetBackup は、クラウドオブジェクトストアの作業負荷の増分バックアップをサポートしています。アクセラレータを有効にしなくても増分バックアップを使用できます。

クラウドオブジェクトストアの作業負荷の場合、オブジェクトまたは BLOB の変更時刻を変更しないメタデータプロパティがいくつかあります。たとえば、Azure Blob の `Tags` です。これらのメタデータプロパティを変更しても、対応するオブジェクトは次回の増分バックアップで考慮されません。このため、増分バックアップ中にデータが失われたかのように見える場合があります。

Azure Data Lake と Azure Data Lake Government プロバイダの場合、ファイルまたはディレクトリの ACL を更新しても、ファイルまたはディレクトリの最終更新日時は変更されません。そのため、ACL のみを変更した場合は、ファイルとディレクトリは増分バックアップの対象になりません。

オブジェクトまたは BLOB の変更時刻を変更しないメタデータプロパティの詳細なリストについては、各クラウドプロバイダのマニュアルを参照してください。

増分バックアップの場合、オブジェクト名にパス形式の命名規則があると、パスごとに、エントリが NetBackup に追加されます。このパス形式の命名の最後のノードで表されるオブジェクトが、最後のバックアップ (使用される増分スケジュールに基づく、完全バックアップまたは最後の増分バックアップ) 以降に変更されていない場合、そのオブジェクトは次回の増分バックアップに含まれません。この動作が原因で、空のパスがカタログに表示され、リストアの参照ビューにも表示されます。

動的マルチストリームについて

クラウドオブジェクトストアポリシーのマルチストリームバックアップは、特定のバックアップ対象に対して同時バックアップストリームを実行します。バックアップ対象は複数のストリームに分割され、並列で実行されるため、バックアップ時間が短縮されます。クラウドオブジェクトストアポリシーの[バックアップ対象 (Backup Selection)]タブで、各ポリシーに対してストリーム数を構成できます。各バックアップストリームは一意のバックアップイメージを作成します。最終的に、ストリームによってそのバックアップ対象に作成されるすべてのイメージがその特定の選択のバックアップを表します。

動的マルチストリームは、新しく作成されたすべてのクラウドオブジェクトストアポリシーでデフォルトで有効になっています。

ストリームの最大数の指定

ポリシー属性で、バケットまたはコンテナに使用するストリームの最大数を指定できます。

p.46 の「ポリシーの属性」を参照してください。

動的マルチストリームの使用に関する考慮事項

- 動的マルチストリームを使用すると、バケットまたはコンテナ全体がバックアップされます。
- ポリシーで指定したストリームの数は、ポリシーが保護する各バケットに適用されます。たとえば、ポリシーに 10 個のストリームを指定し、バックアップ用に 5 個のバケットを選択すると、並列実行ストリームの数は 50 個になります。ポリシーに対して選択されたストレージユニットで許可される並列実行ジョブの最大数が、異なるポリシー全体で実行されているストリームの合計数より少ない場合、一部のストリームはキューに投入される場合があります。最適なパフォーマンスを得るために、選択したストレージで許可される[最大並列実行ジョブ数 (Maximum concurrent jobs)]プロパティを、ポリシー全体で実行すると予想されるストリームの合計数より大きく保ちます。
- 動的マルチストリームを使用する場合は、スケールアウトサーバーをバックアップホストとして使用できません。
- ジョブの再試行機能は、バックアップジョブでは機能しません。
- 「チェックポイントから再開」機能はサポートされません。
- 動的マルチストリームは、バケットまたはコンテナのすべてのバックアップストリームを同時に開始し、ストレージユニットに書き込みます。したがって、プライマリバックアップコピーのターゲットとしてテープストレージユニットを使用することはお勧めしません。最初のバックアップコピーのターゲットとして MSDP ストレージを使用し、セカンダリコピーまたは複製コピーのターゲットとしてテープストレージを構成できます。

クラウドオブジェクトストア資産のポリシーについて

バックアップポリシーは、NetBackup がオブジェクトのバックアップを作成するときに従う指示を提供します。単一のポリシーを作成して、クラウドオブジェクトストアアカウント内の複数のバケットまたはコンテナを保護できます。ポリシーを使用して保護するオブジェクトを選択できます。オブジェクトは NetBackup 環境で自動的に検出され、バックアップされます。クラウドオブジェクトストアアカウント内のオブジェクトに異なるバックアップロジックを適用するには、異なるポリシーが必要です。バックアップできるようにするには、すべてのクラウドオブジェクトストアアカウントが少なくとも 1 つのポリシーに含まれる必要があります。

ポリシーを使用して次の内容を構成できます。

- 使用するストレージユニットおよびストレージメディア
- バックアップスケジュール: 完全、差分増分、累積増分

- バックアップ対象: バケットまたはコンテナ全体、またはクエリーで指定した条件に一致するオブジェクトのグループ。
  バケットまたはコンテナ全体をポリシーに追加したり、クエリーを使用してバックアップするバケット内の必要なオブジェクトをインテリジェントに選択したりできます。

ポリシーの計画

ポリシーの構成は十分な柔軟性を備えているため、NetBackup 環境内のあらゆるクラウドオブジェクトストアアカウントのさまざまなニーズに対応できます。この柔軟性を活用するには、ポリシーの構成を開始する前に時間をかけて計画を立てます。

次の表は、ポリシー構成から最適な結果を確実に得るために行う手順の概要を説明したものです。

表 3-1　ポリシーの計画の手順

手順	処理	説明
手順 1	クラウドオブジェクトストアアカウントに関する情報を収集します。	各バケットまたはコンテナについて次の情報を収集します。 ■ アカウント名: アカウントに記載されているクレデンシャルと接続の詳細は、バックアップ中に REST API を使用してクラウドリソースにアクセスするために使用されます。アカウントは単一の地域に関連付けられているため、ポリシーにはその地域に関連付けられたバケットまたはコンテナのみを含めることができます。 ■ バケット名またはコンテナ名 ■ 各バケットまたはコンテナのバックアップ対象オブジェクトの概数。 ■ オブジェクトの典型的なサイズ。 あるアカウントにはいくつかのオブジェクト内に大量のデータが含まれ、別のアカウントにはそれよりも少ないオブジェクトが含まれる場合があります。バックアップ時間が長くならないように、大きいアカウントを 1 つのポリシーに含め、小さいアカウントは別のポリシーに含めてください。大きいアカウントには複数のポリシーを作成することをお勧めします。
手順 2	バックアップ要件に基づくオブジェクトのグループ分け	さまざまなバックアップおよびアーカイブ要件に応じて、アカウント内のさまざまなオブジェクトをグループ分けします。

手順	処理	説明
手順 3	格納要件の考慮	NetBackup 環境には、バックアップポリシーで対応する必要がある特別なストレージの必要条件があることがあります。 ストレージユニットおよびボリュームプールの設定は、ポリシーによってバックアップされるすべてのオブジェクトに適用されます。オブジェクトに特別なストレージの必要条件がある場合、スケジュールなどの他の要素が同じである場合でも、それらのオブジェクト用に個別のポリシーを作成します。
手順 4	バックアップスケジュールの考慮	1 つのポリシーのスケジュールがアカウント内のすべてのオブジェクトに対応していない場合、追加のバックアップポリシーを作成します。 追加のポリシーを作成することにした場合、次の要因を考慮します。 ■ バックアップを行う最適な時間帯。 異なるスケジュールで異なるオブジェクトをバックアップするには、異なるタイムスケジュールを指定した追加のポリシーが必要になることがあります。たとえば、夜間に稼働するオブジェクトと昼間に稼働するオブジェクト用に別々のポリシーを作成します。 ■ オブジェクトの変更頻度。 一部のオブジェクトが他のオブジェクトよりも高頻度で変更される場合、または、バケット/コンテナに新しいオブジェクトがより頻繁に追加される場合、その差によっては、異なるバックアップ頻度で別のポリシーの作成を検討する価値は十分にあります。 ■ バックアップを保持する期間。 各スケジュールには、そのスケジュールによってバックアップされるオブジェクトが NetBackup によって保持される期間を決定する値が設定されています。スケジュールはバックアップ対象リスト内のすべてのオブジェクトをバックアップするため、すべてのオブジェクトの保持要件が類似している必要があります。オブジェクトの完全バックアップを永久に保持する必要がある場合、そのオブジェクトを完全バックアップが 4 週間しか保持されないポリシーに含めないでください。

手順	処理	説明
手順 5	マルチストリームによるパフォーマンスの最適化	ご使用の環境での NetBackup のパフォーマンスは、次の 3 つの主要な要因に依存します。 ■ バックアップホスト (メディアサーバー) とクラウドストレージサービス間のネットワーク帯域幅。 ■ 複数の API 要求を処理するクラウドサーバーの機能。 ■ バックアップホスト (メディアサーバー) のシステムメモリ (RAM)。 保護するオブジェクトの数、利用可能なシステムリソースとネットワークリソースに応じて、ストリームを調整する必要があります。 NetBackup では、ポリシーごとに 8 から 16 個のストリームにすることをお勧めします。ただし、環境に応じてストリームの数を指定できます。
手順 6	バックアップ対象を正確に選択します。	必要な場合を除き、オブジェクト全体をバックアップする必要はありません。バックアップが必要なオブジェクトのみを選択してバックアップできるようにクエリーを作成します。

クラウドオブジェクトストアポリシーの前提条件

クラウドオブジェクトストアアカウントのポリシーの作成を開始する前に、次の前提条件を考慮してください。

- バケットとオブジェクトにアクセスするための、有効なクラウドオブジェクトストアアカウント。
- オブジェクトの選択で使用する、バケットと条件に関する有用な情報を[クラウドオブジェクト (Cloud objects)]タブに保存してください。
- クラウドオブジェクトストアアカウントと、ポリシーのためのバックアップホストまたはスケールアウトサーバーを指定するためのアクセスホストを表示および選択する権限が、[クラウドオブジェクト (Cloud objects)]タブで設定されている必要があります。
- 環境内の NetBackup アクセラレータの要件を評価します。アクセラレータを使用する場合は、ポリシーの作成時にこれを指定する必要があります。
- クラウドオブジェクトストアアカウントの検証に使用されるサーバーとは別に、バックアップホストまたはスケールアウトサーバーを使用する場合は、必要なポートが開かれ、構成が完了していることを確認します。これは、REST API 呼び出しを介してクラウドプロバイダのエンドポイントとのサーバー通信を有効にするために不可欠です。

クラウドオブジェクトストアに多数のバケットがある場合は、スケールアウトサーバーを使用できます。NetBackup Snapshot Manager は、実行時に必要な数だけデータムーバーコンテナをスケールアウトし、データ保護ジョブが完了したときに縮小できます。複数のバックアップホストを構成し、これらのバックアップホスト全体で負荷を分散するために複数のポリシーを作成することについて心配する必要はありません。

- 環境内の NetBackup の複数ストリームの要件を評価します。特定のバケットに対して、NetBackup はポリシーのバケットに定義されたクエリーごとに 1 つのストリームを作成します。複数ストリームを使用する場合、ポリシーの作成時にこれを指定できます。複数ストリームを使用するには、プライマリサーバーの[ホストプロパティ (Host properties)]の[クライアント属性 (Client attributes)]セクションで、バケットのジョブ数をクライアントとして構成する必要もあります。クライアント名を追加し、必要に応じて[最大データストリーム数 (Maximum data streams)]を設定します。

バックアップポリシーの作成

バックアップポリシーは、NetBackup がオブジェクトのバックアップを作成するときに従う指示を提供します。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。

名前、ストレージ形式、ジョブの優先度などのポリシー属性を定義します。	p.46 の「ポリシーの属性」を参照してください。
バックアップのスケジュールを設定します。	p.50 の「ポリシーのスケジュール属性の作成 」を参照してください。 p.53 の「開始時間帯の構成」を参照してください。 p.55 の「除外日の構成」を参照してください。 p.57 の「含める日の構成」を参照してください。
バックアップするアカウントとオブジェクトを選択します。	p.57 の「[クラウドオブジェクト (Cloud objects)]タブの構成」を参照してください。 p.59 の「条件の追加 」を参照してください。 p.60 の「タグ条件の追加 」を参照してください。 p.41 の「動的マルチストリームについて」を参照してください。

ポリシーの属性

次の手順では、バックアップポリシーの属性を選択する方法について説明します。

ポリシーの属性を選択する

1. 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。
2. [ポリシー名 (Policy name)]フィールドにポリシーの名前を入力します。
3. [ポリシー形式 (Policy type)]ドロップダウンから[Cloud-Object-Store]オプションを選択します。
4. [宛先 (Destination)]セクションで、次のデータストレージパラメータを構成します。
   - [データの分類 (Data classification)]属性では、バックアップを保存するストレージライフサイクルポリシーの分類を指定します。たとえば、ゴールド分類のバックアップはゴールドデータ分類のストレージユニットに送信する必要があります。デフォルトでは、NetBackup には 4 つのデータ分類 (プラチナ、ゴールド、シルバー、ブロンズ) があります。

     この属性は省略可能で、バックアップがストレージライフサイクルポリシーへ書き込まれる場合のみ適用されます。リストに[データの分類なし (No data classification)]が表示される場合、ポリシーは[ポリシーストレージ (Policy storage)]リストに表示されるストレージ選択を使います。データの分類を選択している場合、ポリシーによって作成されるイメージにはすべて分類 ID のタグが付けられます。
   - [ポリシーストレージ (Policy storage)]属性は、ポリシーのデータの格納先を指定します。[スケジュール (Schedule)]タブで、これらの選択を上書きできます。
     - 任意 (Any available): このオプションを選択した場合、ローカル接続されているストレージユニットへのデータの格納が NetBackup によって最初に試行されます。[ポリシーボリュームプール (Policy volume pool)]ドロップダウンから、[NetBackup]または[データストア (DataStore)]を選択します。[ポリシーボリュームプール (Policy volume pool)]属性は、ポリシーのバックアップを格納するデフォルトのボリュームプールを指定します。ボリュームプールは、1 つのアプリケーションで使用するためにグループ化されたメディアのセットです。ボリュームプールは、他のアプリケーションおよびユーザーによるアクセスから保護されます。

5 チェックポイントの間隔 (Take checkpoints every): バックアップ時にチェックポイントが作成される間隔を指定します。バックアップ時にチェックポイントを作成すると、バックアップが失敗した場合に時間を節約できます。バックアップの作成時にチェックポイントを定期的に設定すると、NetBackup は失敗したバックアップを最後のチェックポイントの先頭から再試行できます。通常は、再試行の方がジョブ全体を再開するより早く完了します。

チェックポイントの間隔とは、バックアップ時に NetBackup によってチェックポイントが設定される間隔を示します。デフォルトは 15 分です。管理者は、チェックポイントの間隔をポリシーごとに判断します。チェックポイントの間隔を選択する場合は、失敗したバックアップが再開するときに発生する可能性のある時間損失と、高頻度のチェックポイントによるパフォーマンス低下とのバランスを考慮します。設定したチェックポイントの間隔によってパフォーマンスに影響がある場合は、次のチェックポイントまでの時間を長くします。

チェックポイントはオブジェクトとオブジェクトの間の境界で保存され、バックアップされる、リスト内の次のオブジェクトを指します。チェックポイントはオブジェクトバックアップの途中で設定されることはありません。オブジェクトのバックアップ後、チェックポイントは保存されます。

6 [ポリシーごとにジョブ数を制限する (Limit jobs per policy)] 属性は、ポリシーの実行時に NetBackup によって並列して実行されるジョブの数を制限します。デフォルトでは、このチェックボックスのチェックははずされており、NetBackup が同時に実行するバックアップジョブの数に制限はありません。ジョブ数は、他のリソース設定によって制限される場合があります。

構成内に含まれるデバイス数が多い場合、パフォーマンスに悪影響を及ぼすほど多くの並列実行バックアップが実行される可能性があります。それより低い上限を指定するには、[ポリシーごとにジョブ数を制限する (Limit jobs per policy)] を選択して、1 から 999 の値を指定します。

7 [ジョブの優先度 (Job priority)] フィールドに 0 から 99999 までの値を入力します。この数値は、他のポリシーとの間でリソースが競合した場合のポリシーの優先度を指定します。数値が大きいほど、ジョブの優先度が高くなります。NetBackup は、最も優先度が高いポリシーに最初の利用可能なリソースを割り当てます。

8 [メディア所有者 (Media owner)] フィールドは、[ポリシーストレージ (Policy storage)] 属性が [任意 (Any Available)] に設定されているときに使用できます。[メディア所有者 (Media owner)] 属性は、そのポリシーのバックアップイメージが書き込まれるメディアを所有するメディアサーバーまたはサーバーグループを指定します。

- 任意 (Any) (デフォルト): NetBackup によってメディアの所有者が選択されます。NetBackup によって、メディアサーバーまたはサーバーグループ (構成されている場合) が選択されます。
- なし (None): メディアにイメージを書き込むメディアサーバーがそのメディアの所有者として指定されます。メディアサーバーを明示的に指定しなくても、メディアサーバーがメディアを所有するように設定されます。

9 ポリシーをアクティブ化するには、[有効になる日時 (Go into effect at)]オプションを選択し、アクティブ化の日時を設定します。NetBackup でポリシーを使用するには、そのポリシーを有効にする必要があります。日時が、バックアップを再開する日時に設定されていることを確認します。

ポリシーを無効にするには、オプションを選択解除します。[ポリシー (Policieis)]リストには、無効なポリシーが含まれます。

10 [複数のデータストリームを許可する (Allow multiple data streams)]オプションがデフォルトで選択され、読み取り専用になっています。このオプションにより、NetBackup は、各問い合わせの自動バックアップを複数のジョブに分割できます。ジョブは個別のデータストリームにあるので、並列実行できます。

複数ストリームジョブは、ストリームの検出を実行する 1 つの親ジョブと、各ストリームに対する複数の子ジョブで構成されます。各子ジョブには、そのジョブ ID が、[アクティビティモニター (Activity monitor)]の[ジョブ ID (Job ID)]列に表示されます。親ジョブのジョブ ID は[親ジョブ ID (Parent Job ID)]列に表示されますが、この列はデフォルトでは表示されません。親ジョブの[スケジュール (Schedule)]列には、ダッシュ (-) が表示されます。

11 ポリシーのアクセラレータを有効にするには、[アクセラレータの使用 (Use Accelerator)]オプションを選択します。

NetBackup アクセラレータは、バックアップを高速化します。高速化は、クライアント上の変更検出技術によって実現されます。バックアップホストまたはスケールアウトサーバーは変更検出技術を使用して、クラウドオブジェクトストアのオブジェクトまたは BLOB の現在の状態を判断し、前回のバックアップ以降に発生した変更を特定します。クライアントは、より効率のよいバックアップストリームによって、変更されたデータをメディアサーバーに送信します。メディアサーバーは、変更されたデータと、前回のバックアップで保存されたクライアントデータすべてを結合します。

オブジェクトまたはオブジェクトの一部がすでにストレージに存在し、かつ変更されていない場合、メディアサーバーはクライアントから同じ内容を読み込まず、代わりにストレージ内のコピーを使用します。結果は、NetBackup の完全バックアップです。

12 クライアント側の重複排除オプションから[すべてのクライアントで無効 (Disable for all clients)]オプションを選択します。NetBackup クラウドオブジェクトストアの保護では、バックアップホストがクライアントとして使用されます。

13 [キーワード句 (Keyword phrase)]属性は、NetBackup がポリシーに基づくすべてのバックアップまたはアーカイブに関連付けられる句です。キーワード句がサポートされているのは、Windows および UNIX クライアントインターフェースだけです。

クライアントは複数のポリシーに同じキーワード句を使用できます。同じキーワード句を使用することで、複数の関連するポリシーのバックアップを結び付けることができます。たとえば、別々のポリシーを必要としながらも類似のデータが含まれている複数のクライアントのバックアップに、キーワード句「legal department documents」を使用します。

このキーワード句の最大長は 128 文字です。空白やピリオドを含め、すべての印字可能な (printable) 文字 (ASCII) を使用できます。デフォルトでは、キーワード句は空白です。

ポリシーのスケジュール属性の作成

このトピックでは、クラウドオブジェクトストアポリシーの特定のスケジュールプロパティを設定する方法について説明します。スケジュールプロパティは、ユーザー固有のバックアップ戦略やシステム構成によって異なります。他のスケジュールプロパティについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

スケジュールを作成するには:

1 左側で、[保護 (Protection)]の下の[ポリシー (Policies)]をクリックします。[スケジュール (Schedules)]タブをクリックします。[バックアップスケジュール (Backup schedules)]で、[追加 (Add)]をクリックします。[属性 (Attributes)]タブをクリックします。

2 [属性 (Attributes)]タブの[名前 (Name)]フィールドに、スケジュールの名前を入力します。

3 [バックアップ形式 (Type of backup)]を選択します。

- 完全バックアップ (Full Backup): すべてのデータオブジェクトとログが含まれるオブジェクトの完全なバックアップ。
- 差分増分バックアップ (Differential Incremental Backup): 前回のバックアップ以降に変更されたブロックのバックアップ。差分増分バックアップを設定する場合は、完全バックアップも設定する必要があります。
- 累積増分バックアップ: 前回の完全バックアップ以降に変更されたオブジェクトをすべてバックアップします。バックアップが一度も行われていない場合、すべてのオブジェクトのバックアップが行われます。

4 このポリシーの NetBackup アクセラレータを有効にするには、[アクセラレータ強制再スキャン (Accelerator forced rescan)]オプションを選択します。このオプションを使用すると、バックアップ時に各オブジェクトの内容のチェックサムが作成されます。このチェックサムを使用して変更箇所を検出できます。次回のアクセラレータバックアップの新たな基準を確立することで、セーフティネットの役割を果たします。

5 [ポリシーストレージの選択を上書きする (Override policy storage selection)]属性は次のように機能します。

- 無効 (Disabled): ポリシーの[属性 (Attributes)]タブで指定された[ポリシーストレージ (Policy storage)]を使用するようにスケジュールに指示します。
- 有効 (Enabled): ポリシーの[属性 (Attributes)]タブで指定された[ポリシーストレージ (Policy storage)]を上書きするようにスケジュールに指示します。
  以前に構成されたストレージユニットとストレージライフサイクルポリシーのリストからのストレージを選択します。リストが空なら、ストレージは構成されていません。

6 [ポリシーボリュームプールを上書きする (Override policy volume pool)]属性は次のように機能します。

- 無効 (Disabled): ポリシーの[属性 (Attribute)]タブで[ポリシーボリュームプール (Policy volume pool)]として指定されたボリュームプールを使用するようにスケジュールに指示します。ポリシーのボリュームプールが指定されていない場合、デフォルトで NetBackup が使用されます。
- 有効 (Enabled): ポリシーの[属性 (Attribute)]タブで[ポリシーボリュームプール (Policy volume pool)]として指定されたボリュームプールを上書きするようにスケジュールに指示します。構成済みのボリュームプールのリストからボリュームプールを選択します。

7 [メディア所有者を上書きする (Override media owner)]の選択属性は次のように機能します。

- 無効 (Disabled): ポリシーの[属性 (Attribute)]タブで[メディア所有者 (Media owner)]として指定されたメディア所有者を使用するようにスケジュールに指示します。
- 有効 (Enabled): ポリシーの[属性 (Attribute)]タブで[メディア所有者 (Media owner)]として指定されたメディア所有者を上書きするようにスケジュールに指示します。
  リストから新しいメディア所有者を選択します。
  - 任意 (Any)。
    NetBackup によって、メディアサーバーまたはサーバーグループのいずれかからメディア所有者が選択されます。
  - なし (None)。

メディアに書き込みを行うメディアサーバーをそのメディアの所有者として指定します。メディアサーバーを明示的に指定しなくても、メディアサーバーがメディアを所有するように設定されます。

8 ［スケジュール形式 (Schedule type)］で、［カレンダー (Calendar)］または［間隔 (Frequency)］を選択します。

- カレンダー (Calendar): カレンダーベースのスケジュールにより、カレンダービューに基づいてジョブスケジュールを作成できます。［カレンダー (Calendar)］を選択して［含める日 (Include dates)］タブを表示します。
  ［実行日後の再試行を許可する (Retries allowed after run day)］を有効にすると、バックアップが正常に完了するまで、NetBackup によってスケジュールが試行されます。この属性を有効にした場合、指定した実行日以降もスケジュールの実行が試行されます。
- 間隔 (Frequency): ［間隔 (Frequency)］属性を使用すると、スケジュールされた作業が正常に完了してから次の作業が試行されるまでの間隔を指定できます。たとえば、1 週間に 1 回の間隔で完全バックアップを行うスケジュールを設定すると想定します。月曜日にすべてのクライアントの完全バックアップを正常に完了した場合、次の月曜日までこのスケジュールによる別のバックアップが試行されません。
  間隔を設定するには、リストから間隔の値を選択します。間隔は秒、分、時間、日、または週単位で指定できます。

9 バックアップの［保持 (Retention)］期間を指定します。この属性は NetBackup がバックアップを保持する期間を指定します。保持期間を設定するには、リストから期間 (またはレベル) を選択します。保持期間が満了すると、期限が切れたバックアップの情報が削除されます。バックアップの期限が切れると、そのバックアップ内のオブジェクトをリストアに利用できなくなります。たとえば、保持期間が 2 週間の場合、そのスケジュールによって行われたバックアップのデータをリストアできるのは、バックアップ後 2 週間だけです。

10 ［メディアの多重化 (Media multiplexing)］属性は、NetBackup で任意のドライブ上に多重化できる、スケジュールのジョブの最大数を指定します。多重化とは、1 台または複数のクライアントから 1 つのドライブに並列して複数のバックアップジョブを送信し、バックアップをメディア上に多重化することです。

1 から 32 の数値を指定します。1 を指定すると、多重化されません。スケジュールが次回実行されるときに変更が有効になります。

11 ［追加 (Add)］をクリックして属性を追加するか、［追加してさらに追加 (Add and add another)］をクリックして別のスケジュールに別の属性セットを追加します。

開始時間帯の構成

[開始時間帯 (Start window)]タブは、スケジュールの使用時に NetBackup でジョブを開始できる期間を設定するための制御を提供します。この期間を時間帯と呼びます。ジョブを完了するために必要な要件を満たすように、時間帯を構成します。

たとえば、異なる複数の時間帯を作成します。

- 毎日特定の期間、バックアップを開始できる時間帯。
- 1 週間いつでもバックアップを開始できる時間帯。

ポリシースケジュールでの時間帯の追加、変更、削除

時間帯を追加、変更、または削除するには、次のいずれかの手順を使用します。

開始時間帯を構成するには:

1. 左側で、[保護 (Protection)]の下の[ポリシー (Policies)]をクリックします。[スケジュール (Schedules)]タブをクリックします。[バックアップスケジュール (Backup schedules)]で、[追加 (Add)]をクリックします。[開始時間帯 (Start Window)]タブをクリックします。
2. 時間帯の開始を指定するには、次の操作を実行します。

時間テーブルでカーソルをドラッグします。	その時間帯を開始する日時をクリックし、それを終了する日時までドラッグします。
ダイアログボックスの設定を使用します。	■ [開始日 (Start day)]フィールドで、時間帯を開始する最初の日を選択します。 ■ [開始時刻 (Start time)]フィールドで、時間帯の開始時刻を選択します。

3. 時間帯の終了を指定するには、次のいずれかの操作を実行します。

時間テーブルでカーソルをドラッグします。	その時間帯を開始する日時をクリックし、それを終了する日時までドラッグします。
時間帯の期間を入力します。	[期間 (日 時:分) (Duration (days hours: minutes))]フィールドに期間を入力します。
時間帯の終わりを指定します。	■ [終了曜日 (End day)]リストで日を選択します。 ■ [終了時刻 (End time)]フィールドで時間を選択します。

時間帯は、スケジュール表示にバーで表示されます。

ポリシー内のすべてのクライアントのバックアップが完了できるように、十分な時間を指定します。

また、NetBackup 以外の要因でスケジュールの開始が遅れる場合のために、スケジュールに時間的余裕もとっておきます。(たとえば、利用不能なデバイスが原因で遅延が発生します)。そうしないと、一部のバックアップが開始されない可能性があります。

4 必要に応じて、次のいずれかを実行します。

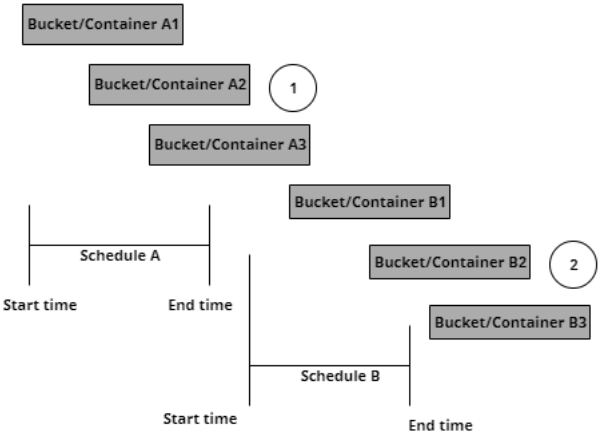
[削除 (Delete)]をクリックします。	選択した時間帯を削除します。
[消去 (Clear)]をクリックします。	スケジュール表示からすべての時間帯を削除します。
[複製 (Duplicate)]をクリックします。	選択した時間帯を週全体にレプリケートします。
[元に戻す (Undo)]をクリックします。	最後の操作を取り消します。

5 次のいずれかを実行します。

[追加 (Add)]をクリックします。	時間帯を保存し、ダイアログボックスを開いたままにする場合。
[追加してさらに追加 (Add and add another)]をクリックします。	時間帯を保存し、別の時間帯を追加する場合。

スケジュールの期間の例

この例では、2 つの完全バックアップスケジュールにスケジュールの期間が与える影響を示します。スケジュール B の開始時刻が、前のスケジュール A の終了時刻の少し後に設定されています。どちらのスケジュールにも、バックアップが予定されている 3 つのバケット/コンテナが含まれています。



図は次の点を示しています。

ポイント 1

バケット/コンテナ A3 はスケジュール A の時間帯内に開始しますが、スケジュール B の開始時刻の後まで完了しません。ただし、バックアップが実行されている間に時間帯が終了しても、バケット/コンテナ A3 は完了するまで実行されます。スケジュール B のバケット/コンテナ B1 は、バケット/コンテナ A3 が完了するとすぐに開始されます。

ポイント 2

スケジュール A により、スケジュール B のすべてのバケット/コンテナをバックアップするための十分な時間が残されません。その結果、時間帯が終了したため、バケット/コンテナ B3 は開始できません。バケット/コンテナ B3 は、次にスケジュール B が実行されるときまで待機する必要があります。

除外日の構成

バックアップポリシーのスケジュールから特定の日付を除外するには、[除外日 (Exclude dates)]タブを使用します。日付がスケジュールから除外されると、その日にジョブは実行されません。タブには連続した 3 カ月のカレンダーが表示されます。表示される最初の月または年を変更するには、カレンダー上部のリストを使用します。

スケジュールから日付を除外するには:

1. 左側で、[保護 (Protection)]の下の[ポリシー (Policies)]をクリックします。[スケジュール (Schedules)]タブをクリックします。[バックアップスケジュール (Backup schedules)]で、[追加 (Add)]をクリックします。[除外日 (Exclude dates)]タブをクリックします。
2. 次のいずれか、または複数の方法を使用して、除外する日付を指定します。
   - 除外する曜日を 3 カ月カレンダーで選択します。月または年を変更するには、カレンダーの上部にあるドロップダウンリストを使用します。
   - [曜日指定 (Recurring week days)]を設定するには:
     - 毎年の毎月のすべての曜日を選択するには、[すべて設定 (Set all)]をクリックします。
     - 既存のすべての選択を削除するには、[すべてクリア (Clear all)]をクリックします。
     - 毎月の特定の曜日を除外するように選択するには、マトリックスのボックスにチェックマークを入れます。
     - 毎月の特定の曜日を除外するには、曜日の列ヘッダーをクリックします。
     - 毎月の特定の週を除外するには、[1 番目 (1st)]、[2 番目 (2nd)]、[3 番目 (3rd)]、[4 番目 (4th)]、または[最終週 (Last)]の行ラベルをクリックします。
   - [日付指定 (Recurring days of the month)]を設定するには:
     - 毎月のすべての日付を選択するには、[すべてを設定 (Set All)]をクリックします。
     - 既存のすべての選択を削除するには、[すべてクリア (Clear all)]をクリックします。
     - 毎月の特定の曜日を除外するように選択するには、マトリックスのボックスにチェックマークを入れます。
     - 毎月の最終日を除外するには、[最終日 (Last Day)]をクリックします。
   - [特定日指定 (Specific dates)]を設定するには:
     - [新規 (New)]をクリックします。ダイアログボックスに月、日および年を入力します。
       その日付が[特定日指定 (Specific dates)]リストに表示されます。
     - 日付を削除するには、リストの日付を選択します。[削除 (Delete)]をクリックします。
3. [追加 (Add)]をクリックして変更を保存します。

含める日の構成

［含める日 (Include dates)］タブは［スケジュールの追加 (Add schedule)］または［スケジュールの変更 (Edit schedule)］タブに表示されます。タブを表示するには、［属性 (Attributes)］タブで［スケジュール形式 (Schedule type)］として［カレンダー (Calendar)］オプションを選択する必要があります。カレンダーを基準としてスケジュールを設定すると、作業の実行日付を決定するときに、複数の実行日付オプションを指定できます。

タブには連続した 3 カ月のカレンダーが表示されます。表示される最初の月または年を変更するには、カレンダー上部のリストを使用します。

［クラウドオブジェクト (Cloud objects)］タブの構成

［クラウドオブジェクト (Cloud objects)］タブでは、クラウドリソースに接続して目的のバケット内のオブジェクトを保護するために使用するクラウドオブジェクトストアアカウントを選択できます。NetBackup では、ポリシーを使用して保護するバケット/コンテナ、およびオブジェクトを個別に選択できます。問い合わせを使用することで、保護する項目をインテリジェントにフィルタ処理したり選択したりできます。

NetBackup は、ポリシーごとに 1 つのバックアップホストまたはスケールアウトサーバーをサポートします。したがって、負荷を分散するには複数のポリシーを作成する必要があります。クエリーを使用すると、複数のバックアップホストまたはスケールアウトサーバー間でバックアップされるバケットまたはオブジェクトの負荷を二分割できます。

クラウドオブジェクトを構成するには:

1 [クラウドオブジェクトストアアカウント (Cloud object store account)]と[ホスト (Host)]を選択します。アクセス権のあるアカウントとバックアップホストの一覧を表示できます。アカウントにスケールアウトサーバーを使用する場合、[ホスト (Host)]フィールドは無効になります。ポリシーの作成時にスケールアウトサーバーを変更することはできません。

2 (オプション) [動的マルチストリームを許可する (Allow dynamic multi-streaming)]オプションを選択すると、NetBackup は、各バケットまたはコンテナの自動バックアップを並列実行の複数のストリームに分割できます。このオプションを使用すると、保護対象のバケットまたはコンテナのバックアップ時間を大幅に短縮できます。

この[バケット/コンテナあたりの最大ストリーム数 (Maximum number of streams per bucket/container)]フィールドで、1 から 64 までの数を指定します。デフォルト値は 8 です。

ポリシーに対して選択されたストレージユニットで許可される並列実行ジョブの最大数が、ポリシーに対して実行されているストリームの合計数より少ない場合、一部のストリームはキューに投入される場合があります。最適なパフォーマンスを得るために、選択したストレージで許可される[最大並列実行ジョブ数 (Maximum concurrent jobs)]プロパティを、ポリシーが処理すると予想されるストリームの合計数より大きく保ちます。ストレージの[最大並列実行ジョブ数 (Maximum concurrent jobs)]の最小値は 64 である必要があります。

メモ: 動的マルチストリームを有効にすると、選択したすべてのバケットとコンテナが完全にバックアップされます。選択したバケットまたはコンテナの問い合わせは定義できません。

---

3 バケットまたはコンテナを追加するには、[バケット/コンテナ (Buckets/Containers)]テーブルの近くにある[追加 (Add)]をクリックします。[バケットまたはコンテナの追加 (Add bucket/containers)]ダイアログで、次のいずれかを実行してバケットまたはコンテナを追加します。

- 特定のコンテナを追加するには、[バケット/コンテナ名 (Bucket/Container name)]フィールドに名前を入力し、[追加 (Add)]をクリックします。
- [バケット/コンテナ (Bucket/Containers)]テーブルからバケットまたはコンテナを 1 つ以上選択し、[追加 (Add)]をクリックします。テーブル上部の検索ボックスを使用して、リストをフィルタ処理できます。

クラウドオブジェクトストアアカウントのクレデンシャルにバケットを一覧表示する権限がない場合、バケットリストは空のままです。ただし、バケットは手動で追加できます。

[クラウドオブジェクト (Cloud objects)]タブで、[バケット/コンテナ (Buckets/Containers)]テーブルの任意のバケット/コンテナ名の行にある[削除

(Remove)]をクリックして、ポリシーから削除します。検索ボックスにキーワードを入力して、テーブルをフィルタ処理します。

4 選択したバケットまたはコンテナに問い合わせを追加するには、[問い合わせ (Queries)]で[問い合わせの追加 (Add query)]をクリックします。

5 問い合わせの名前を入力し、問い合わせを使用してフィルタ処理するバケットを選択します。

6 [オブジェクト/BLOB を選択 (Select objects/blobs)]テーブルで[選択されたバケット/コンテナ内にあるすべてのオブジェクト/BLOB を含める (Include all objects/blobs in the selected buckets/containers)]オプションを選択して 1 つ以上のバケット全体をバックアップします。

7 [問い合わせなしのバケット (Buckets with no queries)]で、問い合わせを追加するバケットまたはコンテナを選択します。バケットですべての問い合わせを含めることが事前に選択されている場合、そのバケットはこのリストには表示されません。条件またはタグ条件を追加するには、[条件の追加 (Add condition)]または[タグ条件の追加 (Add Tag condition)]をクリックします。詳しくはそれぞれ、p.59 の「条件の追加 」を参照してください。 およびp.60 の「タグ条件の追加 」を参照してください。を参照してください。

条件の追加

NetBackup では、インテリジェントな問い合わせを使用して、バケットまたはコンテナ内のバックアップオブジェクト/コンテナを選択的にバックアップできます。条件またはタグ条件を追加して、バックアップするバケットまたはコンテナ内のオブジェクト/BLOB を選択できます。

動的マルチストリームを有効にすると、選択したすべてのバケットとコンテナが完全にバックアップされます。選択したバケットまたはコンテナの問い合わせは定義できません。

条件を追加するには:

1. ポリシーの作成時に、[クラウドオブジェクト (Cloud objects)]タブの[問い合わせ (Queries)]で[問い合わせの追加 (Add query)]をクリックします。
2. [問い合わせの追加 (Add a query)]ダイアログで、問い合わせの名前を入力し、問い合わせを適用するバケットを選択します。バケットのリストには、すべてのオブジェクトを含めるよう選択されていないバケットのみが表示されます。

   メモ: 問い合わせの編集中に、すべてのオブジェクトを含めるよう選択されたバケットを表示できますが、編集オプションが無効になっています。

   [問い合わせ (Queries)]テーブルには、追加した問い合わせが表示されます。[問い合わせ名 (Query name)]と[問い合わせ (Queries)]列の値を使用して、問い合わせを検索できます。[問い合わせ (Queries)]列の値には、[選択されたバケット/コンテナ内にあるすべてのオブジェクト/BLOB を含める (Include all objects/blobs in the selected buckets/containers)]オプションを選択した問い合わせは含まれません。
3. 選択したバケット内のすべてのオブジェクトをバックアップするには、[選択したバケットのオブジェクトをすべて含める (Include all objects in the selected buckets)]オプションを選択します。
4. 条件を追加するには、[条件の追加 (Add condition)]をクリックします。

   接頭辞またはオブジェクトのいずれかを使用して条件を設定できます。同じ問い合わせに接頭辞とオブジェクトの両方は使用できません。条件に空のフィールドを残さないでください。
5. ドロップダウンから[接頭辞 (prefix)]または[オブジェクト (object)]を選択し、テキストフィールドに値を入力します。[条件 (Condition)]をクリックして、別の条件を追加します。ブール演算子 OR で条件を結合できます。
6. [追加 (Add)]をクリックして条件を保存します。

タグ条件の追加

タグ条件を追加してキーと値のペアやブール条件を使用することで、バックアップするオブジェクトまたは BLOB を選択できます。

この機能は、Azure Data Lake Storage プロバイダおよび Azure Data Lake Storage Government プロバイダでは利用できません。

タグ条件を追加するには:

1. ポリシーの作成時に、[クラウドオブジェクト (Cloud objects)]タブの[問い合わせ (Queries)]で[問い合わせの追加 (Add query)]をクリックします。
2. [問い合わせの追加 (Add a query)]ダイアログで、問い合わせの名前を入力し、問い合わせを適用するバケットを選択します。バケットのリストには、すべてのオブジェクトを含めるよう選択されていないバケットのみが表示されます。
3. 選択したバケット内のすべてのオブジェクトをバックアップするには、[選択したバケットのオブジェクトをすべて含める (Include all objects in the selected buckets)]オプションを選択します。
4. タグ条件を追加するには、[タグ条件の追加 (Add Tag Condition)]をクリックします。
5. [タグキー (Tag Key)]と[タグの値 (Tag Value)]の値を入力して条件を作成します。ブール演算子 AND は値を結合します。NetBackup はキーと値のペアが一致するオブジェクトをバックアップします。
6. 条件を追加するには、[タグ条件 (Tag condition)]をクリックします。AND または OR ブールパラメータを使用してタグ条件を接続できます。
7. [追加 (Add)]をクリックして条件を保存します。

条件とタグ条件の例

条件とタグ条件の使用方法の例を次に示します。

コンテナまたはバケットに、次のファイルまたはディレクトリが存在するとします。

- 次の BLOB は「Project」:「HR」タグでタグ付けされます
  - OrganizationData/Hr/resumes/resume1_selected.pdf
  - OrganizationData/Hr/resumes/resume2_rejected.pdf
  - OrganizationData/Hr/resumes/resume3_noupdate.pdf
- 次の BLOB は「Project」:「Finance」タグ値でタグ付けされます
  - OrganizationData/Fin/accounts/account1/records1.txt
  - OrganizationData/Fin/accounts/account2/records2.txt
  - OrganizationData/Fin/accounts/account3/records3.txt
  - OrganizationData/Fin/accounts/monthly_expenses/Jul2022.rec
  - OrganizationData/Fin/accounts/monthly_expenses/Aug2022.rec
- 次の BLOB は「Project」:「Security」でタグ付けされます
  - BLOB Getepass.pdf: 「TypeOfData」:「ID_Cards」というもう 1 つのタグが存在するため、これは 2 つのタグ (Security と ID_Cards) でタグ付けされます。

- OrganizationData/newJoinees/tempPassesList.xls

- 次の BLOB は「Project」:「Environment」でタグ付けされます
  - EnvironmentContribution.xls
  - NewPlantedTrees.xls

接頭辞条件の例:

- ケース 1: `OrganizationData` から、状態 (採用、不採用など) に関係なくすべての履歴書をバックアップするには、次の問い合わせを追加します。
  `prefix Equal to OrganizationData/Hr/resumes/resume`
  結果: `OrganizationData/Hr/resumes/resume` で始まるすべてのレコードがバックアップされます。
- ケース 2: Fin と HR からすべての履歴書とレコードをバックアップするには、次のいずれかの問い合わせを追加します。
  `prefix Equal to OrganizationData/Hr/resumes/resume`
  または
  `prefix Equal to OrganizationData/Fin/accounts/account1/rec`

  メモ: 複数の接頭辞を OR 条件で追加できます。

結果: `OrganizationData/Hr/resumes/resume` または `OrganizationData/Fin/accounts/account1/rec` で始まるすべてのレコードがバックアップされます。

オブジェクト条件の例:

特定のオブジェクトまたは BLOB をバックアップするには、次の問い合わせを追加します。

```
object Equal to
OrganizationData/Fin/accounts/monthly_expenses/Jul2022.rec
```

結果: `Jul2022.rec` という名前の BLOB のみが選択されます。

タグ条件の例:

- ケース 1: 「Project」:「Finance」でタグ付けされたすべての BLOB をバックアップするには、次の問い合わせを追加します。
  tagKey Equal to 'Project' and tagVal Equal to 'Finance'
  結果: 「Project」=「Finance」でタグ付けされたすべてのオブジェクトまたは BLOB が選択されます。
- ケース 2: プロジェクト Finance または Security と一致するデータをバックアップするには、次の問い合わせを追加します。

tagKey Equal to 'Project' and tagValue eq 'Finance' OR tagKey Equal to 'Project' and tagValue eq 'Security'
結果:「Project」:「Finance」または「Project」:「Security」でタグ付けされたすべてのオブジェクトまたは BLOB が選択されます。

- ケース 3:「Project」:「Security」かつ「TypeOfData」:「ID_Cards」のデータをバックアップするには、次の問い合わせを追加します。
  (tagKey Equal to 'Project' and tagValue Equal to 'Security') AND (tagKey Equal to 'TypeOfData' and tagValue Equal to 'ID_Cards')
  結果: タグ「Project」:「Security」かつ「TypeOfData」:「ID_Cards」のデータが選択されます。

クラウドオブジェクトストアポリシーの管理

ポリシーを追加、編集、削除、コピー、および無効化できます。ポリシーの手動バックアップを実行することもできます。

クラウドオブジェクトストアポリシーの表示

1. 左側で[ポリシー (Policies)]をクリックします。表示する権限を持っているすべてのポリシーが表示されます。
2. クラウドオブジェクトストアポリシーのテーブルをフィルタ処理するには、フィルタアイコンをクリックして[Cloud-Object-Store]を選択します。

   ポリシーを検索するには、テーブルの上部にある検索ボックスを使用します。

クラウドオブジェクトストアポリシーを編集するには、ポリシーを選択します。[編集 (Edit)]をクリックします。

p.46 の「バックアップポリシーの作成」を参照してください。

ポリシーのコピー

ポリシーをコピーすると、類似したポリシー属性、スケジュール、クラウドオブジェクトをポリシー間で再利用できます。また、ポリシーをコピーして複雑なクエリーを再利用して、時間を節約することもできます。

ポリシーをコピーするには:

1. 左側で[ポリシー (Policies)]をクリックします。表示する権限を持っているすべてのポリシーが[ポリシー (Policies)]タブに表示されます。
2. コピーするポリシーの行にある省略記号メニュー (3 つのドット) をクリックします。[ポリシーのコピー (Copy policy)]をクリックします。

   または、ポリシーの行のオプションを選択し、テーブルの上部にある[ポリシーのコピー (Copy policy)]をクリックします。

3 [ポリシーのコピー (Copy policy)]ダイアログボックスで、必要に応じて、[コピーするポリシー (Policy to copy)]フィールドのポリシー名を変更します。

4 [新規ポリシー (New policy)]フィールドに新しいポリシーの名前を入力します。

5 [コピー (Copy)]をクリックしてコピーを開始します。

ポリシーの無効化または削除

ポリシーを無効化すると、次の影響を受けます。

- 無効化されたポリシーに対して手動バックアップを実行することはできません。
- 無効化されたポリシーのスケジュールバックアップはトリガされません。
- 編集、コピー、削除などの操作は正常に機能します。
- 無効化されたポリシーをコピーすると、無効状態の新しいポリシーが作成されます。

ポリシーを削除すると、そのポリシーで構成されたスケジュールバックアップは行われません。

ポリシーを無効化または削除するには:

1 左側で[ポリシー (Policies)]をクリックします。表示する権限を持っているすべてのポリシーが[ポリシー (Policies)]タブに表示されます。

2 コピーするポリシーの行にある省略記号メニュー (3 つのドット) をクリックします。必要に応じて[無効化 (Deactivate)]または[削除 (Delete)]をクリックします。

または、ポリシーの行のオプションを選択し、テーブルの上部にある[無効化 (Deactivate)]または[編集 (Edit)]を必要に応じてクリックします。

ポリシーはすぐに無効になります。ポリシーを再度アクティブ化するには、無効化されたポリシーの行にある省略記号メニュー (3 つのドット) をクリックし、[有効化 (Activate)]をクリックします。

3 ポリシーを削除する場合は、確認ボックスの[削除 (Delete)]をクリックします。

資産の手動バックアップ

ポリシーによって実行されるスケジュールバックアップとは別に、必要に応じてポリシーに対してアドホックの手動バックアップを実行できます。

手動バックアップを実行する方法

1. 左側で[ポリシー (Policies)]をクリックします。表示する権限を持っているすべてのポリシーが[ポリシー (Policies)]タブに表示されます。
2. バックアップを実行するポリシーの行にある省略記号メニュー (3 つのドット) をクリックします。[手動バックアップ (Manual backup)]をクリックします。

   または、ポリシーの行のオプションを選択し、テーブルの上部にある[手動バックアップ (Manual backup)]をクリックします。
3. [手動バックアップ (Manual backup)]ダイアログボックスで、バックアップのスケジュールを選択します。ポリシーで定義されているスケジュールを確認できます。
4. バックアップするクライアントを 1 つ以上選択します。何も選択しないと、すべてのクライアントがバックアップされます。
5. [OK]をクリックして、バックアップを開始します。

4

クラウドオブジェクトストア資産のリカバリ

この章では以下の項目について説明しています。

クラウドオブジェクトストアのオブジェクトをリカバリするための前提条件

リカバリを開始する前に、以下の条件が満たされていることを確認してください。

- リカバリに使用する宛先バケットまたはコンテナについての情報を手元に用意します。
- プライマリサーバーで、[クライアント接続のタイムアウト (Client connect timeout)]パラメータと[クライアントの読み込みタイムアウト (Client read timeout)]パラメータを 3,600 秒に設定していることを確認します。これらのパラメータは、[ホストプロパティ (Host properties)]で設定できます。
  - 左側で[ホスト (Hosts)]をクリックし、その後[ホストプロパティ (Host properties)]をクリックします。
  - プライマリサーバーを選択し、[プライマリサーバーの編集 (Edit primary server)]をクリックします。
  - 左側の[タイムアウト (Timeout)]をクリックし、パラメータ[クライアント接続のタイムアウト (Client connect timeout)]と[クライアントの読み込みタイムアウト (Client read timeout)]の値を 3,600 秒として入力します。[保存 (Save)]をクリックします。

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

- リカバリするオブジェクトを選択します。選択したイメージからすべてのオブジェクトまたは BLOB を選択して、オブジェクトをリカバリできます。または、個々のオブジェクトを選択するか、一連のフォルダのすべてのオブジェクト、または一連の接頭辞に一致するすべてのオブジェクトを選択します。
- バケット、コンテナ、およびオブジェクト/BLOB にアクセスするための、有効なクラウドオブジェクトストアアカウントが必要です。アカウントの作成時に、クラウドオブジェクトストアアカウントに関連する情報を NetBackup に追加できます。リストアに必要な権限は、バックアップに必要な権限とは異なります。必要な場合は、リカバリ用に別のクラウドオブジェクトストアアカウントを作成できます。
- クラウドオブジェクトストアアカウントとアクセスホストを表示および選択する権限があることを確認します。ポリシーのリカバリホストを選択できるようにするには、[クラウドオブジェクト (Cloud objects)]タブを使用します。
- 必要な場合は、クラウドオブジェクトストアアカウントの検証に使用されるリカバリホストとは異なるリカバリホストを使用できます。新しいリカバリホストで必要なポートが開かれていること、およびバックアップホストまたはスケールアウトサーバーからクラウドプロバイダエンドポイントへの REST API 呼び出しを使用した通信用に構成されていることを確認してください。
- スループットを向上させるために複数のリストアジョブを並行して開始することを計画できます。リカバリするオブジェクトは、個々のオブジェクトで、またはフォルダや接頭辞を使用して選択できます。

クラウドオブジェクトの保持プロパティの構成

NetBackup 10.3 以降、オブジェクトロック機能を使用すると、元のオブジェクトロックプロパティを保持し、オブジェクトロックプロパティをカスタマイズするオプションも使用できます。リストアされたオブジェクトにオブジェクトロックプロパティを適用すると、保持期間が終了するかリーガルホールドが解除されるまで、リストアされたオブジェクトは削除できません。オブジェクトロックと保持プロパティのバックアップを使うために、ポリシーの作成およびバックアップ中に構成する必要はありません。

メモ: このオプションでは、データを長期間保持するために追加のクラウドストレージコストが発生する場合があります。オブジェクトを参照した後または別の場所にコピーした後で、削除するデータの一時的なコピーが必要な場合は、これらのオプションを使用しないでください。

リストアされたオブジェクトにオブジェクトの保持ロックまたはリーガルホールドを適用するため、リストア時に、組織のコンプライアンスと保持の必要条件を満たすためのオプションを複数選択できます。[リカバリオプション (Recovery options)]ページの[詳細リストアオプション (Advanced restore options)]でオプションを選択できます。p.68 の「クラウドオブジェクトストア資産のリカバリ」を参照してください。

クラウドオブジェクトストア資産のリカバリ

クラウドオブジェクトストア資産は、元のバケットやコンテナまたは別のバケットやコンテナにリカバリできます。また、オブジェクトごとに異なるバケットまたはコンテナにリストアすることもできます。

資産をリカバリするには:

1. 左側の[リカバリ (Recovery)]をクリックします。[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。
2. [基本プロパティ (Basic properties)]ページで、[ポリシー形式 (Policy type)]として[Cloud-Object-Store]を選択します。
3. リストアする資産を選択するには、[バケット/コンテナ (Buckets/Containers)]フィールドをクリックします。
   - [バケット/コンテナの追加 (Add bucket/container)]ダイアログのデフォルトオプションでは、完了したバックアップが含まれる、利用可能なすべてのバケットまたはコンテナが表示されます。検索ボックスを使用してテーブルを検索できます。
   - 特定のバケットまたはコンテナを追加するには、[バケットまたはコンテナの詳細の追加 (Add the bucket/container details)]オプションを選択します。Azure Data Lake の作業負荷を選択した場合は、[ファイル/ディレクトリの追加 (Add files/directories)]を選択します。
     クラウドプロバイダを選択し、バケットまたはコンテナの名前と、クラウドオブジェクトストアアカウントの名前を入力します。Azure 作業負荷の場合、UI で利用可能な場合は、ストレージアカウント名を指定します。

     メモ: まれに、選択用の表に必要なバケットが見つからない場合があります。ただし、同じバケットが、カタログビューにバックアップ ID として表示されます。バケットの選択は、バックアップ ID に従ってバケット名、プロバイダ ID、クラウドオブジェクトストアアカウント名を手動で入力することで行えます。バックアップ ID は <プロバイダ ID>_<クラウドアカウント名>_<一意の名前>_<タイムスタンプ> で構成されます。

     Azure の場合、<一意の名前> は `storageaccountname.bucketname` になり、S3 プロバイダの場合は、バケット名になります。
4. [追加 (Add)]をクリックし、[次へ (New)]をクリックします。
5. [オブジェクトの追加 (Add objects)]ページで、リストアする期間の[開始日 (Start date)]と[終了日 (End date)]を選択します。

   (オプション) イメージをフィルタするキーワード句を入力し、[適用 (Apply)]をクリックします。

6 [バックアップ履歴 (Backup history)]をクリックし、[バックアップ履歴 (Backup history)]ダイアログから、リカバリに必要なイメージを選択します。[選択 (Select)]をクリックします。

7 [リカバリの詳細 (Recovery details)]ページでは、オブジェクトやフォルダ、または接頭辞を追加し、イメージをリストアする前に、選択したイメージに対してマルウェアをスキャンできます。

- (オプション) [オブジェクトとフォルダの追加 (Add objects and folders)]をクリックし、[オブジェクト/BLOB とフォルダの追加 (Add objects/blobs and folders)]ダイアログボックスから、リカバリに必要なオブジェクトを選択します。[すべてのオブジェクト/BLOB とフォルダを含める (Include all objects/blobs and folders)]を選択し、利用可能なすべての資産を含めます。Azure Data Lake の作業負荷の場合、このオプションは[すべてのファイル / ディレクトリを含める (Include all files/directories)]として利用可能です。左側のナビゲーションツリー構造を使用して、テーブルをフィルタ処理できます。[追加 (Add)]をクリックします。
スキャンされていないイメージをリカバリ対象として選択すると、次の警告メッセージが表示されます。

```
One or more images selected for recovery are not scanned.
```

メモ: マルウェアに感染したイメージからリストアするには、管理者の役割または同等の RBAC 権限が必要です。

マルウェアに感染したイメージからのリカバリについて詳しくは、『セキュリティおよび暗号化ガイド』を参照してください。

- (オプション) [リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]を選択します。[次へ (Next)]をクリックします。このオプションは、マルウェアスキャンホストが構成されている場合にのみ表示されます。

メモ: [マルウェアに感染したイメージの選択を許可 (Allow the selection of images that are malware-affected)]オプションは、ユーザーが[リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]オプションを選択する場合は無効になります。

- (オプション) [接頭辞の追加 (Add prefix)]をクリックします。[接頭辞の追加 (Add prefix)]ダイアログで、検索ボックスに接頭辞を入力し、関連する結果をテーブルに表示します。テーブルに表示されたすべての一致する接頭辞をリカバリ用に選択するには、[追加 (Add)]をクリックします。選択した接頭辞は、選択したオブジェクト/BLOB の下のテーブルに表示されます。[次へ (Next)]をクリックします。

メモ: Cloud-Object-Store では、リカバリの一部としてのクリーンファイルリカバリ (感染ファイルのスキップ) はサポートされていません。

8 [リカバリオプション (Recovery options)]ページでは、コンテナのソースバケットにリストアするか、別のリストア先を使用するかを選択できます。以下に、オブジェクトのリストアのオプションを示します。

- 元のバケットまたはコンテナにリストア (Restore to the original bucket or container): バックアップが作成されたのと同じバケットまたはコンテナにリカバリする場合に選択します。
  必要に応じて次のようにします。
  - [接頭辞の追加 (Add a prefix)]フィールドに、リカバリする資産の接頭辞を追加します。
  - Azure Data Lake の作業負荷を選択した場合は、[リストアするディレクトリ (Directory to restore)]に値を入力します。
- 別のバケットまたはコンテナにリストア (Restore to a different bucket or container): バックアップが作成されたのとは別のバケットまたはコンテナにリカバリする場合に選択します。
  - 上の一覧から、別のクラウドオブジェクトストアアカウントをリストア先として選択できます。
  - リストア先の[バケット/コンテナ名 (Bucket/Container name)]を選択します。元のバケットにアクセスできる異なるクラウドオブジェクトストアアカウントを使用できます。この方法は、バックアップおよびリストア用に制限された特定の権限を持つアカウントを作成するのにも役立ちます。この場合、元のバケットまたはコンテナにリストアするために、元のバケットと同じバケットを指定できます。
  - 必要に応じて、[接頭辞の追加 (Add a prefix)]フィールドに、リカバリする資産の接頭辞を追加します。
- オブジェクト/BLOB または接頭辞を別のリストア先にリストア (Restore object/blobs or prefixes to different destinations): 選択した各資産を別の場所にリカバリする場合に選択します。
  - 一覧から、別のクラウドオブジェクトストアアカウントをリストア先として選択できます。
  - [オブジェクトの宛先を編集 (Edit object destination)]をクリックし、[宛先 (Destination)]と[宛先のバケット/コンテナ名 (Destination bucket/container name)]を入力します。[保存 (Save)]をクリックします。

メモ: 手順 7 で[すべてのオブジェクト/BLOB とフォルダを含める (Include all objects/blobs and folders)]を選択した場合は、[オブジェクト/BLOB または接頭辞を別のリストア先にリストア (Restore objects/blobs or prefixes to different destinations)]オプションが無効になります。

9 [リカバリホスト (Recovery host)]を選択します。デフォルトでは、クラウドオブジェクトストアアカウントに関連付けられているリカバリホストが表示されます。必要に応じて、バックアップホストを変更します。クラウドオブジェクトストアアカウントがスケールアウトサーバーを使用している場合、このフィールドは無効になります。

10 必要に応じて、リカバリされた資産を使用して既存のオブジェクトまたは BLOB を上書きするには、[既存のオブジェクト/BLOB を上書き (Overwrite existing objects/blobs)]を選択します。

11 (任意)リストアジョブのデフォルトの優先度を上書きするには、[デフォルトの優先度を上書きする (Override default priority)]を選択し、必要な値を割り当てます。

12 [詳細リストアオプション (Advanced restore options)]で、次のように指定します。

- バックアップ済みのオブジェクトから元のオブジェクトロック属性を適用するには、[オブジェクトの元のロックプロパティを保持する (Retain original object lock properties)]を選択します。
- 異なるプロパティの値を変更するには、[オブジェクトのロックプロパティをカスタマイズする (Customize object lock properties)]を選択します。[オブジェクトのロックモード (Object lock mode)]リストから、次のように実行します。
  - Amazon またはその他の S3 作業負荷で[コンプライアンス (Compliance)]または[ガバナンス (Governance)]を選択します。
  - Azure 作業負荷で[Locked]または[Unlocked]を選択します。
  - オブジェクトロックの有効期限となる将来の日時を選択します。リカバリされたオブジェクトは、この指定した日時までロックされることに注意してください。
- リストアされたオブジェクトに実装するには、[オブジェクトのロックのリーガルホールドの状態 (Object lock legal hold status)]を選択します。

p.67 の「クラウドオブジェクトの保持プロパティの構成」を参照してください。

[詳細リストアオプション (Advanced restore options)]は、Azure Data Lake の作業負荷には適用できません。

13 [マルウェアスキャンおよびリカバリオプション (Malware scan and recovery options)]で次を実行します。

メモ: これらのオプションは、[リカバリの詳細 (Recovery details)]ページで[リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]を選択した場合にのみ表示されます。

- (*非推奨*) マルウェアに感染したファイルをリカバリするには、[マルウェアに感染したファイルがある場合は、感染したファイルを含むすべてのファイルをリカバリします (If any files are infected with malware, recover all files, including infected files)]オプションを選択します。
- [マルウェアに感染したファイルがある場合は、リカバリジョブを実行しないでください (If any files are infected with malware, do not perform the recovery job)]オプションを選択します。デフォルトではこのオプションが選択されています (推奨)。
- 目的のスキャンホストプールを選択します。

メモ: マルウェアスキャンが実行された後にリカバリする場合、Cloud-Object-Store ではクリーンリカバリはサポートされないため、[マルウェアに感染したファイルのリカバリを許可 (Allow recovery of files infected by malware)]オプションは常にデフォルトで有効になっています。

14 [確認 (Review)]ページで、すべての選択項目の概要を確認し、次をクリックします。

- [リカバリの開始 (Start recovery)]
  または
- ([リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]が選択されている場合に該当) [スキャンとリカバリの開始 (Start scan and recovery)]

アクティビティモニターでリストアジョブの進行状況を確認できます。

5

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。

バージョン 10.5 にアップグレードすると、初回の完全バックアップ時の加速が減少する

説明:

10.5リリースでは、一部のメタデータが、リリース間バックアップの一部として保護されるように変更されています。新しいメタデータ形式を追跡するため、BLOB のメタデータプロパティの不一致により、すべてのオブジェクトが変更されたと見なされます。

回避方法:

これは想定される動作です。

アップグレード後、NetBackup は完全再スキャンバックアップを実行して、リリース間のイメージの依存関係を回避します。

バックアップ後、shm フォルダと共有メモリ内の一部のファイルがクリーンアップされない

説明:

動的マルチストリームを使用するバックアップでは、一部の NetBackup プロセスがクラッシュすると、バックアップが部分的に成功または失敗することがあります。このような場合、一部のファイルや共有メモリはクリーンアップされません。これらのファイルとバッファは小さく、それほど容量を消費しないはずです。

回避方法:

次を実行します。

- ファイルを消去するには、バックアップホストのフォルダに移動します。
  `<install_directory>/netbackup/db/config/shm/`
  これらのフォルダには、失敗したバックアップまたは部分的に完了したバックアップについて、`<parentid_streamNumber>` という形式のファイルが格納されます。ファイルを削除します。
- 共有メモリを消去するには:
  - 次のコマンドを使用して、バックアップホストの共有メモリを表示できます。
    `ipcs -m`
  - 実行中のすべてのバックアップとリストアが完了するまで待機してから、バックアップホストを再起動します。これにより、共有メモリが消去されます。

NetBackup バージョン 10.5 にアップグレードした後、古いポリシーについて、ポリシーのコピー、有効化、および無効化が失敗することがある

説明:

次のメッセージが表示されます。

属性「useMultipleDataStreams」は false です。この属性は有効にする必要があります。

NetBackup バージョン 10.5 では、ポリシーによる複数のデータストリームの使用は必須ですが、古いポリシーにこの属性はありません。

回避方法:

1. 古いポリシーを編集し、複数のデータストリームを許可するオプションがデフォルトで選択されているかどうかを確認します。ポリシーを保存します。
2. 操作を再試行します。

バックアップがデフォルトのストリーム数で失敗し「NetBackup COSP プロセスの開始に失敗しました (Failed to start NetBackup COSP process)」というエラーが返される

説明:

このエラーは、クラウドプロバイダの API への呼び出しを担当する nbcosp サービスが停止またはクラッシュしたために発生します。

回避方法:

次のいずれかを実行します。

- バックアップサーバーで、次のコマンドを実行して nbcosp サービスを起動します。
  `<install_directory>/pdde/pdcr/bin/nbcosp start`
- バックアップサーバーで、すべての NetBackup サービスを起動し、次を実行します。
  `<install_directory>/netbackup/bin/bp.start_all`

コンテンツのエンコードが GZIP であるオブジェクトの GCP ストレージでバックアップが失敗するか、部分的に成功する。

説明:

GCP クラウドストレージの解凍型トランスコーディング機能は、アップロードされたデータについて、コンテンツ長ヘッダーの一部としてオブジェクトのサイズを提供しません。サイズが戻されない場合、NetBackup はオブジェクトをバックアップできません。

詳しくは、GCP マニュアルのページを参照してください。

回避方法:

GZIP 以外のコンテンツエンコードモードを使用します。

元のバケットリカバリオプションのリカバリが開始されたが、ジョブがエラー 3601 で失敗する

説明

このエラーは次の 4 つのいずれかの理由で発生します。

- リカバリを実行するためにクラウドに接続する際に必要なクラウドオブジェクトストアアカウントが存在しません。
- バケットのバックアップ時に使用されるクラウドオブジェクトストアアカウントが、NetBackup ドメインに存在しません。
- これは、AIR 構成または DR シナリオのターゲットドメインです。
- クラウドオブジェクトストアアカウントが削除されました。

回避方法

元のクラウドオブジェクトストアアカウントと同じ名前とプロバイダを使用してクラウドオブジェクトストアアカウントを作成し、リカバリを再試行します。

リカバリジョブが開始しない

説明

元のバケットにリカバリすると、[資産の詳細を取得できません (Unable to retrieve asset details)]というエラーが表示されます。同じ名前のクラウドオブジェクトストアアカウントがバックアップ中に使用されていても発生します。

回避方法

次を実行します。

1. Web UI で同じクラウドオブジェクトストアアカウントを使用します。
2. 同じアカウントの別のバケットへのリカバリを試行します。この処理によってキャッシュが更新されます。

   キャッシュなしの資産 API を使用して cloudObjectStoreAccount (/netbackup/asset-service/workloads/cloud-object-store/assets/?filter=assetType eq 'cloudObjectStoreAccount') のすべての資産をフェッチすることで、キャッシュの更新を強制できます。アカウントが出力に一覧表示されていることを確認してください。
3. ここでも元のバケットのリカバリオプションを使用し、リカバリを実行します。

リストアが失敗しました:「エラー bpbrm (PID=3899) クライアントのリストア 終了状態 40: ネットワーク接続が切断されました (Error bpbrm (PID=3899) client restore EXIT STATUS 40: network connection broken)」

説明

バックアップイメージへのアクセスとリストア用の BLOB のアップロードの遅延。このプロセスでは、bptm がタイムアウトしています。

回避方法

アクティビティモニターにネットワークエラーメッセージが表示されてリストアが失敗した場合は、システム構成のタイムアウトを 900/1200 秒または十分に高い値 (秒数) に変更します。新しいリストアジョブを開始します。

タイムアウトを設定する手順は次のとおりです。左側で[ホスト (Hosts)]、[ホストプロパティ (Host properties)]、[プライマリサーバー (Primary server)]または[メディアサーバー (Media server)]、[タイムアウト (time-out)]オプションの順に選択し、タイムアウト値を設定して[保存 (Save)]をクリックします。詳しくは、『Web UI 管理者ガイド』を参照してください。

元の場所にある既存のオブジェクトを上書きした後にアクセス層プロパティがリストアされない

説明

ホットアクセス層でのリストアによって上書きされるクールアクセス層を持つオブジェクトは、アクセス層をホットに変更せず、クールのままです。

回避方法

Azure クラウドストレージの場合、クール accessTier を持つオブジェクトがあり、上書きオプションを使用してホット (推論) accessTier で同じ名前のオブジェクトまたは BLOB をアップロードしようとすると、accessTier はコールドのままです。新しいアクセス層は設定されません。この動作は、ファイルがポータルからアップロードされる場合に発生します。Azure ポータルで[上書き (Overwrite)]オプションが選択されている場合、accessTier をクールからホット (推論) に変更しません。

複数のタグがある OR クエリーに対する Azure でのアクセラレータ最適化の低下

説明

「OR」演算子を使用して複数のタグ条件を組み合わせたクエリーが 1 つ以上あるクラウドオブジェクトストアポリシーがある場合、アクセラレータ対応クラウドオブジェクトストアポリシーを使用した Azure コンテナのバックアップは、加速が低下するか、変更されていないデータをバックアップします。

これは、複数のタグにわたるオブジェクトの順序付けがアクセラレータに対して予想どおりに行われていないために発生します。トラックログに存在しているのにトラックログに見つからないオブジェクトは少ないため、これらのオブジェクトはアクセラレータの利点を得ることなく繰り返しバックアップされます。

回避方法

Azure に対して複数のタグ条件を組み合わせる際に OR 条件を使用しないでください。代わりに、タグごとに個別のクエリーを作成します。

例:

クエリー名とデータ型を指定するクエリー (tagKey eq 'type' and tagValue eq 'text') or (tagKey eq 'type' and tagValue eq 'none) があるとします

データ型が text のクエリー (tagKey eq 'type' and tagValue eq 'text') と、データ型が none のクエリー (tagKey eq 'type' and tagValue eq 'none') という 2 つのクエリーを作成できます。

メモ: こうすることで、最初のバックアップではこれらの新しいクエリーの加速は行われません。以降のバックアップでは、問題が解決していることを確認できます。

バックアップが失敗し、ドット (.) を含む Amazon S3 バケット名で証明書エラーが表示される

回避方法

次の 2 つの回避方法のいずれかを使います。

- `Use path-style URL to access the bucket`: パススタイル URL は、ホスト名ではなく URL パスの一部としてバケットを追加するため、名前にドット (.) があるバケットの場合でも SSL の問題は発生しません。ただし、NetBackup デフォルト構成は `s3.dualstack.<region-id>.amazonaws.com` など、すべてのデュアルスタック URL に仮想スタイルを使用します。パススタイルとして古い S3 URL を追加し、名前にドット (.) を含むバケットに接続できます。これを行うには、プレーンな S3 エンドポ

イント (s3.<region-id>.amazonaws.com) で地域を追加し、URL アクセススタイルをパススタイルとして選択します。

- SSL の無効化: この回避方法は安全なエンドポイントを安全でない/暗号化されていないエンドポイントに置き換えるため推奨されません。SSL をオフにすると、サーバー証明書のピアホスト検証が無効になります。証明書にサブジェクト名 (*.s3.dualstack.us-east-1.amazonaws.com) が含まれるバケット (bucket.123.s3.dualstack.us-east-1.amazonaws.com) の仮想ホストスタイル URL に対するホスト名の一致を回避します。

タグキーの名前または値のタグクエリーにスペースが含まれていると Azure バックアップジョブが失敗する。

回避方法

Azure バックアップジョブのタグクエリーでタグキー名または値にスペースを使用しないでください。

クラウドオブジェクトストアアカウントでエラーが発生した

説明

Web UI で、クラウドオブジェクトストアアカウントの状態は次のように表示されます。

クラウドオブジェクトストアアカウントでエラーが発生しました。ユーザーマニュアルを参照してアカウントを再作成してください。

この状態では、クラウドオブジェクトストアアカウントを編集できません。クラウドオブジェクトストアアカウントに対応するすべてのジョブが失敗し続けます。

原因

クラウドオブジェクトストアアカウントは、次の場合にエラー状態になります。

- csconfig CLI を使用して、クラウドオブジェクトストアアカウントに対応するエイリアスが誤って削除された。
- csconfig CLI を使用して、クラウドオブジェクトストアアカウントに対応するエイリアスが誤って更新された。

メモ: クラウドオブジェクトストアアカウントに対応するエイリアスの更新には、csconfig CLI を使用しないことをお勧めします。同じように更新する正しい方法は、編集ワークフローまたは create-or-update API を使用することです。クラウドオブジェクトストアアカウントと同じ名前のエイリアスが、クラウドオブジェクトストアアカウントに対応するエイリアスです。

回避方法

NetBackup ドメイン名は、クラウドオブジェクトストアアカウント、クラウドストレージサーバー、MSDP-C LSU 間で一意である必要があります。これらでは、単一の名前空間が共有されます。そのため、想定される使用状況のシナリオは次のとおりです。

Case 1: クラウドオブジェクトストアアカウントと同じ名前の有効なクラウドストレージサーバーまたは MSDP-C LSU が環境内に存在しない場合。

- 環境に応じてクラウドオブジェクトストアアカウントの詳細を収集し、取得した詳細をクロスチェックします。
  - 必要に応じて、クラウドオブジェクトストアアカウントに対応するエイリアスが存在する場合は、csconfig CLI を使用してエイリアスの詳細を書き留めます。
    - 次のコマンドを使用して、このタイプのすべてのインスタンスを一覧表示し、クラウドオブジェクトストアアカウントとそのインスタンスを特定します。

      ```
      <install-path>/csconfig cldinstance -i -pt <provider_type>
      ```

    - 次のコマンドを使用して、インスタンスとクラウドオブジェクトストアアカウントの詳細を取得します。

      ```
      <install-path>/csconfig cldinstance -i -in <instance name>
      ```

    - 収集した情報で詳細を検証します。
    - 次のコマンドを使用してエイリアスを削除します。

      ```
      <install-path>/cscpnfig cldinstance -at <api_type> -rs -in
      <instance_name> -sts <cloud_object_store_account_name>
      ```

- エラー状態のクラウドオブジェクトストアアカウントを削除します。
- 書き留めた詳細を使用して、クラウドオブジェクトストアアカウントを作成します。

Case 2: クラウドオブジェクトストアアカウントと同じ名前で使用中の有効なクラウドストレージサーバーまたは MSDP-C LSU が環境内に存在する場合。

- 同じ名前は再利用できません。
- 環境に応じてクラウドオブジェクトストアアカウントの詳細を収集する必要があります。
- クラウドオブジェクトストアアカウントの新しい名前を決めます。
- エラー状態のクラウドオブジェクトストアアカウントを削除します。ポリシーからアカウントを削除します。
- 新しい名前と収集した詳細を使用して、クラウドオブジェクトストアアカウントを作成します。古いアカウントが使用していたのと同じポリシーに、このアカウントを割り当てます。
- これにより、次回のバックアップ以降、バケットに使用されるクライアント名が変更されます。
- NetBackup は古いアカウント名を使用して、古いバックアップを識別します。

ポリシーの選択中にバケットの一覧が空になる

説明:

NetBackup では、領域エントリを追加することでクラウドオブジェクトストアアカウントを追加する際に、正しい領域のロケーション制約を指定する必要がありません。領域が構成されていない一部のプライベートクラウドでは、アカウントは正常に追加されます。

アカウントでそのような無効な領域を使用していると、空のバケット一覧が返される場合があります。

回避方法:

次を実行します。

1. バケットで `getBucketLocation` API を呼び出し、アカウント構成の正しいロケーションの制約を取得します。

   この API で空のロケーションの制約が返された場合、領域のロケーションの制約として「us-east-1」を使用します。

2. アカウント構成を編集し、領域の詳細を修正します。p.21 の「クラウドオブジェクトストアアカウントの追加」を参照してください。

3. クラウド構成を編集するには、次の手順を実行します。

   - 左側で、[ホストプロパティ (Host Properties)]をクリックします。
   - 必要なプライマリサーバーを選択して接続します。[プライマリサーバーの編集 (Edit primary server)]をクリックします。
   - [クラウドストレージ (Cloud storage)]をクリックします。
   - 必要に応じて、検索フィールドにクラウドプロバイダ名を入力し、リストをフィルタ処理します。
   - クラウドプロバイダサービスホストに対応する行で、正しい領域の詳細を入力して保存します。

または、アカウントを削除し、正しい領域のロケーションの制約を使用してアカウントを再作成します。

既存の領域を選択すると Cloudian で 2 番目のアカウントの作成が失敗する

説明:

us-east-1 ロケーション制約を持つ領域を追加して Cloudian のクラウドオブジェクトストレージアカウントを追加した後、同じリージョンを再利用して 2 つ目のアカウントを作成しようとすると、アカウントの作成が失敗します。

これは、領域の一覧表示 API が、Web UI で表示中に、領域のロケーションの制約「us-east-1」を「<空白>」に変換しているために発生します。追加された領域のロケーションの制約が us-east-1 で、一覧表示されたロケーションの制約フィールドは空白になっていることがわかります。リストからそのような領域を選択して作成されたアカウントは失敗します。

回避方法:

NetBackup 資産問い合わせ API を使用してアカウントを作成します。領域の詳細に関する部分はペイロードで提供される場合があります。

```
"s3RegionDetails": [
  { "regionId": "us-east-1",
    "regionName": "<region name same as listed from prior account>",

   "serviceHost": "<service host same as listed from prior account>"

  }
]
```

スキーマ API から API DOC を取得できます。

```
https://<primary-server-hostname>/netbackup/asset-service
/workloads/saas/schemas/create-or-update-assets-named-query-request
```

2825 未完了のリストア操作によりリストアに失敗した

バックアップイメージから一部のオブジェクトがリストアされません。2825 未完了のリストア操作により、リストアに失敗しました。

説明:

このエラーは、複数の原因により発生します。このエラーが発生する可能性が高いのは、リストア中に NetBackup によって開始されたクラウド API が HTTP 400 状態コード (不正な要求) などのエラーを返したときです。その理由は、クラウドベンダーによって異なります。たとえば、AWS と比較すると、GCP は異なる Content-Language メタデータをサポートしています。場合によっては、特定のクラウドアカウントまたはバケットで有効または無効になっている機能によってエラーが発生することもあります。

nbcosp ログに、次のメッセージが表示されます。

```
{"level":"warn","error":"InvalidArgument: Invalid argument.¥n¥tstatus
 code: 400, request id: , host id: ","object
key":"meta-user-defined/t2.rtf","time"…}
```

nbtar ログに、次のメッセージが表示されます。

```
15:56:15.739 [22496.22496] <16> operation_to_cloud_by_type: ocsd
reply with error, error_code: 400
15:56:15.739 [22496.22496] <16> CloudObjectStore::InitMultiPartUpload:
 operation_to_cloud_by_type() failed, status=3600
15:56:15.739 [22496.22496] <16> CloudObjectStore::ObjectOpen:
InitMultiPart Upload call failed with status = 3600
15:56:15.739 [22496.22496] <16> cCloudApiRestoreHandler::writeOpen:
 ERR - ObjectOpen failed with error code [3600]
```

回避方法:

エラーが致命的ではない場合、リストアジョブは部分的に成功します。アクティビティモニターで、リストアできないオブジェクトのリストを確認します。別の場所 (バケット、コンテナ、または別のアカウント) へのリストアを試して、リストア先のクラウドアカウントまたはバケットの設定に問題がないかを確認します。

エラーが致命的である場合、リストアジョブは失敗します。nbcosp ログを確認して、リストアが失敗したオブジェクトを特定します。次回のリストアで個別オブジェクトの選択を使用し、オブジェクトの選択時に、以前に失敗したオブジェクトをスキップします。

クラウドプロバイダのマニュアルを参照して、クラウドベンダーが完全にはサポートしていない機能やメタデータを使用していないか、またはさらに構成が必要かを確認します。クラウドオブジェクトストアのオブジェクトを正しい属性で修正し、新しいバックアップジョブを開始します。このバックアップが完了すると、この回避方法なしでオブジェクトをリストアできます。

[クラウドオブジェクト (Cloud objects)]タブでバケットを追加すると、クラウドプロバイダのバケットの一覧表示に失敗する

説明

バケットの一覧表示でエラーが発生する最も一般的な理由は、NetBackup に提供されたクラウドクレデンシャルに、バケットを一覧表示する権限がないためです。

もう 1 つの理由は、クラウドプロバイダが、エンドポイントの適切な DNS エントリをサポートしていない場合です。同様に、誤って構成された DNS や、仮想ホスト形式の命名も、バケット名をホスト名として指定せずにクラウドプロバイダに対して要求を発行できない原因になります。s3-fips.us-east-1.amazonaws.com は、このようなクラウドエンドポイントの一例です。

回避方法

バケットリストは利用できませんが、[クラウドオブジェクト (Cloud objects)]タブで、バックアップ用にいつでも手動でバケットを追加できます。

DNS の問題である場合、必要に応じて、/etc/hosts ファイルに IP ホスト名のマッピングエントリを追加するという一時的な回避方法を使用してバケットを一覧表示できます。仮想ホスト形式の要求のみがサポートされている場合は、ping、dig、nslookup などのコマンドを使用してクラウドエンドポイントの IP を判断する際に、まず、ランダムなバケット名を使用してエンドポイントに接頭辞を付けます。例:

```
ping randombucketname.s3-fips.us-east-1.amazonaws.com
```

その後、判明した IP と実際のエンドポイント名 (ランダムなバケット名の接頭辞なし) を /etc/hosts ファイルに追加します。

これは、バケットを一覧表示するためにコンピュータの DNS エントリを編集する一時的な回避方法である点に注意してください。クラウドエンドポイントが静的 IP アドレスを永続的に使用できるプライベートクラウド設定でないかぎり、ポリシーの構成が完了したら、追加したエントリを削除してください。

クラウドストアアカウントがターゲットドメインに追加されていない場合、ターゲットドメインで AIR インポートイメージのリストアが失敗する

エラー

クラウドオブジェクトストア保護の操作を実行できません。オブジェクトをスキップします:[], エラー: [3605] (Cannot perform the Cloud object store protection operation, skipping the object:[<object name>], error: [3605])

説明

クラウドオブジェクトストアアカウントが、ソースドメインと同じ名前のターゲットドメインに存在しません。

回避方法

ソリューション 1:

ソースドメインと同じ名前のターゲットドメインにクラウドオブジェクトストアアカウントを作成し、リストアを実行します。p.21 の「クラウドオブジェクトストアアカウントの追加」を参照してください。

ソリューション 2:

有効なクレデンシャルを持つクラウドオブジェクトストアアカウントがターゲットドメインに存在する場合は、次の手順を実行します。

1. [リカバリ (Recover)]タブで、ソースアカウント名を持つバケットまたはコンテナを選択します。[次へ (Next)]をクリックします。
2. バックアップイメージを選択し、オブジェクト、フォルダ、または接頭辞を追加します。[次へ (Next)]をクリックします。
3. [リカバリオプション (Recovery options)]ページで、[別のバケットまたはコンテナにリストア (Restore to a different bucket or container)]オプションを選択します。リストアに使用する別の既存のクラウドオブジェクトストアアカウントを選択します。

バックアップホストまたはストレージサーバーのバージョン 10.3 で旧バージョンのメディアサーバーを使用すると Azure Data Lake に対するバックアップが失敗する

エラーメッセージ

bpbkar Exit: INF - EXIT STATUS 3600: Cannot perform the COSP operation.

Error nbpem (pid=13052) backup of client azuredatalake_COSv17_adlsgen2xxxxx.xxxxxxx exited with status 3600 (cannot perform the COSP operation).

説明

Azure Data Lake のサポートは NetBackup バージョン 10.3 で導入されたため、この作業負荷は 10.3 より前のバージョンのメディアまたはストレージサーバーでは機能しません。

回避方法

メディアサーバー、バックアップホストまたはスケールアウトサーバーと、ストレージサーバーのバージョンが 10.3 以降であることを確認します。

Azure Data Lake でバックアップが部分的に失敗する: エラー nbpem (pid=16018) クライアントのバックアップ (Error nbpem (pid=16018) backup of client)

説明

ディレクトリ名 + ファイル名 (すべての「/」を含む) が 1,024 文字以上である場合に発生します。

回避方法

1,024 文字以下のディレクトリパス + ファイル名 (すべて「/」を含む) で構成されるパスが必要です。ディレクトリの最大長は、パスの先頭と末尾の「/」を含めて 1,023 文字まで指定できます。

Azure データレイクのリカバリが失敗する:「パスが深すぎるため、この操作は許可されません (This operation is not permitted as the path is too deep)」

説明

リカバリ用に選択したディレクトリの深さが 60 を超えると発生します。このエラーメッセージは nbcosp ログに表示されます。

回避方法

ディレクトリの深さが 60 未満のパス (コンテナを除く) を使用する必要があります。

空のディレクトリが Azure Data Lake でバックアップされない

説明

空のディレクトリ、またはコンテンツのないリーフレベルのディレクトリを、ポリシーの問い合わせフィルタを追加するときに発生します。バックアップ中、その空のディレクトリはバックアップされません。

回避方法

空のディレクトリをバックアップするには、[選択したバケット/コンテナ内にあるすべてのファイル/ディレクトリを含める (Include all files/directories in the selected buckets/containers)]オプションを選択します。

リカバリエラー:「代替ディレクトリの場所が無効です。(Invalid alternate directory location.) 文字列は、1,025 文字より短い有効な文字で指定する必要があります。(You must specify a string with length less than 1025 valid characters.)」

説明

Web UI の[リストア元のディレクトリ (Directory to restore)]フィールドに指定した値が 1,024 文字を超えると発生します。この値は、API の alternateDirectoryLocation 属性に内部的にマップされます。

回避方法

1,024 文字未満のリストア場所を指定します。

メモ: このエラーはアクティビティモニターには表示されません。

リカバリエラー:「無効なパラメータが指定されました (Invalid parameter specified)」

説明

API に alternateDirectoryLocation 属性と addPrefix 属性の値が含まれている場合に発生します。API は、指定された入力パラメータの 1 つをサポートしていません。

回避方法

Azure Data Lake Storage Gen2 は AlternateDirectoryLocation 属性のみをサポートするため、API 要求では addPrefix 属性を空にする必要があります。

メモ: このエラーはアクティビティモニターには表示されません。詳しくは、NetBackup API のマニュアルを参照してください。

リストアが失敗する:「COSP 操作を実行できません。次のオブジェクトをスキップしています: [/testdata/FxtZMidEdTK] (Cannot perform the COSP operation, skipping the object: [/testdata/FxtZMidEdTK])」

説明

DFS API の上書き機能を使用して Azure Data Lake Gen2 アカウントにアップロードされたファイルまたはディレクトリが元のファイルを置き換えると、リストアジョブが失敗します。

nbcosp ログに次のエラーが表示される場合があります。

```
 *RESPONSE ERROR (ServiceCode=BlobOperationNotSupported)
=====¥nDescription=Blob operation is not supported.
```

メモ: この問題では、[アップロード (Upload)]オプションを使用して Azure ポータルにアップロードされたファイルは含まれません。

回避方法

次のいずれかを実行します。

- 同じコンテナのリストア操作を別のディレクトリで試行します。
- リストア操作を別のコンテナで試行します。
- リストア操作を別の宛先で試行します。
- 元のディレクトリを削除し、同じ場所にリストアを試行します。

誤ったクレデンシャルでクラウドストアアカウントの作成が失敗する

AWS アカウントの場合:

nbcosp ログを確認します。

場所:

- バックアップホストの場合: /usr/openv/netbackup/logs/nbcosp
- スケールアウトサーバーの場合:
  /cloudpoint/openv/dm/datamover.<datamover_id>/netbackup/logs/nbcosp

```
{"level":"error","Error Code":"SignatureDoesNotMatch","Message":"The
 request signature we calculated does not match the signature you
provided. Check your key and signing method.
","time":"2023-07-25T10:58:48.130601182Z","caller":"main.validateNBCosCreds:s3_ops.go:1634",
"message":"Error in getBucketLocation for credential validation"}
{"level":"error","errmsg":"Unable to validate creds.","storage
server":"aws-acc","time":"2023-07-
```

ncfnbcs ログを確認します。

場所:

- バックアップホストの場合: /usr/openv/logs/ncfnbcs
- スケールアウトサーバーの場合:
  /cloudpoint/openv/dm/datamover.<datamover_id>/logs/ncfnbcs

```
2,51216,309,366,474,1690282728130,1673,140536982484736,0:,0:,0:,2,(28|S113:ERR
 - OCSD reply with error,error_code=1003 error_msg:
updateStorageConfig Failed as credential validation failed|)
2,51216,309,366,475,1690282728131,1673,140536982484736,0:,0:,0:,2,(28|S60:ERR
 - operation_to_ocsd failed, storageid=aws-acc, retval=23|)
0,51216,526,366,6,1690282728131,1673,140536982484736,0:,132:Credential
 validation failed for given account,
```

回避方法:

クレデンシャルを更新し、アカウントの作成を再試行します。

不適切な権限による検出エラー

nbcosp ログを確認します。

場所:

- バックアップホストの場合: /usr/openv/netbackup/logs/nbcosp
- スケールアウトサーバーの場合:
  /cloudpoint/openv/dm/datamover.<datamover_id>/netbackup/logs/nbcosp

```
25T11:14:14.761525555Z","caller":"main.(*OCSS3).
listBucketsDetailsCOSP:s3_ops.go:5261","message":"Unable
to listBucketsDetailsCOSP"} {"level":"debug","status code"
:403,"errmsg":"AccessDenied: Access Denied¥n¥tstatus code: 403,
request id: K7JVVPWAGW4KYSQ6, host id:
```

回避方法:

必要な権限を追加します。p.16 の「Amazon S3 クラウドプロバイダのユーザーに必要な権限」を参照してください。

オブジェクトロックによるリストアエラー

説明:

リストア時に、[オブジェクトの元のロックプロパティを保持する (Retain original object lock properties)]オプションを選択すると、NetBackup でオブジェクトロックプロパティが適用されます。

アクティビティモニターのログの確認:

```
Warning bpbrm (pid=21103) from client
ip-10-176-97-167.us-east-2.compute.internal: WRN - Cannot set Object
```

```
 lock on the object. Access to perform the operation was denied.

Jul 25, 2023 11:26:00 AM - Error bpbrm (pid=21103) from client
ip-10-176-97-167.us-east-2.compute.internal: ERR - Cannot complete
restore for any of the objects.

Jul 25, 2023 11:26:00 AM - Warning bpbrm (pid=21103) from client
ip-10-176-97-167.us-east-2.compute.internal: WRN - The 3 files
restored partially as object lock cannot be applied.

Jul 25, 2023 11:26:00 AM - Info tar (pid=1697) done. status 5
```

nbcosp ログの確認:

```
{"level":"info","SDK log body":"<?xml version=¥"1.0¥"
encoding=¥"UTF-8¥"?>¥n<Error><Code>AccessDenied
 </Code><Message>Access
Denied</Message><RequestId>ZNT4GXHP70HX573A</RequestId>
<HostId>
3scBmke9ImOwtuK5lnYv0ozyKgbne+ey04qXtSt6s/OQbpSCyfxiwvdi2CPG3cHU+H/ztz7C3mHeoX5Cnvb2xg==</HostId>

</Error>¥n","time":"2023-07-25T05:56:00.708117368Z","caller":
"internal/logging.ExtendedLog.Log:zerolog_wrapper.go:18","message":"SDK
 log entry"}
{"level":"debug","status code":403,"errmsg":"AccessDenied:
Access Denied¥n¥tstatus code: 403, request id: ZNT4GXHP70HX573A,
host id:
3scBmke9ImOwtuK5lnYv0ozyKgbne+ey04qXtSt6s/OQbpSCyfxiwvdi2CPG3cHU+H/ztz7C3mHeoX5Cnvb2xg==",
"time":"2023-07-25T05:56:00.708145345Z","caller":"main.s3StatusCode:s3_ops.go:8447",
"message":"s3StatusCode(): get http status code"}
{"level":"error","error":"AccessDenied: Access Denied¥n¥tstatus code:
 403,
request id: ZNT4GXHP70HX573A,
 host id:
3scBmke9ImOwtuK5lnYv0ozyKgbne+ey04qXtSt6s/OQbpSCyfxiwvdi2CPG3cHU+H/ztz7C3mHeoX5Cnvb2xg==",

"object
key":"cudtomer35jul/squash.txt","time":"2023-07-25T05:56:00.708160142Z",
"caller":"main.(*OCSS3).commitBlockList:s3_ops.go:2655",
"message":"s3Storage.svc.PutObjectRetention Failed to Put
ObjectRetention"}
```

回避方法:

オブジェクトの保持に必要な権限が必要です。役割に必要な権限は次のとおりです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectLock",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention",
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

p.67 の「クラウドオブジェクトの保持プロパティの構成」を参照してください。