NetBackup™ Web UI クラウド管理者ガイド

リリース 11.0

VERITAS
now part of Cohesity

最終更新日: 2025-04-25

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

クラウド資産の管理と保護

この章では以下の項目について説明しています。

クラウド資産の保護について

NetBackupを使用して、クラウド内の作業負荷を保護できるようになりました。クラウドデータ保護フレームワークは、Snapshot Manager インフラを利用して、クラウドプロバイダのより迅速な拡大を促進します。NetBackup 8.3 以降、Snapshot Manager は AWS、Azure、Azure Stack Hub、GCP、および 10.4 以降の OCI クラウドの資産の保護もサポートするようになりました。

次の表では、タスクについて説明します。

表 1-1　クラウド資産に対する保護の構成

タスク	説明
開始する前に、適切なアクセス権があることを確認します。	クラウド資産を Web UI で管理して保護するには、作業負荷管理者の役割または同様のアクセス権が必要です。NetBackup セキュリティ管理者は、個々の資産レベル、アカウントまたはサブスクリプションレベル、あるいはクラウドプロバイダレベルで、役割のアクセス権を管理できます。 『NetBackup Web UI 管理者ガイド』を参照してください。 **メモ:** ホストアプリケーションの管理には、[資産の管理 (Manage Assets)]と[保護計画の管理 (Manage Protection Plans)]の権限が必要です。
Snapshot Manager の配備 Snapshot Manager の構成	環境に Snapshot Manager をインストールします。 p.15 の「Snapshot Manager の追加」を参照してください。 Snapshot Manager と NetBackup の制限事項を確認します。 p.12 の「制限事項および考慮事項」を参照してください。
	NetBackup で Snapshot Manager を登録します。 『NetBackup Snapshot Manager インストールおよびアップグレードガイド』を参照してください。
構成の追加	すべてのサポート対象クラウドプロバイダが、Web UI に表示されます。 必要なクラウドプロバイダに対して、クラウドアカウントを追加 (クラウドプラグインを構成) する必要があります。プロバイダごとに複数の構成を作成できます。 p.15 の「Snapshot Manager のクラウドプロバイダの追加」を参照してください。

タスク	説明
資産の検出	NetBackup で構成されているクラウドアカウントに関連するクラウド資産を NetBackup が取得します。資産は、NetBackup の資産 DB に入力されます。 デフォルトで、資産の検出は 2 時間ごとに行われますが、これは構成可能です。 アプリケーションの場合は、15 分から 45 分の間で検出間隔を設定できます。 p.21 の「Snapshot Manager の資産の検出」を参照してください。
保護計画またはポリシーの作成	保護計画またはポリシーを作成します。保護計画を使用して、バックアップの開始時間帯をスケジュール設定します。 『NetBackup Web UI 管理者ガイド』を参照してください。 スナップショットレプリケーションの保護計画を構成することもできます。p.81 の「AWS スナップショットレプリケーションの構成」を参照してください。 p.39 の「クラウド資産のポリシーの管理」を参照してください。
仮想マシン、アプリケーション、またはボリュームの保護の選択	各クラウドプロバイダについて、検出済み資産のリストが表示されます。保護計画に資産を追加します。 『NetBackup Web UI 管理者ガイド』を参照してください。 アプリケーションの整合性スナップショットを使用してアプリケーションの保護を選択することもできます。p.88 の「アプリケーションの整合性スナップショットを使用したクラウド内アプリケーションの保護」を参照してください。
クラウド資産のポリシーの管理	NetBackup Web UI を使用して、クラウド作業負荷の種類 (IaaS および PaaS) をサポートするポリシーを作成できます。ポリシーは、クライアントに存在するデータを保護するために作業負荷に適用されます。 p.39 の「クラウド資産のポリシーの管理」を参照してください。

タスク	説明
クラウド資産のリカバリ	■ リカバリポイントを使用して資産をリカバリできます。 p.137 の「クラウド資産のリカバリ」を参照してください。 p.137 の「クラウド資産のリカバリ」を参照してください。 p.147 の「クラウド資産のロールバックリカバリの実行」を参照してください。 ■ また、nbcloudrestore CLI ユーティリティを使用して、資産をリストアすることもできます。 **メモ:** リストアに bprestore CLI を使用しないでください。 『NetBackup コマンドリファレンスガイド』を参照してください。
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トリガし、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。
トラブルシューティング	p.185 の「クラウドの作業負荷の保護に関する問題のトラブルシューティング」を参照してください。

制限事項および考慮事項

クラウド作業負荷を保護するときは、次の点を考慮してください。

- Snapshot Manager ホストエントリとそれに関連付けられているプラグインの削除は NetBackup でサポートされていません。
  NetBackup に構成されているプラグインを削除した場合、そのプラグインに関連付けられている Snapshot Manager イメージはリカバリできません。
- Snapshot Manager の機能について詳しくは、『NetBackup Snapshot Manager インストールおよびアップグレードガイド』を参照してください。
- 以前にインストールした Snapshot Manager がある場合、Cohesityでは、Snapshot Manager を再インストールせずに、アップグレードすることをお勧めします。
  Snapshot Manager サーバーを再インストールした場合は、Snapshot Manager サーバーを再構成して、保護関連のすべての手順を実行する必要があります。
- デフォルトでは、Snapshot Manager はポート 443 で構成されます。
- Snapshot Manager サーバーが追加されると、ホストマシンは IPv6 アドレスを使用してクラウド上の資産を検出しようとします。アプリケーションは、IPv6 アドレスがホストで検出された場合はこのアドレスを使用するように構成されています。IPv6 アドレスが検出されなかった場合は、IPv4 アドレスが使用されます。

- Snapshot Manager では、拡張監査はサポートされません。このため、root 以外の NetBackup 管理者権限を使用して Snapshot Manager を追加または更新する場合、監査中にユーザーは root として表示されます。
- CloudFormation テンプレートを使用して Snapshot Manager を配備する場合、コマンドを使用して Snapshot Manager ノードにオンホストエージェントを登録するときに使用する IP アドレスは、パブリック IP ではなくプライベート IP である必要があります。

メモ: Cohesityでは、クラウド資産グループのスナップショットジョブからのバックアップを実行するために使用されるNetBackupプライマリサーバーでスワップ領域を有効にすることをお勧めします。スワップ領域の推奨サイズは、システムメモリの 1.5 倍以上です。スワップ領域を有効にできない状況では、より大きなメモリ構成のシステムを使用することをお勧めします。

AWS と Azure の政府向けクラウドサポート

8.3 以降、Snapshot Manager は、アマゾンウェブサービスおよび Microsoft Azure の米国政府機関向けクラウドの作業負荷を検出できます。Snapshot Manager が NetBackup に追加された後、NetBackup によって作業負荷を保護できます。NetBackup は、AWS と Azure の米国政府向けクラウドの作業負荷に Snapshot Manager を配備するための、IPv6 サポートを含む規制要件に準拠しています。

AWS または Azure 米国政府向けクラウドを構成すると、指定した地域に基づいてクラウド資産を検出する AWS および Azure エージェントサービスが作成されます。検出された資産は NetBackup に表示されます。現在は、選択した地域とマッピングされたエンドポイントの作業負荷のみが検出および保護されます。同じ Snapshot Manager ホストで、パブリッククラウドと政府向けクラウドの組み合わせは使用できません。

プラグインの資産の操作が進行中にクラウドプラグインを更新すると、エラーが発生することがあります。

Snapshot Manager は、次の GovCloud (米国) 地域をサポートします。

クラウドプロバイダ	GovCloud (米国) 地域
アマゾンウェブサービス	■ us-gov-east-1 ■ us-gov-west-1
Microsoft Azure	■ US Gov アリゾナ ■ US Gov テキサス ■ US Gov バージニア

メモ: PaaS 資産は政府向けクラウドをサポートしません。

AWS と Microsoft Azure の構成について詳しくは、p.15 の「Snapshot Manager のクラウドプロバイダの追加」を参照してください。

Snapshot Manager を NetBackup で構成します。

NetBackup Web UI を使用して Snapshot Manager を追加できます。8.3 以降、Snapshot Manager は Amazon Web Services、Azure、Azure Stack Hub、GCP、およびバージョン 10.4 以降の OCI クラウドのクラウド資産を検出できるようになりました。

次の重要な点に注意してください。

- 複数の Snapshot Manager サーバーを NetBackup マスターサーバーに関連付けることができます。ただし、Snapshot Manager サーバーに複数の NetBackup マスターサーバーを関連付けることはできません。
- Snapshot Manager インターフェースで操作しなくても、Snapshot Manager を管理し、NetBackup Web UI、REST API、CLI から資産の検出を制御できるようになりました。
- スナップショットジョブからのバックアップでは、Snapshot Manager に関連付けられたメディアサーバーの代わりに NetBackup メディアストレージに関連付けられたサーバーが使用されます。Snapshot Manager 関連のすべての操作を円滑に進めるには、NetBackup メディアストレージに関連付けられたサーバーを Snapshot Manager サーバーに接続する必要があります。

次の表では、基になるタスクについて説明します。

表 1-2 Snapshot Manager の構成

タスク	説明
Snapshot Manager の追加	p.15 の「Snapshot Manager の追加」を参照してください。
クラウドプロバイダの追加	Snapshot Manager の資産を検出するには、クラウドプロバイダを追加する必要があります。p.15 の「Snapshot Manager のクラウドプロバイダの追加」を参照してください。
Snapshot Manager の資産の検出	Snapshot Manager の資産を検出できます。p.21 の「Snapshot Manager の資産の検出」を参照してください。

タスク	説明
メディアサーバーの関連付け	メディアサーバーにスナップショットをオフロードしてワークフローをリストアするには、メディアサーバーを Snapshot Manager に関連付ける必要があります。p.21 の「メディアサーバーと Snapshot Manager の関連付け」を参照してください。

Snapshot Manager の追加

NetBackup Web UI を使用して Snapshot Manager を追加できます。

メモ: スナップショットからのバックアップを許可するには、Snapshot Manager と NetBackup サーバー間に双方向の接続が必要です。

Snapshot Manager を追加するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [Snapshot Manager]タブをクリックします。
3. [追加 (Add)]をクリックします。
4. [Snapshot Manager]フィールドに次のいずれかを入力します。
   - Snapshot Manager のホスト名または IP アドレス。
     ホスト名または IP アドレスは、Snapshot Manager のインストール中に Snapshot Manager を構成する際に指定したものと同じである必要があります。
   - DNS サーバーが構成されている場合、Snapshot Manager の FQDN を入力します。
5. [ポート (Port)]フィールドに Snapshot Manager のポート番号を入力します。
   ポートのデフォルト値は 443 です。
6. [保存 (Save)]をクリックします。

Snapshot Manager のクラウドプロバイダの追加

AWS (アマゾンウェブサービス)、GCP (Google Cloud Platform)、Microsoft Azure、Microsoft Azure Stack Hub、OCI (Oracle Cloud Infrastructure) プロバイダ上の資産を保護できます。9.0 以降、Snapshot Manager は、アマゾンウェブサービスおよび Microsoft Azure の米国政府機関向けクラウドの作業負荷を検出できます。

Snapshot Manager のクラウドプロバイダを追加するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [プロバイダ (Providers)]タブをクリックするか、構成を追加するクラウドプロバイダの下にある[追加 (Add)]をクリックします。
3. [構成の追加 (Add configuration)]ペインの[構成名 (Configuration Name)]フィールドに値を入力します。
4. 優先する Snapshot Manager を選択します。

5 必要な詳細情報を入力します。

クラウドプロバイダ	パラメータ	説明
Microsoft Azure	クレデンシャルの種類: アプリケーションサービスプリンシパル	
	テナント ID (Tenant ID)	アプリケーションを作成した AAD ディレクトリの ID。
	クライアント ID (Client ID)	アプリケーション ID。
	シークレットキー (Secret Key)	アプリケーションのシークレットキー。
	クレデンシャルタイプ: システム管理 ID	Azure の Snapshot Manager ホストでシステム管理 ID を有効にします。 **メモ:** システム管理 ID に役割を割り当てます。
	クレデンシャルタイプ: ユーザー管理 ID	
	クライアント ID (Client ID)	Snapshot Manager ホストに接続されているユーザー管理 ID の ID。 **メモ:** ユーザー管理 ID には、役割が割り当てられている必要があります。
	次のパラメータは、上記のすべてのクレデンシャルタイプに適用されます。	
	リージョン (Regions)	クラウド資産を検出する 1 つ以上の地域。 **メモ:** 行政クラウドを設定する場合は、US Gov アリゾナ、US Gov テキサス、または US Gov バージニアを選択します。
	リソースグループの接頭辞 (Resource Group prefix)	リソースグループ内のすべてのリソースを追加するために使用する文字列。
	接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)	このチェックボックスにチェックマークを付けるかどうかによって、資産がどのリソースグループにも関連付けられていない場合に、その資産を保護するかどうかを決めます。

クラウドプロバイダ	パラメータ	説明
Microsoft Azure Stack Hub	*AAD を使用:*	次の形式のエンドポイント URL により、Snapshot Manager は Azure リソースに接続できます。
	Azure Stack Hub Resource Manager エンドポイントの URL (Azure Stack Hub Resource Manager endpoint URL)	`https://management.<location>.<FQDN>`
	テナント ID (Tenant ID)	アプリケーションを作成した AAD ディレクトリの ID。
	クライアント ID (Client ID)	アプリケーション ID。
	シークレットキー (Secret Key)	アプリケーションのシークレットキー。
	認証リソースの URL (省略可能) (Authentication Resource URL (optional))	認証トークンの送信先の URL。
	ADFS を使用:	Snapshot Manager を Azure リソースに接続できるようにする、次の形式のエンドポイント URL。
	Azure Stack Hub Resource Manager エンドポイントの URL (Azure Stack Hub Resource Manager endpoint URL)	`https://management.<location>.<FQDN>`
	テナント ID (Tenant ID)	アプリケーションを作成した AAD ディレクトリの ID。
	クライアント ID (Client ID)	アプリケーション ID。
	シークレットキー (Secret Key)	アプリケーションのシークレットキー。
	認証リソースの URL (省略可能) (Authentication Resource URL (optional))	認証トークンの送信先の URL。
Amazon AWS	アクセスキー (Access key)	アクセスキー ID をシークレットアクセスキーと共に指定すると、AWS API との通信が Snapshot Manager に許可されます。 **メモ:** IAM の役割の作成方法について詳しくは、AWS のマニュアルを参照してください。
	シークレットキー (Secret Key)	アプリケーションのシークレットキー。
	メモ: Snapshot Manager が IAM で構成されている場合、[アクセスキー (Access Key)]と[シークレットキー (Access Key)]オプションは利用できません。	
	リージョン (Regions)	クラウド資産を検出する 1 つ以上の AWS リージョン。 **メモ:** 政府機関向けクラウドを設定する場合は、us-gov-east-1 または us-gov-west-1 を選択します。
	VPC エンドポイント (VPC Endpoint)	ゾーンが指定されていない、AWS STS (セキュリティトークンサービス) エンドポイントサービスの最初の DNS 名。

クラウドプロバイダ	パラメータ	説明
Google Cloud Platform	プロジェクト ID (Project ID)	リソースの管理元であるプロジェクトの ID。`project_id` として JSON ファイルに記載されています。
	クライアントの電子メール (Client Email)	クライアント ID の電子メールアドレス。`client_email` として JSON ファイルに記載されています。
	秘密鍵 (Private Key)	秘密鍵。`private_key` として JSON ファイルに記載されています。 **メモ:** この鍵は引用符なしで入力する必要があります。鍵の先頭または末尾にスペースや改行文字を入力しないでください。
	リージョン (Regions)	プロバイダが動作する領域のリスト。
Oracle Cloud Infrastructure	クレデンシャルタイプ: API キー	
	ユーザー OCID (User OCID)	クレデンシャルを生成するユーザーの OCID。
	テナンシー (Tenancy)	OCI アカウントのテナント ID。
	指紋 (Fingerprint)	クレデンシャルの生成中に取得した指紋。
	秘密鍵 (Private Key)	クレデンシャルの生成中に取得した秘密鍵。
	リージョン (Regions)	クラウド資産を検出する 1 つ以上の OCI のリージョン。
	クレデンシャルタイプ: IAM	NetBackup Snapshot Manager は、動的グループに含まれている必要があり、その動的グループには十分な権限が必要です。 **メモ:** Snapshot Manager が IAM 構成で構成されている場合、[リージョン (Regions)]を除く他のフィールドは利用できません。

6 [構成の追加 (Add Configuration)]ペインで、接続と認証の詳細を入力します。

7 [保存 (Save)]をクリックします。

クラウドプロバイダの資産が自動的に検出されます。

新しい地域の追加

構成を編集して、Snapshot Manager に新しい地域を追加できます。

新しい地域を追加するには:

1 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。

2 [Snapshot manager]タブをクリックします。1 つ以上の地域を追加するプロバイダのタブをクリックします。新しい地域を追加するプラグイン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。

または

[プロバイダ (Providers)]タブをクリックし、地域を追加するプロバイダの[構成 (Configurations)]をクリックします。新しい地域を追加するプラグイン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。

3 [地域 (Regions)]リストから 1 つ以上の新しい地域を追加します。

4 [保存 (Save)]をクリックし、プラグインのプロパティページの[検出状態 (Discovery status)] 列に[成功 (Success)]と表示されるまで待機します。

5 プラグイン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。検出が完了するまで待機します。

AWS の構成の IAM ロール

Snapshot Manager をクラウドに配備している場合、AWS の構成で認証に IAM ロールを使用するように構成できます。

p.15 の「Snapshot Manager のクラウドプロバイダの追加」を参照してください。

先に進む前に、IAM ロールが AWS 内で構成されていることを確認します。詳しくは、『NetBackup Snapshot Manager インストールおよびアップグレードガイド』を参照してください。

メモ: AWS CSP の構成後に、NetBackup Snapshot Manager ホストの IAM ロールを変更する場合は、CSP 構成を編集し、同じ構成で一度保存する必要があります。

サポートされる IAM ロールの実装は次のとおりです。

- ソースアカウント: この場合、保護が必要なクラウド資産は Snapshot Manager と同じ AWS アカウントにあります。したがって、AWS のアカウント ID とロール名が AWS クラウドで認識されるため、必要な作業は領域の選択だけです。
- クロスアカウント: この場合、保護が必要なクラウド資産は Snapshot Manager とは別の AWS アカウントにあります。したがって、それらの資産に Snapshot Manager からアクセスできるように、領域に加えてターゲットアカウントとターゲットロール名の詳細を入力する必要があります。
  ソースとターゲットアカウント間で信頼関係を確立する必要があります。たとえば、プラグインの構成に使用する役割の ARN が次の場合:
  arn:aws:iam::935923755:role/TEST_IAM_ROLE

プラグインを構成するには、ARN の最後の部分の名前 *TEST_IAM_ROLE* を指定します。
詳しくは、アマゾンウェブサービスのマニュアルで、IAM ロールを使用した AWS アカウントへのアクセスに関連する情報を参照してください。

OCI の構成の IAM ポリシー

Snapshot Manager をクラウドに配備している場合、認証に IAM ポリシーを使用するように OCI を構成できます。

p.15 の「Snapshot Manager のクラウドプロバイダの追加」を参照してください。

先に進む前に、IAM ポリシーが OCI 内で構成されていることを確認します。詳しくは、『NetBackup Snapshot Manager インストールおよびアップグレードガイド』を参照してください。

OCI は、IAM ポリシーのソースアカウントの実装をサポートします。Snapshot Manager は、Snapshot Manager が配備されているのと同じテナントで、OCI の IAM ポリシー構成をサポートします。したがって、OCI テナンシ ID が OCI クラウドで認識されるため、必要な作業は領域の選択だけです。

メディアサーバーと Snapshot Manager の関連付け

メディアサーバーを使用して、スナップショットをオフロードし、クラウドのジョブをリストアできます。この機能を有効にするには、1 つ以上のメディアサーバーを Snapshot Manager に関連付ける必要があります。スナップショットまたはリストアジョブを実行するには、メディアサーバーがアクティブな状態になっている必要があります。Snapshot Manager と関連付けるメディアサーバーは、NetBackup プライマリサーバーにも関連付ける必要があります。ただし、検出ジョブは NetBackup プライマリサーバーでのみ実行されます。

メディアサーバーと Snapshot Manager を関連付けるには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [Snapshot Manager]タブをクリックします。
3. Snapshot Manager の横のメニューで[詳細設定 (Advanced settings)]をクリックします。
4. [メディアサーバー (Media server)]タブで、Snapshot Manager と関連付ける 1 つ以上のメディアサーバーを選択します。
5. [保存 (Save)]をクリックします。

Snapshot Manager の資産の検出

Snapshot Manager を使用してクラウドプロバイダを構成すると、自動検出がトリガされ、クラウドから資産が検出されます。定期検出で、NetBackup は 2 時間ごとに Snapshot

Manager から資産データを、Snapshot Manager は 1 時間ごとにクラウドプロバイダ構成から資産データを取得します。Snapshot Manager を無効にすると、そのサーバーに関連付けられているすべての資産は保護されなくなり、NetBackup と同期しなくなります。

必要に応じて、個々のクラウドプロバイダ構成の *[検出 (Discover)]* オプションを使用してクラウド資産の検出を手動でトリガしたり、Snapshot Manager で検出をトリガして、Snapshot Manager で利用可能な資産データをフェッチしたりもできます。

最初の完全検出後に、NetBackup は構成済みの Snapshot Manager に対して資産の増分検出を定期的に実行します。前回の検出と今回の検出の間に発生した資産の追加、削除、修正などの変更のみを検出します。

メモ: 正確に増分を検出し、検出の問題を回避するため、NetBackup プライマリサーバーと Snapshot Manager 上で、これらのサーバーが配置されているタイムゾーンに従って時刻が正しく設定されていることを確認します。

次の手順では、Snapshot Manager レベルで検出を実行する方法について説明します。これはクラウドから資産を検出するのではなく、Snapshot Manager からの特定時点のデータをフェッチするだけです。

Snapshot Manager の資産を検出するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [Snapshot Manager]タブをクリックします。
3. Snapshot Manager の横のメニューで[検出 (Discover)]をクリックします。

次の手順では、構成レベルで検出を実行する方法について説明します。これは資産の詳細検出をトリガし、クラウド内の資産の追加、変更、削除を検出した資産の特定時点の状態をフェッチします。

クラウドプロバイダ構成の資産を検出するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [Snapshot Manager]タブをクリックします。
3. クラウドプロバイダを表示する Snapshot Manager の IP またはホスト名をクリックします。
4. 構成を表示するプロバイダのタブをクリックします。
5. 構成名の横にあるメニューで[検出 (Discover)]をクリックします。

メモ: クラウドプロバイダ構成における検出が 30 分を超えると、最初の検出操作がタイムアウトします。ただし、後続の操作が続行され、NetBackup 資産は Snapshot Manager の資産と同期されます。

Snapshot Manager の自動検出の間隔を変更

自動検出オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。例:

CLOUD_AUTODISCOVERY_INTERVAL = 秒数

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

Snapshot Manager の有効化または無効化

必要に応じて、Snapshot Manager を有効または無効にできます。Snapshot Manager を無効にすると、資産の検出または保護計画の割り当てを行えなくなります。

Snapshot Manager を有効化または無効化するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [Snapshot Manager]タブをクリックします。
3. Snapshot Manager の状態に基づいて、[有効化 (Enable)]または[無効化 (Disable)]を選択します。

メモ: Snapshot Manager を無効化すると、関連付けられている資産の保護がそのサーバーで失敗するようになります。その場合は、保護計画から資産をサブスクライブ解除するか、保留中の SLP 操作をキャンセルして、無効化中のジョブの失敗を回避します。

(オプション) Snapshot Manager 拡張機能の追加

Snapshot Manager 拡張機能の目的は、パフォーマンス容量がピーク時に Snapshot Manager サーバー上で多数の要求を同時に実行するため、Snapshot Manager ホストの容量を拡大縮小させることです。要件に応じて、1 つ以上の Snapshot Manager 拡張機能をオンプレミスまたはクラウドにインストールし、ホストに余分な負荷をかけることなくジョブを実行できます。拡張機能によって、Snapshot Manager ホストの処理容量を増加できます。

Snapshot Manager 拡張機能では、Snapshot Manager ホストと同等以上の構成が可能です。

サポート対象の Snapshot Manager 拡張機能の環境:

- オンプレミスの VM ベースの拡張機能
- 管理対象 Kubernetes クラスタを備えたクラウドベースの拡張機能

『NetBackup Snapshot Manager インストールおよびアップグレードガイド』の「Snapshot Manager 拡張機能の配備」の章を参照してください。

クラウド資産のインテリジェントグループの管理

問い合わせと呼ばれるフィルタのセットに基づいて、インテリジェントクラウド資産グループを定義して、資産のダイナミックグループを作成および保護できます。NetBackup は問い合わせに基づいてクラウド仮想マシン、アプリケーション、および PaaS 資産を選択し、それらをグループに追加します。インテリジェントグループでは、資産の環境内の変更が自動的に反映されるため、環境内で資産を追加または削除しても、グループ内の資産のリストを手動で修正する必要がないことに注意してください。

インテリジェントクラウド資産グループに保護計画を適用すると、今後資産環境が変更された場合に、問い合わせ条件を満たすすべての資産が自動的に保護されます。

メモ: インテリジェントグループの作成、更新、削除は、管理が必要なクラウド資産に対する必要な RBAC 権限が役割に付与されている場合にのみ実行できます。NetBackup セキュリティ管理者は、特定のアカウントまたはサブスクリプションに関連付けられている資産タイプ (VM、PaaS、アプリケーション、ボリューム、ネットワーク) またはクラウドプロバイダレベルで、アクセス権を付与できます。『NetBackup Web UI 管理者ガイド』を参照してください。

クラウドインテリジェントグループの考慮事項

クラウドインテリジェントグループを作成する前に、次の点を考慮します。

- インテリジェントグループフィルタに指定する値では、大文字と小文字が区別されます。
- [状態 (Status)]属性は、[ジョブの状態 (State)]から導出されます。[状態 (Status)]属性に条件フィルタを追加するには、[フィルタ (Filter)]ドロップダウンから[ジョブの状態 (State)]を選択します。
- インテリジェントグループのアカウント ID オプション:
  - [アカウント ID (Account ID)]リストの[すべてのアカウント (All Accounts)]オプションは、NetBackup のデフォルトのクラウド管理者ロールで使用できます。
  - [アカウント ID (Account ID)]リストの[すべてのアカウント (All Accounts)]オプションは、1 つまたは複数のクラウドサービスプロバイダに対して[すべてのクラウド資産 (All cloud assets)]権限を持つ NetBackup のカスタムロールで使用できます。
  - アカウントまたはサブスクリプションの明示的な資産アクセス権限があるカスタムロールでは、[すべてのアカウント (All Accounts)]オプションを使用できません。

PaaS インテリジェントグループの考慮事項

- 資産でサポートされているバックアップ形式に基づいて、異なる保護計画に資産をサブスクライブできます。ただし、増分スケジュールを含む保護計画には、AWS RDS Oracle 資産を含むインテリジェントグループをサブスクライブできません。
- インテリジェントグループは、AWS DocumentDB と AWS Neptune の作業負荷に対してはサポートされません。
- [サービス形式 (Service type)]ドロップダウンには、検出された資産に関係なく、プロバイダで利用可能なサービスの種類が表示されます。
- PaaS 資産のインテリジェントグループは、Azure、AWS、GCP 資産の保護をサポートします。
- インテリジェントグループは、Redshift クラスタではサポートされません。ただし、Redshift データベース資産のインテリジェントグループはサポートされます。
- Azure MySQL 資産の場合、データベースとサーバー資産を混在させたインテリジェントグループを作成することはできません。インテリジェントグループには、データベースまたはサーバーのグループを含めることができます。Azure MySQL 用のインテリジェントグループを作成する場合は、entityType フィルタをサーバーまたはデータベースとして指定する必要があります。
- Azure SQL Server と Azure Managed Instance のタグの処理:
  - SQL Server では、タグがデータベースレベルでコピーされるときに、「Server」キーワードがタグの接頭辞として追加されます。
  - Azure Managed Instance では、タグがデータベースレベルでコピーされるときに、「Instance」キーワードがタグの接頭辞として追加されます。
  - 他の作業負荷のタグには接頭辞は追加されません。

アプリケーションインテリジェントグループの考慮事項

アプリケーションのインテリジェントグループを作成する際、AWS では RDS 資産のみがサポートされます。

クラウド資産用インテリジェントグループの作成

クラウド資産用にインテリジェントグループを作成するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [インテリジェントグループ (Intelligent groups)]タブ、[+ 追加 (+ Add)]の順に選択します。
3. グループの名前と説明を入力します。

4 クラウドプロバイダ、アカウント ID、領域を選択します。

メモ: 領域が指定されていない場合、検出されたすべての領域の資産にクラウドインテリジェントグループフィルタが適用されます。

5 ［資産タイプ (Asset type)］を選択します。

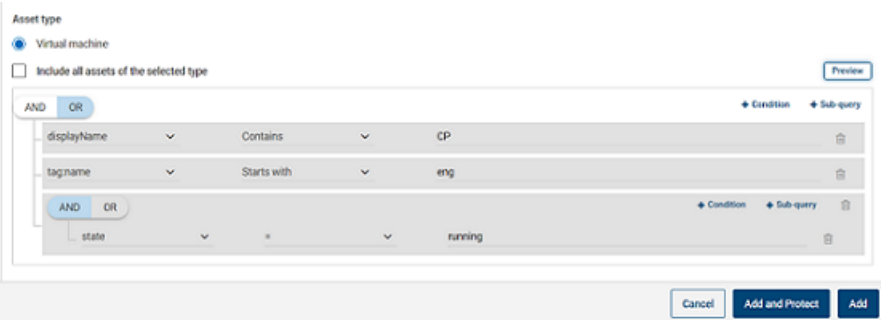
6 その後、次のいずれかを実行します。

- ［選択したタイプの資産をすべて含める (Include all assets of the selected type)］を選択します。
  このオプションでは、デフォルトの問い合わせを使用して、保護計画の実行時にすべての資産をバックアップ対象として選択します。
- 特定の条件を満たす資産のみを選択するには、独自の問い合わせを作成します。［条件の追加 (Add condition)］をクリックします。

7 条件を追加するには、ドロップダウンを使用してキーワードと演算子を選択し、値を入力します。

p.28 の「クラウド資産用インテリジェントグループ作成のための問い合わせオプション」を参照してください。

問い合わせの効果を変更するには、[+ 条件 (+ Condition)]をクリックし、[AND]または[OR]をクリックして、キーワード、演算子、条件の値を選択します。例:



この例では、OR を使用して問い合わせの範囲を絞り込みます。表示名に cp が含まれ、eng という名前のタグを持つ**実行状態**の VM のみが選択されます。

メモ: タグ名では特殊文字「<」はサポートされていません。この文字が存在すると、資産グループの作成は失敗します。

メモ: NetBackup の既知の制限事項 - スペースや特殊文字 (`(`, `)`, `&`, `¥`, `/`, `"`, `[`, `]`, `{`, `}`, `:` など) を含む資産タグ名 (クラウドプロバイダから参照) を含む問い合わせを作成すると、後でパラメータを編集するために問い合わせを編集できません。この制限により、インテリジェントグループの正常な作成と、そのグループへの保護計画の適用が妨げられることはありません。この制限の影響を受けるのは、問い合わせの編集機能のみです。

この問題を回避するには、指定された特殊文字がタグ名に含まれていないことを確認し、新しいタグ名を使用して新しい問い合わせを作成します。

条件にサブクエリーを追加することもできます。[+ サブクエリー (+ Sub-query)]をクリックし、[AND]または[OR]をクリックしてから、サブクエリーの条件のキーワード、演算子、値を選択します。

8 問い合わせをテストするには、[プレビュー (Preview)]をクリックします。

問い合わせベースの選択処理は動的です。仮想環境の変更は、保護計画の実行時に問い合わせが選択する資産に影響する可能性があります。その結果、保護計画が後で実行された時に問い合わせが選択する資産が、プレビューに現在表示されているものと同一でなくなる可能性があります。

メモ: [インテリジェントグループ (Intelligent groups)]で問い合わせを使用する場合、問い合わせ条件に英語以外の文字が含まれていると、NetBackup Web UI に、問い合わせに一致する正確な資産のリストが表示されないことがあります。

任意の属性に `not equals` フィルタ条件を使用すると、属性に値が存在しない (null) 資産を含む資産が戻されます。`tag` などの複数値の属性では、属性値のうち少なくとも 1 つに一致しないと資産は戻されません。

メモ: [プレビュー (Preview)]をクリックするかグループを保存した場合、グループの資産を選択するときに、問い合わせオプションでは大文字と小文字が区別されます。[仮想マシン (Virtual machines)]で、グループに選択されていない VM をクリックすると、[インテリジェントグループ (Intelligent groups)]フィールドは `none` になります。

---

9 グループを保護計画に追加せずに保存するには、[追加 (Add)]をクリックします。

グループを保存して保護計画をグループに適用するには、[追加と保護 (Add and protect)]をクリックします。計画を選択し、[保護 (Protect)]をクリックします。

クラウド資産用インテリジェントグループ作成のための問い合わせオプション

メモ: 属性値は、クラウドプロバイダのポータルに表示される値と正確に一致しない場合があります。個々の資産について、資産の詳細ページまたはクラウドプロバイダの API レスポンスを参照できます。

表 1-3 問い合わせキーワード

キーワード	説明 (すべての値で大文字と小文字が区別されます)
`displayName`	資産の表示名。
`state`	たとえば、実行中、停止などです。
`tag`	分類のために資産に割り当てられたラベル。

キーワード	説明 (すべての値で大文字と小文字が区別されます)
instanceType / machineType / vmSize/shape	クラウドプロバイダの選択に応じて、資産のインスタンス、マシンの種類、または VM のサイズ。 たとえば、t2.large、t3.large、b2ms、d2sv3 などです。
parentEntityName	資産の親エンティティの名前。
parentEntityType	資産の親エンティティのエンティティ型。
resourceGroup	資産のリソースグループ。
entityType	資産のエンティティ型。
compartmentId	資産のコンパートメント OCID。OCI は、compartmentId を使用して、クラウドリソースを編成および分離します。

表 1-4　　問い合わせ演算子

演算子	説明
Starts with	文字列の先頭に値が出現する場合に一致します。
Ends with	文字列の末尾に値が出現する場合に一致します。
Contains	入力した値が文字列のどこにある場合でも一致します。
=	入力した値にのみ一致します。
≠	入力した値と等しくない任意の値と一致します。

メモ: インテリジェントグループの作成後、そのクラウドプロバイダの選択は編集できませんが、必要に応じて名前と説明を編集し、問い合わせを修正できます。

クラウド資産用インテリジェントグループの削除

クラウド資産用インテリジェントグループを削除するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [インテリジェントグループ (Intelligent groups)]タブでインテリジェントグループを見つけます。
3. グループが保護されていない場合は、グループを選択して[削除 (Delete)]をクリックします。
4. グループが保護されている場合は、グループをクリックし、下にスクロールして[保護の削除 (Remove protection)]をクリックします。
5. 次に、[インテリジェントグループ (Intelligent groups)]タブでこのグループを選択し、[削除 (Delete)]をクリックします。

クラウド資産またはクラウド資産用インテリジェントグループの保護

クラウド作業負荷に対してクラウドプロバイダ固有の保護計画を作成できます。その後、クラウドプロバイダに関連付けられている資産をプロバイダ固有の保護計画にサブスクライブできます。

メモ: 以前に異なるクラウドプロバイダの資産に適用された保護計画がある場合、自動的に新しいプロバイダ固有の形式に変換されます。この変換は NetBackup 9.1 へのアップグレード後に行われます。たとえば、Google Cloud と AWS クラウドの資産を 1 つの保護計画にサブスクライブしていた場合、保護計画が分割されます。保護計画は、プロバイダごとに 2 つの個別の保護計画に分割されます。

p.31 の「NetBackup 9.1 以降へのアップグレード後の保護計画の変換」を参照してください。。

次の手順を使用して、クラウド VM、アプリケーション、ボリューム、またはインテリジェントグループを保護計画にサブスクライブします。保護計画に資産をサブスクライブするときに、定義済みのバックアップ設定を資産に割り当てます。

メモ: 自分に割り当てられている RBAC の役割によって、管理する資産と、使用する保護計画にアクセスできるようにする必要があります。

クラウド資産またはインテリジェントグループを保護するには

1 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。

2 [仮想マシン (Virtual machine)]タブ、[アプリケーション (Applications)]タブ、[ボリューム (Volumes)]タブ、または[インテリジェントグループ (Intelligent groups)]タブで、資産または資産グループにチェックマークを付けて[保護の追加 (Add protection)]をクリックします。

3 保護計画を選択し、[次へ (Next)]をクリックします。

4 次の設定を調整できます。

- スケジュールと保持 (Schedules and retention)
- ストレージオプション (Storage options)
  Web UI のストレージオプションについて詳しくは、『NetBackup Web UI 管理者ガイド』の「ストレージの構成」セクションを参照してください。
- バックアップオプション (Backup options)

5 [保護 (Protect)]をクリックします。

即時保護のための[今すぐバックアップ (Backup now)]オプション

スケジュール設定された保護計画とは別に、[今すぐバックアップ (Backup now)]オプションを使用して資産をすぐにバックアップし、計画外の状況に対して保護することもできます。

1. クラウド資産またはインテリジェントグループを選択し、[今すぐバックアップ (Backup now)]をクリックします。
2. 次に、適用する保護計画を選択します。資産の特定のクラウドプロバイダに関連する保護計画のみが、オプションとして表示されます。
3. [バックアップの開始 (Start Backup)]をクリックします。

   バックアップジョブがトリガされます。これは[アクティビティモニター (Activity Monitor)]ページで追跡できます。

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

NetBackup 9.1 以降へのアップグレード後の保護計画の変換

古い保護計画の新しい形式への自動変換について、次の点に注意してください。

- NetBackup 9.1 以降へのアップグレード後に資産の移行が完了すると、保護計画の変換が開始されます。
- 資産がサブスクライブされていない古い保護計画は、新しい形式に変換されません。これらは手動で削除できます。
- 変換前または変換中

- すべての資産は古い保護計画からサブスクライブ解除され、変換された保護計画にサブスクライブされます。
- 新しい資産は古い保護計画にサブスクライブできません。
- ［今すぐバックアップ (Backup now)］操作は古い計画では失敗します。
- 古い保護計画のカスタマイズまたは編集はできません。

- 正常に変換された後
  - 古い保護計画を使用して 1 つのクラウドプロバイダのみの資産を保護していた場合、新しい計画は変換時に同じ名前と資産のサブスクリプションを保持します。
  - 古い保護計画を使用して複数のクラウドプロバイダの資産を保護していた場合、古い保護計画の名前は以前と同じ名前が保持されます。保護計画名が更新され、変換時にいずれか 1 つのクラウドプロバイダの資産のサブスクリプションが保持されます。
    古い計画の一部だったその他のクラウドプロバイダについては、変換時に新しい保護計画が作成され、それぞれのプロバイダの資産のみがその保護計画にサブスクライブされます。新しい計画の名前は `<old_plan_name>_<cloud_provider>` の形式です。
  - したがって、Web UI の *[保護計画 (Protection Plans)]* メニューに以前よりも多くの計画が表示される場合があります。
  - 成功メッセージは次のように通知に表示されます。
    「新しい形式に変換中に保護計画 <protectionPlanName> が作成されました。(The protection plan <protectionPlanName> created during conversion to new format.)」
    「保護計画 <protectionPlanName> を新しい形式に正常に変換しました。(Successfully converted the protection plan <protectionPlanName> to the new format.)」
    その後、変換された保護計画の管理と適用を通常どおり開始できます。

エラーシナリオ

保護計画の変換中または変換後にエラーシナリオがどのように処理されるのかについては、次を参照してください。また、エラーアラートの通知を確認し、必要な処理を実行します。

- 一部の資産は、古い保護計画からのサブスクライブ解除に失敗することがあります。その場合、正常にサブスクライブ解除された資産の変換が続行されます。失敗した資産の変換プロセスは、4 時間ごとに再試行されます。
- 変換後、一部の資産は新しい計画に自動的に再サブスクライブされない場合があります。その場合、変換済みの保護計画にそれらの資産を手動でサブスクライブする必要があります。

- 新しい変換済みの保護計画に必要なアクセス権を割り当てる際に、エラーが発生する可能性があります。その場合、アクセス権を手動で割り当てる必要があります。

クラウド資産またはインテリジェントグループの保護のカスタマイズまたは編集

スケジュールバックアップの時間帯や他のオプションなど、保護計画の特定の設定を編集できます。

クラウド資産の保護計画をカスタマイズまたは編集するには

1. 左側で[作業負荷 (Workloads)]、[クラウド]の順にクリックします。
2. [仮想マシン (Virtual machine)]タブ、[アプリケーション (Applications)]タブ、[ボリューム (Volumes)]タブ、または[インテリジェントグループ (Intelligent groups)]タブで、保護をカスタマイズする資産をクリックします。
3. [保護のカスタマイズ (Customize protection)]、[続行 (Continue)]の順にクリックします。
4. 次の 1 つ以上の設定を調整できます。
   - スケジュールと保持 (Schedules and retention)
     バックアップの開始時間帯を変更します。
   - バックアップオプション (Backup options)
     Google Cloud 資産の地域別スナップショットを有効または無効にするか、Azure および Azure Stack Hub 資産のスナップショットの宛先リソースグループを指定または変更します。

クラウド資産またはインテリジェントグループの保護の削除

保護計画からクラウド資産のサブスクライブを解除できます。資産のサブスクライブが解除されると、バックアップは実行されなくなります。

クラウド資産の保護を削除するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual machine)]タブ、[アプリケーション (Applications)]タブ、[ボリューム (Volumes)]タブ、または[インテリジェントグループ (Intelligent groups)]タブで、保護を削除する資産をクリックします。
3. [保護の削除 (Remove protection)]、[はい (Yes)]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について

SLP (ストレージライフサイクルポリシー) は、一連のバックアップのストレージ計画です。SLP は NetBackup 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)]の順に選択します。

SLP はストレージ操作の形式の手順を含み、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 SLP に追加され、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します。NetBackup は、必要に応じてコピーを再試行し、すべてのコピーを作成します。

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動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、さまざまなバックアップの短期的または長期的な利点を活かすことができます。

このセクションでは SLP について簡単に説明します。詳しくは、『NetBackup™ 管理者ガイド Vol. 1』を参照してください。

SLP のベストプラクティスについては、ナレッジベースの記事 https://www.veritas.com/content/support/ja_JP/article.100009913 を参照してください。

SLP の追加

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、次の手順を使用します。

このセクションでは SLP の作成について簡単に説明します。詳しくは、『NetBackup™ 管理者ガイド Vol. 1』を参照してください。

SLP のベストプラクティスについては、ナレッジベースの記事 https://www.veritas.com/content/support/ja_JP/article.100009913 を参照してください。

SLP を作成するには

1. NetBackup Web UI を開きます。
2. 左側で[ストレージ (Storage)]、[ストレージライフサイクルポリシー (Storage lifecycle policy)]の順に選択します。
3. [追加 (Add)]をクリックして新しい SLP を作成します。

4 [ストレージライフサイクルポリシー (Storage lifecycle policy)]ペインで、次の詳細を指定します。

- [ストレージライフサイクルポリシー名 (Storage lifecycle policy name)]: SLP が作成された後は、名前を変更できません。
- [データの分類 (Data classification)]: 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)]の分類も含まれます。[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。
- [セカンダリ操作の優先度 (Priority for secondary operations)]: 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。

5 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。[追加 (Add)] をクリックして、SLP に操作を追加します。[新規操作 (New operation)]ペインで、次の情報を入力します。操作の種類を選択します。

ソースストレージ (Source storage) > 操作 (Operation)	バックアップ (Backup) スナップショット (Snapshot) インポート (Import)
宛先ストレージの属性 (Destination storage attributes) > 宛先ストレージ (Destination storage)	■ スナップショット ■ ストレージユニットなし ■ スナップショット
宛先ストレージの属性 (Destination storage attributes) > ボリュームプール (Volume pool)	NetBackup **メモ:** [スナップショット (Snapshot)]と[インポート (Import)]操作では、このオプションは無効になります。

保持 (Retention) > 保持形式 (Retention type)	■ [固定 (Fixed)]の保持を指定すると、ストレージのデータが指定した期間保持され、その期間が過ぎるとバックアップまたはスナップショットが期限切れになります。 ただちに期限切れにする、1 週間、2 週間、3 週間以上。 保持が固定されているイメージコピーは、次の条件がすべて満たされると期限切れの対象になります。 ■ [固定 (Fixed)]のコピーが保持される期間が期限切れになりました。 ■ 子のコピーはすべて作成されました。 ■ ミラーコピーである子のコピーすべてが、期限切れの対象になります。 ■ [コピー後に期限切れにする (Expire after copy)]の保持を指定すると、イメージのダイレクト (子) コピーがすべて他のストレージに正常に複製された後に、このストレージのデータが期限切れになります。後続のコピーが構成されないので、SLP の最後の操作で[コピー後に期限切れにする (Expire after copy)]の保持形式を使うことができません。このため、この保持形式の操作には子が必要です。 ■ [管理対象の容量 (Capacity managed)]操作は、各ボリュームの[高水準点 (High water mark)]の設定に基づいて、ストレージ上の空き容量が NetBackup によって自動的に管理されることを意味します。 ディスクストレージユニットまたはディスクプールの[高水準点 (High water mark)]設定および[低水準点 (Low Water Mark)]設定によって、領域の管理方法が決まります。

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。操作の種類を選択します。子操作の場合、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 [時間帯 (Window)]タブには、利用可能な操作形式が表示されます。これらを使用してセカンダリ操作を実行するタイミングを指定して、操作の時間帯を作成します。

7 必要に応じて、[ソースコピーが期限切れになりそうになるまで、このコピーの作成を延期します (Postpone creation of this copy until the source copy is about to expire)]を選択します。

8 ［詳細 (Advanced)］で、時間帯が終了した後 NetBackup でアクティブなイメージを処理するかどうかを指定します。

9 ［複製 (Duplication)］で、異なるメディアサーバーによって書き込まれたバックアップイメージの読み込みを、代替読み込みサーバーに許可できます。

さまざまなスナップショット操作とバックアップ操作の異なる SLP 構成を理解するには:

p.37 の「 PaaS と IaaS ポリシーの SLP 構成」を参照してください。

PaaS と IaaS ポリシーの SLP 構成

クラウドポリシー形式の場合は、SLP の操作階層を作成することをお勧めします。さまざまなスナップショット操作やバックアップ操作のさまざまな SLP 構成と、バックアップオプションの組み合わせを理解するには、表を参照してください。また、保護計画を使用して実行される各ユースケース間の違いも示します。

表 1-5 IaaS ポリシー形式の保護計画とポリシー SLP

保護計画	保護計画のバックアップオプション	ポリシーに対する同等の SLP 操作	ポリシーのバックアップオプション
A.I.R (レプリケーション)	該当なし	■ スナップショット ■ スナップショットからのバックアップ ■ レプリケーション	該当なし
スナップショットからのバックアップ + 個別リカバリ	ファイルおよびフォルダの個別リカバリを有効にします。	■ スナップショット ■ スナップショットからのバックアップ	ファイルおよびフォルダの個別リカバリを有効にします。

保護計画	保護計画のバックアップオプション	ポリシーに対する同等の SLP 操作	ポリシーのバックアップオプション
スナップショットからのバックアップ + スナップショットの有効期限が近いときにバックアップを開始。	ファイルおよびフォルダの個別リカバリを有効にします。	■ スナップショット ■ クラウドスナップショットインデックス ■ スナップショットからのバックアップ ([ソースコピーが期限切れになりそうになるまで、このコピーの作成を延期します (Postpone creation of this copy until the source copy is about to expire)]を選択)	ファイルおよびフォルダの個別リカバリを有効にします。
コピーの複製	該当なし	■ スナップショット ■ スナップショットからのバックアップ ■ 複製	該当なし
スナップショットの有効期限が近いときにバックアップを開始。	該当なし	■ スナップショット ■ スナップショットからのバックアップ ([ソースコピーが期限切れになりそうになるまで、このコピーの作成を延期します (Postpone creation of this copy until the source copy is about to expire)]を選択)	該当なし

保護計画	保護計画のバックアップオプション	ポリシーに対する同等の SLP 操作	ポリシーのバックアップオプション
バックアップのみを保持	該当なし	■ スナップショット([コピー後に期限切れにする (Expire after copy)]保持形式を選択) ■ スナップショットからのバックアップ	該当なし
バックアップとともにスナップショットを保持	該当なし	■ スナップショット ■ スナップショットからのバックアップ	該当なし
スナップショットのみを保持	該当なし	スナップショット	該当なし
スナップショットのみ + 個別リカバリ	ファイルおよびフォルダの個別リカバリの有効化	■ スナップショット ■ クラウドスナップショットインデックス	ファイルおよびフォルダの個別リカバリの有効化

表 1-6 PaaS ポリシー形式の保護計画とポリシー SLP

保護計画	ポリシーに対する同等の SLP 操作
バックアップ	プライマリとしてバックアップ操作
A.I.R. (レプリケーション)	■ バックアップ ■ レプリケーション
複製	■ バックアップ ■ 複製

クラウド資産のポリシーの管理

バックアップポリシーは、NetBackup が作業負荷をバックアップするときに従う指示を提供します。NetBackup Web UI を使用して、クラウド作業負荷の種類 (IaaS および PaaS) をサポートするポリシーを作成できます。ポリシーは、クライアントに存在するデータを保護するために作業負荷に適用されます。

クライアントにあるポリシーユーティリティを使用して、NetBackup 環境のさまざまなクライアント要件を満たすように複数の形式のポリシーを構成できます。ポリシーに対して、ポリシーの追加、編集、削除、スケジュール設定など、さまざまな操作を実行できます。

同様に、保護計画にはジョブ操作階層を表示するプロビジョニングがあります。同様に、ジョブ操作階層を指定するために SLP を作成する必要があります。

制限事項および考慮事項

クラウド作業負荷をサポートするポリシーを作成する場合は、次の制限事項を考慮してください。

- IaaS 用の AWS CSP のスナップショットレプリケーションはサポートされません。

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 1-7　　ポリシーの計画の手順

手順	処理	説明
手順 1	保護する資産に関する情報を収集します。	各資産について次の情報を収集します。 ■ 資産名とその地域。 ■ 各資産のバックアップ対象ファイルの概数。 ■ ファイルの典型的なサイズ。 ある資産にはいくつかのファイル内に大量のデータが含まれている可能性がありますが、別のアカウントはファイル数が少なく、データ量も少ないです。バックアップ時間が長くならないように、大きい資産を 1 つのポリシーに含め、小さい資産は別のポリシーに含めてください。大きい資産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	バックアップおよびリストア要件に基づく資産のグループ分け	さまざまなバックアップおよびリストア要件に応じて、さまざまな資産をグループ分けします。

手順	処理	説明
手順 3	ストレージ要件の考慮	ストレージユニットの設定は、ポリシーによってバックアップされるすべての資産に適用されます。資産に特別なストレージ要件がある場合、スケジュールなどの他の要素が同じである場合でも、それらの資産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保護対象のすべての資産には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、夜間のバックアップと昼間のバックアップ用に別々のポリシーを作成します。 ■ 資産の変更頻度。 一部の資産が他の資産よりも高頻度で変更される場合、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が十分にあります。 ■ 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資産が NetBackup によって保持される期間を決定する保持設定が含まれます。スケジュールはバックアップのために選択したすべての資産をバックアップするため、すべての資産の保持要件が類似している必要があります。資産の完全バックアップを永久に保持する必要がある場合、その資産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 5	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、検出されたすべての資産をバックアップする必要はありません。必要な資産のみを選択してバックアップするためのクエリーを作成します。

クラウド資産のポリシーの作成

さまざまな形式の作業負荷のクラウドポリシーを追加できます。ポリシーを作成する前に、ジョブ操作階層を表示するために、そのポリシー用に SLP (ストレージライフサイクルポリシー) が作成されていることを確認します。p.34 の「SLP の追加」を参照してください。

ポリシーを作成する方法:

1. 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。
2. [追加 (Add)]をクリックして新しいポリシーを作成します。
3. ポリシーを設定します。

属性	p.44 の「IaaS 資産の属性の設定」を参照してください。 p.42 の「PaaS 資産の属性の設定」を参照してください。
スケジュール	p.46 の「スケジュールの作成」を参照してください。 p.48 の「バックアップ間隔について」を参照してください。 p.50 の「保持期間の割り当てについて」を参照してください。 p.52 の「開始時間帯の構成」を参照してください。 p.54 の「含める日の構成」を参照してください。 p.56 の「除外日の構成」を参照してください。
クラウド資産	p.58 の「IaaS のクラウド資産の構成」を参照してください。 p.57 の「PaaS のクラウド資産の構成」を参照してください。
バックアップオプション **メモ:** このタブは IaaS クラウドポリシー形式でのみ表示されます。	p.60 の「IaaS のバックアップオプションの構成」を参照してください。

4. ポリシーの構成が完了したら、[作成 (Create)]をクリックします。

PaaS 資産の属性の設定

新しいポリシーを追加するか、既存のポリシーを変更する場合は、[属性 (Attributes)]タブを使用してバックアップ設定を構成します。ポリシーを作成するときに、ポリシーの名前を指定し、ポリシー形式を選択します。すべての属性がすべてのポリシー形式に適用されるわけではなく、利用できない属性は灰色で表示されます。

属性を設定するには

1. 左側で、[保護 (Protection)]の下の[ポリシー (Policies)]をクリックします。
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。[ポリシー形式 (Policy type)]には、[クラウド (Cloud)]を選択します。
3. [クラウドの作業負荷 (Cloud workload)]で、オプション[PaaS]を選択します。

   [クラウドスナップショットの実行 (Perform cloud snapshot)]オプションは、cloud-PaaS 資産のスナップショットベースの保護を可能にします。
4. (オプション) [クラウドスナップショットの実行 (Perform cloud snapshot)]を選択した場合、[宛先 (Destination)]セクションは表示されません。このパラメータは、完全バックアップスケジュールを使用する AWS DocumentDB、AWS Neptune、RDS Custom Oracle、RDS Custom SQL、および Redshift クラスタ資産にのみ適用できます。
5. [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。[データの分類なし (No data classification)]を選択した場合、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用します。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。
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、このボックスをチェックして、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 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。たとえば、今日が月曜日であり、水曜日の午前 0 時を指定した場合、ポリシーはその日時になるまで実行されません。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。

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。バックアップを再開するには、このオプションを再度選択します。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。

この属性を使用すると、一連のポリシーを有効にする前にそれらのポリシーを構成できます。

9 [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のみです。

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。

IaaS 資産の属性の設定

新しいポリシーを追加するか、既存のポリシーを変更する場合は、[属性 (Attributes)]タブを使用してバックアップ設定を構成します。ポリシーを作成するときに、ポリシーの名前を指定し、ポリシー形式を選択します。すべての属性がすべてのポリシー形式に適用されるわけではなく、利用できない属性は灰色で表示されます。

IaaS クラウドの場合、プライマリ操作としてスナップショットを持つ SLP (ストレージライフサイクルポリシー) を作成し、セカンダリ操作としてストレージユニットとともにスナップショットからのバックアップを作成する必要があります。p.34 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。

属性を設定するには

1 左側で、[保護 (Protection)]の下の[ポリシー (Policies)]をクリックします。

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。[ポリシー形式 (Policy type)]には、[クラウド (Cloud)]を選択します。

3 [クラウドの作業負荷 (Cloud workload)]で、オプション[IaaS]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。［データの分類なし (No data classification)］を選択した場合、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用します。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。SLP を作成し、それをドロップダウンから選択することもできます。［スケジュール (Schedule)］タブで、これらの選択を上書きできます。

5 ［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、このボックスをチェックして、1 から 999 の値を指定します。

6 ［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。

7 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。たとえば、今日が月曜日であり、水曜日の午前 0 時を指定した場合、ポリシーはその日時になるまで実行されません。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。

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。バックアップを再開するには、このオプションを再度選択します。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。

この属性を使用すると、一連のポリシーを有効にする前にそれらのポリシーを構成できます。

8 [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のみです。

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。

スケジュールの作成

[スケジュール (Schedules)]タブで定義するスケジュールは、選択したポリシーでバックアップを行うタイミングを決定します。また、各スケジュールには、バックアップが保持される期間などのさまざまな条件も含まれます。

スケジュールの属性は、次のタブに表示されます。

[属性 (Attributes)]タブ	作業を実行する時刻および間隔を、スケジュールの他の属性とともにスケジュールします。
[開始時間帯 (Start Window)]タブ	作業を実行する時刻を曜日ごとにスケジュールします。
[日のエクスクルード (Exclude Days)]タブ	ジョブを実行できない日付を指定します。
[含める日 (Include Dates)]タブ	特定の日付、毎週の特定の曜日または毎月の特定の日を指定して、作業の実行日をスケジュールします。(このタブは、スケジュール形式に[カレンダー (Calendar)]を選択した場合にだけ表示されます。)

ポリシーの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。IaaS 作業負荷の場合、[完全バックアップ (Full backup)]のみがサポートされます。

- [完全バックアップ (Full backup)] - ポリシーで指定されたすべてのファイルをバックアップします。ファイルは、それらのファイルが最後に変更またはバックアップされたタイミングに関係なくバックアップされます。完全バックアップは、スケジュールの条件に従って自動的に行われます。増分バックアップを実行する場合、完全なリストアを行うには、完全バックアップもスケジュールする必要があります。
- [差分増分バックアップ (Differential incremental backup)] - 最後の正常な増分 (差分または累積) バックアップまたは完全バックアップ以降に変更されているファイルを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、すべてのファイルのバックアップが行われます。差分増分バックアップは、スケジュールの条件に従って自動的に行われます。完全なリストアを行うには、最後の完全バックアップと、最後の完全バックアップ以降に行われたすべての差分増分バックアップが必要です。
- [アーカイブ REDO ログバックアップ (Archived redo log backup)] - この方式で、NetBackup は最後の完全または増分バックアップ以降に変更されたデータをバックアップします。アーカイブバックアップにより、完全バックアップと増分バックアップの処理時間が大幅に短縮されます。p.124 の「PaaS 作業負荷のアーカイブ REDO ログのバックアップについて」を参照してください。

メモ: Amazon (AWS) RDS Oracle は、トランザクションログのアーカイブをサポートします。

4 [宛先 (Destination)]の下に、適切なパラメータが表示されます。

- [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。
  - 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。

- 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。

5 ［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。

6 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。

7 ［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。

バックアップ間隔について

バックアップ間隔を決定するには、データを変更する頻度を考慮します。たとえば、ファイルを 1 日に数回、1 日に 1 回、毎週、または毎月変更するかどうかを判断します。

通常は、日々の作業内容を保護するために、毎日バックアップを行います。毎日バックアップを行う場合、ディスク障害が発生した場合に失われるのは、1 日分だけです。1 日の間に重要なデータの変更が頻繁に発生し、変更を再度構築することが難しい場合は、バックアップ間隔をさらに短くする必要があります。

日次バックアップは、通常、最後の差分増分バックアップまたは完全バックアップ以降の変更を記録する差分増分バックアップです。差分増分バックアップでは、完全バックアップに比べてストレージの使用量が少なく、時間がかからないため、リソースの節約になります。

完全バックアップは、通常は差分増分バックアップよりも実行間隔が長くなりますが、差分増分バックアップが連続して蓄積することを回避するのに十分な頻度で実行する必要があります。完全バックアップ間の差分増分バックアップの回数が多くなると、ファイルのリストアに時間がかかるようになります。時間がかかるのは、ファイルおよびディレクトリのリストア時にこれらの差分増分バックアップをまとめる必要があるためです。

完全バックアップの間隔を設定する場合、次の点を考慮します。

- 変更の頻度が少ないファイルの完全バックアップの間隔は空けるようにします。間隔を長くすると、使用するシステムリソースが少なくて済みます。また、完全バックアップ間の差分増分バックアップのサイズは小さいため、リストア時間が大幅に長くなることはありません。
- 頻繁に変更されるファイルの完全バックアップの間隔は短くします。間隔を短くすると、リストア時間が短くなります。完全バックアップの間隔を短くすると、使用するリソースも少なくなります。ファイル内の頻繁な変更に対応するのに必要な長時間の差分増分バックアップの累積の影響が軽減されます。

リソースを最も効果的に使用するために、現在のポリシーに含まれるほぼすべてのファイルが、同じ頻度で更新されていることを確認します。たとえば、ポリシーのバックアップ対象リスト内の半分のファイルが毎週の完全バックアップが必要となる程頻繁に変更されるとします。ただし、残り半分のファイルは変更の頻度が少なく、毎月の完全バックアップで十分であるとします。この場合、すべてのファイルが同じポリシー内にあると、すべてのファイルに対して毎週完全バックアップが実行されます。半分のファイルは毎月の完全バックアップで十分であるため、システムリソースを浪費することになります。バックアップを 2 つのポリシーに分けて、それぞれに適切なバックアップスケジュールを設定するか、または合成バックアップを使用すると改善されます。

ポリシー内のクライアントに対して複数の自動スケジュールが実行される予定である場合、バックアップ間隔によって、NetBackup に使用されるスケジュールが次のように決定されます。

- 常に、バックアップ間隔が長いスケジュールのジョブほど、優先度が高くなります。たとえば、バックアップ間隔が 1 カ月のスケジュールはバックアップ間隔が 2 週間のスケジュールより優先度が高くなります。
- 2 つのスケジュールをそれぞれ実行する必要がある場合、アルファベット順で最初のスケジュール名を持つスケジュールが最初に実行されます。アルファベット順の優先度は次の両方が該当する場合に適用されます。
  - 各スケジュールが定義されている時間帯内にある。
  - 各スケジュールが同じ間隔で構成されている。

NetBackup では、スケジュール例に対して次に示す順の優先度が設定されます。

表 1-8 スケジュールの間隔と優先度の例

スケジュール名	間隔	優先度 (Priority)
monthly_full	1 カ月	1 番目
weekly_full	1 週間。	2 番目
daily_differential_incremental	1 日	3 番目

保持期間の割り当てについて

データの保持期間は、一定期間後にメディアから情報をリストアする可能性によって決まります。財務の記録などのデータ形式には、法律で定められた保持レベルがあります。また、作成途中の文書などのデータの場合は、文書の最終版の完成後は必要がなくなります。

バックアップの保持期間は、そのバックアップからリカバリする必要性にも依存します。たとえば、毎日の変更内容が重要である場合、そのデータが必要な間は、完全バックアップに加えてすべての増分バックアップを保持します。増分バックアップが毎月のレポートで処理中の作業だけをトラッキングする場合、増分バックアップをすぐに期限切れにします。長期間のリカバリには完全バックアップを使用します。

保持期間を決定する場合、ほぼすべてのデータに適用するガイドラインを作成することが必要です。ガイドラインと異なる保持要件があるファイルまたはディレクトリに注意します。保持要件のガイドラインと異なるデータには、別のポリシーを作成することを計画します。たとえば、より長い保持要件のあるファイルおよびディレクトリを別のポリシーに配置します。すべてのポリシーに長い保持期間を設定するのではなく、別のポリシーでより長い保持期間をスケジュール設定します。

次の表は、さまざまなバックアップ形式の推奨の保持期間を記述したものです。

表 1-9 さまざまなバックアップ形式の推奨の保持期間

バックアップ形式	説明
完全バックアップ	スケジュールに対する間隔の設定より長い期間を指定します。(この間隔は、バックアップの実行間隔です。) たとえば、間隔が 1 週間である場合、2 週間から 4 週間の保持期間を指定します。保持期間を2週間から4週間にすると、十分な時間的余裕が確保され、次に完全バックアップが行われる前に、現行の完全バックアップの有効期限に達しないことが保証されます。
差分増分バックアップ	完全バックアップ間の間隔より長い期間を指定します。たとえば、完全バックアップが毎週実行される場合、差分増分バックアップを 2 週間保存します。

次の表は、要求するよりも早くバックアップが期限切れになることを防ぐことができる複数の方法を提案します。

表 1-10 早く期限切れになるバックアップを防ぐための提案

項目	説明
保持期間	適切な保持期間を割り当てます。保持期間が満了した後は、NetBackup によるバックアップのトラッキングは行われません。保持期間が満了した後は、ファイルをリカバリすることは困難または不可能です。 1 年以上保持する必要があるバックアップの場合、保持期間を無制限に設定します。
完全バックアップと増分バックアップ	ポリシーでは、増分バックアップより長い保持期間を完全バックアップに割り当ててください。完全なリストアを行うには、前回の完全バックアップ、およびそれ以降のすべての差分増分バックアップが必要です。増分バックアップの前に完全バックアップの期限が切れると、すべてのファイルをリストアできない場合があります。
アーカイブスケジュール	保持期間を無制限に設定します。
テープ	保持期間を無制限に設定します。NetBackup データベースの領域制約のため無制限に設定できない場合、データを保存する必要がある期間と一致する保持期間を設定します。

データの保持については、バックアップメディアのオフサイトでの保管も考慮します。オフサイトに保管することによって、プライマリサイトで発生する災害からデータを保護できます。

ディザスタリカバリの注意事項として、次のオフサイト保管方式を考慮します。

- 複製機能を使用してオフサイト保管用にセカンダリコピーを作成します。
- 毎月または毎週行われる完全バックアップをオフサイトの保管施設に送付します。データをリストアするには、保管施設からメディアを要求します。増分バックアップを使用してディレクトリまたはディスク全体のリストアを行うには、最後の完全バックアップとすべての増分バックアップが必要です。
- バックアップ用の特別なスケジュールを構成して、オフサイト保管用に複製を作成します。

オフサイトでの保管方法に関係なく、十分な保持期間を構成することが必要です。

デフォルトでは、NetBackup によって、同じ保持レベルのバックアップがすでに存在するテープボリュームに、各バックアップが格納されます。バックアップの保持レベルが 2 である場合、NetBackup は保持レベルが 2 の、他のバックアップを含むテープボリュームにこのバックアップを格納します。保持レベルが異なるバックアップが発生すると、NetBackup によって適切なボリュームに切り替えられます。テープボリュームは、自身が

格納するすべてのバックアップが有効期限に達するまで NetBackup に割り当てられたままであるため、ボリューム上の保持レベルを一致させることによって、メディアの使用が効率化されます。ボリューム上に保持期間が無制限の小さなバックアップが 1 つでもあると、他のすべてのバックアップが有効期限に達してもボリュームは再利用されません。

各ボリューム上に 1 つの保持レベルだけを保存する場合、必要以上の保持レベルを使用しないでください。複数の保持レベルを使用すると、必要なボリュームの数が増加します。

メモ: ディスクボリューム上では、制限なしに保持レベルを混在できます。

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 でジョブを開始可能な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。

また、スケジュールに対して、削除、消去、複製、取り消しなどの他の操作を実行することもできます。

開始時間帯を構成するには:

1. [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。

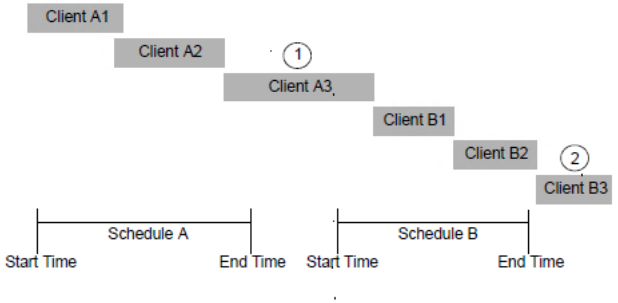
［削除 (Delete)］をクリックします。	選択した時間帯を削除します。
［消去 (Clear)］をクリックします。	スケジュール表示からすべての時間帯を削除します。
［複製 (Duplicate)］をクリックします。	選択した時間帯を週全体にレプリケートします。
［元に戻す (Undo)］をクリックします。	最後の操作を取り消します。

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 つのクライアントが含まれています。



イメージは次のポイントを示しています。

ポイント 1 クライアント 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、クライアント A3 は完了するまで実行されます。スケジュール B のクライアント B1 は、クライアント A3 が完了するとすぐ開始します。

ポイント 2 スケジュール A により、スケジュール B のすべてのクライアント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、クライアント B3 は開始できません。クライアント B3 は、次に NetBackup がスケジュール B を実行するときまで待機する必要があります。

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。

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。

ポリシーの[属性 (Attributes)]タブの[カレンダー (Calendar)]オプションを使用して、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します。[含める日 (Include dates)]タブを使用すると、特定の日付、特定の曜日、月の特定の日に実行されるようスケジュールを設定できます。

メモ: スケジュール一覧を使用しているときに緑の丸が日付に表示されていない場合、その日付はスケジュールに含まれていません。

[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、スケジュールに含まれていない日にジョブが実行される可能性があります。

新しいカレンダーのスケジュールが[実行日後の再試行を許可する (Retries allowed after run day)]で作成されると、バックアップウィンドウが開く次の日に最初のジョブがスケジュールにより実行されます。その日はスケジュールに含まれている最初の実行日の前になることもあります。

カレンダーを使用して実行日をスケジュール設定する方法:

1. [属性 (Attributes)]タブで[カレンダー (Calendar)]オプションを有効にします。
2. [含める日 (Include dates)]タブを選択します。
3. 1 つ以上の方法でジョブが実行される日付をスケジュール設定します。
   - ジョブを実行する日付を 3 カ月分のカレンダー上で選択します。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います。
   - [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含めるように選択するには、マトリックスのボックスを選択します。
     - 毎月特定の曜日を含めるには、その曜日の列ヘッダーをクリックします。
     - 毎月特定の週を含めるには、[1 番目 (1st)]、[2 番目 (2nd)]、[3 番目 (3rd)]、[4 番目 (4th)]、[最後 (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。
     - 毎月特定の日付を選択するには、表にあるその日付のチェックボックスにチェックマークを付けます。
     - 毎月の最終日を含めるには、[最終 (Last)]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。

4 ［追加 (Add)］をクリックして、含まれる日を保存します。

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 1 日以上の曜日を 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を選択します。
  - 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を選択します。
- 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。

PaaS のクラウド資産の構成

[クラウド資産 (Cloud assets)]タブでは、クラウド環境で自動管理データベースを構成できます。

PaaS 資産にスケジュールを追加する複数のコピーのオプションはサポートされていません。

表 1-11 クラウドプロバイダに対するクラウド資産タイプ PaaS

クラウドプロバイダ	DB サービス
アマゾンウェブサービス	Aurora MySQL Aurora PostgreSQL DynamoDB MariaDB MySQL Oracle PostgreSQL Redshift SQL Server Custom SQL Custom Oracle DocumentDB Neptune

クラウドプロバイダ	DB サービス
Microsoft Azure	Cosmos DB for MongoDB Cosmos DB for noSQL MariaDB MySQL PostgreSQL SQL Managed Instance SQL Server
Google Cloud Platform	GCP SQL Server GCP MySQL GCP PostgreSQL GCP BigQuery

ポリシーに資産を追加するには

1. [クラウド資産 (Cloud assets)]タブで、ドロップダウンから[プロバイダ (Provider)]を選択します。
2. [DB サービス (DB service)]ドロップダウンから資産タイプを選択します。
3. [資産の追加 (Add assets)]をクリックします。
4. [資産の追加 (Add assets)]ペインには、手順 2 で選択した資産タイプが表示されます。1 つまたは複数の資産タイプを選択します。

   [資産の追加 (Add assets)]ペインから 1 つまたは複数のインテリジェントグループを追加することもできます。
5. [追加 (Add)]をクリックします。資産タイプが[クラウド資産 (Cloud assets)]タブのリストに追加されます。

資産を削除するには

1. [クラウド資産 (Cloud assets)]タブで、リストから資産タイプを削除できます。
2. 資産タイプにチェックボックスにチェックマークを付け、[削除 (Remove)]をクリックします。[処理 (Actions)]、[削除 (Remove)]から削除オプションを使用することもできます。

IaaS のクラウド資産の構成

[クラウド資産 (Cloud assets)]タブでは、クラウドの仮想マシン、アプリケーション、ボリュームなどの資産を構成できます。クラウド環境で構成するために、既存のインテリジェントグループを選択することもできます。

バックアップのクラウド資産は、クラウドプロバイダによって異なります。次のものが含まれます。

表 1-12　クラウドプロバイダに対するクラウド資産タイプ IaaS

クラウドプロバイダ	バックアップ用のクラウド資産
アマゾンウェブサービス	仮想マシン アプリケーション ボリューム
Google クラウドプロバイダ	仮想マシン アプリケーション ボリューム
Microsoft Azure	仮想マシン アプリケーション ボリューム
Microsoft Azure Stack Hub	仮想マシン アプリケーション ボリューム
Oracle Cloud Infrastructure	仮想マシン Oracle アプリケーション

ポリシーに資産を追加するには

1. [クラウド資産 (Cloud assets)]タブで、ドロップダウンから[プロバイダ (Provider)]を選択します。
2. [バックアップ用の資産 (Assets for backup)]ドロップダウンから資産タイプを選択します。
3. [資産の追加 (Add assets)]をクリックします。
4. [資産の追加 (Add assets)]ペインには、手順 2 で選択した資産タイプ (仮想マシン、アプリケーション、またはボリューム) が表示されます。1 つまたは複数の資産タイプを選択します。

   [資産の追加 (Add asset)]ペインから 1 つ以上の資産またはインテリジェントグループを選択します。
5. [追加 (Add)]をクリックします。資産タイプが[クラウド資産 (Cloud assets)]タブのリストに追加されます。

[削除 (Remove)]オプションを使用して資産を削除できます。

資産を削除するには

1 [クラウド資産 (Cloud assets)]タブで、リストから資産タイプ (仮想マシン、アプリケーション、またはボリューム) を削除できます。

2 資産タイプにチェックボックスにチェックマークを付け、[削除 (Remove)]をクリックします。[処理 (Actions)]、[削除 (Remove)]から削除オプションを使用することもできます。

IaaS のバックアップオプションの構成

[バックアップオプション (Backup options)]タブには、ファイルやフォルダのリカバリ用にバックアップを有効にするための複数のオプションとその他のオプションが含まれています。このタブは IaaS クラウド形式でのみ表示されます。

[バックアップオプション (Backup options)]タブのオプションは、[クラウド資産 (Cloud assets)]タブで選択したクラウドサービスプロバイダによって異なります。

表 1-13 クラウドプロバイダに対するバックアップオプション

クラウドプロバイダ	バックアップオプション
アマゾンウェブサービス	ファイルまたはフォルダの個別リカバリを有効にします。 選択したディスクをバックアップから除外します。
Google Cloud Platform	ファイルまたはフォルダの個別リカバリを有効にします。 地域別スナップショットを有効にします。 選択したディスクをバックアップから除外します。
Microsoft Azure	ファイルまたはフォルダの個別リカバリを有効にします。 スナップショットの宛先リソースグループを指定します。 選択したディスクをバックアップから除外します。
Microsoft Azure Stack Hub	ファイルまたはフォルダの個別リカバリを有効にします。 スナップショットの宛先リソースグループを指定します。 選択したディスクをバックアップから除外します。
Oracle Cloud Infrastructure	ファイルまたはフォルダの個別リカバリを有効にします。

クラウドポリシーの管理

NetBackup Web UI を使用して、クラウドポリシーで複数の操作を実行できます。

表 1-14 クラウドポリシーの操作

操作	説明
編集 (Edit)	ポリシーの名前を除き、すべての属性を編集できます。
ポリシーのコピー (Copy policy)	ポリシーのコピーを作成できます。新しいコピーが編集モードで開きます。
削除 (Delete)	このオプションを使用してポリシーを削除できます。
有効化 (Activate)/無効化 (Deactivate)	ポリシーをアクティブ化または非アクティブ化できます。
手動バックアップ (Manual backup)	ポリシーの手動バックアップを開始できます。手動バックアップは有効なポリシーに対してのみ可能です。

- p.61 の「ポリシーのコピー」を参照してください。
- p.62 の「ポリシーの無効化または削除」を参照してください。
- p.62 の「資産の手動バックアップ」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。

マルウェアのスキャン

NetBackup は、クラウドの作業負荷の種類を使用した、クラウド資産でのマルウェアのスキャンをサポートします。

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のスキャン

このセクションでは、特定のポリシーのクライアントバックアップイメージ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)］の順に選択します。

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
  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
  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
  マルウェアスキャンが有効になっているすべてのサポート対象ポリシーを表示します。

メモ: Nutanix-AHV ポリシーを使用してバックアップを作成した場合、Nutanix-AHV ポリシーは Nutanix-AHV イメージを表示します。

警告: Hypervisor ポリシー形式には、Nutanix AHV イメージと RHV イメージが表示されます。NetBackup は、Nutanix AHV イメージに対してのみマルウェアスキャンをサポートします。

- バックアップ形式
- コピー
  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
  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
  MSDP (PureDisk)、OST (DataDomain)、AdvancedDisk のディスク形式が一覧表示されます。
- 感染状態
  バックアップイメージのマルウェア感染状態の検索は、[マルウェアスキャンで検出された感染 (Infection detected by malware scan)]、[ファイルハッシュの検索 (File Hash Search)]、[感染なし (Not Infected)]、[未スキャン (Not scanned)]、または[すべて (All)]に基づいて行われます。
- [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)]をクリックします。

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、[スキャンの状態 (Scan status)]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。

作業負荷の種類ごとの資産

このセクションでは、クラウド VM 資産でマルウェアをスキャンする手順について説明します。

このセクションでは、VMware、ユニバーサル共有、Kubernetes、Nutanix、およびクラウド VM の資産でマルウェアをスキャンする手順について説明します。

サポート対象の資産でマルウェアをスキャンするには、次の手順を実行します。

1. 左側の[作業負荷 (Workloads)]で、サポートされている作業負荷を選択します。
2. バックアップが完了したリソースを選択します。

   例: VMware、ユニバーサル共有、Kubernetes、Nutanix、およびクラウド VM

   例: クラウド VM

   例: Nutanix AHV
3. [処理 (Actions)]、[マルウェアのスキャン (Scan for malware)]を選択します。
4. [マルウェアスキャン (Malware scan)]ページで、次の操作を行います。
   - [開始日時 (Start date/time)]と[終了日時 (End date/time)]を選択して、スキャンの日付範囲を選択します。
   - [スキャナホストプール (Scanner host pool)]を選択します

- ［現在の感染状態 (Current infection status)］リストから、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)
  - マルウェアスキャンで検出された感染 (Infection detected by malware scan)
  - ファイルハッシュ検索で検出された感染 (Infection detected by file hash search)
  - すべて (All)

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

メモ: マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

6 スキャンが開始されると、［マルウェアの検出 (Malware detection)］に［スキャンの状態 (Scan status)］が表示され、次のフィールドが表示されます。

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

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。

- 処理中 (In progress)
- 保留中 (Pending)

リソースグループを使用した Microsoft Azure リソースの保護

NetBackup では、保護された仮想マシンとボリュームを含むすべてのリソースグループに対して、ピアリソースグループのスナップショットの保存先を定義できます。

Microsoft Azure のすべてのリソースは、1 つのリソースグループに関連付けられます。スナップショットが作成されると、そのスナップショットはリソースグループに関連付けられます。また、各リソースグループは 1 つの地域に関連付けられます。次を参照してください。

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal

Snapshot Manager は、スナップショットを作成して、次の条件に該当する場合でも、リソースが属するリソースグループにスナップショットを配置します。

- リソースグループの接頭辞を指定しない
- ピアリソースグループが作成されていない
- スナップショットの作成を許可している

リソースに関連付けられているリソースグループとは別のリソースグループにスナップショットを配置するように設定できます。ただし、次の重要な点に注意してください。

- ピアリソースグループは、リソースのリソースグループの地域と同じ地域に存在する必要があります。
- ピアリソースグループが見つからない場合、スナップショットの作成が成功したか失敗したかは、構成によって決定されます。

この機能を有効にするには、ピアリソースグループを作成する必要があります。Snapshot Manager はその後、リソースに関連付けられているリソースグループの接頭辞を追加します。スナップショットが作成されると、リソースが関連付けられているリソースグループの接頭辞とリソースグループに基づいてピアリソースグループ名が生成されます。

メモ: 保護計画の作成時に、既存のピアリソースグループにスナップショットを直接関連付けられるようになりました。ただし、このセクションで説明する接頭辞を指定してピアリソースグループを定義する機能はまだ存在します。

保護計画の作成手順について詳しくは、『NetBackup Web UI 管理者ガイド』で完全な手順を参照してください。

開始する前に

- ピアリソースグループは、リソースグループを使用して保護されているリソースで利用可能である必要があります。
- 接頭辞が指定されている場合、プラグイン構成の地域は別の構成と重複しないようにする必要があります。

制限事項および考慮事項

- リソースグループ名には英数字、ピリオド、アンダースコア、ハイフン、または丸カッコのみを指定できます。
- 接頭辞の長さは 89 文字未満にする必要があります。

- Azure 構成では、リソースグループの命名規則で許可されていない文字は使用できません。

リソースグループの構成と結果について

次の表に、仮想マシンとリソースグループの設定シナリオ、リソースの構成、結果の一覧を示します。

表 1-15 構成と結果

リソースグループの接頭辞 (Resource Group prefix)	[接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックス	結果
指定されていない	選択しない	NetBackup は、リソースのリソースグループに新しく作成されたスナップショットを関連付けます。
指定	選択しない	次の条件を満たしている場合、NetBackup は新しいスナップショットを作成し、そのスナップショットをピアリソースグループに関連付けます。 ■ ピアリソースグループが作成されます。 ■ ピアリソースグループは、リソースグループと同じ地域に存在する必要があります。 条件を満たしていないと、スナップショットジョブは失敗します。

リソースグループの接頭辞 (Resource Group prefix)	[接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックス	結果
指定	選択済み	次の条件を満たしている場合、NetBackup は新しいスナップショットを作成し、そのスナップショットをピアリソースグループに関連付けます。 ■ ピアリソースグループが作成されます。 ■ ピアリソースグループは、リソースグループと同じ地域に存在する必要があります。 ピアリソースグループが作成されていない、または別の地域に存在する場合、新しく作成されたスナップショットは、保護されているリソースのリソースグループに関連付けられます。

リソースグループの構成の例

次の表に、リソースグループの構成の例を示します。

表 1-16　構成例

条件	構成	結果
■ OS とすべてのディスクが、同じリソースグループに存在する。 ■ ピアリソースグループには正しく名前が付けられている。 ■ ピアリソースは、リソースのリソースグループと同じ地域に配置されている。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いている。	スナップショットはピアリソースグループで作成されます。

条件	構成	結果
■ OS とすべてのディスクが、個別のリソースグループに存在する。 ■ ピアリソースグループには正しく名前が付けられている。 ■ ピアリソースは、リソースのリソースグループと同じ地域に配置されている。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いている。	スナップショットはピアリソースグループで作成されます。
■ OS とすべてのディスクが、同じリソースグループに存在する。 ■ ピアリソースグループは、リソースのリソースグループとは異なる地域に作成されている。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いている。	スナップショットはピアリソースグループではなく、元のリソースグループで作成されます。
■ OS とすべてのディスクが、同じリソースグループに存在する。 ■ ピアリソースグループが作成されていない。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いている。	スナップショットはピアリソースグループではなく、元のリソースグループで作成されます。
■ OS とすべてのディスクが、個別のリソースグループ RG1 と RG2 に存在する。 ■ ピアリソースグループ RG1 は、リソースと同じ地域に配置されている。 ■ ピアリソースグループ RG2 が作成されていない。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いている。	スナップショットは、RG1 のピアリソースグループと元のリソースグループ RG2 で作成されます。

条件	構成	結果
■ OS とすべてのディスクが、同じリソースグループに存在する。 ■ ピアリソースグループには正しく名前が付けられている。 ■ ピアリソースグループは、リソースのリソースグループとは異なる地域に配置されている。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いていない。	スナップショットは作成されず、ジョブは失敗します。
■ OS とすべてのディスクが、同じリソースグループに存在する。 ■ ピアリソースグループが作成されていない。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いていない。	スナップショットは作成されず、ジョブは失敗します。
■ OS とすべてのディスクが、個別のリソースグループ RG1 と RG2 に存在する。 ■ RG1 と RG2 のピアリソースグループ、snapRG1 と snapRG2 が異なる地域に存在する。 ■ ピアリソースグループ snapRG1 が、リソースグループ RG1 と同じ地域に配置されている。 ■ ピアリソースグループ snapRG2 が、リソースグループ RG2 と異なる地域に配置されている。	■ リソースグループの接頭辞の値が指定されている。 ■ [接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)]チェックボックスにチェックマークが付いていない。	スナップショットは作成されず、ジョブは失敗します。

リソースグループの権限のトラブルシューティング

リソースグループに適切な権限が割り当てられていない場合、リソースグループに関連付けられている Azure リソースのスナップショットの作成が失敗します。

回避方法:

この問題を解決するには、次の手順を実行します。

1. https://portal.azure.com/#blade/HubsExtension/BrowseResourceGroups に移動します。
2. スナップショットで使用するリソースグループをクリックします。
3. [Access control (IAM)]をクリックします。
4. [Add Role Assignment]をクリックします。
5. [Role]として[Owner]、[Assign Access to]に[User]を選択し、Application (API 呼び出しのため、Snapshot Manager 用に作成) を選択します。
6. 保存し、再度バックアップを試行します。

クラウド作業負荷のための NetBackup アクセラレータ

NetBackup アクセラレータはクラウドのバックアップにかかるバックアップ時間を減らします。NetBackup は、仮想マシン内で行われた変更を識別するために参照スナップショットを使用します。変更されたデータブロックだけが、I/O およびバックアップ時間を大幅に減らすために NetBackup メディアサーバーに送信されます。メディアサーバーは以前のバックアップデータと新しいデータを組み合わせ、完全な仮想マシンファイルが含まれている NetBackup の従来の完全なイメージを生成します。

NetBackup は、AWS、Azure、および Azure Stack Hub の作業負荷のためのアクセラレータバックアップをサポートします。

メモ: アクセラレータは、変更頻度が高くない仮想マシンデータに使うのが最適です。

アクセラレータには次の利点があります。

- 従来のバックアップより完全バックアップを速く実行できます。バックアップホストとサーバーの間に、コンパクトなバックアップストリームを作成するので、ネットワーク回線容量が少なくてすみます。アクセラレータはバックアップのために変更されたデータブロックだけを送信します。その後、NetBackup は変更されたブロックデータが含まれている NetBackup の完全な従来のイメージを生成します。
- アクセラレータバックアップは Granular Recovery Technology (GRT) をサポートします。
- Snapshot Manager の I/O を減らします。
- Snapshot Manager の CPU 負荷を減らします。

NetBackup アクセラレータが仮想マシンと連携する仕組み

Azure と Azure Stack Hub のバックアップの場合、アクセラレータは、アクセラレータがサポートするストレージ形式 (MSDP、OpenStorage、CloudStorage、MSDP-C (Azure および AWS) など) を選択すると有効になります。

NetBackup アクセラレータは、各仮想マシンの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。

- 仮想マシンに以前のバックアップがない場合、NetBackup は完全バックアップを実行します。
- 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を識別します。変更されたブロックとヘッダー情報のみが、完全 VM バックアップを作成するためにバックアップに含まれます。変更されたブロックは、前回の参照スナップショットと現在のスナップショットを比較して識別されます。保護計画で[バックアップのみを保持 (Keep backup only)]または[スナップショットの有効期限が近いときにのみバックアップを開始 (Initiate backup only when the snapshot is about to expire)]オプションを選択すると、スナップショットは、次回のバックアップが完了するまでアクセラレータ用に保持されます。
- バックアップホストは、仮想マシン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) で構成される tar のバックアップ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仮想マシンにより変更されたブロック、バックアップ ID および変更されていないブロックのデータエクステントに関する情報を読み込みます。メディアサーバーは、読み込んだバックアップ ID とデータエクステントから、既存のバックアップにあるその他仮想マシン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を次のもので構成される新しく完全なイメージを生成するために指示します。それは、新しく変更されたブロックとストレージサーバーに存在する既存の変更されていないブロックです。ストレージサーバーは既存のブロックに書き込むのではなく、イメージにリンクすることがあります。
- Microsoft Azure は、200 を超える後続の増分スナップショットを許可しません。保護計画で[バックアップとともにスナップショットを保持 (Keep snapshot along with backup)]オプションを選択し、200 を超える増分スナップショットが作成されるようにスナップショットの保持期間を指定すると、アクセラレータの代わりに完全バックアップが実行されます。アクセラレータのメリットを得るため、スナップショットの保持期間を適正に保つことをお勧めします。
- 2 回のアクセラレータバックアップの間で VM に新しいディスクが追加されるなどにより、VM の構成が変更された場合は、そのディスクの完全バックアップが実行され、既存のディスクに対してはアクセラレータバックアップが実行されます。

仮想マシンのアクセラレータ強制再スキャン (スケジュールの属性)

アクセラレータ強制再スキャンは、ForcedRescan コマンドを手動で実行することで発生するバックアップイメージの破損の問題を防ぐのに役立ちます。[アクセラレータ強制再スキャン (Accelerator forced rescan)]を使用すると、仮想マシンのすべてのデータがバックアップされます。このバックアップは、ポリシーの最初のアクセラレータバックアップに似ています。したがって、強制再スキャンジョブの場合、アクセラレータの最適化の割合は 0 です。バックアップの所要時間は、アクセラレータを使わない場合の完全バックアップの所要時間とほぼ同様です。

強制再スキャンによって安全性が強化され、次回のアクセラレータバックアップの基準が確立されます。また、ステージング領域内のデータのチェックサム検証の失敗など、潜在的な損害から保護されます。

強制再スキャンを使用する場合の推奨事項:

- オフになっている VM の強制再スキャンをトリガしないでください。
- ストレージの場所のメモリが一杯になると、UI に通知が表示されます。ストレージの場所で十分なメモリを利用できる場合にのみ、強制再スキャンを開始します。

NetBackup は、保護対象の VM ごとに「ForcedRescan」という名前のスケジュールを作成します。手動で強制再スキャンを実行してバックアップをトリガするには、コマンドプロンプトまたは Linux 端末で次のコマンドを実行します。

```
bpbackup -i -p <policy_name> -s ForcedRescan
```

例: `bpbackup -i -p msdp_10mins_FRS+5d990ab5-f791-474f-885a-ae0c30f31c98 -s ForcedRescan`

ポリシー名は、関連する保護計画から Web UI を介して取得できます。

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。

バックアップジョブ詳細ログのアクセラレータメッセージ

仮想マシンを最初にバックアップするときは、そのバックアップにアクセラレータは使用されません。[ジョブの詳細 (Job Details)]ログには次のメッセージが表示されます。

```
Jul 21, 2021 1:55:52 PM - Info bpbrm (pid=78332) accelerator enabled
Jul 21, 2021 1:55:53 PM - Info bpbrm (pid=78332) There is no
complete backup image match with track journal, a regular full
```

```
backup will be performed.

..

Jul 21, 2021 1:56:11 PM - Info bpbkar (pid=1301) accelerator sent
402666496 bytes out of 402664960 bytes to server, optimization 0.0%
```

それ以降の仮想マシンのバックアップでアクセラレータを使う場合は、次のメッセージがジョブ詳細のログに表示されます。

```
Jul 21, 2021 2:01:33 PM - Info bpbrm (pid=79788) accelerator enabled

..

Jul 21, 2021 2:02:00 PM - Info bpbkar (pid=1350) accelerator
sent 1196032 bytes out of 402664960 bytes to server, optimization
99.7%
```

このメッセージはアクセラレータの主要トレースです。この例では、アクセラレータはバックアップデータの 99.7 % 削減に成功しました。

保護計画を使用したクラウド作業負荷のバックアップスケジュールの構成

Azure、Azure Stack Hub、AWS、OCI、GCP のクラウド作業負荷の保護計画を作成する際、[バックアップスケジュールの追加 (Add backup schedule)]ダイアログの[属性 (Attributes)]タブでバックアップスケジュールを追加できます。

保護計画の作成方法について詳しくは、『NetBackup Web UI 管理者ガイド』の「保護計画の管理」のセクションを参照してください。

クラウド作業負荷にバックアップスケジュールを追加するには

1. 左側で[保護 (Protection)]、[保護計画 (Protection plans)]、[追加 (Add)]の順にクリックします。
2. [基本プロパティ (Basic properties)]で、[名前 (Name)]と[説明 (Description)]を入力し、[作業負荷 (Workload)]ドロップダウンリストから[クラウド (Cloud)]を選択します。
3. ドロップダウンリストからクラウドプロバイダを選択し、[次へ (Next)]をクリックします。[スケジュール (Schedules)]で、[スケジュールの追加 (Add schedule)]をクリックします。

   [バックアップスケジュールの追加 (Add backup schedule)]タブで、バックアップとスナップショットを保持するためのオプションを構成できます。

4 (Azure SQL Server、GCP SQL Server、SQL Managed Instance PaaS 資産の場合のみ。) 保護計画に対して[PaaS 資産のみを保護 (Protect PaaS assets only)]を選択した場合、[バックアップ形式 (Backup type)]に[増分バックアップ (Incremental backup)]または[完全 (Full)]を選択します。増分バックアップ形式の場合、NetBackup で最初の完全バックアップが実行された後で実行されるすべてのバックアップでは、データベース内の増分の変更のみがキャプチャされます。この機能により、バックアップパフォーマンスが大幅に向上します。スキーマが変更された場合、増分バックアップから完全バックアップに戻り、アクティビティモニターにこのアクティビティが通知されます。

ポリシーで、増分バックアップより長い保持期間を完全バックアップに割り当ててください。完全なリストアを行うには、前回の完全バックアップ、およびそれ以降のすべての差分増分バックアップが必要です。増分バックアップの前に完全バックアップの期限が切れると、すべてのファイルをリストアできない場合があります。p.122 の「PaaS 作業負荷の増分バックアップについて」を参照してください。

5 [反復 (Recurrence)]ドロップダウンから、バックアップの頻度を指定します。

6 [スナップショットとバックアップのオプション (Snapshot and backup options)]で、次の操作のいずれかを実行します。

- スナップショットとバックアップの両方を保持するには、[バックアップとともにスナップショットを保持 (Keep snapshot along with backup)]オプションを選択します。[スナップショットの保持期間 (Keep snapshot for)]と[バックアップの保持期間 (Keep backup for)]ドロップダウンを使用して、スナップショットとバックアップの両方の保持期間を指定します。[バックアップ形式 (Backup type)]ドロップダウンから[完全 (Full)]を選択します。保持されたスナップショットが期限切れになる直前にバックアップジョブを開始するには、[スナップショットの有効期限が近いときにのみバックアップを開始 (Initiate backup only when the snapshot is about to expire)]オプションを選択します。
(Amazon RDS Oracle 資産の場合のみ) 保護計画の[PaaS 資産のみを保護 (Protect PaaS assets only)]オプションを選択した場合は、バックアップ形式を[完全 (Full)]、[差分増分 (Differential incremental)]、または[アーカイブ REDO ログ (Archived REDO Log)]として選択できます。
増分とアーカイブ REDO ログのバックアップ形式の場合、NetBackup は、最初の完全バックアップを実行し、その後増分とアーカイブで実行されるすべてのバックアップでは、データベース内の変更がキャプチャされます。この機能により、バックアップパフォーマンスが大幅に向上します。
増分スケジュールを持つ複数の保護計画は使用しないでください。また、アーカイブログスケジュールの間隔が 24 時間を超える保護計画は使用しないでください。リストアを正常に行うには、NetBackup では前回の完全バックアップ、それ以降のすべての増分バックアップおよびそれ以降のすべてのアーカイブバックアップが必要です。増分バックアップまたはアーカイブバックアップの前に完全バックアップの期限が切れると、すべてのファイルをリストアできない場合があります。

- スナップショットのみを保持するには、[スナップショットのみを保持 (Keep snapshot only)]オプションを選択します。[スナップショットの保持期間 (Keep snapshot for)]ドロップダウンを使用して、スナップショットの保持期間を指定します。
  - (オプション) Amazon AWS としてプロバイダを選択し、上記の 2 つのオプションのいずれかを選択してスナップショットの保持を選択した場合、この時点でスナップショットのレプリケーションを構成できます。クラウドスナップショットのレプリケーションについて詳しくは、p.81 の「AWS スナップショットレプリケーションの構成」を参照してください。
  - [スナップショットレプリケーションを有効にする (Enable Snapshot replication)]を選択します。
  - 表内で、レプリケートするスナップショットについて[地域 (Region)]、[AWS アカウント (AWS Account)]、[保持期間 (Retention period)]の順に選択します。

    メモ: 構成したレプリケーションコピーの数が、[スケジュール (Schedules)]タブの [スケジュールと保持 (Schedules and retention)]表にある[スナップショットレプリカ (Snapshot replicas)]列に表示されます。

- バックアップのみを保持するには、[バックアップのみを保持 (Keep backup only)]オプションを選択します。バックアップの直後にスナップショットが期限切れになります。[バックアップの保持期間 (Keep backup for)]ドロップダウンを使用して、バックアップの保持期間を指定します。[バックアップ形式 (Backup type)]ドロップダウンから[完全 (Full)]を選択します。

7 『NetBackup Web UI 管理者ガイド』の「保護計画の管理」のセクションにある説明に従って、[開始時間帯 (Start window)]タブでスケジュールの作成を続行します。

さまざまなバックアップオプションでの個別リカバリの可用性

ファイルまたはフォルダオプションの個別リカバリの可用性は、作業負荷に対して選択するさまざまなバックアップオプションによって異なります。

- [バックアップとともにスナップショットを保持 (Keep snapshot with backup)]オプションを選択すると、個別リカバリを利用できます。
- [スナップショットのみを保持 (Keep snapshot only)]オプションを選択すると、個別リカバリを利用できます。
- [バックアップのみを保持 (Keep backup only)]オプションを選択すると、個別リカバリを利用できます。

バックアップジョブとスナップショットジョブの間のインデックス付け処理

- NetBackup は、スナップショットジョブからのバックアップ中に、スナップショットからの VxMS (Veritas Mapping Service) ベースのインデックス付け処理、およびインラインインデックス処理を実行します。ファイルのインデックス付け処理は、Snapshot Manager の地域および場所とは関係なく行えます。VxMS ベースのインデックス付けは現在、GCP、AWS、Azure、OCI、Azure Stack Hub クラウドでサポートされています。
- インデックス付け処理は、実際のバックアップジョブまたはスナップショットジョブ中に実行されますが、[ファイルまたはフォルダの個別リカバリの有効化 (Enable granular recovery for files or folders)]オプションを使用すると、個々のファイルやフォルダのリカバリをスナップショットおよびバックアップコピーからのみ実行できます。
- VM 資産のスナップショットが作成されると、各資産の「スナップショットからのインデックス」ジョブがトリガされます。インデックス付けジョブの詳細は、アクティビティモニターで確認できます。
- VxMS のデバッグログとクラウドコネクタのデバッグログは、Snapshot Manager の */cloudpoint/openv/dm/datamover.<datamover-id>/netbackup/logs* フォルダにあります。
- `/etc/fstab`と同じマウントパスを使用してファイルとフォルダにインデックス付けするには、Linux サーバーの `/etc/fstab` ファイルにデバイスパスではなく UUID ファイルシステムに基づくエントリが必要です。デバイスパスは、Linux がシステムブート中にデバイスを検出する順序によって変わる場合があります。

メモ: VM が接続状態ではない場合、VM のバックアップは続行し、バックアップジョブは部分的に成功とマークされます。この場合、VM が接続されていないとインデックス処理を利用できないので、個々のファイルまたはフォルダをリストアできません。

クラウド作業負荷のバックアップオプション

メモ: 接続された VM の場合、ファイルシステム整合スナップショットが試行されます。接続された VM が後で停止した場合、アプリケーションはエラー状態になり、ファイルシステム整合スナップショットの代わりにクラッシュ整合スナップショットが作成されます。ジョブモニターおよびログを参照して、作成されたスナップショットがクラッシュ整合スナップショットであるかファイルシステム整合スナップショットであるかを確認できます。

GCP の地域別スナップショット

保護計画の作成中に、GCP 作業負荷の地域別スナップショットを有効にできます。

地域別スナップショットオプションが有効になっている場合、資産が存在するのと同じ地域にスナップショットが作成されます。それ以外の場合、スナップショットは複数の地域の場所に作成されます。

Azure および Azure Stack Hub のスナップショットの宛先リソースグループ

Azure または Azure Stack Hub の保護計画の作成時に、スナップショットの宛先ピアリソースグループを指定できます。接頭辞を指定してピアリソースグループを定義する以前の機能はまだ存在しますが、保護計画の作成時に既存のピアリソースグループにスナップショットを直接関連付けられるようになりました。

保護計画の作成時に、クラウドプロバイダに Microsoft Azure または Azure Stack Hub を選択した場合は、[スナップショットの宛先リソースグループを指定する (Specify snapshot destination resource group)]を選択して、資産が存在するのと同じ地域内の特定のピアリソースグループにスナップショットを関連付けることができます。次に、スナップショットの宛先の構成、サブスクリプション、リソースグループを選択します。

スナップショットは、次の優先順位で、宛先リソースグループの 1 つに保存されます。

- 保護計画で指定された宛先リソースグループ
- プラグインの構成で指定されている、接頭辞が付いたリソースグループ (Azure のみ)
- 資産が存在するリソースグループ (宛先リソースグループまたは接頭辞が付いたリソースグループが NetBackup で指定されていない場合)

選択したディスクのバックアップからの除外

GCP を含むすべてのサポート対象クラウドベンダーに適用されるバックアップとスナップショットから一部のディスクを除外するように保護計画を構成できます。これにより、バックアップする必要がない冗長なディスクイメージが作成されないようにし、処理するデータ量を減らすことでバックアップを高速化できます。

AWS、Azure、Azure Stack Hub、または GCP クラウドの保護計画を作成する場合、[選択したディスクをバックアップから除外 (Exclude selected disks from backups)]オプションを選択して、バックアップイメージに含めないディスクを指定できます。除外する対象には、すべての非ブートディスクか、対応するクラウドプロバイダアカウントで、特定のタグが関連付けられているディスクを選択できます。

メモ: ディスク除外オプションが有効になっている保護計画は、クラウド VM タイプの資産と VM インテリジェントグループにのみ適用できます。

その後、[リカバリポイント (Recovery Points)]タブから VM をリストアする際に、[ディスクのインクルード (Includes disks)]列を参照して、バックアップイメージに含める、または除外するディスクのリストを表示できます。

手順について詳しくは、『NetBackup Web UI 管理者ガイド』で、保護計画の作成に関する情報を参照してください。

注意:

- LVM の場合、一部のディスクを除外すると、システムが正常にブートしないことがあります。
- サポートされていないファイルシステムがディスクに構成されている場合に、そのディスクをスナップショットから除外するとします。サポートされていないファイルシステムを含むディスクは除外されるため、スナップショットは引き続きクラッシュ整合スナップショットとなります。
- ディスクを除外するには、/etc/fstab ファイルにスナップショットを作成する前に、データディスクに nofail フラグを付ける必要があります。これが必要なのは、(ボリュームを別のインスタンスに移動した後など) このボリュームが接続されていないインスタンスを再ブートする場合です。nofail マウントオプションを使用すると、ボリュームのマウント時にエラーが発生してもインスタンスをブートできます。詳しくは、/etc/fstab ファイル内の次のエントリ例を参照してください。
  例: UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2
- クラウドプロバイダからタグへの変更が行われた場合は、資産が正しく検出されていることを確認してください。資産に対してポリシーの実行がスケジュールされると、検出されたデータのみに従ってディスクが除外されます。スナップショットの作成中にタグを接続した場合、NetBackup はそのタグを除外の対象として考慮しません。検出が完了すると、次の保護サイクル時に考慮されます。
- 英語以外のロケールの OS では、保護計画でタグベースの除外を選択した場合、ディスクタグに英語以外の文字が含まれていても、ディスクの除外は想定どおりに機能します。ただし、ディスクの除外が正しく考慮されるため、機能への影響はありませんが、英語以外の文字のタグは job(try) ログと監査ログに正しくキャプチャされない場合があります。

AWS スナップショットレプリケーション

スナップショットのレプリケートとは、スナップショットのコピーを別の場所に保存することを意味します。AWS では、別の場所に次のいずれかを指定できます。

- 同じアカウント内の異なる地域。
- 別のアカウント内の同じ地域。
- 別のアカウント内の異なる地域。

たとえば、AWS クラウド管理者が資産を地域 X に所有しているとします。これらの資産のスナップショットも地域 X に格納されます。ただし、保護レベルを高めるために、スナップショットを同じアカウント内の地域 Y にレプリケートしたり、別のアカウント内の地域 X または Y にレプリケートしたりすることもできます。NBU Snapshot Manager の用語では、元の場所 (X) がレプリケーションソース、スナップショットがレプリケートされる場所 (Y) がレプリケーション先となります。

レプリケーションは 3 つの手順で実行されます。このメカニズムは内部で処理されるため、プロセス全体がユーザーに対して完全に透過的です。

- スナップショットを共有します (クロスアカウントにレプリケートする場合のみ)。詳しくは、AWS のマニュアルの「スナップショットの共有」セクションを参照してください。
- スナップショットをコピーします。詳しくは、AWS のマニュアルの「CopySnapshot」セクションを参照してください。
- スナップショットの共有を解除します (クロスアカウントにレプリケートする場合のみ)。

AWS スナップショットレプリケーションの構成

スナップショットをレプリケートするための要件

- 暗号化されていないスナップショットのレプリケート
  ソースとターゲットのアカウントまたはリージョンが、NetBackup Snapshot Manager の AWS クラウドプロバイダを使用して構成されていることを確認します。暗号化されていないスナップショットのレプリケートには、追加の要件はありません。
- AWS KMS を使用した、暗号化されていないスナップショットのレプリケート
  ソースとターゲットのアカウントまたはリージョンが、NetBackup Snapshot Manager の AWS クラウドプロバイダを使用して構成されていることを確認します。
  さらに、暗号化されたスナップショットをクロスアカウントにレプリケートするには、元の場所の暗号化 CMK キーをターゲットアカウントと共有する必要があります (この共有 KMS キーは、ターゲットアカウントでスナップショットをコピーするときに暗黙的に使用され、コピーされたスナップショットは別のキーによってレプリケートできます)。
  ソースとターゲットの両方の場所に同じ名前の暗号化キー (KMS キー) が必要です。つまり、(AWS の観点から) 同じキーエイリアスが必要です。
  同じ名前の暗号化キーがターゲットにない場合、レプリケートされたスナップショットはターゲットの場所のデフォルトの KMS キーを使用して暗号化されます。
- クロスアカウントレプリケーションの権限
  異なる AWS アカウントで異なる領域にレプリケーションを実行する場合は、ターゲット AWS アカウントで (保護対象の VM が存在する) ソース領域を有効にする必要があります。
  クロスアカウントレプリケーションの場合、スナップショットソース領域の AWS アカウント (ソース AWS アカウント) に関連付けられている AWS IAM ユーザーまたはロールには、次の権限が必要です。
  - EC2 インスタンスに対する `ModifySnapshotAttribute` および `CopySnapshot`。
  - 元のスナップショットの暗号化に使用された KMS キーに対する `DescribeKey` および `ReEncrypt`。

クロスアカウントレプリケーションの場合、スナップショットレプリケーションターゲット領域の AWS アカウント (ターゲット AWS アカウント) に関連付けられている AWS IAM ユーザーまたはロールには、次の権限が必要です。

- 元のスナップショットの暗号化に使用された KMS キーに対する `CreateGrant`、`DescribeKey`、および `Decrypt`。
- 元のスナップショットの `CopySnapshot` 操作の実行中に使用された KMS 暗号化キーに対する `CreateGrant`、`Encrypt`、`Decrypt`、`DescribeKey`、`GenerateDataKeyWithoutPlainText`。

AWS クラウド資産のスナップショットをプライマリの場所からリモートやセカンダリの場所にレプリケートできます。Snapshot Manager は、領域間およびアカウント間のレプリケーションをサポートしています。スナップショットレプリケーションを使用すると、次を実現できます。

- 長期保持および監査要件のため、異なる宛先でクラウド資産のコピーを維持する
- 領域の停止が発生した場合、別の領域からレプリケートされたコピーからクラウド資産をリカバリする
- ユーザーアカウントが危殆化された場合、別のアカウントからレプリケートされたコピーからクラウド資産をリカバリする

構成

スナップショットレプリケーションを構成するには、次の情報を確認します。

- スナップショットレプリケーションは保護計画の作成時に構成できます。『NetBackup™ Web UI バックアップ管理者ガイド』を参照してください。
- クロスアカウントレプリケーションでは、ソースアカウントとターゲットアカウント間で信頼関係を確立する必要があります。詳しくは、アマゾンウェブサービスのマニュアルで、AWS アカウント間の IAM ロールの使用に関連する情報を参照してください。

注意事項

クラウドスナップショットレプリケーションを構成する場合は、次の点を考慮します。

- 複数のスケジュールを構成しても、構成済みの宛先領域のレプリケーションがすべてのスケジュールに適用されます。
- クラウドスナップショットレプリケーションは Amazon クラウドプロバイダでのみサポートされています。

資産の保護条件

クラウドスナップショットレプリケーションのために構成されている保護計画にクラウド資産を追加する前に、次の点を考慮します。

- 異なる領域にスナップショットをレプリケートする保護計画に、資産を追加する必要があります。

たとえば、領域「aws_account_1-us-east-1」に属する資産は、同じ領域「aws_account_1-us-east-1」にレプリケートする保護計画にサブスクライブできません。

- 資産は同じ領域内の別のアカウントにレプリケートできます。
  たとえば、領域「aws_account_1-us-east-1」に属する資産は、同じ領域にある別のアカウント「aws_account_2-us-east-1」にレプリケートする保護計画にサブスクライブできます。
- Snapshot Manager で検出された資産は、同じ Snapshot Manager で検出された領域にレプリケートする必要があります。
  たとえば、Snapshot Manager「CP1」で検出された資産は、Snapshot Manager「CP2」によって検出された領域にレプリケートする保護計画にはサブスクライブできません。
- クラウドスナップショットレプリケーション用に構成された保護計画にサブスクライブできるのは、Amazon 資産のみです。

同時スナップショットレプリケーションの管理

パフォーマンスを向上させるため、同時スナップショットレプリケーションの数を調整できます。Amazon 社では、単一宛先領域に対する同時スナップショットレプリケーションの実行について、資産タイプごとに異なる制限があります。たとえば、RDS は 5、EBS は 5、EC2 は 50 に制限されています。詳しくは、アマゾンウェブサービスのマニュアルで、スナップショットのコピーに関連する情報を参照してください。

NetBackup では、この制限は `bp.conf` ファイルの次のパラメータを使用して定義されます。

```
MAX_CLOUD_SNAPSHOT_REPLICATION_JOBS_PER_DESTINATION
```

デフォルト値は 5 です。

AWS スナップショットレプリケーションの使用

このセクションでは、AWS スナップショットレプリケーション機能を使用してスナップショットのレプリカを作成し、必要に応じてレプリケートされたスナップショットをリストアする方法について説明します。これらの手順について詳しくは、『NetBackup Snapshot Manager インストールおよびアップグレードガイド』と『NetBackup Web UI 管理者ガイド』の該当箇所を参照してください。

スナップショットレプリケーションの作成

このセクションでは、ターゲット領域でスナップショットレプリカを作成するためにソース領域を構成する方法について説明します。

レプリカを作成するには

1 Web UI に Snapshot Manager (CP1) を追加します。

p.15 の「Snapshot Manager の追加」を参照してください。

2 レプリケーションのソース領域とターゲット領域に AWS プラグインを追加します。

3 保護計画を作成し、[領域 (Region)]と[アカウント (Account)]を選択します。

p.75 の「保護計画を使用したクラウド作業負荷のバックアップスケジュールの構成」を参照してください。

4 OnHost エージェントを使用して、アプリケーションの整合性ゲスト VM に接続して設定します。

5 スナップショットベースのバックアップを開始し、保護計画を使用してスナップショットをレプリケートします。

6 スナップショットとレプリカコピーのリカバリポイントを確認します。

ターゲット領域でのスナップショットレプリカからのリストア

ソース領域で障害が発生した場合は、スナップショットレプリカを作成したターゲット領域から、この領域に属する VM をリストアできます。ソース領域が停止しているため、まずはターゲット領域で VM をリストアする必要があります。

メモ: フェイルオーバーした領域で代替の Snapshot Manager によって検出されたレプリカから、単一のファイルまたはフォルダはリストアできません。

ターゲット領域でのリストア

1 ソース領域で、サーバー CP1 を Web UI から無効にします。

p.23 の「Snapshot Manager の有効化または無効化」を参照してください。

2 ターゲット領域で、新しい Snapshot Manager (CP2) を Web UI から登録します。

3 ターゲット領域とアカウントにのみ AWS プラグインを追加します。検出の完了を待ちます。

4 VM をリストアするには、次の手順を実行します。

- NetBackup Web UI にサインインします。
- 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。[仮想マシン (Virtual machines)]タブで、リカバリするコンピュータをクリックします。
- [リカバリポイント (Recovery points)]タブをクリックします。イメージの一覧で、必要な[レプリカ (Replica)]イメージの前にある[リストア (Restore)]をクリックし、[仮想マシンのリストア (Restore virtual machine)]をクリックします
- VM の表示名を変更するには、新しい名前を入力します。

- サブネット (VPC があるサブネットパス) を選択します。
  p.137 の「クラウド資産のリカバリ」を参照してください。

5 リモートアクセスを有効にするため、リストアされた VM に適切なセキュリティグループを追加します。

6 リストアされた VM から Snapshot Manager エージェントをアンインストールして再インストールし、新しい CP2 サーバーに Snapshot Manager エージェントを登録します。

7 AWS プロバイダコンソールから詳細検出を実行します。

8 リストアされた VM を保護するための新しい保護計画を作成します。スナップショットベースのバックアップを開始します。

ターゲット領域からソース領域へのリストア

ソース領域がオンラインに戻ったら、ターゲット領域からソース領域に VM をリストアできます。

ソース領域へのリストア

1 CP2 の AWS プラグインを編集し、ソース領域を追加します。

2 ソース領域にスナップショットレプリカを作成するための新しい保護計画を作成します。

3 スナップショットベースのバックアップを開始して、レプリケートします。

4 Web UI で CP2 サーバーを無効にします。p.23 の「Snapshot Manager の有効化または無効化」を参照してください。

5 CP1 サーバーを有効にして、AWS プロバイダコンソールから詳細検出を開始します。

6 ターゲット領域から VM の完全リストアを実行します。

7 リストアされた VM へのリモートアクセスを有効にするため、適切なセキュリティグループを追加します。

8 リストアされた VM から Snapshot Manager エージェントをアンインストールして再インストールします。次に、Snapshot Manager エージェントを CP1 サーバーに登録します。

9 AWS コンソールから詳細検出を実行します。

10 既存の保護計画を使用して、新しくリストアされた VM を保護します。

アカウントのレプリケーションのサポートマトリックス

表 1-17 同じアカウントのレプリケーションのサポートマトリックス

資産タイプ	ソース資産 (地域 X)	ソーススナップショット (地域 X)	レプリケートされたスナップショット (地域 Y)
EBS ボリューム、EC2 インスタンス、RDS/Aurora	非暗号化	非暗号化	非暗号化
	デフォルトの AWS KMS キーを使用して暗号化された接続済みディスク。	デフォルトの AWS KMS キーを使用して暗号化された接続済みディスク。	デフォルトの AWS KMS キーを使用して暗号化された接続済みディスク。
	AWS KMS CMK キー (とエイリアス ABC) を使用して暗号化。	AWS KMS CMK キー (エイリアス ABC) を使用して暗号化。	名前付きの AWS KMS CMK キー (エイリアス ABC) が存在する場合はそのキーを使用して暗号化、それ以外の場合はデフォルトの AWS KMS キーを使用して暗号化。

表 1-18 同じ地域内にある異なるアカウントのレプリケーションのサポートマトリックス

資産タイプ	ソース資産 (アカウント A、地域 X)	ソーススナップショット (アカウント A、地域 X)	レプリケートされたスナップショット (アカウント B、地域 Y)
EBS ボリューム、EC2 インスタンス、RDS/Aurora	非暗号化	非暗号化	非暗号化
	デフォルトの AWS KMS キーを使用して暗号化。	デフォルトの AWS KMS キーを使用して暗号化。	サポートされない
	AWS KMS CMK キー (とエイリアス ABC) を使用して暗号化。	AWS KMS CMK キー (とエイリアス ABC) を使用して暗号化。	名前付きの AWS KMS CMK キー (とエイリアス ABC) が存在する場合はそのキーを使用して暗号化、それ以外の場合はデフォルトの AWS KMS キーを使用して暗号化。

表 1-19　異なる地域内にある異なるアカウントのレプリケーションのサポートマトリックス

資産タイプ	ソース資産 (アカウント A、地域 X)	ソーススナップショット (アカウント A、地域 X)	レプリケートされたスナップショット (アカウント B、地域 Y)
EBS ボリューム、EC2 インスタンス	非暗号化	非暗号化	非暗号化
	デフォルトの AWS KMS キーを使用して暗号化。	デフォルトの AWS KMS キーを使用して暗号化。	サポートされない
	AWS KMS CMK キー (とエイリアス ABC) を使用して暗号化。	AWS KMS CMK キー (とエイリアス ABC) を使用して暗号化。	名前付きの AWS KMS CMK キー (とエイリアス ABC) が存在する場合はそのキーを使用して暗号化、それ以外の場合はデフォルトの AWS KMS キーを使用して暗号化。
RDS	非暗号化	非暗号化	非暗号化
	デフォルトの AWS KMS キーを使用して暗号化。	デフォルトの AWS KMS キーを使用して暗号化。	サポートされない
	デフォルトの AWS KMS キーを使用して暗号化。	デフォルトの AWS KMS キーを使用して暗号化。	サポートされない
Aurora	非暗号化	非暗号化	サポートされない
	デフォルトの AWS KMS キーを使用して暗号化。	デフォルトの AWS KMS キーを使用して暗号化。	サポートされない
	デフォルトの AWS KMS キーを使用して暗号化。	デフォルトの AWS KMS キーを使用して暗号化。	サポートされない

アプリケーションの整合性スナップショットを使用したクラウド内アプリケーションの保護

クラウドの VM に配備されているアプリケーションのアプリケーション整合性 (ポイントインタイム) スナップショットを取得できます。これにより、アプリケーションの指定した時点へのリカバリを実行できます。

これらの作業負荷については、元の場所および代替の場所へのリストアを実行できます。

代替の場所へのリストアを行う場合、次の点を考慮してください。

- MS SQL の作業負荷を代替の場所にリストアする場合、ターゲットホストを検出する必要がありますが、アプリケーションの状態が接続状態または構成済みであってはいけません。
- Oracle の作業負荷を代替の場所にリストアする場合、ターゲットホストを検出する必要がありますが、そのアプリケーションの状態が接続状態または構成済みであってはいけません。
- Oracle データベースの代替の場所へのリストアを行う場合、元の VM のクローンである代替 VM に対して、次のコマンドを使用して fstab エントリを削除し、デーモンを再起動します。

```
# systemctl daemon-reload
```

開始する前に

データベースのスナップショットの準備が整っていることを確認します。詳しくは、『NetBackup Snapshot Manager for Cloud インストールおよびアップグレードガイド』のプラグイン構成に関する注意事項を参照してください。

アプリケーションの指定した時点へのリカバリを構成するには

1. アプリケーションのホストである仮想マシンに接続します。
   - クラウド資産が検出されたら、[仮想マシン (Virtual Machines)]タブに移動します。
   - アプリケーションがホストされている仮想マシンを選択します。右上の[クレデンシャルの管理 (Manage credentials)]をクリックします。
   - クレデンシャルを入力します。VM のクレデンシャルが構成されていない場合は、クレデンシャルを構成する必要があります。『NetBackup Web UI 管理者ガイド』の「クレデンシャルの管理」の章を参照してください。
   - 仮想マシンが接続されると、仮想マシンの状態が[接続状態 (Connected)]に更新されます。
2. アプリケーションがホストされている仮想マシンを選択します。右上の[アプリケーションの構成 (Configure application)]をクリックします。

3 処理が完了すると、アプリケーションの状態が[構成済み (Configured)]に更新されます。

4 次回の検出後に、アプリケーションが[アプリケーション (Applications)]タブに表示されます。

5 保護計画を適用します。『NetBackup Web UI 管理者ガイド』を参照してください。

仮想マシンのクレデンシャルを編集または更新するには

1 [仮想マシン (Virtual Machines)]タブに移動します。

2 クレデンシャルを更新する仮想マシンを選択します。右上の[クレデンシャルの管理 (Manage credentials)]をクリックします。

3 クレデンシャルを更新します。

アプリケーションの構成を編集または更新するには

1 [アプリケーション (Applications)]タブに移動します。

2 更新するアプリケーションを選択します。右上の[構成の編集 (Edit configuration)]をクリックします。

3 クレデンシャルを更新し、[構成 (Configure)]をクリックします。

VMware へのリカバリのための AWS VM または Azure VM の保護

NetBackup では、AWS VM と Azure VM を保護し、保護された VM をオンプレミスの VMware VM としてリストアできます。このセクションでは、その考慮事項と前提条件について説明します。

- NetBackup は、Glacier または Archive モードを使用しない、MSDP ストレージサーバーと MSDP クラウドの AWS EC2 VM または Azure VM からのバックアップイメージのリカバリをサポートします。
- ソース VM のサポート対象オペレーティングシステム:
  - Windows Server 2022 シリーズ
  - RHEL 9.x
  - SUSE 15SP5: AWS プロバイダのソース VM の場合は、HVM AMI から作成する必要があります。NetBackup は ARM 形式の VM 変換をサポートしません。
- 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必要があります。

- ソース VM プラットフォームが Linux の場合は、/etc/fstab で使用される UUID Linux VM である必要があります。ソース VM プラットフォームが Windows の場合は、C ドライブの pagefile を有効にします。

VM の準備に必要な考慮事項と前提条件について詳しくは、次のセクションを参照してください。

p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。

クラウド資産のクリーンアップ

クラウド資産のクリーンアップは、クリーンアップサイクル中に自動的に実行されるか、次の基準に基づいて手動で実行します。

- クラウド資産のアクティブな保護計画がない。
- 過去 30 日間 (クリーンアップ期間) に資産が検出されていない。
- リカバリポイントが存在しない。
- 資産は削除対象としてマークされている (資産は Snapshot Manager で削除されます)。

クリーンアップ期間を更新し、bp.conf ファイルで特定のフィルタ基準を資産に対して指定することで、このクラウド資産のクリーンアップの基準を強化できます。次のパラメータは bp.conf ファイルで構成する必要があります。

- CLOUD.CLEANUP_AGE_MINUTES
- CLOUD.CLEANUP_FILTER

例:

```
/usr/openv/netbackup/bin/nbsetconfig

nbsetconfig> CLOUD.CLEANUP_AGE_MINUTES = 180

nbsetconfig> CLOUD.CLEANUP_FILTER = provider eq 'aws'

nbsetconfig>
```

次の例に示すように、ユーザーは次の要求本文で名前付き問い合わせ cleanup-assets を使用して POST 問い合わせを手動で実行してから、POST レスポンスで取得した問い合わせ ID を使用して GET を実行することもできます。

```
{
    "data":{
    "type":"query",
    "attributes":{
        "queryName":"cleanup-assets",
        "workloads":["cloud"],
```

```
        "parameters": {
            "cleanup_age_minutes": 180
        },
        "filter": "provider eq 'aws'"
      }
    }
}
```

クラウド資産のフィルタ処理

属性に基づいてカスタムフィルタを定義できます。NetBackup では、このフィルタを使用して、資産を[仮想マシン (Virtual machines)]、[アプリケーション (Applications)]、[PaaS]、[ボリューム (Volumes)]の各タブに一覧表示できます。

フィルタを作成するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual machines)]、[アプリケーション (Applications)]、[PaaS]、または[ボリューム (Volumes)]タブで、画面の右上にある[フィルタ (Filter)]アイコンをクリックします。

   [フィルタの作成 (Create filter)]オプションが表示されます。
3. [フィルタの作成 (Create filter)]オプションをクリックして、カスタムフィルタを属性に基づいて定義し、資産を[仮想マシン (Virtual machines)]、[アプリケーション (Applications)]、[PaaS]、または[ボリューム (Volumes)]タブに一覧表示します。
4. フィルタを作成するには、次のパラメータの詳細を入力します。

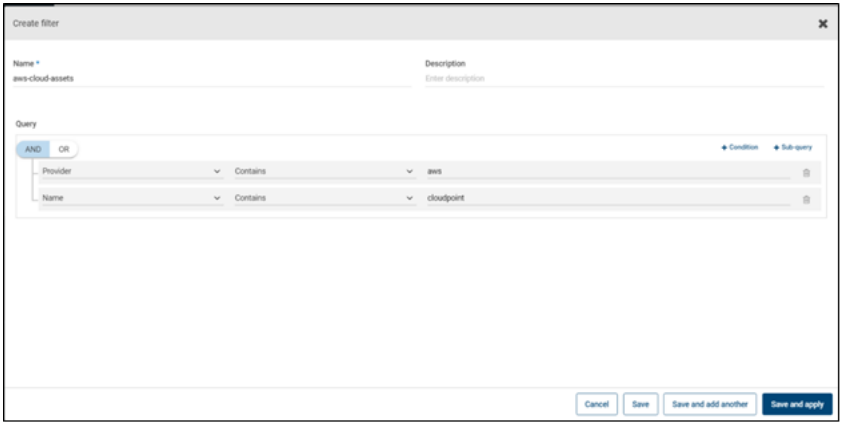
パラメータ	説明
名前 (Name)	フィルタの名前。
説明 (Description)	フィルタの説明を記入します。
問い合わせ (Query)	特定の条件を満たす資産のみを選択するには、独自の問い合わせを作成します。

5 特定の条件を満たす資産のみを選択するには、独自の問い合わせを作成します。そのためには、[+ 条件 (+ condition)]をクリックします。

6 条件を追加するには、ドロップダウンを使用してキーワードと演算子を選択し、値を入力します。

p.28 の「クラウド資産用インテリジェントグループ作成のための問い合わせオプション」を参照してください。

問い合わせの効果を変更するには、[+ 条件 (+ Condition)]をクリックし、[AND]または[OR]をクリックして、キーワード、演算子、条件の値を選択します。例:



この例では、AND を使用して問い合わせの範囲を絞り込みます。表示名に `aws` が含まれ、名前が `cloudpoint` で、**実行状態**の資産のみが選択されます。

条件にサブクエリーを追加することもできます。[+ サブクエリー (+ Sub-query)]をクリックし、[AND]または[OR]をクリックしてから、サブクエリーの条件のキーワード、演算子、値を選択します。

フィルタを作成するための問い合わせオプション

メモ: 属性値は、クラウドプロバイダのポータルに表示される値と正確に一致しない場合があります。個々の資産について、資産の詳細ページまたはクラウドプロバイダの API レスポンスを参照できます。

表 1-20 問い合わせキーワード

キーワード	説明 (すべての値で大文字と小文字が区別されます)
`Server type`	サーバーの種類。

キーワード	説明 (すべての値で大文字と小文字が区別されます)
Instance ID	クラウドプロバイダの選択に応じて、資産のインスタンス ID。
Instance name	クラウドプロバイダの選択に応じて、資産のインスタンス名。
Name	資産の表示名。
Provider	資産のクラウドプロバイダ名。
Region	資産のクラウドプロバイダの地域名。
構成 ID (Config ID)	資産の構成 ID。
データベースサービス (Database service)	資産のデータベースサービス。
削除済み (Deleted)	削除された資産。
エンティティのタイプ (Entity type)	資産のエンティティタイプ。
サービスドメイン (Service domain)	資産のサービスドメイン。
Snapshot Manager	資産が登録される Snapshot Manager のインスタンス。

表 1-21　問い合わせ演算子

演算子	説明
Starts with	文字列の先頭に値が出現する場合に一致します。
Ends with	文字列の末尾に値が出現する場合に一致します。
Contains	入力した値が文字列のどこにある場合でも一致します。
=	入力した値にのみ一致します。
≠	入力した値と等しくない任意の値と一致します。

2

PaaS 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。

PaaS 資産の保護

[アプリケーション (Applications)]タブには PaaS RDS 資産が表示され、[PaaS]タブには RDS PaaS 以外の資産が表示されます。この 2 つのタブで PaaS 資産を表示、保護、リカバリできます。

PaaS 資産を保護するための前提条件

NetBackup では、さまざまな資産について、さまざまなクラウドプラットフォームで PaaS 資産を検出、保護、リストアできます。このセクションでは、サポート対象のプラットフォームとデータベースについて説明します。

サポート対象のクラウドプロバイダ

NetBackup では、次のクラウドプロバイダを使用して PaaS 資産を保護できます。

- Microsoft Azure
- AWS
- GCP

プロバイダごとのサポート対象データベース

次の表に、クラウドプロバイダごとのサポート対象データベースを示します。

表 2-1 PaaS でサポートされるデータベース

プロバイダ	サポート対象データベース
Microsoft Azure	PostgreSQL、SQL Managed Instance、SQL、MariaDB、Azure Cosmos DB for NoSQL、Azure Cosmos DB for MongoDB、および MySQL。 次のコンポーネントはサポートされません。 Azure SQL - エラスティックプール Azure SQL Managed Instance - Azure Arc Azure Cosmos DB for MongoDB vCore Azure PostgreSQL - HyperScale (Citus) サーバーグループと Azure Arc 対応 PostgreSQL HyperScale

プロバイダ	サポート対象データベース
AWS	RDS SQL、RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS Aurora MySQL、RDS Aurora PostgreSQL、Amazon RDS for Oracle、Amazon Redshift、DynamoDB、RDS Custom for Oracle、RDS Custom for SQL、AWS DocumentDB、および AWS Neptune。
GCP	SQL、PostgreSQL、MySQL、および BigQuery。

サポート対象プラットフォーム

このセクションでは、プライマリサーバーおよびメディアサーバーのサポート対象プラットフォームについて説明します。

表 2-2 PaaS のサポート対象プラットフォーム

NetBackup サーバー	サポート対象プラットフォーム
プライマリ	RHEL、SUSE、Windows
メディア	RHEL
ストレージサーバー	基になる MSDP ブロックストレージまたは MSDP クラウドストレージ STU のユニバーサル共有

必要なクラウドプロバイダ権限

クラウドプロバイダの追加に使用するクレデンシャルには、『NetBackup Snapshot Manager インストールおよびアップグレードガイド』に記載されている必要なアクセス権および権限が割り当てられている必要があります。

サポート対象ポート

各 PaaS データベースでサポートされるポートを次に示します。AWS Neptune と AWS RDS の作業負荷では、デフォルトポートとともにカスタムポートがサポートされることに注意してください。

表 2-3 PaaS のサポート対象ポート

データベース PaaS の作業負荷	サポート対象ポート
Azure SQL Server	1433
Azure SQL 管理対象インスタンス	1433
Azure MySQL	3306

データベース **PaaS** の作業負荷	サポート対象ポート
Azure PostgreSQL	5432
Azure MariaDB	3306
GCP PostgreSQL	5432
GCP MySQL	3306
AWS DynamoDB	なし
AWS RDS PostgreSQL	5432
AWS RDS MySQL	3306
AWS MariaDB	3306
AWS RDS AuroraDB Postgres	5432
AWS RDS AuroraDB MySQL	3306
AWS RDS SQL Server	1433
AWS RDS for Oracle	1521
AWS DocumentDB	27017
AWS Neptune	8182
RDS Custom for Oracle	1521
RDS Custom for SQL	1433
Azure Cosmos DB for NoSQL	443
Azure Cosmos DB for MongoDB	10255
GCP BigQuery	なし
GCP SQL Server ポート	1433
Amazon Redshift	5439

MySQL および MariaDB データベースのバイナリログの有効化

- AWS の場合は、次を参照してください:
  https://aws.amazon.com/premiumsupport/knowledge-center/rds-mysql-functions/
- Azure の場合、リンクの説明に従って、パラメータ `log_bin_trust_function_creators` の値を 1 に設定します:
  https://learn.microsoft.com/ja-jp/azure/mysql/single-server/how-to-server-parameters
- GCP の場合は、次の手順を実行します。
  - インスタンスを開いて[Edit]をクリックします。
  - [Flags]セクションまで下方向にスクロールします。
  - フラグを設定するには、[Add item]をクリックし、ドロップダウンメニューから log_bin_trust_function_creators フラグを選択し、フラグの値をオンに設定します。
  - [Save]をクリックして、変更を保存します。[Overview]ページの[Flags]で変更を確認できます。

Kubernetes でのバックアップとリストアの有効化

AKS と EKS の配備でバックアップとリストア操作を実行する前に、プライマリサーバーポッドの `bp.conf` ファイルで MEDIA_SERVER_POD_CIDR パラメータを構成する必要があります。メディアサーバーポッドを配備するサブネットとして値を指定します。カンマ区切り値を使用できます。次に例を示します。

```
MEDIA_SERVER_POD_CIDR=10.0.0.0/8, 10.0.0.0/16
```

Amazon RDS SQL Server データベースの資産を保護するための前提条件

RDS SQL 資産を保護するには、オプショングループのネイティブなバックアップとリストアのオプションを有効にする必要があります。

このオプショングループは、*AWSBackupServiceRolePolicyForRestores/Backup* ポリシーが関連付けられている IAM ロールの一部である必要があります。

オプショングループを作成するには:

1. AWS ポータルで、IAM に移動し、新しいロールを作成します。
2. 次の権限を割り当てます。

- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForBackup
- sqlNativeBackup

3 ［RDS］、［Option groups］の順に選択します。次を実行します。

メモ: RDS SQL Server のオプショングループにネイティブなバックアップとリストアのオプションを追加する最新の手順については、AWS のマニュアルを参照してください。

- グループを作成します (名前: SqlServerBackupRestore、説明: xxx、エンジン: データベースエンジンを選択、メジャーエンジンのバージョン: DB インスタンスのバージョンを選択)。
- ［Create］をクリックします。
- 作成したグループをクリックして編集します。次を実行します。
  - ［Add option］をクリックします。
  - SQLSERVER_BACKUP_RESTORE オプションを選択します。
  - 前の手順で作成した IAM ロールを選択します。
  - 即時変更をスケジュール設定するには、［Immediately］を選択します。

4 ［RDS］、［Databases］の順に選択し、インスタンスを選択します。次を実行します。

- ［Modify］をクリックします。
- 前の手順で作成したオプショングループを選択します。
- ［Next］をクリックします。
- サービスの停止時間を避けるため、［Apply immediately］を選択します。
- ［Modify DB instance］をクリックして変更を適用します。
- SQL Management Studio からデータベースに接続している場合は、終了してから再度接続します。

Amazon RDS SQL Server データベースの資産を保護するためのバケットを使用するには:

10.2 より前のバージョンの NetBackup の場合:

1 NetBackup AWS S3 バケットを `netbackup-<AWS_ACCOUNT_IDENTIFIER>` として作成します。

2 同じ規則のバケットがすでに存在する場合、NetBackup はそれを使用します。

10.2 以降のバージョンの NetBackup の場合:

- バケットがない場合は、netbackup-<AWS_ACCOUNT_IDENTIFIER>-region という規則に従ってバケットが自動的に作成されます。

RDS Custom インスタンスの保護

NetBackup では、データベースのネイティブエクスポートを使用して、RDS Custom for SQL Server と RDS Custom for Oracle のデータベースを保護できます。

RDS Custom for SQL Server 資産の保護

RDS Custom For SQL Server インスタンスを保護するには、RDS Custom For SQL Server インスタンスが実行されている EC2 インスタンスに NetBackup を配備します。NetBackup は、Microsoft SQL Server の作業負荷でこれらのインスタンスを検出します。MS-SQL-Server ポリシー形式と保護計画を使用して、インスタンスレベルおよびデータベースレベルのバックアップを実行できます。ポリシーの構成、バックアップおよびリストア操作の実行について詳しくは、『NetBackup for Microsoft SQL Server 管理者ガイド』を参照してください。

RDS Custom for SQL Server 資産の保護の考慮事項

- インスタンスとデータベースの完全バックアップ、差分増分バックアップ、トランザクションログバックアップを実行できます。
- リストアは、個々のデータベースレベルでのみサポートされます。
- 個々のデータベースは元の場所、代替の場所、代替パスにリストアできます。代わりの RDS Custom SQL Server にデータベースをリストアすることもできます。
- Amazon RDS Custom SQL Server にデータベースをリストアする場合、リストアの宛先パスは D:¥rdsdbdata フォルダの下にある必要があります。
- データベースを Amazon RDS Custom SQL Server にリストアしている間は、インスタントアクセスの構成はサポートされません。

RDS Custom for Oracle 資産の保護

RDS Custom for Oracle データベースを保護するには、RDS Custom Oracle が実行されている EC2 インスタンスに NetBackup を配備します。これらのインスタンスは Oracle の作業負荷で検出されます。NetBackup では、RMAN を使用してバックアップおよびリストア操作を実行します。ポリシーの構成、バックアップ、リストアの操作について詳しくは、『NetBackup for Oracle 管理者ガイド』を参照してください。

RDS Custom for Oracle 資産の保護の考慮事項

- Oracle ユーザーに対して、[OS 認証のみ (OS authentication only)]オプションを使用してクレデンシャルの検証を実行できます。
- RDS Custom Oracle データベースの完全バックアップを実行するには、Oracle ポリシーの[完全および増分スケジュールにアーカイブ REDO ログを含める (Include archived redo logs in full and incremental schedules)]オプションを無効にする必要があります。
- 完全、差分増分バックアップ、累積増分バックアップ、アーカイブ REDO ログバックアップのスケジュールがサポートされます。
- アーカイブログのバックアップを実行するには、archivedLogRetentionHours を最大値に設定して、クライアント RDS Custom Oracle インスタンスでアーカイブログを最大期間保持します。
  次を実行します。
  - 次の名前のテキストファイルを作成します。
    `/opt/aws/rdscustomagent/config/redo_logs_custom_configuration.json`
  - 次の形式で JSON オブジェクトを追加します。
    `{"archivedLogRetentionHours" : "num_of_hours"}`
    数値は、1 から 840 の範囲の整数である必要があります。
- フォルダ内にある、バックアップとリストアのサンプルスクリプトを見つけます。
  `/usr/openv/netbackup/ext/db_ext/oracle/samples/rman/samples`
  サンプルスクリプトを、クライアント上の別のディレクトリにコピーします。ご使用の環境に合わせてスクリプトを変更します。
  スクリプトの ORACLE_HOME、ORACLE_SID、ORACLE_USER の各フィールドを更新します。
- スクリプトを使用してコールドデータベースバックアップとホットデータベースバックアップを実行するためのスクリプトオプションを使用して、クライアントのポリシーを作成します。
- バックアップおよびリストアは、RMAN リストアスクリプトを使用した場合にのみサポートされます。
- 完全なデータベースリストアと PIT データベースのリストアスクリプトがサポートされます。
- バックアップとリストア操作を正常に実行するために、RDS Custom Oracle データベースの削除保護を無効にします。
- 正常にリストアするには、RDS Custom Oracle インスタンスを自動化が一時停止された状態に移行します。

Azure Managed Instance データベースの保護

NetBackup バージョン 11.0 以降、ネイティブバックアップメカニズムの T-SQL を使用した Azure Managed Instance のバックアップがサポートされます。このバックアップ方式では、バックアップ時に一時データベースを作成する必要はありません。.bak ファイルが Azure Blob ストレージのステージング領域に生成され、後でユニバーサル共有に移動されます。マネージドインスタンスは、Azure SAS トークンを使用して、データを Azure Blob に .bak の形式で安全に保存します。この方式は完全バックアップでのみサポートされます。AMI を使用する場合は、ストレージアカウントに同じ AMI を接続する必要があります。これらのデータベースのバックアップとリカバリのワークフローは、他のデータベースと同じです。

Azure Managed Instance データベースの保護の前提条件

一時データベースを作成せずに Azure Managed Instance データベースを保護するには、次の前提条件が必要です。

メモ: マネージドインスタンスは、Azure SAS トークンを使用して、データを Azure Blob に .bak ファイルの形式で安全に保存します。

- 次の例を使用して、ストレージアカウント名を作成します。
  - サブスクリプション ID と地域を組み合わせて形成される文字列のハッシュを計算します。次のコマンド例に従います。

    ```
    echo -n "aaaaaaa-bbb-ccc-dd11-aabbccdd11223344eastus" |
    sha256sum
    2e5fb564552100a6060794937fedc33aefe4d01eb7e27971c1a0ed52c3f78b6c
    ```

  - ハッシュの最初の 16 文字のみを取り、文字 nbu の接頭辞を付けます。
  - 文字列は nbu + 2e5fb564552100a6 になります。
  - したがって、Azure ストレージアカウントの名前は nbu2e5fb564552100a6 になります。
- コンテナの場合は、次の名前の形式を使用します。
  - azure-netbackup-<region>
  - コンテナが存在しない場合、NetBackup エージェントは権限の可用性に応じてコンテナを作成します。
- 暗号化キーの管理は組織に応じて行うことができます。

Azure Managed Instance データベースの保護に必要な権限

一時データベースを作成せずに Azure Managed Instance データベースを保護するには、次の権限が必要です。

メモ: マネージドインスタンスは、Azure SAS トークンを使用して、データを Azure Blob に `.bak` ファイルの形式で安全に保存します。

- Storage/storageAccounts/write
- Storage/storageAccounts/delete
- Storage/storageAccounts/listKeys/action
- Storage/storageAccounts/regenerateKey/action
- Storage/storageAccounts/read
- Storage/storageAccounts/blobServices/containers/read
- Storage/storageAccounts/blobServices/containers/write
- Storage/storageAccounts/blobServices/containers/delete
- Storage/storageAccounts/blobServices/containers/read
- Storage/storageAccounts/blobServices/generateUserDelegationKey/action
- Storage/storageAccounts/blobServices/containers/blobs/write
- Storage/storageAccounts/blobServices/containers/blobs/delete
- Storage/storageAccounts/blobServices/containers/blobs/read

制限事項および考慮事項

PaaS 作業負荷を保護するときは、次の点を考慮してください。

すべてのデータベース

- RHEL 7.x での NetBackup Snapshot Manager の配備は、PaaS 資産の保護ではサポートされません。
- Flex Appliance と Flex Scale の NetBackup の配備では、PaaS の作業負荷はサポートされません。
- データベースについてはバックアップとリストアはサポートされないため、NetBackup への接続にはクライアント証明書の使用が必須です。

- AWS RDS の作業負荷インスタンスを除き、他のすべての作業負荷インスタンスはデフォルトポートのみをサポートします。カスタムポートはサポートされません。
- 「#」と「/」の文字を含むデータベース名は、バックアップおよびリストア操作ではサポートされていません。また、データベース名はクラウドベンダーが推奨する命名規則に従う必要があります。
- サーバーまたはデータベースのパスワードでは「;」はサポートされません。
- 7 ビット以外の ASCII 文字を使用したデータベースのバックアップおよびリストアは、Windows を実行する、または 10.1.1 より古い旧バージョンのメディアサーバーを含むプライマリサーバーではサポートされません。
- サポート対象のストレージサーバーに PaaS バックアップイメージを複製できます。ただし、リストアを開始する前に、ユニバーサル共有が有効な MSDP サーバーにイメージを複製して戻す必要があります。p.159 の「AdvancedDisk からの複製イメージのリカバリ」を参照してください。
- NetBackup 10.3 では、管理対象 ID データベース認証を使用して、サポート対象の Azure PaaS データベースのバックアップとリストアを実行できます。これは、MariaDB サーバー用の Azure データベースではサポートされません。この機能には、バージョン 10.2 以上のメディアサーバーが少なくとも 1 台必要です。
- Azure データベースの認証がすべてのメディアサーバーで機能するためには、ユーザーが割り当てた管理対象 ID を使用することをお勧めします。メディアサーバーまたは vm-scale-set (AKS/EKS) に関連付けられた、システムが割り当てた管理対象 ID を持つデータベースユーザーは、他のメディアサーバーや他の vm-scale-set (AKS/EKS) のメディアでは機能しません。
- Azure Managed Identity は、異なるテナントまたは同じテナントのサブスクリプション間ではサポートされません。
- PaaS 資産の場合、リカバリログは[リカバリ (Recovery)]、[ジョブ ID (JobID)]、[ログ (Logs)]では利用できません。リカバリログは、アクティビティモニターまたは[リストアアクティビティ (Restore activity)]タブの資産の詳細で表示できます。
- PaaS 資産のリストア操作には、ストレージサーバーの表示権限が必要です。ストレージサーバーのバージョンが 10.2 より古い場合、ストレージサーバーの表示権限とともに、Ushare に対する表示および作成権限が追加で必要です。
  ログオンしたユーザーにストレージサーバーの表示権限がない場合、NetBackup はリストア中に既存の UShare をフェッチしようとします。Ushare が存在しない場合、NetBackup ではリストア時に `dbpaasrestore` という名前で新しく作成されます。NetBackup は、リカバリジョブを後で開始します。

PostgreSQL の場合

- セキュリティ権限のリストアはサポートされていません。

- リストア時には、-no-owner オプションと -no-privileges オプションを使用できます。リストア後、バックアップ時に取得されたメタデータは、Web UI の進捗ログのリストアアクティビティで所有者または ACL として表示されます。
- リストア先に所有者または役割が存在しない場合、リストアは失敗しません。
- リストア後は、リストア先インスタンスに対して NetBackup で指定されたクレデンシャルに従って、データベースに役割が関連付けられます。
- ユーザーは、リストア後にデータベースの所有権を変更する必要があります。
- クラウドプロバイダの制限により、単一サーバーと柔軟なサーバーとの間の Azure Postgres データベースリストアはサポートされません。
- リストアワークフローのデータベース名では、次の文字はサポートされていません: `、@、¥、[、]、!、#、%、^、.、,、&、*、(、)、<、>、?、/、|、}、{、~、:、'、"、;、+、=、-。
- PostgreSQL サーバーの作成後に新しいユーザーを追加する場合、大文字のユーザー名はサポートされていません。
- (RDS と Azure PostgreSQL のみ) データベースインスタンスで構成されている SCRAM 認証はサポートされません。
- 完全バックアップまたは差分増分バックアップが一時オブジェクトで失敗した場合は、一時オブジェクトを手動で削除し、バックアップを再実行します。

Azure PostgreSQL の増分バックアップの場合

- Azure PostgreSQL サーバーの資産は、保護計画とポリシーを使用して保護できます。完全スケジュールと差分増分スケジュールを使用できます。
- wal_level サーバーパラメータは、常に論理として設定します。
- バックアップユーザーは管理者ユーザーである必要があります。
- バックアップユーザーには CREATEROLE と REPLICATION の権限が必要です。
- 他のユーザーのテーブルをバックアップするには、テーブルにプライマリキーが必要です。
- インテリジェントグループがサポートされます。
- レプリカサーバーデータベースは完全バックアップと増分バックアップではサポートされません。
- 増分バックアップでは、大きいオブジェクトデータ形式はサポートされません。
- エスケープ値を指定した bytea_output サーバーパラメータを使用した増分バックアップはサポートされません。
- 増分バックアップでは、Azure SMI と UMI はサポートされません。

- 増分バックアップのリストア後は、シーケンスジェネレータの最後の値が一貫性を持たない可能性があります。
- データベースの名前を変更するには、次の手順を実行します。
  - データベース用に作成されたレプリケーションスロットの名前を書き留めます。
    ```
    SELECT slot_name FROM pg_replication_slots WHERE database =
    <database name that needs to be renamed>
    ```
  - データベースの名前を変更した後、レプリケーションスロットを削除します。
    ```
    SELECT pg_drop_replication_slot('<replication slot name>')
    ```

AWS RDS PostgreSQL および AWS Aurora PostgreSQL の場合

- バックアップとリストアには、NetBackup バージョン 10.4 以上とローカル LSU を搭載したメディアサーバーが必要です。
- バックアップイメージにマテリアライズドビューが含まれている場合は、リストア後にマテリアライズドビューを手動で更新する必要があります。マテリアライズドビューを更新するには、次の記事を参照してください:
  https://www.veritas.com/support/en_US/article.100062910
- リストアに使用されるユーザークレデンシャルが IAM ユーザーのものである場合、データベースオブジェクトはソースデータベースと同じ所有権でリストアされます。
- オブジェクトの所有権と権限はリストアされません。次のシナリオでは、リストアに使用するユーザーは、リストアされたすべてのデータベースオブジェクトの所有者になります。
  - リストアされたユーザークレデンシャルがユーザー名とパスワードの場合。
  - バックアップイメージがバージョン 10.4 より前の NetBackup バージョンで作成されている場合。

AWS DynamoDB の場合

- 地域とアカウントの代替リストアはサポートされていません。
- 別のプライマリサーバーからインポートされたイメージからのリストアは、NetBackup REST API を使用した場合にのみサポートされます。
- リストア中の S3 からのインポート機能は、メディアバージョン 10.3.1 以降でサポートされます。この機能を使用すると、テーブルの書き込み容量を消費することなく、より高速なリストアが可能になります。
- S3 からのインポート機能は、ローカルセカンダリインデックスのリストアをサポートしません。この機能はデフォルトで有効です。

- ローカルセカンダリインデックスをリストアするには、[ローカルセカンダリインデックスを含める (Include local secondary indexes)]オプションを選択します。これによりテーブルの書き込み容量が消費され、リストアに時間がかかることがあります。

AWS DocumentDB の場合

- スナップショットベースの保護とスナップショットからのリストアのみがサポートされます。
- NetBackup ポリシーのみを使用して資産を保護できます。保護計画はサポートされません。
- NetBackup レプリケーション機能はサポートされません。
- インテリジェントグループはサポートされません。
- クラウド資産の下に、DocumentDB 用の IG を作成できます。
- スナップショットオプションを使用した NetBackup ポリシーでは、バックアップ対象として DocumentDB IG は表示されません。

AWS Neptune の場合

- スナップショットベースの保護とスナップショットからのリストアのみがサポートされます。
- NetBackup ポリシーのみを使用して資産を保護できます。保護計画はサポートされません。
- NetBackup レプリケーション機能はサポートされません。
- インテリジェントグループはサポートされません。
- クラウド資産の下に、Neptune 用の IG を作成できます。
- スナップショットオプションを使用した NetBackup ポリシーでは、バックアップ対象として Neptune IG は表示されません。

AWS RDS SQL の場合

- クレデンシャルの検証では、IAM は AWS RDS SQL ではサポートされません。ユーザー名およびパスワード方式を使用できます。
- FILESTREAM ファイルグループを含むデータベースはリストアできません。
- 既存のデータベースと同じ名前のデータベースをリストアすることはできません。データベース名は一意である必要があります。
- 特定の RDS SQL インスタンスに対して、最大で 2 つのバックアップまたはリストアタスクを同時に実行できます。
- RDS SQL は、最大 16 TB のデータベースのネイティブリストアをサポートします。SQL Server Express Edition では 10 GB のデータベースのみをリストアできます。

- メンテナンス期間中、または Amazon RDS SQL がデータベースのスナップショットを作成中の場合、ネイティブバックアップはサポートされません。ネイティブバックアップタスクは、RDS の日単位のバックアップ処理時間帯と重なるとキャンセルされます。
- TDE が有効なデータベースの代替の場所へのリストアを実行するには、ソース RDS SQL インスタンスの TDE 証明書がターゲット RDS SQL インスタンスに存在する必要があります。
- TDE 対応データベースのネイティブバックアップを作成できますが、これらのバックアップをオンプレミスデータベースにリストアすることはできません。

Azure、AWS RDS、Aurora MySQL の場合

- 10.2 より前のバージョンで取得されたバックアップで、ダンプファイルに CREATE DEFINER 文が含まれている場合、リストア操作にはスーパーユーザー権限が必要です。
- バージョン 10.3 以降で取得されたバックアップを、10.2 より前のバージョンを使用してリストアすることはできません。
- GCP MySQL 作業負荷に対してサーバーレベルで SSL 接続のみが適用されている場合、バックアップとリストアはサポートされません。
- MySQL のバージョンの互換性に応じて、MySQL データベースをバックアップインスタンスとは MySQL バージョンが異なる代替インスタンスにリストアできます。

Azure MySQL サーバーを使用した増分バックアップの場合

- Azure MySQL サーバーの資産は、保護計画とポリシーを使用して保護できます。インスタンスレベルでは、完全スケジュールと差分増分スケジュールを使用できます。個々のデータベースは、完全スケジュールを使用してのみ保護できます。
- 個々のデータベースは、取得したサーバーのバックアップから、別の宛先サーバーにリカバリできます。宛先サーバーに同じ名前のデータベースがあると、リストアは失敗します。
- 現在、NetBackup は、ユーザーとその権限を宛先サーバーにはリストアしません。すべてのデータベースオブジェクトは、バックアップ時のソースデータベースにあったのと同じユーザーを使用してリカバリされます。ユーザーの作成と必要な権限の付与はリストア後に行えます。
- ストレージエンジン形式 MEMORY で作成されたテーブルのレコードは、増分スケジュール中にはバックアップされません。これらのレコードはメモリに残り、これらのテーブルに加えられる変更は、バイナリログに反映されません。
- NetBackup は、次のシナリオで、増分スケジュール中に完全バックアップを実行します。

- サーバー上の 1 つ以上のバイナリログが、後続の増分バックアップ間でパージされる場合。binlog_expire_logs_seconds 値が、増分スケジュールの間隔に基づいて、適切な値に設定されていることを確認します。
- サーバー上の 1 つ以上のデータベースのスキーマを変更し、それらのデータベースのいずれかで DDL 処理を実行する場合。
- 1 つ以上のデータベースがサーバーに追加されるか、サーバーから削除される場合。
- サーバーが高可用性として構成されているときに、サーバー上でフェールオーバーが発生した場合。
- サブスクライブ済みのポリシーまたは保護計画で、資産の増分リカバリポイントの最大条件 (100) に達した場合。

GCP SQL Server を使用した増分バックアップの場合

- DML 変更後の増分バックアップは、CDC がテーブルで有効になった後にテーブルの名前を変更すると失敗することがあります。回避策として、名前を変更したテーブルを参照するオブジェクトを手動で修正する必要があります。たとえば、トリガで参照されているテーブルの名前を変更した場合、そのトリガを変更して新しいテーブル名を含める必要があります。この Azure マニュアルのリンクを参照して、名前を変更する前にテーブルの依存関係を一覧表示します。
- バイナリまたはイメージデータがあるデータベースのバックアップとリストアはサポートされません。Cloud SQL Server での一括挿入には、GCP が許可しない sysadmin 権限が必要です。
- 異なるストレージサーバーで増分バックアップを複製している間に、NetBackup は同じリカバリポイントに対して異なるコピー番号を生成します。以前の完全バックアップとその他の増分バックアップがない増分コピーをリストアしようとすると、リストアは失敗する場合があります。
- 複数のメディアサーバーがある場合、増分バックアップはバージョン 10.3 以降でのみ実行できます。
- システムデータベースと CDC スキーマがバックアップされ、ターゲットデータベースにリストアされます。
- CDC 保持期間は、増分バックアップ間隔のスケジュールに使用される期間よりも長く設定する必要があります。
- 複数のテーブルを持つデータベースの増分バックアップでは、複数のテーブルに対する CDC 有効化に時間がかかるため、バックアップに時間がかかる場合があります。
- Web および Express のデータベースエディションでは、増分バックアップはサポートされません。

- CDC という名前のカスタムスキーマまたはユーザーがデータベースに存在する場合、CDC を有効にしようとすると失敗します。
- アプリケーションの一貫性を確保するために、NetBackup は、前回の完全バックアップと、後続のすべての増分バックアップに依存します。ランダムなバックアップイメージが期限切れになると、データ損失のためにアプリケーションの不整合が発生する可能性があります。
- CDC には、Standard または Enterprise エディションの SQL Server が必要です。データベースが KEEP_CDC オプションを使用して Standard または Enterprise 以外のエディションに接続またはリストアされている場合、バックアップは失敗します。エラーメッセージ 932 が表示されます。

Azure SQL と SQL Managed Instance の場合

これらの制限事項は、一時データベースを使用する Azure SQL データベースと Azure Managed Instance のバックアップに適用されます。

- メディアサーバーとして使用される Azure VM は、Azure 管理対象インスタンスと同じ Vnet に存在する必要があります。または、メディアサーバーと SQL 管理対象インスタンスが異なる Vnet に存在する場合は、両方の Vnet がピア接続されてデータベースインスタンスにアクセスする必要があります。
- データベースまたはリソースグループに読み取りロックが設定されていると、バックアップは失敗します。
- データベースに次の種類のテーブルが含まれている場合、CDC の制限によりバックアップが失敗します。
  - グラフテーブル
  - テンポラルテーブル
  - 台帳テーブル (更新可能な台帳)
  - メモリ最適化テーブル (ビジネスクリティカル層のみ)
    Azure Managed Instance データベースでは、ネイティブバックアップデータベースワークフローによってバックアップが生成された場合、顧客管理キーで有効化された TDE を使用するか、TDE を無効にして、これらの種類のテーブルがサポートされます。
- データベース図はリストアされません。
- NetBackup は、Azure SQL の指定した時点のリカバリポイントを使用して保護対象の SQL インスタンスに一時データベースを作成し、バックアップの目的で一貫したステージングデータベースを読み取り専用で保持します。NetBackup では、一時データベースに対応するためにインスタンスに追加の領域が必要です。一時データベースのサイズは、保護対象のデータベースと同じです。

- データベースまたはリソースグループに削除ロックが設定されていると、バックアップは部分的に成功します。
  NetBackup は、バックアップの完了後に一時データベースのクリーンアップを実行します。サーバーに存在するデータベースまたはリソースグループに削除ロックが設定されている場合、NetBackup は一時データベースを削除できず、結果的にバックアップは部分的に成功します。これらの古い一時データベースが Azure Managed Instance の領域を占有し、インスタンスの領域が不足すると、それ以降バックアップエラーが発生する可能性があります。このような場合は、このインスタンスで NetBackup バックアップジョブが実行されていないときに、一時データベースを手動でクリーンアップします。
- Azure SQL Server または Azure Managed Instance のデータベースをリストアするには、ターゲットサーバーの AAD 管理者権限を割り当てる必要があります。リストアする前に、次のいずれかに権限を割り当てます。
  - システムまたはユーザーが管理するメディアサーバーの ID。
  - NetBackup メディアが配備される `vm-scale-set` (AKS または EKS の配備の場合)。

Azure SQL と SQL Managed Instance の場合 (一時データベースなし)

これらの制限事項は、一時データベースを使用しない Azure SQL データベースと Azure Managed Instance のバックアップに適用されます。

- このバックアップ方式は、Azure Managed Instance の完全バックアップにのみ適用されます。
- Azure Managed Instance のクロスアカウント、サブスクリプション、テナントリストアはサポートされません。
- 次のシナリオでは、バックアップは前提条件の一部として一時データベースを作成します。
  - TDE が有効で、サービス管理キーに設定されている場合。
  - ポリシーまたは保護計画に完全スケジュールと増分スケジュールがある場合。
  - Azure Managed Instance の DB 増分スケジュールの場合。
  - Azure SQL の DB バックアップの場合。
  - サポートされるプライマリサーバーの最小バージョンは 10.5.1 です。

Azure SQL Server と SQL Managed Instance の増分バックアップの場合

- テーブルの列が暗号化されているデータベースでは、バックアップまたはリストアの問題が発生する場合があります。回避策として、Microsoft 社はこの問題に対処するために Publish/Extract コマンドを使用することを提案しています。
- テーブルに blob データがあるデータベースのリストアが失敗する場合があります。
- 異なるストレージサーバーで増分バックアップを複製するために、NetBackup は同じリカバリポイントに対して異なるコピー番号を生成します。完全バックアップまたはその他の増分バックアップの以前の参照がない増分コピーをリストアしようとすると、リストアは失敗します。

メモ: Azure SQL Server の増分バックアップはバージョン 10.2 以降の NetBackup メディアサーバーでのみ実行できます。Azure SQL Managed Instance の増分バックアップはバージョン 10.3 以降の NetBackup メディアサーバーでのみ実行できます。

- BLOB データテーブルを使用してデータベースをバックアップしないでください。テーブルに BLOB データが含まれている場合、バックアップは成功する場合がありますが、リストアは失敗します。
- リストア中、Azure SQL Server または Azure SQL Managed Instance データベースの暗号化設定が保持されない場合があります (*Is_encryption=0*)。

Azure Cosmos DB for MongoDB の場合

- アカウントが vCore クラスタを使用して構成されている場合、検出、保護、リストアはサポートされません。
- アカウントにカスタマイズキーが構成されている場合、バックアップとリストアはサポートされません。
- NetBackup は、Azure Cosmos DB for MongoDB バージョン 3.2 をサポートしません。
- [既存のデータベースを上書き (Overwrite existing database)]オプションはサポートされていません。
- データベースの命名規則:
  - データベース名の長さは、3 文字から 63 文字にする必要があります。
  - データベース名では、#、/、?、&、<、>、=、}、$、{、]、[、"、'、.、¥ 以外のすべての文字がサポートされています。

Azure Cosmos DB for NoSQL の場合

- アカウントにカスタマイズキーが構成されている場合、バックアップとリストアはサポートされません。
- [既存のデータベースを上書き (Overwrite existing database)]オプションはサポートされていません。
- データベースの命名規則:
  - データベース名の長さは、3 文字から 63 文字にする必要があります。
  - データベース名では、#、/、?、&、<、>、=、}、$、{、]、[、"、'、.、¥ 以外のすべての文字がサポートされています。

Amazon RDS for Oracle の場合

- 完全、差分増分、およびアーカイブ REDO ログのタイプの保護について、バックアップとリストアがサポートされます。
- Oracle 21c と 19c CDB がサポートされます。19c の非 CDB バージョンもサポートされます。
- マルチテナントおよびシングルテナントのコンテナデータベースを含む CDB データベースと、非 CDB データベースがサポートされます。
- Oracle Enterprise Edition と Standard Edition がサポートされます。
- バックアップとリストアはどちらもステージングパスとして S3 でサポートされます。
- バックアップとリストアは、TDE が有効な RDS Oracle インスタンスまたは読み取りレプリカではサポートされません。
- クレデンシャルの検証では、IAM は AWS RDS Oracle ではサポートされません。ユーザー名およびパスワード方式を使用できます。
- RDS Oracle に接続されているオプショングループには、同じデータベースエンジンバージョンと同じデータベースエンジン名が必要です。
- リストアは、[インスタントアクセスデータベース (Instant access database)]タブからの手動リカバリを含む、S3 ステージングパスのみを使用してサポートされます。
- S3 統合が構成されていないか S3 構成が失敗した場合、EFS が構成されていれば、バックアップは 19c バージョンでのみ EFS にフォールバックされます。
  EFS を削除する前に、その EFS の EFS ID エントリをオプショングループから削除したことを確認します。
- アーカイブログのバックアップを実行する前に、保護計画の保持期間を設定します。
  次のナレッジベースの記事を参照してください:
  https://www.veritas.com/support/ja_JP/article.100059038

- データの一貫性を維持するために、インスタンスの `RDS rman` API を使用して外部バックアップを作成しないでください。
- リカバリスクリプトは EC2 またはオンプレミス VM をサポートします。
- NetBackup では、次の 3 つの場合に完全バックアップが実施されます。
  - バックアップがキャンセルされたか、失敗した場合。NetBackup は、以前の DBPaaS の状態ファイルのフラグを保持して、このようなイベントを追跡します。
  - 最初のバックアップを増分またはアーカイブログのバックアップとしてスケジュール設定する場合。
  - 複数の増分バックアップまたはアーカイブバックアップを実行する場合は、しきい値を超えます。しきい値は、増分バックアップおよびアーカイブログバックアップのリカバリポイント数を参照します。

Amazon Redshift データベースの場合

- Redshift データベースの代替領域または代替アカウントへのリストアはサポートされません。
- 現在、FIPS は Redshift データベースではサポートされていません。
- ユーザーデータベースのみが保護されます。システムデータベースは表示または保護されません。
- 別のプライマリサーバーからインポートされたイメージからのリストアは、NetBackup REST API を使用した場合にのみサポートされます。
- Redshift クラスタのみがサポートされます。サーバーレス Redshift はサポートされません。
- データベースバックアップを開始する前に、Redshift クラスタが利用可能な状態である必要があります。
- 二重引用符を使用し、大文字と小文字を区別する名前を持つテーブル名はリストアされません。
- リストア中のファイル数は、バックアップファイルの合計数より 1 つ少ないファイルを示すことがあります。
- 空のテーブルを持つデータベースのバックアップは作成しないことをお勧めします。
- NetBackup は、クラッシュ整合の Redshift データ保護を提供します。バックアップを作成する前に、アクティビティの種類とアプリケーション要件を考慮して、アプリケーションがバックアップ操作でチェックポイントまたは静止する必要があるかどうかを判断します。

Amazon Redshift クラスタの場合

- プライマリ、メディア、およびスナップショット管理サーバーをサポートする最小バージョンは NetBackup 10.5 です。
- 現在、FIPS は Redshift クラスタではサポートされていません。
- AWS Secrets Manager のクレデンシャルを使用して作成された Redshift クラスタはサポートされません。
- Redshift クラスタの代替領域または代替アカウントへのリストアはサポートされません。
- クラスタスナップショットをトリガする前に、Redshift クラスタが利用可能な状態である必要があります。
- クラスタのリストアジョブは、ジョブがまだ進行中であっても、成功したとアクティビティモニターにすぐに表示される場合があります。AWS コンソールで、クラスタのリストアジョブの実際の状態を監視してください。
- Redshift クラスタあたりの手動スナップショットの最大数は 20 です。
- リストア中、リストアされたクラスタの `PubliclyAccessible` プロパティが False に設定されます。これは、必要に応じて、リストア後に手動で変更できます。
- リストアの進行中は、Redshift クラスタのスナップショットイメージに対し、NetBackup イメージを有効期限切れにしないでください。リストアの進行中に、自動化されたイメージの有効期限切れジョブが実行されると、AWS ポータルからのスナップショットのクリーンアップは失敗します。
- NetBackup アクティビティモニターには、次のスナップショットパラメータの値は表示されません: 転送済みのバイト数、書き込み済みのファイル、現在のファイル、残りのファイル数の概算、概算ファイル数。

GCP SQL Server の場合

- 読み取り専用データベースのバックアップとリストアはサポートされません。
- プロバイダクレデンシャルは、データベースのクレデンシャルとしてではなく、完全バックアップおよびリストア用に検証されます。
- シングルユーザーモードデータベースのバックアップとリストアはサポートされません。
- 1 つの操作が進行中の場合、後続のジョブはキュー内で待機します。実行中のジョブの完了に時間がかかると、キュー内のジョブがタイムアウトして失敗する場合があります。

GCP BigQuery の場合

- GCP プロジェクトのユーザーとその権限はリストアされません。リストアされたデータセットの所有者は、クラウドプロバイダの追加時に NetBackup で構成された GCP サービスプリンシパルです。
- データエクスポート制限の最大値は、プロジェクトごとに 1 日あたり 50 TB です。
- データセットとテーブルに接続されているタグはリストアされません。
- 複数のリージョン (米国、EU) 用に作成されたデータセットはサポートされません。
- RANGE データ形式のエクスポートは、GCP エクスポート API ではサポートされていません。
- リンクされたデータセットの検出、バックアップ、リストアは行われません。
- データ型が DATETIME であるテーブル内のレコードは、バックアップではサポートされません。
- NetBackup は、列またはスキーマなしでテーブルをバックアップすることはしません。
- 列レベルのアクセス制御または行レベルのセキュリティを備えたテーブルのバックアップはサポートされません。

ネイティブクライアントユーティリティのインストール

BYO (build-your-own) セットアップを使用する場合、PaaS 作業負荷を機能させるには、NetBackup 環境にネイティブクライアントユーティリティをインストールする必要があります。権限のないユーザー (またはサービスユーザー) アカウントを使用するように BYO 設定が構成されている場合、ネイティブクライアントユーティリティに必要な実行権限が NetBackup サービスユーザーにあることを確認します。

AKS (Azure Kubernetes Services) または EKS (Elastic Kubernetes Services) での NetBackup 配備の場合、ネイティブクライアントユーティリティは NetBackup メディアサーバー、プライマリサーバー、およびデータムーバーコンテナイメージの一部としてパッケージ化されています。これらのために手動インストールは必要ありません。

クラウドプロバイダ内のデータベースにアクセスするために、ファイアウォール、セキュリティグループ、DNS の設定などのネットワーク設定が適切に構成されていることを確認します。

NetBackup 10.4 以降、DBPaaS エージェントとネイティブクライアントユーティリティは、サービスユーザーが構成されている場合はサービスユーザーで実行されます。

メモ: これらのパッケージのいずれかがメディアサーバーにすでにインストールされている場合、インストールする新しいバージョンのパッケージとの競合を避けるため、そのパッケージを削除します。

MySQL クライアントユーティリティのインストール

次のデータベースを保護するには、このユーティリティをインストールする必要があります。

- Azure MySQL
- Azure MariaDB
- AWS MySQL
- AWS MariaDB
- AWS Aurora MySQL
- GCP MySQL

MySQL クライアントユーティリティの推奨バージョンは 8.0.34 です。

RPM のダウンロード場所 https://downloads.mysql.com/archives/community/

インストールするには、端末で次のコマンドを実行します。

1. `rpm -ivh mysql-community-common-<version_no>.x86_64.rpm`
2. `rpm -ivh mysql-community-client-plugins- <version_no>.x86_64.rpm`
3. `rpm -ivh mysql-community-libs- <version_no>.x86_64.rpm`
4. `rpm -ivh mysql-community-client- <version_no>.x86_64.rpm`

メモ: MySQL によって報告されているバグがあるため、MySQL クライアントユーティリティ 8.0.32 バージョンは使用しないでください。

---

sqlpackage クライアントユーティリティのインストール

次のデータベースを保護するには、このユーティリティをインストールする必要があります。

- Azure SQL
- Azure SQL Managed Instance
- AWS RDS SQL Server
- GCP SQL Server

`sqlpackage` クライアントユーティリティの推奨バージョンは 19.2 (ビルド: 162.0.52) です。

ダウンロード場所 https://docs.microsoft.com/ja-jp/sql/tools/
/sqlpackage-download?view=sql-server-ver15

https://packages.microsoft.com/rhel/7/prod/msodbcsql17-17.9.1.1-1.x86_64.rpm

https://packages.microsoft.com/rhel/7/
prod/unixODBC-2.3.7-1.rh.x86_64.rpm

インストールするには、端末で次のコマンドを実行します。

1. `cd ~`
2. `mkdir sqlpackage`
3. `unzip ~/Downloads/sqlpackage-linux-<version string>.zip -d ~/sqlpackage`
4. `echo "export PATH=¥"¥$PATH:$HOME/sqlpackage¥""">> ~/.bashrc`
5. `chmod a+x ~/sqlpackage/sqlpackage`
6. `source ~/.bashrc`

メモ: `sqlpackage` がデフォルトのパス変数として追加されていることを確認します。`sqlpackage` が見つからないことを通知するエラーが引き続き発生する場合は、メディアサーバーで NetBackup サービスを再起動します。

---

7. `sqlpackage`
8. `rpm -ivh unixODBC-2.3.7-1.rh.x86_64.rpm`
9. `rpm -ivh msodbcsql17-17.10.2.1-1.x86_64.rpm`

エラーが引き続き表示される場合: `sqlpackage` クライアントユーティリティが指定のホストに存在しません。パス `/usr/bin/sqlpackage` に `sqlpackage` のソフトリンクを作成します。

例:

`sqlpackage` が `/root/sqlpackage/sqlpackage` にある場合は、ソフトリンクを作成し、次のようにバックアップを実行します。

```
ln -s /root/sqlpackage/sqlpackage/usr/bin/sqlpackage
```

RHEL 9 ユーザーは、次の追加手順を実行します。

1. 次のリンクから Microsoft.NETCore.App.Runtime.linux-x64 をダウンロードします。

   https://www.nuget.org/api/v2/package/Microsoft.NETCore.App.Runtime.linux-x64/6.0.10

   ファイル `microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg` を見つけます。
2. 7zip のような解凍ツールを使用してファイルを抽出します。
3. 移動先:

   microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg¥runtimes¥linux-x64¥lib¥net6.0¥
4. そこから、`System.Security.Cryptography.X509Certificates.dll` ファイルを、*sqlpackage* クライアントユーティリティタスクのインストールの手順 2 で作成した `~/sqlpackage` フォルダにコピーします。

10.1.1 NetBackup のセットアップで 10.1 メディアサーバーを外部メディアサーバーとして接続する場合、10.1 メディアサーバーで次の手順を実行します。

BYO NetBackup セットアップの場合:

- 次のコマンドを実行します。

  `mkdir -p <backup and restore ushare export path>`
- `/etc/nfsmount.conf` ファイルで、NFS の `Defaultvers` 値を確認します。
  - `Defaultvers` の値が `nfs3` の場合、`nolock` オプションを使用してバックアップをマウントし、ushare パスをリストアします。例: `mount <ushare mount path> <ushare export path> -o nolock`
  - `Defaultvers` が `nfs4` の場合、`nolock` オプションを使用せずにバックアップをマウントし、ushare パスをリストアします。

AKS 環境と EKS 環境に配備された NetBackup の場合:

- 次のコマンドを実行します。

  `mkdir -p <backup and restore ushare export path>`
- `/etc/nfsmount.conf` ファイルで、NFS の `Defaultvers` 値を確認します。
  - `Defaultvers` の値が `nfs3` の場合、`nolock` オプションを使用してバックアップをマウントし、ushare パスをリストアします。例: `mount <ushare mount path> <ushare export path> -o nolock`
  - `Defaultvers` の値が `nfs4` の場合、`nolock` オプションを使用せずに v4 バージョンのバックアップをマウントし、ushare パスをリストアします。

PostgreSQL クライアントユーティリティのインストール

次のデータベースを保護するには、このユーティリティをインストールする必要があります。

- Azure PostgreSQL シングルサーバーおよびフレキシブルサーバー
- AWS RDS PostgreSQL
- AWS RDS Aurora PostgreSQL
- GCP PostgreSQL

PostgreSQL クライアントユーティリティの推奨バージョンは 15.3 です。

ダウンロード場所
RHEL 7 https://download.postgresql.org/pub/repos/yum/15/redhat/rhel-7-x86_64/
RHEL 8 https://download.postgresql.org/pub/repos/yum/15/redhat/rhel-8-x86_64/
RHEL 9 https://download.postgresql.org/pub/repos/yum/15/redhat/rhel-9-x86_64/

インストールするには、端末で次のコマンドを実行します。

1. `rpm -ivh postgresql15-libs-15.3-1PGDG.rhel7.x86_64.rpm`
2. `rpm -ivh postgresql15-15.3-1PGDG.rhel7.x86_64.rpm`

メモ: RHEL 8 と 9 上の `postgresql15-15.3-1PGDG.rhel8.x86_64.rpm` には、`lz4` 圧縮パッケージと `libicu` が必要です。

MongoDB クライアントユーティリティのインストール

Azure Cosmos DB for MongoDB データベースを保護するには、このユーティリティをインストールする必要があります。

MongoDB クライアントユーティリティの推奨バージョンは 100.10.0 です。

ダウンロード場所 https://www.mongodb.com/try/download/database-tools/releases/archive

インストールするには、ターミナルで次のコマンドを実行します。

```
rpm -ivh mongodb-database-tools-rhel70-x86_64-100.9.4.rpm
```

さまざまな配備のストレージの構成

このセクションでは、さまざまな NetBackup 配備のストレージを構成する方法について説明します。

MSDP クラウド配備の場合

MSDP ストレージターゲットはメディアサーバーを使用します。ネイティブクライアントユーティリティをメディアサーバーにインストールし、そのメディアサーバーを PaaS 作業負荷に接続します。

MSDP クラウドボリュームストレージの場合、NetBackup はユニバーサル共有アクセラレータを使用して、DMC (データムーバーコンテナ) を介して PaaS 資産を保護します。

ユニバーサル共有アクセラレータは、DMC 内に一時メタデータを格納するための永続的なストレージとして、最小 500 GB のストレージ領域を必要とします。このストレージパスは、MSDP ストレージサーバーで使用されているものと同じである必要があります。

Kubernetes の配備の場合

次の場合を検討します。

- ディスクベースのストレージクラスと削除ポリシーのストレージクラスを使用して永続ボリューム要求を作成し、ストレージパスのコンテナに接続します。
- デフォルトのストレージサイズが 600 Gi のストレージのデフォルトストレージクラスを使用することをお勧めします。ストレージクラスまたはストレージサイズを変更するには、次のように Kubernetes 配備の `pdconf` 構成マップを更新する必要があります。

```
STORAGE_CLASS=<disk-based storage class>
STORAGE_SIZE=<pv size>
```

VM ベースの BYO 配備の場合

次の場合を検討します。

- NetBackup Snapshot Manager のパス :`/datamover_storage` に 600 GB のストレージがある新しいディスクをマウントします。
- 各datamoverコンテナは、マウントされたディスクパスにディレクトリを作成し、ストレージパスとして symlink を作成します。このパスは、datamoverコンテナ内にストレージパスとして表示されます。このパスは、ユニバーサル共有アクセラレータ操作の一時ストレージの MSDP ストレージパスと同じです。

配備で利用可能な十分なストレージ領域がない場合は、ストレージ要件を上書きできます。次を実行します。

1. `/cloudpoint/openv/netbackup/vpfs_override_parameters.json` に移動します。
2. `CloudCacheSize` パラメータを、利用可能なストレージサイズ (GB 単位) で更新します。

```
{
"DataTransferManagementOptions": {
"CloudCacheSize": 200
}
}
```

インスタントアクセス用のストレージサーバーの構成

インスタンスアクセスをサポートするためにストレージサーバーに必要な構成を次に示します。

1. NFS と NGINX がインストールされていることを確認します。
2. 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と同じである必要があります。対応する RHEL yum ソース (EPEL) からインストールします。
3. `policycoreutils` と `policycoreutils-python` 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ます。
   - `semanage port -a -t http_port_t -p tcp 10087`
   - `setsebool -P httpd_can_network_connect 1`
4. どのマウントポイントも、ストレージサーバーの `/mnt` フォルダを直接マウントしていないことを確認します。マウントポイントをサブフォルダのみにマウントします。
5. 次のコマンドを使用して、`selinux` の `logrotate` 権限を有効にします。

   ```
   semanage permissive -a logrotate_t
   ```

PaaS 作業負荷の増分バックアップについて

NetBackup は、Azure SQL Server、Azure SQL Managed Instance、AWS RDS Oracle、GCP SQL Server の作業負荷の差分増分バックアップをサポートします。増分バックアップでは、NetBackup のバックアップ処理時間が大幅に短縮されます。この方式で、NetBackup は最後の完全バックアップ以降に変更されたデータだけをバックアップします。

差分増分バックアップは、Azure SQL Server、GCP SQL Server、AWS RDS Oracle、Azure SQL Managed Instance で変更データキャプチャ機能が有効になっている作業負荷でのみサポートされます。

PaaS 作業負荷の増分バックアップを使用する場合のガイドライン:

- ポリシーで、増分バックアップより長い保持期間を完全バックアップに割り当ててください。完全なリストアを行うには、前回の完全バックアップ、およびそれ以降のすべて

の差分増分バックアップが必要です。増分バックアップの前に完全バックアップの期限が切れると、すべてのファイルをリストアできない場合があります。

- 完全バックアップと増分バックアップには 1 つのストレージを使用します。
- 増分バックアップの長期コピーは作成しないでください。
- ランダム増分バックアップイメージを期限切れにしないでください。期限切れにすると、データ損失のためにアプリケーションの不整合が発生する可能性があります。NetBackup は、前回の完全バックアップと、後続のすべての増分バックアップに依存します。
- 複製中に、完全バックアップのコピーと増分バックアップのコピーがターゲットストレージに複製されていることを確認します。以前の完全イメージまたは増分イメージのいずれかが失われると、データが失われる可能性があります。
- インポート中に、完全バックアップのコピーとすべての増分バックアップのコピーが一緒にインポートされていることを確認します。以前の依存する完全イメージまたは増分イメージのいずれかが失われると、エラーが発生する可能性があります。
- 差分増分バックアップは、RDS によってスキーマの変更が管理されている場合にのみ、AWS RDS Oracle でサポートされます。

Azure MySQL サーバーの増分バックアップの構成

NetBackup は、Azure MySQL Server の完全バックアップと差分増分バックアップのスケジュールを両方ともサポートします。完全バックアップの実行中、NetBackup はすべてのユーザーデータベースの論理ダンプを取得します。増分バックアップの実行中、NetBackup は、後続の増分バックアップ間で、MySQL サーバーで生成されるバイナリログをダウンロードします。データベースをリストアする際、NetBackup は完全バックアップでデータベースを作成し、バイナリログを時系列順に適用します。

サーバーパラメータの構成

Azure ポータルで次のパラメータを構成します。

表 2-4　　増分バックアップのパラメータ

パラメータ	説明	推奨事項
binlog_expire_logs_seconds	バイナリログファイルがパージされるまでに待機する秒数。	この値は、スケジュール内のバックアップの間隔より大きくする必要があります。サーバー上のバイナリログが、後続の増分バックアップ間でパージされないようにします。

パラメータ	説明	推奨事項
log_bin	サーバーでのバイナリログの状態 (有効 (ON) または無効 (OFF))。	増分バックアップの場合、このパラメータは ON に設定する必要があります。バイナリログファイルの変更をキャプチャします。
log_bin_trust_function_creators	この変数は、バイナリログが有効な場合に適用されます。これにより、ストアド関数の作成者は信頼され、安全でないイベントをバイナリログに書き込むストアド関数を作成できます。	データベースをサーバーにリストアするには、このパラメータを ON に設定します。
default_table_encryption	ENCRYPTION 句を指定せずにスキーマおよび一般的な表領域を作成した場合に、それらに使用するデフォルトの暗号化設定を指定します。	データベースをサーバーにリストアするには、このパラメータを ON に設定します。
max_binlog_cache_size	トランザクションにこの指定値より多くのメモリが必要な場合、サーバーはストレージエラーを生成します。	この値がトランザクションの最大合計サイズに対応できることを確認します。このパラメータのデフォルト値は維持することをお勧めします。

PaaS 作業負荷のアーカイブ REDO ログのバックアップについて

NetBackup は、AWS RDS Oracle 作業負荷のアーカイブログのバックアップをサポートします。アーカイブバックアップにより、完全バックアップと増分バックアップの処理時間が大幅に短縮されます。

この方式で、NetBackup は最後の完全または増分バックアップ以降に変更されたデータをバックアップします。

PaaS 作業負荷のアーカイブログバックアップを使用する場合のガイドライン:

- 保護計画では、アーカイブログのバックアップ間隔を 24 時間より短いままにしておくことをお勧めします。
- ポリシーの作成時に、完全バックアップまたは増分バックアップには、アーカイブログバックアップより長い保持期間を割り当てます。完全なリストアを行うには、前回の完全バックアップ、それ以降のすべての増分バックアップ、およびそれ以降のすべてのアーカイブログバックアップが必要です。完全バックアップの期限が、それ以降のバックアップの前に切れると、すべてのファイルをリストアできない場合があります。

- 完全バックアップ、増分バックアップ、およびアーカイブバックアップには単一のストレージを使用します。
- ランダムアーカイブバックアップイメージを期限切れにしないでください。期限切れにすると、データ損失のためにアプリケーションの不整合が発生する可能性があります。NetBackup は、リストアを正常に実行するために、前回の完全バックアップと、後続のすべての増分バックアップおよびアーカイブバックアップに依存します。

PaaS 作業負荷の自動イメージレプリケーションについて

NetBackup は、ローカルまたはクラウドでホストされているターゲット LSU への AIR (自動イメージレプリケーション) をサポートします。LSU のターゲットドメインには、1 対 1 の AIR モデルを使用する標準またはアーカイブストレージクラスまたは階層が必要です。

現在、Amazon Redshift の作業負荷は AIR ではサポートされていません。

保護計画を使用して AIR を構成できます。保護計画にスケジュールを追加するときに、[このバックアップをレプリケートする (Replicate this backup)]オプションを選択します。保護計画のスケジュールで AIR が有効になっている場合は、その保護計画のすべてのスケジュールで有効にすることをお勧めします。

メモ: アーカイブ階層ストレージクラス LSU の場合、完全バックアップスケジュールのみがサポートされます。

ストレージとしてストレージライフサイクルポリシーを選択することで、ポリシーを使用して AIR を構成することもできます。

PaaS 資産の検出

NetBackup では、PaaS データベース資産を検出、保護、リストアできます。Microsoft Azure がバックアップする Azure SQL データベースおよび Azure SQL 管理対象データベースの資産を検出およびリストアできます。サポートされるバックアップモードは、指定した時点のバックアップと長期保持用バックアップです。

メモ: NetBackup Snapshot Manager (以前は CloudPoint) をバージョン 10.0 から 10.1 にアップグレードした場合。カスタム役割を持つすべてのユーザーの PaaS 資産は[PaaS]タブで削除済みとしてマークされます。資産にはリカバリポイントが表示されず、同じ名前の新しい資産が表示されます。古い資産は、後続のスケジュール済み資産のクリーンアップ後に[PaaS]タブから削除されます (デフォルトの期間は 30 日)。この問題を回避するには、すべての新しい資産の権限を既存の RBAC の役割に再割り当てするか、新しいカスタム役割を作成します。詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

メモ: Snapshot Manager のクラウドプラグイン構成を Azure サービスプリンシパルから Azure 管理 ID に変更した場合、以前に検出された PaaS 資産の状態は削除済みとして表示されます。NetBackup Snapshot Manager は、削除された資産を 24 時間ごとに除去します。スケジュールされたクリーンアップの前にバックアップまたはリカバリを実行する場合は、ベリタステクニカルサポートにお問い合わせください。

PaaS 資産を検出するには:

1. Snapshot Manager を追加します。p.15 の「Snapshot Manager の追加」を参照してください。
2. Microsoft Azure、GCP、または AWS をプロバイダとして追加します。p.15 の「Snapshot Manager のクラウドプロバイダの追加」を参照してください。
3. 検出を実行します。p.21 の「Snapshot Manager の資産の検出」を参照してください。

   検出が完了すると、[クラウド (Cloud)]作業負荷の[PaaS]タブで、検出されたすべての資産を検索できます。

   検出されたすべての AWS RDS 資産は、[アプリケーション (Applications)]タブに表示されます。RDS インスタンスは、プロバイダによるスナップショットベースのバックアップおよび NetBackup によって管理されるバックアップをサポートします。

   NetBackup は、[PaaS]タブに一覧表示されているすべての資産を管理および保護できます。また、Azure SQL データベースおよび Azure SQL 管理対象データベースの資産は、Microsoft Azure でバックアップできます。

メモ: 同じ名前の PaaS 資産を定期的に作成および削除しているときに、検出後に PaaS 資産を削除すると、次回の定期的な検出が実行されるまで、Web UI には古いデータが表示されます。

PaaS 資産の表示

PaaS 資産を表示するには:

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [PaaS]タブに、利用可能な資産が表示されます。RDS 資産は[アプリケーション (Applications)]タブに表示されます。

   表示された資産では、[保護の追加 (Add protection)]、[今すぐバックアップ (Backup now)]、[クレデンシャルの管理 (Manage credential)]といった操作を実行できます。

   DynamoDB 資産と Amazon Redshift 資産の場合、[クレデンシャルの管理 (Manage credentials)]オプションは利用できません。

   削除された資産の場合は、クレデンシャルのみを管理できます。

PaaS のクレデンシャルの管理

[クラウド (Cloud)]作業負荷の[PaaS]と[アプリケーション (Applications)]タブに一覧表示されているデータベースにクレデンシャルを追加できます。NetBackup の中央の[クレデンシャル管理 (Credential management)]コンソールから PaaS のクレデンシャルを追加、編集、削除できます。GCP BigQuery、DynamoDB、Amazon Redshift、RDS Custom for Oracle、RDS Custom for SQL、AWS DocumentDB、AWS Neptune などの一部の作業負荷は、NetBackup を介したクレデンシャル管理をサポートせず、プロバイダのクレデンシャルを活用します。

データベースに適用されているクレデンシャル名の表示

[PaaS]タブの[クレデンシャル名 (Credential name)]列に、データベース用に構成された名前付きクレデンシャルを表示できます。特定の資産に対してクレデンシャルが構成されていない場合は、このフィールドは空白です。

PaaS データベースのクレデンシャルを表示するには:

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]、[PaaS]タブの順に選択します。
2. データベース一覧表の上の[列を表示または非表示 (Show or hide columns)]をクリックします。
3. [クレデンシャル名 (Credential name)]を選択し、クレデンシャル名の列を表示します。

データベースへのクレデンシャルの追加

[PaaS]タブに一覧表示されているデータベースのクレデンシャルを追加または変更できます。

クレデンシャルを追加または変更するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックします。

   [PaaS]タブに、利用可能な資産が表示されます。RDS 資産は[アプリケーション (Applications)]タブに表示されます。

2. テーブルでデータベースを選択し、[クレデンシャルの管理 (Manage credentials)]をクリックします。

3. 検証ホストを選択します。検証ホストは、PaaS 作業負荷と接続している RHEL メディアサーバー、または NetBackup Snapshot Manager である必要があります。NetBackup Snapshot Manager を使用すると、Snapshot Manager ホストに datamoverコンテナが追加されます。

   既存のクレデンシャルを追加することも、データベース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から選択 (Select from existing credentials)]オプションを選択し、下のテーブル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。
   - アカウントの新しいクレデンシャルを追加するには、[クレデンシャルを追加 (Add credentials)]を選択して[次へ (Next)]をクリックします。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。[サービスクレデンシャル (Service credentials)]で次の手順を実行します。
     - AWS IAM、Azure のシステム管理認証とユーザー管理認証を使用するには、[役割ベースのデータベース認証 (サポート対象のデータベースサービスに適用可能)(Role based database authentication (Applicable for supported database service))]を選択します。
       - Amazon RDS 資産に対してのみ[IAM データベース認証 (Amazon RDS のみに適用可能)(IAM database authentication (Applicable for Amazon RDS only))]を選択し、[データベースユーザー名 (Database user name)]を指定します。
         p.130 の「IAM データベースユーザー名の作成」を参照してください。

メモ: Snapshot Manager が、必要な権限が付与された IAM ロールを持つクラウドに配備されている場合は、メディアサーバーを同じクラウド環境に配備し、同じ IAM ロールを割り当てる必要があります。そうしないと、AWS 資産のバックアップジョブが失敗します。

メモ: メディアサーバーまたは NetBackup Snapshot Manager インスタンスでインスタンスメタデータサービス (IMDsv2) が有効になっている場合、ホストしている VM の *HttpPutResponseHopLimit* パラメータが *2* に設定されていることを確認します。*HttpPutResponseHopLimit* パラメータの値が *2* に設定されていない場合、VM に作成されたメディアサーバーまたは NetBackup Snapshot Manager コンテナからメタデータを取得する AWS 呼び出しが失敗します。IMDsv2 サービスについて詳しくは、Amazon のマニュアルの「IMDSv2 の使用」を参照してください。

- 必要に応じて、[Azure システム管理 ID 認証 (Azure System Managed Identity authentication)]または[Azure ユーザー管理 ID 認証 (Azure User Managed Identity authentication)]を選択します。データベースのユーザー名を入力し、[次へ (Next)]をクリックします。
  管理 ID 認証を使用してバックアップおよびリストア操作を実行するには、ソースデータベースサーバーとターゲットデータベースサーバーに AAD 管理者を構成する必要があります。
  p.131 の「システムまたはユーザー管理 ID のユーザー名の作成」を参照してください。

  メモ: 必要な権限を持つ管理 ID が関連付けられてクラウドに Snapshot Manager が配備されている場合は、メディアサーバーに同じ ID を関連付けます。AKS と EKS の配備では、VM スケールセットに同じ管理 ID を関連付けます。

- [パスワード認証 (Password authentication)]を選択し、データベースサーバーのユーザー名とパスワードを指定します。
  AWS RDS Oracle を使用している場合は、AWS RDS Oracle マルチテナント配備アーキテクチャを使用するために、ユーザー名を *username@tenantdatabasename* の形式にする必要があります。
  Azure Cosmos DB for NoSQL を使用している場合は、次の手順を実行します。
  - ユーザー名は、Azure ポータルの[設定]、[キー]、[URI]で確認できる[アカウント URI]です。
  - パスワードは、Azure ポータルの[設定]、[キー]、[主キー]または[2 次キー]の順に選択して確認できる[主キー]または[2 次キー]です。
  - 読み取りキーはバックアップのみを取ることができます。読み書き可能なキーを使用してデータベースをリストアすることをお勧めします。

  Azure Cosmos DB for MongoDB を使用している場合は、次の手順を実行します。

- ユーザー名は、Azure ポータルの［設定］、［接続文字列］、［URI］で確認できるアカウント名です。
- パスワードは、Azure ポータルの［設定］、［キー］、［主キー］または［2 次キー］の順に選択して確認できる［主キー］または［2 次キー］です。
- 読み取りキーはバックアップのみを取ることができます。読み書き可能なキーを使用してデータベースをリストアすることをお勧めします。

［次へ (Next)］をクリックします。

- 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。役割に新しい権限を追加する方法:
  - ［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。
  - ［保存 (Save)］をクリックします。

4 ［次へ (Next)］をクリックしてクレデンシャルの作成を終了します。

クレデンシャルについて、およびクレデンシャルを編集または削除する方法について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

IAM データベースユーザー名の作成

IAM ユーザー名を作成するには:

1 RDS DB インスタンスで IAM DB 認証を有効にします。

2 マスターログイン (rds_iam) を使用してデータベースユーザーを作成します。

- MySQL の場合、マスターログイン (rds_iam) を使用してユーザー名を作成します。
  - mysql --protocol=tcp --host=instance_fqdn --user=admin -p --port=3306
  - CREATE USER iamuser IDENTIFIED WITH AWSAuthenticationPlugin as 'RDS';
  - GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, LOCK TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT, TRIGGER ON *.* '<db_user>'@'%';
- PostgreSQL の場合、サーバー上でユーザーを作成します。
  - psql -h instance_fqdn -U postgres
  - CREATE USER iamuser WITH LOGIN;

- GRANT rds_iam TO iamuser;
- ALTER ROLE iamuser WITH LOGIN CREATEDB;
- GRANT rds_superuser TO iamuser;

3 NetBackup メディアサーバーに割り当てられている IAM ロールに、RDS ポリシーを割り当てます。

詳しくは、最新バージョンの『NetBackup Snapshot Manager インストールおよびアップグレードガイド』の「NetBackup Snapshot Manager に必要な AWS アクセス権」セクションを参照してください。

システムまたはユーザー管理 ID のユーザー名の作成

Azure SQL Server と Managed Instance の場合

次の構成のいずれかを実行します。

管理対象 ID ユーザーを AAD 管理者として構成します。

- SQL Server または Managed Instance で AAD 管理者を設定します。
- [Settings]、[Microsoft Entra ID]、[Set admin]の順に移動します。システム割り当てまたはユーザー割り当ての管理対象 ID を検索して設定し、保存します。

メモ: システム割り当ての管理対象 ID と AAD 管理者の権限を構成したメディアサーバーのみが、バックアップとリストアを実行できます。

SSMS クライアントを使用して、データベースに管理対象 ID ユーザーを作成します。

- ユーザーを作成するために SQL Server 用 AAD 管理者を設定するには、[Settings]、[Active Directory admin]、[Set admin]の順に移動します。ユーザー用に Active Directory を選択して保存します。
- SQL データベースまたは管理対象データベースにログインして、そのデータベースの下にユーザーを作成します。

```
CREATE USER [<managed_identity>] FROM EXTERNAL PROVIDER;
ALTER ROLE db_owner ADD MEMBER [<managed_identity>];
```

- SQL Server でそのユーザーのログイン権限を指定し、次のコマンドを実行します。

```
# CREATE USER [<managed_identity>] FROM EXTERNAL PROVIDER;
# ALTER ROLE loginmanager ADD MEMBER [<managed_identity>];
```

メモ: システムで割り当てられた管理対象 ID を使用して、データベースと通信するすべてのメディアサーバーのユーザーを作成する必要があります。

メモ: データベースをリストアするには、ターゲットサーバーで管理対象 ID ユーザーを AAD 管理者として構成する必要があります。

MySQL の場合

- MySQL サーバーの AAD 管理者を構成するには、ユーザーを作成します。[Settings]、[Active Directory admin]、[Set admin]の順に移動します。Active Directory ユーザーを選択して保存します。
- Azure CLI を使用して管理対象 ID のクライアント ID を取得します。次のコマンドを実行します。

```
# az ad sp list --display-name <managed_identity> --query [*].appId
 --out tsv
```

- Azure CLI を使用して、ログオンのためのアクセストークンを生成します。次のコマンドを実行します。

```
# az account get-access-token --resource-type oss-rdbms
```

- AAD 管理ユーザーとアクセストークンを使用してログオンします。次のコマンドを実行します。

```
# mysql -h <server name> --user <user name>
--enable-cleartext-plugin --password=<token>
```

- 管理対象 ID ユーザーを作成し、権限を付与します。次のコマンドを実行します。

```
# SET aad_auth_validate_oids_in_tenant = OFF;
  # CREATE AADUSER '<db_user>' IDENTIFIED BY
'<Generated_client_id>';
  # GRANT USAGE, DROP, SELECT, CREATE, SHOW VIEW, EVENT, LOCK
TABLES , ALTER, CREATE VIEW, INSERT, REFERENCES, ALTER ROUTINE,
PROCESS ON *.* TO '<db_user>'@'%'
```

PostgreSQL の場合

- PostgreSQL サーバーの AAD 管理者を構成するには、ユーザーを作成します。[Settings]、[Active Directory admin]、[Set admin]の順に移動します。Active Directory ユーザーを選択して保存します。

- 管理対象 ID のクライアント ID を取得します。

```
 # az ad sp list --display-name <managed_identity>  --query
[*].appId --out tsv
```

- ログインに必要なアクセストークンを生成します。次のコマンドを実行します。

```
# az account get-access-token --resource-type oss-rdbms
```

- 生成されたトークンのパスワードをエクスポートします。次のコマンドを実行します。

```
# export PGPASSWORD=<token>
```

- AAD 管理ユーザーとアクセストークンを使用してログインします。次のコマンドを実行します。

```
 # psql “host=<host name> port=5432 dbname=<dbname> user=<user
name> sslmode=require”
```

- ユーザーを作成し、権限を付与するには、次のコマンドを実行します。

```
# SET aad_auth_validate_oids_in_tenant = OFF;
  # CREATE ROLE <db_user> WITH LOGIN PASSWORD '<client_id>' IN
ROLE azure_ad_user;
  # GRANT azure_pg_admin TO <db_user>;
  # ALTER USER smipguser CREATEDB;
  # ALTER USER smipguser Replication;
```

メモ: MySQL Flexible Server ではユーザー管理 ID のみがサポートされます。PostgreSQL Flexible Server では、管理対象 ID のサポートは利用できません。

Azure Cosmos DB for NoSQL の場合

1. Azure ポータルにログオンします。
2. Cosmos DB 組み込みデータコントリビュータの役割を管理対象 ID に割り当てるには、次のコマンドを実行します。

```
# az cosmosdb sql role assignment create -a <Account_Name> -g
<Resource_Group_Name> -s "/" -p <Object_ID/Principle_ID> -d
00000000-0000-0000-0000-000000000002
```

以下はその説明です。

- *Account_Name* は、Azure Cosmos アカウント名です。

- *Resource_Group_Name* は、アカウントのリソースグループ名です。
- *Object_ID/Principle_ID* は、管理対象 ID オブジェクトまたはプリンシパル ID です。
- *00000000-0000-0000-0000-000000000002* は、Cosmos DB 組み込みデータコントリビュータの役割 ID です。

データベースユーザーの権限の構成

MySQL の場合

マスターログインを使用してデータベースユーザーを作成し、次の権限を付与します。

- mysql --protocol=tcp --host=instance_fqdn --user=admin -p --port=3306
- CREATE USER dbuser IDENTIFIED BY '<password>';
- GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, LOCK TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, SHOW_ROUTINE, EVENT, TRIGGER ON *.* TO `dbuser`@'%' WITH GRANT OPTION;
- Azure MySQL の増分保護の場合は、次の追加の権限を追加します。
  GRANT SET_USER_ID, REPLICATION CLIENT, SESSION_VARIABLES_ADMIN, REPLICATION_APPLIER ON *.* TO `dbuser`@'%' WITH GRANT OPTION;

PostgreSQL の場合

サーバーの下にデータベースユーザーを作成し、次の権限を付与します。

- psql -h instance_fqdn -U postgres
- CREATE USER dbuser WITH PASSWORD '<password>' CREATEDB;
- (AWS RDS PostgreSQL の場合) GRANT rds_superuser TO dbuser;
- (AZURE PostgreSQL の場合) GRANT azure_pg_admin TO dbuser;
- (GCP PostgreSQL の場合) GRANT cloudsqlsuperuser TO dbuser;

SQL Server の場合

サーバーの下にデータベースユーザーを作成し、次の権限を付与します。

- サーバーにログインを作成します。
  CREATE LOGIN dbuser WITH PASSWORD='<password>'
- サーバーでデータベースのユーザーを作成します。
  - CREATE USER [dbuser] FOR LOGIN [dbuser]

- ALTER ROLE [db_owner] ADD MEMBER [dbuser]

メモ: データベースユーザーは、どのデータベース拒否の役割にも含まれていない必要があります。例: db_denydatareader および db_denydatawriter。

PaaS 資産への保護の追加

PaaS 資産を検出したら、[クラウド (Cloud)] 作業負荷の[アプリケーション (Applications)] タブまたは[PaaS]タブで保護を追加できます。

RDS Custom for Oracle、RDS Custom for SQL、AWS DocumentDB、および AWS Neptune の資産の場合、保護の追加オプションは利用できません。

PaaS 資産に保護を追加するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックします。
2. AWS RDS でサポートされているデータベース資産を保護するには、[アプリケーション (Applications)]タブをクリックします。その他の PaaS 資産の場合は、[PaaS] タブをクリックします。
3. 保護する資産にクレデンシャルがあるかどうかを確認します。

   p.127 の「データベースに適用されているクレデンシャル名の表示」を参照してください。。

   [クレデンシャル名 (Credential name)]列が空の場合、資産にクレデンシャルを割り当てる必要があります。

   p.128 の「データベースへのクレデンシャルの追加 」を参照してください。
4. 資産に保護を追加するには、資産を選択して[保護の追加 (Add protection)]をクリックします。

   ほとんどの操作を実行できるようにするには、資産にクレデンシャルが割り当てられている必要があります。たとえば、資産の保護計画への割り当て、今すぐバックアップの実行などが該当します。
5. 保護計画を選択し、[次へ (Next)]をクリックします。
6. 構成の設定を確認し、[保護する (Protect)]をクリックします。

Redshift クラスタ、AWS DocumentDB、および AWS Neptune の資産は、保護計画を使用して保護されません。ポリシーを使用して保護できます。p.39 の「クラウド資産のポリシーの管理」を参照してください。

今すぐバックアップの実行

このオプションを使用すると、選択した資産のワンタイムバックアップを作成できます。このバックアップは、今後のバックアップ、またはスケジュールバックアップには影響しません。

次の点に注意してください。

- Azure SQL データベース、GCP SQL Server、および AWS RDS Oracle の増分バックアップの場合、バックアップ形式が差分増分の保護計画で資産が保護されている場合でも、NetBackup は完全バックアップを実行します。
- アーカイブ REDO ログ形式のスケジュールの場合、NetBackup は、保護計画で指定した内容に関係なく、今すぐバックアップの完全バックアップを実行します。
- Redshift クラスタ、AWS DocumentDB、および AWS Neptune の資産の場合、今すぐバックアップオプションは利用できません。ポリシーの手動バックアップを使用してバックアップを開始できます。

今すぐバックアップを実行するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックします。

   AWS RDS でサポートされているデータベース資産をバックアップするには、[アプリケーション (Applications)]タブをクリックします。その他の PaaS 資産の場合は、[PaaS]タブをクリックします。

   メモ: ユーザーが作成したデータベースを表示して保護できます。システムデータベースのバックアップとリストアを実行するには、クラウドプロバイダのスーパーユーザー権限が必要であるため、システムデータベースは表示および保護されません。

2. 資産を選択し、[保護の追加 (Add protection)]をクリックします。
3. 必要な保護計画を選択し、[バックアップの開始 (Start backup)]をクリックします。

   バックアップジョブの状態は、アクティビティモニターに表示されます。

   データベースエージェントは、メディアサーバー (AKS および EKS 環境で NetBackup が配備されている場合はコンテナ) 内からデータベースにアクセスし、メディアサーバー (バックアップホスト) 上のユニバーサル共有パスの NFS マウントを実行します。

3

クラウド資産のリカバリ

この章では以下の項目について説明しています。

クラウド資産のリカバリ

スナップショットコピー、バックアップコピー、または複製コピーから、AWS、Azure、Azure Stack Hub、OCI、GCP VM の資産をリストアできます。AWS の場合は、レプリカコピーからもリストアできます。AWS EC2 VM または Azure VM からオンプレミスの VMware VM にバックアップイメージをリストアすることもできます。

VM のリストア中、NetBackup には、元のバックアップまたはスナップショットコピーの特定のパラメータを変更するためのオプションが表示されます。これには、VM 表示名の変更、VM の電源オプションの変更、リストア時のタグ関連付けの削除、代替ネットワークへのリストアなどのオプションが含まれます。また、代替構成、異なるゾーン、異なるサブスクリプションに VM を、異なるリソースグループに VM またはディスクをリストアできます。

- GCP の場合: ファイアウォールルールを選択します。
- Azure の場合: ネットワークセキュリティグループを選択します。
- AWS の場合: セキュリティグループを選択します。
- OCI の場合: ネットワークセキュリティグループを選択します。

VM のリカバリ前チェックについて

リカバリ前チェックは、リストアを開始する前に、リストアが失敗する可能性を示します。リカバリ前チェックでは、次の項目が確認されます。

- サポート対象の文字の使用と表示名の長さ
- 宛先ネットワークの存在。
- (Azure および Azure Stack Hub) VM とディスクに選択したリソースグループの存在。
- ソース VM スナップショットの存在 (スナップショットからのリストアに適用可能)。
- ファイル `/cloudpoint/azurestack.conf` に追加されたステージング場所の存在 (Azure Stack Hub のバックアップからのリストアに適用可能)
- 同じ表示名を持つ VM の存在
- Snapshot Manager との接続とクラウドクレデンシャルの検証
- 選択した暗号化キーの有効性。

クラウド資産のリストアでサポートされるパラメータ

次の表に、異なるクラウドプロバイダの資産をリストアする際に変更できるさまざまなパラメータの概略を示します。

表 3-1 Azure、Azure Stack Hub、GCP、OCI、AWS のスナップショットとバックアップコピーでサポートされるパラメータ

パラメータ	スナップショットコピー				バックアップコピー			
	Azure	Azure Stack Hub	GCP と AWS	OCI	Azure	Azure Stack Hub	GCP と AWS	OCI
VM の表示名を変更する	Y	Y	Y	Y	Y	Y	Y	Y
VM の電源状態を変更する	Y	Y	Y	Y	Y	Y	Y	Y

タグの関連付けを削除する	Y	Y	Y	Y	Y	Y	Y	Y
異なるネットワークにリストアする	Y	Y	Y	Y	Y	Y	Y	Y
サブスクリプション ID					Y	Y	Y	
リソースグループを変更する	Y	Y			Y	Y		
VM の領域を変更する					Y	Y	Y	
プロバイダの構成を変更する					Y	Y		
ディスクのリソースグループを変更する	Y	Y			Y	Y		

ゾーン/可用性ドメイン	Y		Y	Y	Y		Y	Y
セキュリティグループ、ファイアウォールルール、ネットワークセキュリティグループ	Y	Y	Y	Y	Y	Y	Y	Y
ディスクの暗号化の編集	Y		Y	Y	Y		Y	Y

仮想マシンのリカバリ

VM をリカバリするには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual Machines)]タブをクリックします。

   対応するカテゴリで検出されたすべてのクラウド資産が表示されます。
3. リカバリする保護された資産をダブルクリックします。
4. [リカバリポイント (Recovery points)]タブをクリックします。

   利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。AWS の作業負荷については、レプリカとバックアップイメージが表示されます (利用可能な場合)。

5 [コピー (Copies)]列で、リカバリするコピーをクリックします。バックアップ、スナップショット、レプリカのコピーを表示できます (利用可能な場合)。[リカバリ (Recover)]をクリックします。リストアするコピーを選択しない場合は、プライマリコピーが選択されます。

6 [仮想マシンのリストア (Restore Virtual Machine)]をクリックします。

7 リカバリターゲットのページで、次の操作を行います。

バックアップコピーをリストアする場合は、必要に応じてこれらのパラメータの値を変更します。

- [構成 (Configuration)]: 代替構成にリストアするには、ドロップダウンから構成を選択します。
- [領域 (Region)]: 代替領域にリストアするには、ドロップダウンから領域を選択します。
- [サブスクリプション (Subscription)]: 代替サブスクリプションにリストアするには、ドロップダウンからサブスクリプションを選択しますAzure および Azure Stack Hub のみの場合。
- [リソースグループ (Resource group)]: 代替リソースグループにリストアするには、検索アイコンをクリックし、[リソースグループの選択 (Select resource group)]ダイアログで、必要なリソースグループを選択しますAzure および Azure Stack Hub のみの場合。
- [表示名 (Display name)]: 表示名を変更するには、このフィールドに新しい表示名を入力します。指定した表示名は、リカバリ前チェックで検証されます。

メモ: AWS および OCI の作業負荷を除き、表示名に特殊文字「` ~ ! @ # $ % ^ & * ( ) = + _ [ ] { } ¥¥ | ; : ' ¥" , < > / ?."」は使用できません。

スナップショットのコピーをリストアする場合は、[リソースグループ (Resource group)]と[表示名 (Display name)]のみを指定します。

スナップショットまたはバックアップコピーからの VM のリストア時に、次のように、個々のディスクまたはすべてのディスクから同時に暗号化キーを選択できます。

- [ボリューム (Volume)]を選択し、[暗号化キーを編集する (Edit the encryption key)]オプションをクリックします。

メモ: ADE で暗号化されたディスクの場合、[暗号化キーを編集する (Edit the encryption key)]オプションは無効になります。

[Azure Disk Encryption]列には、ADE 暗号化の状態が表示されます。

- 必要な［暗号化の種類 (Encryption type)］を選択します。
- 必要な暗号化の［キー (Key)］を選択し、［保存 (Save)］をクリックします。

8 ［次へ (Next)］をクリックします。

9 ［リカバリオプション (Recovery Options)］ページで、次の操作を行います。

- (Azure および AWS の場合のみ) ソース VM と同じネットワーク構成の VM をリストアするには、［ネットワーク構成のリストア (Restore network configuration)］オプションを選択します。
- ネットワーク構成を変更するには、［ネットワーク構成の変更 (Change network configuration)］オプションを選択し、リカバリするターゲットネットワークを選択します。

  次を選択することも可能です。

  - GCP の場合: ファイアウォールルール
  - Azure の場合: ネットワークセキュリティグループ
  - AWS の場合: セキュリティグループ
  - OCI の場合: ネットワークセキュリティグループ
- (*GCP の場合のみ*) スナップショットコピーをリストアする場合、別の領域にリストアするには［領域 (Region)］を選択します。そのゾーンで利用可能なネットワークを選択するには、［ネットワーク構成 (Network configuration)］にある検索アイコンをクリックし、リカバリするターゲットネットワークを選択します。リストには、そのゾーンで利用可能なネットワークが表示されます。
- スナップショットコピーをリストアする場合、別のゾーンにリストアするには、［ゾーン (Zone)］または［可用性ドメイン (Availability domain)］を選択します。そのゾーンで利用可能なネットワークを選択するには、［ネットワーク構成 (Network configuration)］にある検索アイコンをクリックし、リカバリするターゲットネットワークを選択します。リストには、そのゾーンまたは可用性ドメインで利用可能なネットワークが表示されます。

  AWS、Azure、OCI、GCP クラウドプロバイダにセキュリティグループ、ネットワークセキュリティグループ、ファイアウォールルールをそれぞれ選択することもできます。

［詳細 (Advanced)］ セクションで、次の操作を行います。

- リカバリ後に VM の電源をオンのままにするには、［リカバリ後に電源をオン (Power on the VM after recovery)］を選択します。
- バックアップまたはスナップショットの作成時に資産に関連付けられているタグを削除するには、［タグの関連付けを削除する (Remove tag associations)］を選択します。

メモ: [タグの関連付けを削除する (Remove tag associations)]オプションを選択しない場合は、資産のタグ値のカンマの前後にスペースを含められません。資産のリストア後、タグ値のカンマの前後のスペースが削除されます。たとえば、タグ名 created_on の値 *Fri, 02-Apr-2021 07:54:59 PM , EDT* は、*Fri,02-Apr-2021 07:54:59 PM,EDT* に変換されます。手動でタグ値を編集し、スペースを元に戻せます。

メモ: ゾーンに[なし (None)]を選択した場合、VM はどのゾーンにも配置されません。ネットワークセキュリティグループ、セキュリティグループ、またはファイアウォールルールに[なし (None)]を選択すると、リストアされた VM にセキュリティルールは適用されません。

10 [次へ (Next)]をクリックします。リカバリ前チェックが開始されます。このステージでは、すべてのリカバリパラメータを検証し、エラー (存在する場合) が表示されます。リカバリを開始する前にエラーを修正できます。

11 [リカバリの開始 (Start recovery)]をクリックします。

[リストアアクティビティ (Restore activity)]タブには、ジョブの進捗状況が表示されます。

VM のプロビジョニング状態が更新中の場合、リカバリジョブは失敗しませんが、状態が更新から成功に変わるまで 5 分間待機の状態になります。

メモ: ADE が有効な VM で、VM のプロビジョニング状態が更新中になっていて拡張機能がインストールされていない場合、VM の作成は失敗し、リソースはクリーンアップされます。

リカバリの状態コードについて詳しくは、次の場所から入手できる『NetBackup 管理者ガイド』または『NetBackup 状態コードリファレンスガイド』を参照してください。

http://www.veritas.com/docs/000003214

アプリケーションとボリュームの元の場所へのリカバリ

GCP では、アップグレード前に作成されたスナップショットをリストアすると、ソースディスクが存在しない場合は、デフォルトのリストアされたディスクである pd 標準が作成されます。

アプリケーションとボリュームを元の場所にリカバリするには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [アプリケーション (Applications)]タブまたは[ボリューム (Volumes)]タブをクリックします。

   対応するカテゴリで検出されたすべてのクラウド資産が表示されます。
3. リカバリする保護された資産をダブルクリックします。
4. [リカバリポイント (Recovery points)]タブをクリックします。カレンダービューで、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が、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。
5. 望ましいリカバリポイントの右上で、[元の場所 (Original location)]を選択します。
6. [リカバリの開始 (Start recovery)]をクリックします。
7. 左側の[アクティビティモニター (Activity monitor)]をクリックして、ジョブ状態を表示します。

アプリケーションとボリュームの代替の場所へのリカバリ

注意事項

- AWS 内の暗号化された VM を代替の場所にリストアする場合、レプリケーション元とレプリケーション先の領域で鍵ペアの名前が同じである必要があります。同じでない場合は、レプリケーション元の領域の鍵ペアと一貫性がある新しい鍵ペアをレプリケーション先の領域で作成してください。

アプリケーションとボリュームを代替の場所にリカバリするには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [アプリケーション (Applications)]タブまたは[ボリューム (Volumes)]タブをクリックします。

   対応するカテゴリで検出されたすべてのクラウド資産が表示されます。
3. リカバリする保護された資産をダブルクリックします。
4. [リカバリポイント (Recovery points)]タブをクリックします。カレンダービューで、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が、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。
5. 望ましいリカバリポイントの右上で、[代替の場所 (Alternate location)]を選択します。
6. クラウド資産をリストアする場所を選択します。

7 [リカバリの開始 (Start recovery)]をクリックします。

8 左側の[アクティビティモニター (Activity monitor)]をクリックして、ジョブ状態を表示します。

次の点に注意してください。

- (Azure クラウドに該当) ADE が有効な VM の代替の場所へのアプリケーションリストアはサポートされません。
- (OCI の場合) スナップショットの作成時にボリュームにデバイス名がない場合、そのボリュームの元の場所のリストアは、元の VM で次に利用可能なデバイスに接続されます。

読み取り専用ボリュームを伴う GCP VM のリカバリシナリオ

次の表は、NetBackup が、読み取り専用ボリュームがある GCP VM のリストアまたはリカバリをどのように処理するかを示しています。

表 3-2 読み取り専用 GCP VM のリカバリシナリオ

シナリオ	処理
クラウド作業負荷にある[ボリューム (Volumes)]タブで、接続された読み取り専用ディスクのスナップショットからボリュームをリストアします。	リストア時に、ディスクは元の場所または代替の場所に読み取り/書き込みモードで接続されます。
クラウド作業負荷にある[仮想マシン (Virtual machines)]タブで、クラッシュ整合スナップショットから読み取り専用ディスクのある VM をリストアします。	このような VM を元の場所または代替の場所にリストアする際、読み取り専用ディスクが読み取り/書き込みモードでリストアされます。

シナリオ	処理
クラウド作業負荷にある[仮想マシン (Virtual machines)]タブで、アプリケーション整合スナップショットから読み取り専用ディスクのある VM をリストアします。	読み取り専用ディスクは複数の VM に接続できますが、NetBackup は 1 つの VM でのみ検出します。 Windows VM の場合、スナップショットは次のような VSS エラーで失敗します。 失敗: flexsnap。GenericError: スナップショットの作成に失敗しました (エラー: 選択したボリュームの VSS スナップショットの作成に失敗しました。) (Failure: flexsnap.GenericError: Failed to take snapshot (error: Failed to create VSS snapshot of the selected volumes.)) Linux VM の場合、ディスクが検出された VM についてはスナップショットが成功することもありますが、それ以外の VM では依存関係が見つからないために失敗します。エラーの例: linear_flow。フロー: ホスト linux-1 (len=4) のスナップショット (test-win) の作成は ['snap_google- gcepd-us-west 2-b-7534340043 132122994'] を必要としますが、他のエンティティは上記の要件を生成しません¥n MissingDependencies (linear_flow.Flow: create snapshot (test-win) of host linux-1(len=4)' requires ['snap_google- gcepd-us-west 2-b-7534340043 132122994'] but no other entity produces said requirements¥n MissingDependencies) 上記の場合、Linux VM についてスナップショットが成功すると、読み取り専用ディスクは読み取り/書き込みモードでリストアされます。

(GCP のみ) autoDelete ディスクサポートを使用した仮想マシンとボリュームのリストア

ソース VM のスナップショットまたはスナップショットからのバックアップを作成するときに、ディスクに関する追加情報が保存されます。autoDelete フラグによって、VM を削除するときにディスクを削除するかどうかが決まります。そのため、スナップショットまたはスナップショットからのバックアップから新しい VM が作成された場合、ディスクがソース VM として設定されます。

次に例を示します。

ソース VM:

Disk1: autoDelete は true に設定されています (ソース VM が削除され、autoDelete が true に設定されている場合、ディスクは自動的に削除される)。

Disk2: autoDelete は false に設定されています。

リストアされた VM:

Disk1_suffix: autoDelete は true に設定されています。

Disk2_suffix: autoDelete は false に設定されています。

クラウド資産のロールバックリカバリの実行

クラウド資産のロールバックリカバリでは、元の資産の既存のデータが上書きされます。仮想マシンのリストアとは異なり、ロールバックリストアはリストアされるイメージの新しいコピーを作成せず、ソースの既存のデータを置換します。

次の点に注意してください。

- スナップショットレプリカはロールバックをサポートしません。
- Azure Stack Hub、OCI、および GCP の作業負荷はロールバックリストアをサポートしません。

クラウド資産のロールバックリカバリを実行するには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual Machines)]をクリックします。

   対応するカテゴリで検出されたすべてのクラウド資産が表示されます。
3. リカバリする保護された資産をダブルクリックします。
4. [リカバリポイント (Recovery points)]タブをクリックします。利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。[コピー (Copies)]列で、リカバリするスナップショットをクリックします。[リカバリ (Recover)]、[ロールバックリストア (Rollback restore)]をクリックします。
5. [リカバリの開始 (Start recovery)]をクリックします。既存のデータが上書きされます。
6. 左側で[アクティビティモニター (Activity monitor)]、[ジョブ (Jobs)]の順にクリックして、ジョブ状態を表示します。

VMware への AWS VM または Azure VM のリカバリ

NetBackup では、AWS EC2 VM または Azure VM からオンプレミスの VMware VM に、クラウドベースのバックアップイメージをリストアできます。

前提条件

- リカバリホストは RHEL プラットフォームで実行する必要があります。リカバリホストのバージョンについては、Enterprise Server と Server 10.0 - 10.x.x OS のソフトウェア互換性リストで、VMware の互換性に関するセクションを参照してください。
- VM をリカバリする場合、VMware のサポート対象のトランスポートモードは NDB です。
- 変換された VM には、VMware サーバーの既存の VM では使用されていない、別の VM 名を使用することをお勧めします。

VMware にクラウド VM をリカバリするには:

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual Machines)]タブをクリックします。
3. リカバリする保護された資産をダブルクリックし、[リカバリポイント (Recovery points)]タブをクリックします。

   利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。
4. [コピー (Copies)]列で、リカバリするコピーをクリックします。バックアップイメージのみをリカバリできます。
5. コピーの行の省略記号メニュー (3 つのドット) をクリックし、[仮想マシンのリストア (Restore Virtual Machine)]をクリックします。
6. リカバリターゲットのページで、次の操作を行います。
   - [プロバイダ (Provider)]を VMware として選択します。
   - [表示名 (Display name)]: 表示名を変更するには、このフィールドに新しい表示名を入力します。
   - [ESXi サーバーまたはクラスタ (ESXi server or cluster)]: VM が存在する ESXi サーバーまたはクラスタを選択します。
   - [フォルダ (Folder)]: VM を含むフォルダを指定します。
   - [リソースプールまたは vApp (Resource pool or vApp)]: VM のリソースプールを指定します。
   - [データストアまたはデータストアクラスタ (Datastore or datastore cluster)]: VM のデータストアおよびディスクを指定します。
   - [ネットワーク構成 (Network configuration)]: ESXi サーバーのネットワークスイッチを選択します。
7. [次へ (Next)]をクリックします。
8. [リカバリオプション (Recovery options)]ページで、次の操作を行います。

- ［リカバリホスト (Recovery host)］: リカバリの実行に使用するホストを選択します。
- ［リカバリ後に電源をオン (Power on after recovery)］: (オプション) リカバリ後に VM の電源をオンのままにする場合に選択します。
- ［CPU 数 (CPU number)］: 変換された VM の CPU 数を指定します。
- ［メモリサイズ (GB)(Memory size (GB))］: 変換された VM のメモリサイズを指定します。

9 ［次へ (Next)］をクリックします。パラメータを確認して［リカバリの開始 (Start recovery)］をクリックします。

［リストアアクティビティ (Restore activity)］タブには、ジョブの進捗状況が表示されます。

VMware にリカバリされたクラウド VM のリカバリ後の考慮事項

リストアされた VM の考慮事項:

- これらは、リカバリされた VM のデフォルト構成の一部です。VM を使用する前に手動による修正が必要になる場合があります。
  - デフォルトのブート構成は EFI です。
  - デフォルトのディスクコントローラは SCSI です。
  - デフォルトのネットワークアダプタの種類は VMXNET 3 です。
  - デフォルトの OS の種類は x64 です。
- Azure の第 1 世代の VM の場合、「VM オプション」のブート構成を BIOS に変更する必要があります。また、ディスクコントローラを「IDE」に変更します。詳しくは、Azure のマニュアルを参照してください。

  https://docs.azure.cn/ja-jp/virtual-machines/generation-2?view=azs-2102

バックアップされたクラウド VM の前提条件と考慮事項については、p.89 の「VMware へのリカバリのための AWS VM または Azure VM の保護」を参照してください。。

クラウド VM から VMware へのイメージのリカバリ手順

このセクションでは、さまざまな種類のクラウド VM を VMware にリカバリするために実行する必要がある手順の概要について説明します。ソース VM の完全バックアップを MSDP ストレージサーバーに実行したことを確認します。p.30 の「クラウド資産またはクラウド資産用インテリジェントグループの保護」を参照してください。

バックアップされたクラウド VM の前提条件と考慮事項について詳しくは、p.89 の「VMware へのリカバリのための AWS VM または Azure VM の保護」を参照してください。。

AWS から VMware へのイメージのリカバリ

Windows Server 2022

バックアップされたクラウドイメージの前提条件:

- DHCP を使用するようにネットワークインターフェースを変更し、ブート時に有効にします。
- バックアップ前にローカル管理者を作成します。

Windows 2022 VM イメージを VMware にリカバリするには:

1. NetBackup を使用してイメージをリカバリします。p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。
2. VMware サーバーにログオンし、変換された VM 設定を編集します。[VM オプション (VM Options)]ページで、[ブートオプション (Boot Options)]をクリックし、[ファームウェア (Firmware)]を BIOS に変更します。
3. 変換された VM に RDP 経由でログオンするために IP アドレスを取得します。

RHEL 9.x

バックアップされたクラウドイメージの前提条件:

- DHCP を使用するようにネットワークインターフェースを変更し、ブート時に有効にします。
- リカバリされた VM にログオンするための新しいユーザーを作成します。

RHEL 9.x VM イメージを VMware にリカバリするには:

1. NetBackup を使用してイメージをリカバリします。p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。
2. VMware サーバーにログオンし、変換された VM 設定を編集します。[VM オプション (VM Options)]ページで、[ブートオプション (Boot Options)]をクリックし、[ファームウェア (Firmware)]を BIOS に変更します。
3. 変換された VM に SSH 経由でログオンするために IP アドレスを取得します。

SUSE 15SP5

バックアップされたクラウドイメージの前提条件:

- DHCP を使用するようにネットワークインターフェースを変更し、ブート時に有効にします。
- リカバリされた VM にログオンするための新しいユーザーを作成します。

SUSE 15SP5 VM イメージを VMware にリカバリするには

1 NetBackup を使用してイメージをリカバリします。p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。

2 変換された VM に SSH 経由でログオンするために IP アドレスを取得します。

Azure から VMware へのイメージのリカバリ

Windows 2022

バックアップされたクラウドイメージの前提条件:

- DHCP を使用するようにネットワークインターフェースを変更し、ブート時に有効にします。

Windows 2022 VM イメージを VMware にリカバリするには:

1 NetBackup を使用してイメージをリカバリします。p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。

2 Windows 2022 Gen 1 の場合、VMware サーバーにログオンし、変換された VM 設定を編集します。[VM オプション (VM Options)]ページで、[ブートオプション (Boot Options)]をクリックし、[ファームウェア (Firmware)]を[BIOS]に変更します。

3 変換された VM に RDP 経由でログオンするために IP アドレスを取得します。

RHEL 9.x

バックアップされたクラウドイメージの前提条件:

- ソース VM に VMW_PVSCSI ドライバが必要です。ドライバがすでに存在するかどうかを確認するには、次のコマンドを実行します。

  ```
  lsinitrd | grep -i vmw_pvscsi
  ```

  ドライバをインストールするには、次の手順を実行します。

  - `initramfs` をバックアップするには、次のコマンドを 1 つずつ実行します。

    ```
    cd /boot
    cp initramfs-`uname -r`.img initramfs-`uname -r`.img.bak
    ```

  - `dracut.conf` ファイルを開くには、次のコマンドを実行します。

    ```
    vi /etc/dracut.conf
    ```

    #add_drivers+="" 行のコメントを解除します。値「vmw_pvscsi」を行に追加し、既存のモジュールをスペースで区切ります。次に例を示します。

    ```
    # additional kernel modules to the default.
          add_drivers+="vmw_pvscsi"
    ```

  - 新しいモジュールを含む、新しい初期 ramdisk イメージを作成するには、次を実行します。

```
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 vmw_pvscsi
lsinitrd -f /boot/initramfs-`uname -r`.img | grep -i vmw_pvscsi
```

- リカバリされた VM にログオンするための新しいユーザーを作成します。
- DHCP を使用するようにネットワークインターフェースを変更し、ブート時に有効にします。

RHEL 9.x VM イメージを VMware にリカバリするには:

1. NetBackup を使用してイメージをリカバリします。p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。
2. RHEL Gen 1 の場合、VMware サーバーにログオンし、変換された VM 設定を編集します。[VM オプション (VM Options)]ページで、[ブートオプション (Boot Options)]をクリックし、[ファームウェア (Firmware)]を[BIOS]に変更します。
3. 変換された VM に SSH 経由でログオンするために IP アドレスを取得します。

SUSE 15SP5

バックアップされたクラウドイメージの前提条件:

- DHCP を使用するようにネットワークインターフェースを変更し、ブート時に有効にします。
- リカバリされた VM にログオンするための新しいユーザーを作成します。

SUSE 15SP5 VM イメージを VMware にリカバリするには

1. NetBackup を使用してイメージをリカバリします。p.147 の「VMware への AWS VM または Azure VM のリカバリ」を参照してください。
2. ソース VM に既存の vmw_pvscsi ドライバがない場合は、VMware サーバーにログオンし、変換された VM 設定を編集します。[仮想ハードウェア (Virtual Hardware)]ページで[ハードディスク (Hard disk)]をクリックし、[仮想デバイスノード (Virtual Device Node)]を[IDE]に変更します。
3. SUSE 15SP5 Gen 1 の場合、VMware サーバーにログオンし、変換された VM 設定を編集します。[VM オプション (VM Options)]ページで、[ブートオプション (Boot Options)]をクリックし、[ファームウェア (Firmware)]を[BIOS]に変更します。
4. 変換された VM に SSH 経由でログオンするために IP アドレスを取得します。

PaaS 資産のリカバリ

PaaS 資産は[クラウド (Cloud)]作業負荷の下に一覧表示されます。[アプリケーション (Applications)]タブから Amazon RDS 資産をリストアできます。他のすべての PaaS 資産は、[PaaS]タブからリストアできます。Azure 資産のリカバリフローは、NetBackup で保護されているか Azure で保護されているかによって異なります。

NetBackup 10.3 以降で、MySQL データベースのデータまたはスキーマとメタデータを個別にリストアできます。メタデータのリストアにはスーパーユーザーの権限が必要で、バージョン 10.2 以降のメディアサーバーが少なくとも 1 台必要です。

メモ: MySQL のリストアでは、admin または root ユーザーの権限がない場合は、リストア権限に加えて表示権限が必要です。

PaaS 資産はリカバリ中にインスタントアクセスをサポートします。インスタントアクセスにより、データへの高速アクセスが可能になり、全体的なリカバリ時間が短縮されます。

メモ: アクティビティモニターで PaaS リストアジョブを表示している間、フィールド[転送済みのバイト数 (Bytes transferred)]および[残りのバイト数の概算 (Estimated bytes remaining)]は正しい情報を示さないことがあります。[書き込み済みのファイル (Files written)]の数で正しい状態と NetBackup ログを確認できます。

RDS 以外の PaaS 資産のリカバリ

RDS 以外の PaaS 資産は、[クラウド (Cloud)]作業負荷の[PaaS]タブからリストアできます。

RDS 以外の PaaS 資産をリストアするには:

1. 左側で、[作業負荷 (Workloads)]の[クラウド (Cloud)]をクリックし、[PaaS]タブをクリックします。リカバリする資産の名前をクリックします。
2. Azure 資産の[リカバリポイント (Recovery points)]タブをクリックし、さらに[NetBackup 管理対象 (NetBackup managed)]を選択します。

   利用可能なリカバリポイントがテーブルに表示されます。
3. リカバリするイメージの行で、[リカバリ (Recover)]をクリックします。
4. [名前 (Name)]フィールドには、デフォルトでは資産の元の名前が表示されます。フィールドの名前は変更できます。この名前は後で変更できません。
5. (任意) [ターゲットインスタンス (Target instance)]フィールドでは、デフォルトで、資産のソースインスタンスが選択されています。別のインスタンスにリストアするには、必要なインスタンスを選択します。[ターゲットインスタンス (Target instance)]は、DynamoDB 資産では利用できません。

6 (オプション。MySQL データベースの場合のみ。)ビュー、トリガ、ストアプロシージャなどのメタデータをリストアするには、[メタデータのリストア (Restore metadata)]を選択します。

7 (オプション。MySQL データベースの場合のみ。)リストアのターゲットインスタンスクレデンシャルの場合:

- すでにインスタンスに関連付けられているクレデンシャルを使用するには、[すでに関連付けられているクレデンシャルを使用します (Use already associated credentials)]を選択し、[リカバリの開始 (Start recovery)]をクリックします。
- 別のクレデンシャルセットを使用するには(既存のクレデンシャルを使用するか、新しいクレデンシャルを作成)、[別のクレデンシャルを使用 (Use different credentials)]を選択します。
  p.128 の「データベースへのクレデンシャルの追加 」を参照してください。
  これらのクレデンシャルを検証するための検証ホストは、バックアップ中に使用されたものと同じである必要があります。リストア中のクレデンシャル検証でバックアップ中に使用されたホストが利用できない場合、検証は失敗します。
  (オプション) 資産のデフォルトのクレデンシャルとしてこれらのクレデンシャルを設定するには、[デフォルトのクレデンシャルにする (Make default credentials)]を選択します。

8 [リカバリの開始 (Start recovery)]をクリックします。

[リストアアクティビティ (Restore activity)]タブには、状態が表示されます。

Redshift クラスタのリカバリ

Redshift クラスタは、[クラウド (Cloud)]作業負荷の[PaaS]タブからリストアできます。

Redshift クラスタ資産をリストアするには:

1 左側で、[作業負荷 (Workloads)]の[クラウド (Cloud)]をクリックし、[PaaS]タブをクリックします。リカバリする資産の名前をクリックします。

2 [リカバリポイント (Recovery points)]タブで、リカバリポイントを表示する日付をクリックします。利用可能なリカバリポイントが右側に表示されます。

3 リカバリするイメージの行で、[リカバリ (Recover)]をクリックします。

- 元の場所にイメージをリストアするには、[元の場所 (Original location)]をクリックし、[リカバリの開始 (Start recovery)]をクリックします。
- イメージを代替の場所にリストアするには、[代替の場所 (Alternate location)]をクリックします。利用可能な場所の一覧から必要な場所を選択し、[リカバリの開始 (Start recovery)]をクリックします。

Redshift クラスタをリストアした後に必要な追加手順

リストアが成功した場合でも、NetBackup でインスタンスの 1 つ以上のプロパティまたは属性をリストアできない場合があるため、これらの追加手順が必要になります。

Redshift クラスタインスタンスをリストアした後、次の手順を実行できます。

- (オプション) `publicallyaccessible` 属性が `False` に設定されています。AWS コンソールから手動で `True` に設定できます。
- (オプション) `ClusterParameterGroupName` 属性はリストアされません。AWS コンソールから手動で構成できます。

AWS DocumentDB 資産と Neptune 資産のリカバリ

AWS DocumentDB 資産と Neptune 資産は、[クラウド (Cloud)]作業負荷の[PaaS]タブからリストアできます。

AWS DocumentDB 資産と Neptune 資産をリストアするには:

1. 左側で、[作業負荷 (Workloads)]の[クラウド (Cloud)]をクリックし、[PaaS]タブをクリックします。リカバリする資産の名前をクリックします。
2. [リカバリポイント (Recovery points)]タブで、リカバリポイントを表示する日付をクリックします。利用可能なリカバリポイントが右側に表示されます。
3. リカバリするイメージの行で、[リカバリ (Recover)]をクリックします。
   - 元の場所にイメージをリストアするには、[元の場所 (Original location)]をクリックし、[リカバリの開始 (Start recovery)]をクリックします。
   - イメージを代替の場所にリストアするには、[代替の場所 (Alternate location)]をクリックします。利用可能な場所の一覧から必要な場所を選択し、[リカバリの開始 (Start recovery)]をクリックします。

RDS ベースの PaaS 資産のリカバリ

RDS ベースの PaaS 資産は、[クラウド (Cloud)]作業負荷の[アプリケーション (Applications)]タブからリストアできます。

RDS ベースの PaaS 資産をリストアするには:

1. 左側で、[作業負荷 (Workloads)]の[クラウド (Cloud)]をクリックし、[アプリケーション (Applications)]タブをクリックします。リカバリする資産の名前をクリックします。
2. カレンダーで[リカバリポイント (Recovery points)]タブをクリックし、リカバリポイントを表示する日付を選択します。

   利用可能なリカバリポイントが右側に表示されます。
3. リカバリするイメージの行で、[リカバリ (Recover)]をクリックします。

4 [ソースデータベース (Source databases)]で、リストアするデータベースを選択します。[データベースの追加 (Add database)]をクリックし、[データベースの追加 (Add database)]ダイアログで、必要なデータベースを選択してから[選択 (Select)]をクリックします。

5 (Amazon RDS Oracle データベースの場合のみ) [AWS S3 バケット名 (AWS S3 bucket name)]フィールドにステージングパスを入力します。[リカバリの開始 (Start recovery)]をクリックします。リカバリされたデータベースが[インスタントアクセスデータベース (Instant access databases)]タブに表示されます。リカバリは、自己管理インスタンス EC2 またはオンプレミス VM で実行できます。資産のリカバリを完了するには、次のナレッジベースの記事を参照してください。

https://www.veritas.com/support/ja_JP/article.100058945

リストアされたデータをステージングするために、バックアップ中に使用されたものとは異なる S3 バケットを選択できます。別の領域の S3 バケットを選択することもできます。

6 リストアされたデータベースに追加する接頭辞を入力するか、デフォルトを使用します。このフィールドには、値が必要です。

7 (任意) [ターゲットインスタンス (Target instance)]フィールドでは、デフォルトで、資産のソースインスタンスが選択されています。別のインスタンスにリストアするには、必要なインスタンスを選択します。

8 (オプション。MySQL データベースの場合のみ。)ビュー、トリガ、ストアプロシージャなどのメタデータをリストアするには、[メタデータのリストア (Restore metadata)]を選択します。

9 (オプション。MySQL データベースの場合のみ。)リストアのターゲットインスタンスクレデンシャルの場合:

- すでにインスタンスに関連付けられているクレデンシャルを使用するには、[すでに関連付けられているクレデンシャルを使用します (Use already associated credentials)]を選択し、[リカバリの開始 (Start recovery)]をクリックします。
- 別のクレデンシャルセットを使用するには (既存のクレデンシャルを使用するか、新しいクレデンシャルを作成)、[別のクレデンシャルを使用 (Use different credentials)]を選択します。
  p.128 の「データベースへのクレデンシャルの追加 」を参照してください。
  (オプション) 資産のデフォルトのクレデンシャルとしてこれらのクレデンシャルを設定するには、[デフォルトのクレデンシャルにする (Make default credentials)]を選択します。
- 検証ホストを選択して、指定したクレデンシャルを検証します。

10 [リカバリの開始 (Start recovery)]をクリックします。

[リストアアクティビティ (Restore activity)]タブには、状態が表示されます。

これらの 2 つのリストアワークフローは、リカバリポイントに対して暗黙的にインスタントアクセスマウント共有を作成します。

Azure 保護対象資産のリカバリ

NetBackup では、Microsoft Azure がバックアップする Azure SQL データベースおよび Azure SQL 管理対象データベースの資産をリストアできます。サポートされるバックアップモードは、指定した時点のバックアップと長期保持用バックアップです。

メモ: インスタンスプールのエラスティックプールでのリストアはサポートされません。

操作を進める前に、PaaS 資産のリストアに必要な権限があることを確認してください。

指定した時点のバックアップで資産をリカバリするには:

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックします。
2. [PaaS]タブをクリックします。

   検出されたすべての PaaS 資産が表示されます。
3. [リカバリポイントの種類 (Recovery points type)]で、[プロバイダによって保護 (Provider protected)]を選択します。
4. リカバリ対象の保護された Azure SQL データベースおよび Azure SQL 管理対象データベース資産の行で、[リストア (Restore)]をクリックします。
5. [リカバリポイント (Recovery points)]タブの[指定した時点のバックアップ (Point in time backup)]で、[リストア (Restore)]をクリックします。
6. [リストアポイント (UTC) (Restore point (UTC))]で、日付と時刻を選択します。リストアポイントは、最も古い時間から以下の時間までの間で選択できます。

   - オンラインデータベースの最新のバックアップ時刻。
   - 削除されたデータベースのデータベース削除時刻。

   Microsoft Azure は、UTC を使用して、選択した時間を指定可能な最も近いリカバリポイントに調整する場合があります。

   選択した PaaS 資産によっては、Web UI に表示されるデフォルトのリストア日時が異なる場合があります。たとえば、Azure SQL データベースの場合、デフォルトのリストア時間は現在の時刻であり、Azure SQL 管理対象データベースのデフォルトのリストア時間は、現在の時刻より 6 分早い時刻です。

7 Azure SQL データベースの場合は、必要に応じ、リストアされたデータベースの名前を[データベース名 (Database name)]フィールドに入力します。データベース名には、特殊文字 (< > * % & : ¥ / ? など) または制御文字を使用できません。名前の最後にピリオドまたはスペースを使用しないでください。Azure リソースの命名規則について詳しくは、https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql を参照してください。

名前を入力しない場合、NetBackup は自動的に *<dbName>_<UTC でのリストア時刻>* という形式で名前を割り当てます。

8 Azure SQL 管理対象データベースの場合は、必要に応じ、[管理対象インスタンス (Managed instance)]フィールドにインスタンス名を入力します。デフォルトでは、リカバリポイントのインスタンス名が表示されます。検索オプションを使用して管理対象インスタンス名を検索することもできます。リストアは、サブスクリプションの所属先と同じ領域に対して行えます。

目的の管理対象インスタンスが検索結果に表示されない場合は、手動で検出を実行してください。また、管理対象インスタンスに対する RBAC アクセス権があることを確認してください。

9 [次へ (Next)]をクリックします。リカバリ前チェックが完了したら、[リカバリの開始 (Start recovery)]をクリックします。

ジョブの状態は、アクティビティモニターで確認できます。

長期保持用バックアップの資産をリカバリするには:

1 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。

2 [PaaS]タブをクリックします。

検出されたすべての PaaS 資産が表示されます。

3 リカバリ対象の保護された資産の行で、[リストア (Restore)]をクリックします。

4 [リカバリポイント (Recovery points)]タブの[長期保持用バックアップ (Long term retention backup)]で、リストアするイメージに対して[リストア (Restore)]をクリックします。

5 Azure SQL データベースの場合は、必要に応じ、リストアされたデータベースの名前を[データベース名 (Database name)]フィールドに入力します。データベース名には、特殊文字 (< > * % & : ¥ / ? など) または制御文字を使用できません。名前の最後にピリオドまたはスペースを使用しないでください。Azure リソースの命名規則について詳しくは、https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql を参照してください。

名前を入力しない場合、NetBackup は自動的に *restore_<データベース名>* という形式で名前を割り当てます。

6 Azure SQL 管理対象データベースの場合は、必要に応じ、[管理対象インスタンス (Managed instance)]フィールドにインスタンス名を入力します。デフォルトでは、リカバリポイントのインスタンス名が表示されます。検索オプションを使用して管理対象インスタンス名を検索することもできます。リストアは、サブスクリプションの所属先と同じ領域に対して行えます。

7 [次へ (Next)]をクリックします。リカバリ前チェックが完了したら、[リカバリの開始 (Start recovery)]をクリックします。

ジョブの状態は、アクティビティモニターで確認できます。

メモ: ポータルおよび Snapshot Manager のタグはリストアされません。ただし、NetBackup 経由でリストアするときに、「createdby: cloudpoint」タグが作成されます。

メモ: プロバイダによって保護されたリカバリジョブの場合、断続的なエラーが発生しても、次回にスケジュールされているジョブのクリーンアップが実行されるまで、リカバリジョブは実行され続けます。

AdvancedDisk からの複製イメージのリカバリ

イメージが AdvancedDisk ストレージまたは MSDP クラウドストレージに存在する場合、10.1 メディアサーバーは複製イメージからの PaaS のリストアを開始できません。回避方法として、次の手順を実行します。

前提条件:

1. AdvancedDisk の場合、MSDP サーバーに関連付けられているメディアサーバーのバージョンが 10.1 以上である必要があります。
2. MSDP クラウドストレージの場合、リカバリに使用するメディアサーバーのバージョンが 10.1.1 である必要があります。
3. ushare が MSDP サーバーでセットアップおよび構成されていることを確認します。
4. この MSDP ストレージサーバーでユニバーサル共有を作成します。ushare のエクスポートリストに、対応するメディアサーバーのホスト名または IP を追加していることを確認します。

AdvancedDisk からリカバリするには、次の手順を実行します。

1 Web UI のカタログノードを使用して、手動で MSDP ストレージにイメージを複製します。詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

メモ: 2 つ目のコピーから複製するには、カタログビューで複製オプションを選択した後、[検索 (Search)]を再度クリックします。

2 複製ジョブが完了したら、Web UI で指定した資産に対して新しいリカバリポイントが表示されていることを確認します。

リストアジョブを開始するには、p.153 の「PaaS 資産のリカバリ」を参照してください。

REST API を使用してリストアするには、セクション `recovery/workloads/cloud/scenarios/asset/recover` を参照してください。NetBackup API のマニュアルを参照してください。

メモ: RDS インスタンスリカバリの場合、AdvancedDisk ストレージに存在するバックアップイメージからリストアを開始すると、NetBackup はエラーメッセージまたは警告メッセージを表示しません。

4

個別リストアの実行

この章では以下の項目について説明しています。

個別リストアについて

NetBackup では、クラウド仮想マシン上のファイルとフォルダの個別リストアを実行できます。個々のファイルやフォルダを検索してリストアすることもできます。また、仮想マシンからボリュームをリストアすることもできます。

このプロセスは個別リストアとして知られ、スナップショットまたはバックアップの各ファイルが、単一ファイルリストアと一般的に呼ばれる 1 つの細かい単位として考慮されます。NetBackup は、インデックス処理を使用して、スナップショットまたはバックアップ内のすべてのファイルのインベントリを作成します。スナップショットから特定のファイルをリストアするには、NetBackup によってスナップショットのインデックス付けが完了している必要があります。NetBackup によるバックアップのインデックス付けが完了している場合は、バックアップから特定のファイルをリストアすることもできます。

メモ: プロバイダ管理の一貫性が有効になっている未接続の VM で BFS (スナップショットからのバックアップ) と GRT (個別リストア) の保護計画を実行する場合、SFR (シングルファイルリストア) はバックアップコピーからのみ利用可能です。

次の表は、ボリューム、ファイル、フォルダの個別リストアを有効にする流れを理解するのに役立ちます。

表 4-1 個別リストアの作業

作業	説明
仮想マシンを接続	個別リストアを実行するために使用する仮想マシンを接続します。
仮想マシン上の資産の検出	[検出 (Discover)]オプションを使用します。 [クラウド (Cloud)]>[Snapshot Managers]>[*Snapshot Manager*]>[処理 (Actions)]>[検出 (Discover)] に移動します。
保護計画の作成	保護計画を作成します。 [ファイルまたはフォルダの個別リカバリの有効化 (Enable granular recovery for files or folders)]チェックボックスが、保護計画の[バックアップオプション (Backup options)]で選択されていることを確認します。
検出済み資産の保護計画へのサブスクライブ	インデックス付け可能な属性で個別リストアが有効になっている保護計画に、前の手順で接続された VM の資産を追加します。
保護計画の実行	バックアップジョブとインデックスをスケジュール設定するか、[今すぐバックアップ (Backup now)]オプションを使用します。この場合は、すぐにバックアップジョブが開始されます。
	ファイルとフォルダの個別リストアを実行します。

サポート対象の環境リスト

次の表に、サポートされているバージョンのリストを示します。

表 4-2 サポート対象バージョン

アプリケーション	バージョン
NetBackup	11.0

アプリケーション	バージョン
NetBackup バックアップホスト OS	■ RHEL 8.8 以降 ■ Windows 16、19、22 ■ OEL 8.8 以降 ■ SUSE Linux
Snapshot Manager ホスト OS	■ RHEL 8.6 以降 ■ SLES 15 ■ OEL 8.x 以降 ■ Ubuntu 18.04 LTS、20.04 LTS、22.04 LTS、および 24.04 LTS **メモ:** UI に一覧表示されている OS のバージョン (Ubuntu 20.04 LTS) は、コンテナのバージョンです。
クラウドプロバイダ	■ アマゾンウェブサービス ■ Microsoft Azure ■ Microsoft Azure Stack Hub ■ Google Cloud Platform ■ Oracle Cloud Infrastructure
Snapshot Manager またはエージェントインスタンスタイプ	■ Amazon AWS: t2.large/t3.large ■ Microsoft Azure: D2s_V3Standard ■ Microsoft Azure Stack Hub: DS2_v2 Standard、DS3_v2 Standard ■ Google Cloud Platform: n1.Standard2 以上 ■ Oracle Cloud Infrastructure: VM.Standard.E4.Flex/ VM.Standard.E5.Flex/ VM.Standard3.Flex/ VM.Optimized3.Flex
保護対象の Snapshot Manager エージェントホスト	■ Linux OS: RHEL 8.8 以降、OEL 8.x 以降 ■ Windows OS バージョン: 2012 R2、2016、2019、2022

サポートされているファイルシステムのリスト

次の表に、サポートされているファイルシステムについての詳細を示します。

プラットフォーム	検出されたファイルシステム	パーティションレイアウト
RHEL (整合性スナップショットのプロパティを使用) **メモ:** GCP の場合、エージェントホストがオペレーティングシステムバージョン RHEL 8.x 上にある場合は、オペレーティングシステムのバージョンが RHEL 8.x のホストに Snapshot Manager がインストールされている必要があります。	■ ext3 ■ ext4 ■ xfs	■ GPT ■ MBR ■ レイアウトなし (ダイレクト FS)
Windows (整合性スナップショットのプロパティを使用)	NTFS	■ GPT ■ MBR

メモ: アプリケーションの整合性スナップショットは、ext2 ファイルシステムのバージョンではサポートされません。

メモ: GRT は、宛先ファイルシステムまたはパーティションの形式 (FAT、ReFS、LDM、LVM) に関係なく許可されます。

開始する前に

個別リストアを実行する前に、次の点に対応していることを確認します。個別リストアを有効にして保護されるように構成された Snapshot Manager と VM には、次の要件があります。

- 次の要件がスナップショットに適用されます。
  - (Microsoft Azure と Azure Stack Hub) 接続された VM と同じサブスクリプションおよび地域内に Snapshot Manager が配備されていない場合でも、バックアップスケジュールが保護計画の一部として構成されている場合は、個別リストアを実行できます。スナップショット専用の保護計画スケジュールの場合、Azure と Azure Stack Hub の両方で、VM と同じサブスクリプションおよび地域内に Snapshot Manager ホストを配備する必要があります。
  - (OCI および GCP): Snapshot Manager ホストと接続された VM は同じテナンシー/プロジェクトとリージョンにある必要があります。
  - (OCI): ブロックボリューム管理プラグインは、接続された VM に加えて、Snapshot Manager ホストで有効にする必要があります。

- (OCI): Oracle クラウドエージェントがインストールされ、Snapshot Manager と保護対象の VM でアクティブであることを確認します。
- Snapshot Manager ホストが配備されている領域の資産を保護するために、クラウドプラグインを構成する必要があります。

- ホストは接続状態である必要があります。また、必須のサポート構成になっている必要があります。
- ホストでは、接続時に fsConsistent フラグと indexable フラグが有効になっている必要があります。indexable フラグは、スナップショット専用の保護計画のスケジュールに適用されます。
- 保護計画では、[ファイルとフォルダの個別リストアの有効化 (Enable Granular restore for files and folders)]チェックボックスにチェックマークを付ける必要があります。
- ブートディスクと `/cloudpoint` にマウントされているディスクを除いて、追加のディスクを明示的に Snapshot Manager インスタンスに接続する必要はありません。
- ホスト上のファイルシステムをサポートする必要があります。
p.163 の「サポートされているファイルシステムのリスト」を参照してください。
- オープン Snapshot Manager ホスト用にポート 5671 と 443 を構成します。
- Linux システムおよび Windows システムのエージェントレスリストアの場合、インデックス付け可能な仮想マシンでポート 22 を構成します。
- 個別リストアを実行するための適切な権限があることを確認します。『NetBackup Web UI 管理者ガイド』で役割の権限に関する情報を参照してください。
- スナップショットバックアップから単一ファイルのリストアを実行する前に、次の点に対処していることを確認します。
  - NetBackup と Snapshot Manager バージョン 10.2 以降がインストールされています。
  - 個別リストアは、インスタントアクセスが有効な状態でバックアップイメージが MSDP ストレージサーバー (10.3 以降) からリストアされる場合にのみ成功します。
  - MSI および RPM ベースのエージェントインストールの場合、ターゲットホストエージェントは、最新バージョンにアップグレードする必要があります。
  - Windows ターゲットホストでは、管理者がディスクに対して接続と切断のポリシーを有効にしておく必要があります。詳しくは、「AttachVirtualDisk 関数」を参照してください。
  - (Windows の場合) symlink をリストアするには、必要なアクセス権を使用してエージェントを構成する必要があります。このためには、[**設定** (Configuration)]、[Windows **の設定** (Windows Settings)]、[**セキュリティの設定** (Security Settings)]、[**ローカル ポリシー** (Local Policies)]、[**ユーザー権利の割り当て**

(User Rights Assignment)]の[シンボリック リンクの作成 (Create symbolic links)]ポリシーで、管理者ユーザーを追加します。

- バックアップは、[個別ファイルおよびリストア (Granular File and Restore)]オプションを選択して実行する必要があります。
- ターゲット仮想マシンには、NFS/SMB を介した MSDP ストレージサーバーへのアクセス権が必要です。
- (Linux の場合) NFS を介してリストアするには、NFS クライアント (nfs-utils) をインストールする必要があります。
- MSDP ストレージサーバーの MSDP ホストに対して /etc/hosts エントリが作成されている場合は、MSDP ストレージサーバーの FQDN も同じエントリに追加します。
- Windows ターゲットは、次の要件を満たす必要があります。
  - (アクセス制御のリストアリストを使用して Windows イメージの内容をリストアする場合) Samba ユーザークレデンシャルは、MSDP ストレージサーバーの Windows クレデンシャルマネージャに格納する必要があります。このサーバーは、インスタントアクセス共有をエクスポートするサーバーです。
    MSDP サーバーで、次のコマンドを実行して Samba クレデンシャルを生成します。
    ```
    smbpasswd -a <username>
    ```
    DNS 名または MSDP サーバーの IP アドレスを追加します。前の手順のユーザー名と Windows 資格情報マネージャで生成されたパスワードを指定します。
    ユーザーが MSDP サーバーに存在しない場合、smbpasswd コマンドは失敗します。最初に useradd <username> コマンドを使用してユーザーを追加する必要があります。
  - (Linux イメージの内容をリストアする場合) NFS クライアントがインストールされています。

MSDP で SMB/IA を有効にする方法について詳しくは、『NetBackup 重複排除ガイド』を参照してください。
次の事前チェックスクリプトを使用して、MSDP サーバーの SMB 構成を確認します。
```
/usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
```

制限事項および考慮事項

個別リストアには次の制限事項と考慮事項があります。

- ターゲットの場所に十分な領域がない場合、コピー操作が開始される前にリストア操作が失敗します。

- 古いエージェント (事前インストール済みの) サービスを再起動しないと、LVM 資産の代替ホストリストア (GRT とアプリケーション) が失敗する場合があります。LVM 資産のリカバリをサポートするには、古いエージェントを再起動する必要があります。
- 個別リストアは、VxMS のインデックス付け処理を使用して実行できます。VxMS のインデックス付け処理は、Snapshot Manager のすべてのサポート対象ファイルシステムに適用できます。VxMS のインデックス付け処理は、Azure、Azure Stack Hub、AWS、OCI、および GCP に対して実行できます。
  ただし、VxMS のインデックス付けは、ソフトウェア RAID デバイスで作成されたボリュームまたはパーティションではサポートされません。これらのボリュームまたはパーティションは、ファイルシステムのインデックス付け中にスキップされます。
- ホスト整合スナップショットが EXT2 ファイルシステムでサポートされるのは、読み取り専用としてマウントされている場合のみです。
- サポートされていないファイルシステムがホストに存在する場合、個別リストア用に作成された保護計画にホストを追加できます。個別リストアの保護計画では、[ファイルまたはフォルダの個別リカバリの有効化 (Enable granular recovery for files or folders)] チェックボックスの値が true に設定されています。
- インデックス処理中、ファイル、ディレクトリ、またはその他のエントリのクロール中に OS エラーが発生する場合があります。これらのエラーは無視され、インデックス付け操作は続行されます。消失したファイルをリストアするには、親フォルダで個別リストア操作を開始する必要があります。
- Windows VM からディスクを作成またはマウントする場合は、ドライブ文字を追加します。この操作によって、インデックス付け操作で正しいドライブ文字をキャプチャできます。
- リカバリポイントからファイルまたはフォルダを参照するときに、マウントポイントが表示されないことがあります。次のような原因が考えられます。
  - 「/」 (root ファイルシステム) が LVM 上にある。
  - マウントポイントが「/」 (root ファイルシステム) に直接関連付けられていない。

  このような場合、右側のパネルからマウントポイントを検索し、ファイルまたはフォルダを正常にリストアします。
  次の例を考えてみます。ディスクは `/mnt1/mnt2` にマウントされます。ここで、`/mnt1` は「/」の任意のディレクトリです。(LVM セットアップにあるルートファイルシステム。) `mnt2` は、`mnt1` 内のマウントポイントです。`mnt2` は左側のパネルのツリーに表示されません。ただし、マウントポイント内のファイルやフォルダを検索してリストアできます。
- VM スナップショットリカバリポイントからファイルとフォルダをリストアするには、Linux サーバー上の `/etc/fstab` ファイルに、デバイスパスではなく、ファイルシステム UUID に基づくエントリが必要です。デバイスパスは、Linux がシステムブート中にデバイスを検出する順序によって変わる場合があります。

- 1 つの OS バージョンから別の OS バージョンにアプリケーションまたはファイルシステムをリストアする場合は、OS とアプリケーションベンダーの互換性マトリックスを参照してください。新しいバージョンから古いバージョンへのファイルシステムのリストアは、お勧めしません。
- ユーザーグループは、ドライブをソースとして、宛先の代替フォルダにリストアできません。ユーザーグループには、新しいフォルダを作成するライター権限がありません。
- エージェントレス接続では、Windows (または EFS) によって個々のファイルレベルのリストア ([ファイルとフォルダをリストアする (Restore files and folders)]オプション) を使用して暗号化ファイルをリストアできません。ただし、ボリュームレベルのリストアを使用してファイルをリストアした後、そのファイルを復号することはできます。
- フォルダ (接合点) にマウントされたボリュームに格納されたファイルは、下位ディスクに GPT パーティションレイアウトがある場合にのみリストアできます。ボリュームがドライブ文字を使用してマウントされている場合、下位ディスクのパーティションレイアウトに関係なく、ファイルをリストアできます。
- RHEL ターゲットホストに存在しない代替パスが単一ファイルのリストアに指定されているとします。作成された新しいディレクトリは、エージェントが実行されるユーザーのセキュリティコンテキストの下に存在します。ストレージ管理者は、リストアの最終的な場所が必要なユーザーにアクセス可能であることを確認する必要があります。
- NetBackup は、VHDX ディスク (Azure Ultra ディスク、4K セクタサイズの Premium SSD v2) を持つ VM のインデックス付けと個別リストアをサポートしません。
- スナップショットが実行またはインデックス付けされると、次のデバイスは無視されます。
  - 揮発性ストレージデバイス: Amazon AWS インスタンスストアボリュームや Microsoft Azure 一時ディスクなど

    メモ: これらのデバイスは、インデックス付け処理でも無視されます。

  - LDM ディスクで作成されるファイルシステム。

    メモ: LDM ディスクのファイルまたはフォルダは、シングルファイルリストア時に Web UI で選択のために表示されますが、ファイルはリストアされず、リストアジョブは失敗します。

- Linux VM ファイルの場合、拡張属性はリストアされません。
- FIPS 設定の場合、Windows から Windows へのシングルファイルリストアはサポートされません。

- Linux VM のシングルファイルリストア: ディレクトリに 100K を超えるファイルが含まれる場合、インスタントアクセスマウントの制限により、ディレクトリとそのディレクトリ内のファイルのリストアはスキップされます。

OCI でのシングルファイルリストアの制限事項

- VM の作成後にブロックボリュームを接続し、ボリュームの接続時に一貫性のあるデバイスパスを指定する必要があります。
- スナップショットコピーからの個別リストアとボリュームのリストアでは、ターゲット VM でブロックボリューム管理プラグインを有効にする必要があります。プラグインを有効にした後、VM を再起動します。
- Windows インスタンスの場合、スナップショットコピーからの個別リストアはサポートされません。
- バックアップコピーから Windows インスタンスへの個別リストアでは、NFS 共有から手動で対象をコピーする必要があります。
- スナップショットコピーからの個別リストア、ブートボリュームから別のブートボリュームへのリストアは、一部のオペレーティングシステムではサポートされません。
- 一貫性のあるデバイスパスがない、Linux OS からの個別リストアは、ディスクが準仮想化された添付ファイルとして接続されている場合はサポートされません。
- より高いカーネルバージョンのソース VM から、カーネルバージョンが低いターゲット VM への個別リストアはサポートされません。

バックアップコピーからのシングルファイルリストアの制限事項

- ファイルまたはフォルダを Linux ソースホストからリストアするときに、ターゲットホストが Windows の場合、次の点が適用されます。
  - Windows ホストではファイル属性をリストアできず、ファイルの内容のみがリストアされます。
  - リストア用に選択したファイルまたはフォルダに任意の symlink が存在する場合、その symlink はリストアされません。
  - 元の場所にリストアする場合、コピー操作の前に利用可能なサイズの確認はスキップされます。
- ソースホストが Linux でターゲットホストが Linux の場合にファイルまたはフォルダをリストアする場合、ソケットファイルとブロックファイルはリストアされません。
- ファイルとフォルダが LDM ディスク、ダイナミックディスク、またはストレージ領域に存在する場合、ファイルとフォルダのリストアはサポートされません。
- メディアサーバーまたは PureDisk Deduplication Engine および Cohesity プロビジョニングファイルシステムデーモンサービスが再起動された場合、部分的に成功したリストア中に保持されるライブマウントは、保持期間の期限が切れる前に削除されるか期限切れになります。

- メディアサーバーが 10.3 以降にアップグレードされていない場合、バージョン 10.3 以降のプライマリサーバーが NetBackup Snapshot Manager に接続するために使用されます。
- インデックス付け後の Windows の接合点は、次の形式を使用します。
  ボリューム {4e3f8396-490a-400a-8abf-5579cafd4c0f}
  バックアップ操作から単一ファイルのリストアのための接合点をリストアするには、[すべてを異なる場所にリストア (Restore everything to a different location)]を選択し、[詳細 (Advanced)]オプションで[アクセス制御リストのリストアを求める (Require to restore access control list)]を有効にします。

アクティビティモニターの操作上の注意事項

アクティビティモニターには次の動作があります。

- リストアジョブが完了した後は、リストアジョブの[ファイルリスト (File List)]セクションのディレクトリを展開できません。
- アクティビティモニターの概略では、リストアジョブを開始すると、リストア項目の最初のエントリである現在のファイルが表示されます。ジョブが完了すると、概略は表示されなくなります。
- 転送済みのバイト数と推定バイト数は更新されず、0 と表示されます。

クラウド仮想マシンからのファイルとフォルダのリストア

クラウド仮想マシンから 1 つのファイルまたはフォルダをリストアできます。

メモ: Microsoft Azure、GCP、OCI、および AWS の場合、NetBackup は、マネージャが提供するキーを使用して暗号化されたクラウド資産のスナップショットとリカバリをサポートします。

ファイルまたはフォルダをリストアするには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual machines)]タブをクリックします。
3. アプリケーションがホストされている仮想マシンを選択します。右上の[接続 (Connect)]をクリックします。
4. VM が接続された後、右上の[保護の追加 (Add protection)]をクリックします。
5. ファイルとフォルダを個別にリカバリするために作成された保護計画を選択し、[次へ (Next)]をクリックします。
6. [保護 (Protect)]をクリックします。
7. 保護計画を実行するには、[今すぐバックアップ (Backup now)]をクリックします。

8 資産の 1 つのスナップショットおよび 2 つのインデックス付けジョブ、またはスナップショットからのバックアップジョブが 2 つ完了した後、[リカバリポイント (Recovery points)]タブをクリックします。

9 優先リカバリポイントに対して、[処理 (Action)]メニューの[ファイルとフォルダをリストアする (Restore files and folders)]を選択します。

[リカバリ (Recover)]をクリックし、[ファイルとフォルダをリストアする (Restore files and folders)]を選択すると、[スナップショット (Snapshot)]と[バックアップ (Backup)]形式のファイルとフォルダをリストアすることもできます。

10 ファイルの追加手順で、[追加 (Add)]をクリックします。

11 [ファイルとフォルダを追加 (Add files and folders)]ダイアログで、リストアするファイルを選択し、[追加 (Add)]をクリックします。

左側のフォルダまたはドライブをクリックすると、特定のフォルダ内のファイルを展開して表示できます。ファイルの名前または拡張子に基づいてファイルを検索できます。

12 [次へ (Next)]をクリックします。

13 [リカバリターゲット (Recovery target)]のステップで、次の操作を実行します。

ダイアログボックス	スナップショットコピー	バックアップコピー
リストア先 (Restore to)	[ターゲット VM (Target VM)] - VM を選択します。元のターゲットホストと同じオペレーティングシステムを持つ、すべての接続された VM のリストが表示されます。VMを選択しない場合、ファイルは元の VM にリストアされます。	■ [クラウドプロバイダ (Cloud provider)] - 単一ファイルのリストアの実行先となるクラウドプロバイダを選択します。 ■ [構成 (Configuration)] - 代替構成にリストアするには、ドロップダウンから構成を選択します。 ■ [領域 (Region)] - 代替領域にリストアするには、ドロップダウンから領域を選択します。 ■ (Azure および Azure Stack Hub のみ)[サブスクリプション (Subscription)] - 代替サブスクリプションにリストアするには、ドロップダウンからサブスクリプションを選択します。 ■ [ターゲット VM (Target VM)] - VM を選択します。クロスプラットフォームリストア用に、すべての接続または切断された Linux または Windows の VM を含むリストが表示されます。

ダイアログボックス	スナップショットコピー	バックアップコピー
リストアターゲットのオプション	■ すべてを元の場所にリストア (Restore everything to original location) ■ すべてを異なる場所にリストア (Restore everything to a different location) その後、ディレクトリの場所を指定する必要があります。また、場所への UNC パスを入力することもできます。	

クラウドプロバイダ間でのファイルとフォルダのリストアは、バックアップコピーからの個別リストアを使用してサポートされます。個別リストアの実行では、異なるクラウドプロバイダに所属するソース VM とターゲット VM を使用できます。

クロスプラットフォームリストアは、次のシナリオでサポートされます。

- NetBackup と Snapshot Manager が 1 つのクラウド上にあり、ターゲットホストが別のクラウド上にある場合。
- NetBackup と Snapshot Manager が 1 つのクラウド上にあり、別の Snapshot Manager とターゲットホストが別のクラウド上にある場合。
- NetBackup と Snapshot Manager が 1 つのクラウド上にあり、AIR (自動イメージレプリケーション) のリストアを別のドメインで行う場合。

14 [すべてを元の場所にリストア (Restore everything to original location)]オプションを選択した場合、[次へ (Next)]をクリックし、[リカバリオプション (Recovery options)]の手順で次のオプションを選択します。

ダイアログボックス	スナップショットコピー	バックアップコピー
オプション (Options)	■ ファイル名に文字列を追加 (Append string to file names) [文字列 (String)]フィールドに、追加に使用する文字列を入力します。この文字列は、ファイルの最後の拡張子の前に追加されます。 ■ 既存のファイルの上書きを許可 (Allow overwrite of existing files) 適切な権限を所有している必要があります。	

ダイアログボックス	スナップショットコピー	バックアップコピー
詳細オプション (Advanced Options)	該当なし	■ (Windows から Windows へのリストアにのみ適用可能) [アクセス制御リストのリストアを求める (Require to restore access control list)] - 追加の操作を必要とするアクセス制御リストをリストアするには、このチェックボックスにチェックマークを付けます。 ■ [ターゲットホストの NAT ゲートウェイ IP アドレス (Target host NAT gateway IP address)] - ターゲット VM がネットワークゲートウェイの背後にあり、直接アクセスできない場合は、ネットワークアドレス変換ゲートウェイの IP アドレスを入力します。 **メモ:** プライベート IP またはホスト名のみが許可されます。

15 [すべてを異なる場所にリストア (Restore everything to a different location)]オプションを選択した場合は、[リストア用ディレクトリ (Directory for restore)]を指定して[次へ (Next)]をクリックします。

16 レビュー手順で、選択したオプションを表示し、[リカバリの開始 (Start Recovery)]をクリックします。

選択したファイルのリストアジョブがトリガされます。アクティビティモニターでジョブの詳細を表示できます。ジョブが正常に完了した後、ジョブの詳細でリストアされたファイルの概略を確認できます。

メモ: 類似していない環境 (ユーザーまたはグループが一致しない環境) へのリストアでは、uid/guid に基づいてファイルに対する権限が割り当てられます。リストアされるファイルまたはフォルダには、ターゲットホスト上の意図しないユーザーまたはグループに対する権限が必要です。そのため、必要なファイルのリストアが正常に完了した後、ユーザーは必要条件に従ってアクセス権を変更する必要があります。

次の点に注意してください。

スナップショットまたはバックアップからの単一ファイルリストア (ソース Linux VM からターゲット Linux VM) のハードリンクをリストアする場合は、次のガイドラインに従ってください。

- [ファイルとフォルダを追加 (Add files and folders)]ダイアログでフォルダとファイルを選択する場合は、冗長なエントリを選択しないでください。たとえば、フォルダを選

択し、そのフォルダ内に存在するファイルを選択する場合などが該当します。そのファイルはフォルダ内にすでに含まれるためです。

- 冗長なエントリが選択されている場合でも、[リカバリオプション (Recovery option)] の手順で[既存のファイルの上書きを許可 (Allow overwrite of existing files)]オプションを選択しないようにします。このオプションを選択すると、ハードリンクファイルのコピーに失敗します。
- ソースとそのリンクファイル間のハードリンクを保持するには、リストア時にソースファイルとリンクファイルを選択し、[ハードリンクの新しいファイルを作成 (Create new files for hard links)]チェックボックスのチェックマークをはずします。

クラウド仮想マシンでのボリュームのリストア

仮想マシン上の 1 つ以上のボリュームをリストアできます。

ボリュームをリストアするには

1. 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
2. [仮想マシン (Virtual machines)]タブをクリックします。
3. アプリケーションがホストされている仮想マシンを選択します。
4. VM が接続された後、右上の[保護の追加 (Add protection)]をクリックします。
5. 保護計画を選択し、[次へ (Next)]をクリックします。
6. [保護 (Protect)]をクリックします。
7. 保護計画を実行するには、[今すぐバックアップ (Backup now)]をクリックします。
8. リカバリポイントを表示するには、[リカバリポイント (Recovery points)]タブをクリックします。
9. 優先リカバリポイントの右上で、[ボリュームをリストア (Restore volumes)]を選択します。

   また、リカバリポイントにわたって検索する日付フィルタを適用することもできます。
10. [ボリュームをリストア (Restore volumes)]ダイアログボックスで、1 つ以上のボリュームを選択します。

11 [ターゲット VM (Target VM)]リストから、ボリュームのリストア先とする VM を選択します。

レプリケートされた (プライマリ以外の) VM からリストアするには、元の場所へのリストアはサポートされません。VM を選択しない場合、ファイルは元の VM にリストアされます。

12 [リストア (Restore)]をクリックします。

選択したボリュームのリストアジョブがトリガされます。アクティビティモニターでジョブの詳細を表示できます。

メモ: OCI の場合、ボリュームをリストアするには、クライアントの VM でブロックボリューム管理プラグインを有効にする必要があります。

メモ: ボリュームを同じ仮想マシンと場所にリストアする場合は、既存のボリュームを切断し、スロットを解放してからリストアを試行する必要があります。

LVM を含むボリュームリストア後の手順の実行

LVM ボリュームのボリュームリストア後の手順を実行できます。

メモ: SFR (シングルファイルリストア) または GRT (個別リストア) およびアプリケーションリストアは、インストールされているエージェントを介して実行されます。ただし、ボリュームリカバリでは、リカバリの成功後に関連ファイルシステムをオンラインにする必要があります。

ボリュームリストア後の手順を実行するには

1 コマンドを実行して、ホスト PV に新しく接続されたポストボリュームをすべて表示します。

重複する PV がある (上記のコマンドで警告が表示される) 場合は、次のコマンドを実行します。

```
vgimportclone --import /dev/<Device1> /dev/<Device2> ...
--basevgname <NewVGName>
```

または、ホストで新しく作成されたボリュームグループ (VG) を確認します。新しい VG が表示されない場合は、次のコマンドを使用して VG をインポートします。新しい VG は <NewVGName> として検出されます。

```
vgimport -a
```

```
vgs
```

2 次のコマンドを実行して、すべての論理ボリューム (新旧) を一覧表示します。

```
lvs <NewVGName>
```

3 <NewVGName> に属するすべての LV を有効化します。

```
lvchange --activate y /dev/mapper/<NewVGName>-<LVName1>
```

```
lvchange --activate y /dev/mapper/<NewVGName>-<LVName2>
```

```
lvchange --activate y /dev/mapper/<NewVGName>-<LVNameN>
```

4 認証され、新たに有効にされた LV の UUID とファイルシステムを特定します。

```
blkid -p /dev/mapper/<NewVGName>-<LVName1>
```

```
Output: /dev/mapper/<NewVGName>-<LVName1>:
UUID="2a4bdc14-b5eb-4ee6-b876-ebdcb66c55d9"
BLOCK_SIZE="4096"TYPE="xfs" USAGE="filesystem"
```

```
blkid -p /dev/mapper/<OldVGName>-<LVName1>
```

```
Output: /dev/mapper/<OldVGName>-<LVName1>:
UUID="2a4bdc14-b5eb-4ee6-b876-ebdcb66c55d9"
BLOCK_SIZE="4096"TYPE="xfs" USAGE="filesystem"
```

5 UUID が同じ場合は、次のように変更する必要があります。

ファイルシステム	手順

xfs	`mkdir <NewMountPoint>`
	`mount -o nouuid /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>`
	`umount <NewMountPoint>`
	`xfs_admin -U generate /dev/mapper/<NewVGName>-<LVName1>`
	`mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>`

ext2 / ext3/ ext4	`mkdir<NewMountPoint>`
	`tune2fs -U random /dev/mapper/<NewVGName>-<LVName1>`
	`mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>`

6 UUID が異なる場合は、次のコマンドを実行します。

```
mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>
```

トラブルシューティング

Microsoft Azure クラウドのスナップショットリストア処理のトラブルシューティング

同じ VM で後続の 2 回のリストア操作を開始すると、リストア操作中にエラーが発生します。このエラーによって、次の問題が発生する場合があります。

- 元の OS ディスクのタグが、新しく作成およびリストアされた OS ディスクにコピーされない。
- SSH エラーのため、VM をリストアした後、ユーザーのログオンが失敗する可能性がある。

回避方法:

システム上で SSH デーモンが実行されているかどうかを確認します。されていない場合、次の記事の手順を実行します。

learn.microsoft.com/ja-jp/troubleshoot/azure/virtual-machines/troubleshoot-ssh-connection

サポート対象外のファイルとフォルダのフィルタ処理

Snapshot Manager でサポートされていないパーティションまたはファイルシステムからファイルまたはフォルダをリストアしようとすると、リストアジョブで次のエラーが表示されます。

エラー nbcs (pid=<**プロセス** ID>) **資産** <**資産名**> **のスナップショットからのファイルとフォルダのリストアに失敗しました** (Error nbcs (pid=<processs id>) Failed to restore file(s) and folder(s) from snapshot for asset <asset name>)

回避方法:

Snapshot Manager でサポートされていないファイルまたはフォルダをフィルタ処理できます。プライマリサーバーの bp.conf ファイルで、次のフラグを設定して CP DISKMAP チェックを有効にします。

CP_DISKMAP_CHECK = true/yes

リストアからのバックアップ操作が部分的に成功する

選択したターゲットディレクトリのディスクに空きがない場合に、リストアからのバックアップ操作が部分的に成功します。次のメッセージが表示されます。

```
Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244) Granular restore(SFR) is completed
    Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244) Summary of SFR Operation - Success
files/folders count: 0 ,
    Failed files/folders count: 1 , Warning files/folders
    count: 0, Skipped files/folders count: 0
    Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244)
    Detailed restore summary report is available on recovery target host at location:
    /var/log/flexsnap/restore/granular-restore-09b4d44d
    .
    .
    Dec 29, 2022 2:57:51 PM - Warning bprd (pid=1977) Granular Restore from backup
completed with error.
    Copy the files manually from live access mount:

ip-10-239-185-241:/mnt/vpfs_shares/vmfiles/8fcc/8fcc132b-a202-49a8-b654-81ff242a718a/livemount

    Dec 29, 2022 2:57:51 PM - end Restore; elapsed time 0:01:51
    the requested operation was partially successful(1)
```

リストアからのバックアップでは、ライブマウントが正常に作成された場合、ASSET_NOT_FOUND とは別に他のエラーが報告されても、そのバックアップは部分的に成功したと見なされます。ターゲットの場所にネットワークデバイスまたはファイルシステムがマウントされていないか、ディスクがいっぱいの場合は、次のメッセージがジョブの詳細に表示されます。

```
 Jan 02, 2023 12:11:16 AM - Error nbcs (pid=13934)
187776K space required for file/folder restore while 20K is total available space on
/disk1
```

この場合、他のネットワークデバイスまたはファイルシステムがターゲットパスにマウントされている必要があったため、Snapshot Manager エージェントはデバイスまたはファイルシステムの空き容量を考慮します。空き容量のエラーでコピーが失敗すると、概略レポートにそれが記録されます。例:

```
 /var/log/flexsnap/restore/granular-restore-09b4d44d in above Job details log
```

回避方法:

- ターゲットホストの場所の概略レポートを確認します。次に例を示します。

```
/var/log/flexsnap/restore/granular-restore-09b4d44d
[root@ip-10-239-187-148 granular-restore-09b4d44d]# cat root-error.log
Dec 29 09:27:44: ERROR - FILE: /disk1/dl380g9-149-vm15_package.zip
[Error 28] IOError: No space left on device
```

- ディスク領域が原因でファイルのコピー操作が失敗した場合は、いくらかの領域を作成し、ライブマウントからファイルをコピーします。
  ライブマウントパスの詳細は、次のようにジョブの詳細で確認できます。

```
Dec 29, 2022 2:57:51 PM - Warning bprd (pid=1977) Granular Restore from backup completed
 with error.
Copy the files manually from live access mount:
ip-10-239-185-241:/mnt/vpfs_shares/vmfiles/8fcc/8fcc132b-a202-49a8-b654-81ff242a718a/livemount
```

ユーザーが切断されたターゲット仮想マシンを選択すると部分的リカバリが発生する

部分的リカバリは、次の理由により発生する場合があります。

- ターゲット仮想マシンが切断されている場合 (エージェントを介して接続されていない)。
- ターゲット仮想マシンでファイルまたはフォルダのコピー中にエラーが発生した場合。
- Windows 仮想マシンの内容が Linux ターゲット仮想マシンにリストアされた場合。

これらの部分的なリカバリの場合、作成されたインスタントアクセスは削除されず、以降 24 時間利用可能です。

インスタンスアクセスの保持間隔は、bp.conf ファイルの CLOUD_VM_IA_RETENTION_INTERVAL_IN_HOURS パラメータを使用して構成できます。(デフォルト値は 24 時間です。)

回避方法:

ユーザーは、ターゲットホストのインスタントアクセス共有にアクセスし、必要なファイルまたはフォルダを手動でコピーする手順を実行できます。

(NFS 経由でファイルをコピー) Linux ホストで Linux イメージの内容をリストアする方法:

- Linux システムに NFS 共有をマウントするには、次のコマンドを使用して NFS クライアントパッケージをインストールします。

  ```
  $ sudo yum install nfs-utils
  ```

- 次の mount コマンドを使用して、ターゲット Linux ホストでインスタントアクセスをマウントします。

  ```
  # Create a directory say /mnt/restore

  $ mkdir -p /mnt/restore

  # Mount the instant access

  $ mount -t nfs <InstantAccessServer:InstantAccessPath> /mnt/restore
  ```

- インスタントアクセスパスは、次の形式のアクティビティマネージャログから取得できます。

  ```
  <InstantAccessServer>:/mnt/vpfs_shares/vmfiles/<id>/<InstantAccessId>/livemount
  ```

(SMB アクセス) Windows ターゲットホストで Windows イメージの内容をリストアする方法 (ACL を使用):

- ソース仮想マシンイメージの MSDP ストレージサーバーの SMB クレデンシャルを Windows クレデンシャルマネージャに追加する必要があります。
- 指定したライブマウントを使用して、[アクティビティモニター (Activity Monitor)]、[ジョブの詳細 (Job details)]の順に移動して、仮想ハードディスクにアクセスします。
  仮想ハードディスクは、vhd_ の接頭辞付きでフォルダの下に一覧表示されます。
- [処理 (Action)]タブで、必要な仮想ハードディスクを接続して[OK]をクリックします。
- [次のドライブ文字を割り当てる (Assign the following drive letter)]オプションを選択して、データを参照する仮想ディスクに文字を割り当てて[OK]をクリックします。
- 前の手順で割り当てられたドライブに移動し、データを手動でコピーします。

(ライブマウント) Linux ターゲットホストで Windows イメージの内容をリストアする方法:

- Linux には CIFS パッケージが必要です。`# yum install cifs-utils` コマンドを使用してパッケージを取得します。
- `# mkdir <my_mount_dir>` コマンドを使用してマウントディレクトリを作成します。
- 次のように、Samba のユーザー名とパスワードを使用してエクスポートされたパスをマウントします。

```
mount -t cifs -o username=<sambauser>
//<InstantAccessServer>/<InstantAccessPath> <my_mount_dir>
```

- 次のコマンドを使用してファイルをコピーします。

```
# cp <my_mount_dir>/<file_path> <target_dir_path>
```

スナップショットのバックアップからのシングルファイルリストアで発生する問題

問題/エラー	説明	回避方法
確認するログパス	ターゲットホストのリストアについて詳しくは、次のログを確認してください。 ■ エージェントレスの場合: /opt/VRTScloudpoint/.agent/flexsnap-agentless-onhost.log ■ オンホストエージェントの場合: /var/log/flexsnap/flexsnap-agentless-onhost.log ■ 単一ファイルリストア固有のログの場合、アクティビティモニターに指定されたパスを使用します。	Snapshot Manager でのシングルファイルリストア中に発生したエラーまたは例外を解決するには、Snapshot Manager ホスト上の次のログを参照してください。 /cloudpoint/logs/flexsnap.log
リカバリ前チェックの失敗	切断されたターゲット仮想マシンにファイルとフォルダをリストアするときに、リカバリ前チェックが次のエラーで失敗します。 Target VM state: Target VM <vm_name> has no agent configured リカバリが開始されると、リストア操作は部分的に成功します。	リストアが成功するように、ターゲット仮想マシンが、構成されたエージェントに接続されていることを確認します。
ソース Linux VM からターゲット Windows VM への部分的なリカバリ (NFS クライアントなし)	Windows ターゲットコンピュータに NFS クライアントをインストールしない場合、ソース Linux VM からのファイルとフォルダのリストアは部分的に成功します。次のエラーが表示されます。 Error nbcs (pid=42513) Invalid operation for asset: <asset_id> Warning bprd (pid=42045) Granular Restore from backup completed with error. Copy the files manually from live access mount: <livemount_path>. Note that live access mount is available only for 24 hrs.	Linux VM から Windows VM へのリストアを実行する前に、Windows ターゲットコンピュータに NFS クライアントをインストールします。

問題/エラー	説明	回避方法
削除されたターゲット VM のリストアジョブの失敗	クラウド環境から削除されたターゲット VM にファイルとフォルダをリストアするときに、リストアジョブが次のエラーで失敗します。 `Error nbcs (pid=44859) Target VM not found, asset_id <asset_id>`	別のターゲット VM を選択します。
インスタントアクセスの作成の失敗	MSDP 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ない場合、リストアジョブ中にインスタントアクセスの作成が失敗します。	MSDP メディアサーバーでインスタントアクセスがサポートされているかどうかを確認します。次の事前チェックスクリプトを実行します。 /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
ターゲット VM に仮想ディスクを接続する空きドライブがない	選択したファイルを含むボリュームの数がターゲットホストの利用可能な空きドライブの数より多い場合、操作は失敗します。	リストアするボリュームの数を減らします。
十分な領域がありません: '*¥¥driverMapping.json	MSDP が構成されているメディアサーバーで FIPS が有効になっています。	MSDP がインストールされているメディアサーバーで FIPS を無効にします。または、ターゲット VM にドメインユーザー Samba クレデンシャルを追加します。

Azure クラウドプロバイダ VM の問題

VM のディスクの 1 つが初期化されていない場合、インスタントアクセスを使用した VM ファイルのダウンロードまたはリストアが次のエラーで失敗します。

```
Jan 24, 2023 11:58:47 AM - Error NBWMC (pid=3716) Internal Error:
('failed to find operation system information, please check the source
 VM', ('Failed to expose
VMDK', 1006), None)
Failed to create the instant access mount.
(4001)
```

`libguestfs` は、VM バックアップからファイルを取得するためにインスタントアクセスで使用されるサードパーティのツールです。ディスクが初期化されていない場合、`libguestfs` はファイルを取得できません。

回避方法:

ディスクを初期化し、VM をバックアップします。その後、インスタントアクセスを使用して VM ファイルのダウンロードまたはリストアを再試行します。

OCI からのスナップショットリストアでの問題

ターゲットパスが無効。ソースディスクと宛先ディスクの両方がブートディスクである、またはディスクが /dev/oracleoci/oraclevda にマウントされている

このエラーは、ブートボリュームから選択したファイルを少なくとも 1 つ使用し、リストアの宛先ボリュームがブートボリュームである場合に、スナップショットから個別リストアを試行した場合に発生します。

回避方法:

ブートボリュームまたはファイルシステムからファイルとフォルダをリストアするには、ターゲットパスとしてブロックボリュームを指定します。

対応するファイルシステムがスナップショットに含まれていないため、選択したファイルまたはフォルダがリカバリからスキップされた。

スナップショットからの個別リストア中、Oracle Cloud Agent がインストールされていない VM、または準仮想化された接続方式を使用してディスクが接続されている VM でこのエラーが発生します。

アクティビティモニターのエラー:

```
[{'error': 'The selected files/folders were skipped from recovery as
 the snapshot does not contain the corresponding file system.',
'mount': 'Unknown Mount Point/Drive'}]}}"
```

回避方法:

次を実行します。

- Oracle Cloud Agent をインストールします (Oracle がそのプラットフォームをサポートしている場合)。または、iSCSI 接続タイプを使用してすべてのディスクを接続します (ブートディスクを含む)。
- 検出が完了するまで待機してから、バックアップを再試行します。

スナップショットコピーからの個別リストアが「Block Volume Plug-in: must be enabled on the instance…」というエラーで失敗する

このエラーは、Oracle Cloud Agent のブロックボリューム管理プラグインがターゲット VM で有効になっていない場合に発生します。

回避方法:

次を実行します。

1. ターゲット VM で、OCI コンソールからブロックボリューム管理プラグインを有効にします。
2. VM を再起動します。
3. リストアを再試行します。

5

クラウド資産の保護とリカバリの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。

クラウドの作業負荷の保護に関する問題のトラブルシューティング

クラウド資産の保護で発生する問題のトラブルシューティングを行うには、次のログファイルを確認します。

- 「スナップショットの削除のログファイル」

トラブルシューティングの際に、必ず、制限事項も確認します。p.12 の「制限事項および考慮事項」を参照してください。

問題をトラブルシューティングするには、『NetBackup™ 状態コードリファレンスガイド』を参照してください。

Snapshot Manager ログファイルを表示するには、『NetBackup Snapshot Manager インストールおよびアップグレードガイド』の Snapshot Manager のログに関するトピックを参照してください。

構成用のログファイル

クラウド構成の問題のトラブルシューティングを行うには、次のログを使用します。

表 5-1　　構成用のログファイル

プロセス	ログ
tpconfig `tpconfig` コマンドは、Snapshot Manager を NetBackup に登録する唯一の方法です。	Windows の場合 *`NetBackup install path`*`¥Volmgr¥bin¥tpconfig.exe` UNIX の場合 `/usr/openv/volmgr/bin/tpconfig`

nbwebservice
プラグインは、NetBackup REST API を使用して構成します。
	Windows の場合
	`NetBackup install path``¥NetBackup¥wmc¥webserver¥logs`
	UNIX の場合
	`/usr/openv/wmc/webserver/logs`
	`/usr/openv/logs/nbwebservices`

nbemm nbemm は、Snapshot Manager とプラグインの情報を EMM データベースに格納します。	Windows の場合 *`NetBackup install path`*`¥NetBackup¥logs¥nbemm` UNIX の場合 `/usr/openv/logs/nbemm`

資産検出のログファイル

資産検出の問題のトラブルシューティングを行うには、次のログを使用します。

表 5-2 資産検出のログファイル

プロセス	ログ
ncfnbcs 検出が完了したかどうかを確認します。	Windows の場合 *NetBackup install path*/bin/vxlogview –o 366 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -o 366
Picloud 検出操作の詳細を提供します。	Windows の場合 NetBackup install path/bin/vxlogview –i 497 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 497
nbwebservice 検出操作に含まれる資産データベースワークフローについての詳細を取得できます。 **メモ:** 保護計画に追加されている資産について詳しくは、同じログファイルを参照してください。	Windows の場合 NetBackup install path/webserver/logs UNIX の場合 /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices

スナップショット作成のログファイル

スナップショット作成の問題のトラブルシューティングを行うには、次のログを使用します。

表 5-3 スナップショット作成のログファイル

プロセス	ログ
nbpem 特定のジョブの nbpem PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 NetBackup install path/bin/vxlogview –o 116 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -o 116
nbjm 特定のジョブの nbjm PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 NetBackup install path/bin/vxlogview –o 117 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -o 117

プロセス	ログ
nbcs 特定のジョブの nbcs PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 *NetBackup install path*/bin/vxlogview -i 366 -P *nbcs_process_id* UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id* nbcs ログは次の場所から入手できます。 Windows の場合 NetBackup install path/logs/ncfnbcs UNIX の場合 /usr/openv/logs/ncfnbcs
nbrb nbrb は、特定のジョブのメディアサーバーを提供するために要求されます。クラウドの場合、特定のメディアサーバーは、Snapshot Manager に関連付けられたメディアサーバーのリストから選択されます。	Windows の場合 NetBackup install path/bin/vxlogview –o 118 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 118

リストア操作のログファイル

リストアの問題のトラブルシューティングを行うには、次のログを使用します。

表 5-4

プロセス	ログ
nbwebservice スナップショットのリストア操作は、NetBackup REST API によってトリガされます。	Windows の場合 NetBackup install path/webserver/logs UNIX の場合 /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices
bprd NetBackup REST API は、リストアを開始するために bprd と通信します。	Windows の場合 NetBackup install path/netbackup/logs UNIX の場合 /usr/openv/netbackup/logs/bprd

プロセス	ログ
ncfnbcs 特定のジョブの nbcs PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 *NetBackup install path*/bin/vxlogview -i 366 -P *nbcs_process_id* UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*

スナップショットの削除のログファイル

スナップショットの削除の問題のトラブルシューティングを行うには、次のログを使用します。

表 5-5 スナップショットの削除のログファイル

プロセス	ログ
bpdm スナップショットの削除またはクリーンアップ操作は、bpdm によってトリガされます。	Windows の場合 NetBackup install path/netbackup/logs UNIX の場合 /usr/openv/netbackup/logs/bpdm
ncfnbcs 特定のジョブの nbcs PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 *NetBackup install path*/bin/vxlogview -i 366 -P *nbcs_process_id* UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*

代替の場所へのリストア中にリカバリ前チェックがアクセス拒否エラーで失敗する

バックアップイメージコピーからの VM のリカバリを試行したとき、代替の場所へのリストアを実行するために必要な権限が役割に割り当てられていない場合、リカバリ前チェックの操作中にエラーが発生します。

これは、元の場所のリカバリのみを実行する権限があり、代替の場所へのリカバリを実行しようとしている場合に発生する可能性があります。

回避方法

- 元の場所へのリストアを実行中に、リカバリ前ページの事前入力されたフィールドを変更しないでください。

- 代替の場所へのリカバリを実行する場合は、必要な権限が付与されている必要があります。

エラーコード 9855: 資産 <asset_name> のスナップショットのエクスポート中のエラー

説明:

スナップショットからのバックアップジョブを実行するときに、ブロックボリューム管理プラグインが NetBackup Snapshot Manager ホストで有効になっていない場合、バックアップジョブがこのエラーで失敗します。

回避方法:

OCI コンソールの［Oracle Cloud Agent］タブで NetBackup Snapshot Manager ホストのブロックボリューム管理プラグインを有効にします。

CMK を使用して暗号化されたディスクを持つ VM とその他の OCI 資産が、NetBackup UI で削除済みとしてマークされる。

説明:

OCI プロバイダの KMS サービスが停止している場合、CMK を使用して暗号化されたディスクを持つ VM とその他の OCI 資産が、NetBackup UI で削除済みとしてマークされます。KMS サービスがリストアされると、プラグインレベルの検出が正常に完了すると削除済みの状態は解除され、資産または VM がバックアップできるようになります。これ以外の操作は必要ありません。

回避方法:

OCI プロバイダ側の KMS サービスが実行中であることを確認します。

スナップショットからのバックアップジョブに予想より長い時間がかかる

説明:

スナップショットからのバックアップジョブは、約 23 Mbps の遅い転送速度で実行する場合、予測よりも長い時間がかかります。

回避方法:

NetBackup Snapshot Manager ホストの flexsnap.conf ファイルに次のエントリを追加します。

```
[oci]

        vol_max_vpu_cnt_in_bfs_restore = 120
```

Snapshot Manager が Ubuntu ホストに配備されている場合、接続の問題によりスナップショットからのバックアップジョブが失敗する

説明:

OCI では、Ubuntu ホストに Snapshot Manager を配備すると、デフォルトの iptable ルールにより、NetBackup サービス間のネットワーク接続に関する問題が発生する場合があります。これらの接続の問題により、スナップショットからのバックアップ、インデックス付け、バックアップからのリストアの各ジョブが失敗する場合があります。

回避方法:

例に示すように、iptable ファイルの iptable ルールをコメントアウトします。

```
   Workaround:
         If backup from snapshot needs to be run on Ubuntu deployed
 NBSM (on oracle cloud) then the iptable rules file should look like
 this after commenting out the rules present by default:

          root@nbsm-host:/# cat /etc/iptables/rules.v4
          # CLOUD_IMG: This file was created/modified by the Cloud
 Image build process
          # iptables configuration for Oracle Cloud Infrastructure
          # See the Oracle-Provided Images section in the Oracle
Cloud Infrastructure
          # documentation for security impact of modifying or
removing these rule
```

NetBackup UI でのエラーのあいまいさの排除

NetBackup では、PaaS およびアプリケーションのさまざまなプロセス中に発生する可能性のあるエラーに対する簡単なトラブルシューティングオプションを提供します。クレデンシャルの検証、バックアップ、リストアなどの一般的な操作では、NetBackup はエラーの根本原因の識別子を含む通知を生成します。通知には、原因と推奨処置の詳細を含む記事へのリンクが含まれています。

状態コード 150: 管理者から終了が要求されました

説明: これは、アクティビティモニターからバックアップ、スナップショットまたはリストアジョブを手動で取り消すと表示されます。

リストアジョブの場合、仮想マシンまたはボリュームはリストア操作中にポータルで作成されます。リストアジョブが取り消されたため、関連付けられた NetBackup ジョブがない可能性があります。クラウドコストの観点からクラウドにリソースが作成されている場合、クラウド管理者は新しく作成されたリソースを確認する必要があります。

回避策: プロバイダポータルから仮想マシンまたはボリュームを手動でクリーンアップします。また、作成された一時的なステージング領域のボリュームもクリーンアップします。

PaaS の作業負荷の保護とリカバリに関する問題のトラブルシューティング

バックアップがエラー「3808 データベースが存在するかどうかを確認できません。(Cannot check if the database exists.)」で失敗する。

アクティビティモニターに次のメッセージが表示されます。

AuthorizationFailed -Message: The client '<clientId> '<objetId>' does not have authorization to perform action 'Microsoft.Sql/servers/databases/read' over scope '<resoourceId>' or the scope is invalid. アクセス権が最近付与された場合は、クレデンシャルを更新してください。

説明: このエラーは、Snapshot Manager と NetBackup が AKS に配備されており、次の条件に該当する場合に発生します。

- メディアサーバーのポッドノードプールが Snapshot Manager ノードプールとは異なるノードプールである
- 管理対象 ID が Snapshot Manager 仮想マシンスケールセットで有効になっている

回避方法: 次のいずれかを実行します。

- バックアップとリストアのためのメディアサーバーで、スケールセットの管理対象 ID を有効にします。また、この管理対象 ID に割り当てられた役割に必要な権限を割り当てます。
- MSDP サーバーでストレージユニットを作成し、スケールの構成で管理対象 ID 機能が有効になっているメディアサーバーのみを使用します。

データベースまたはリソースグループに読み取り専用ロックが適用されている場合はバックアップが失敗し、削除ロックが適用されている場合は部分的に成功する。

説明: この問題は、読み取り専用ロックまたは削除ロック属性がデータベースまたはリソースグループに適用されている場合に発生します。

回避方法: バックアップまたはリストアを実行する前に、データベースまたはリソースグループから既存の読み取り専用ロックと削除ロック属性を削除します。

状態コード 150: 管理者から終了が要求されました

説明: これは、アクティビティモニターからバックアップジョブまたはリストアジョブを手動で取り消し、部分的なリストアの処理中にポータルでデータベースが作成された場合に表示されます。

回避方法: プロバイダポータル上のデータベースと、データベース名で作成された特定のディレクトリにあるユニバーサル共有のマウント場所の一時ステージング場所を手動でクリーンアップします。

アクティビティモニターに古い状態メッセージが表示される

説明: 新しい Snapshot Manager コンテナサービスが突然再起動すると、プロバイダ保護されたリストアジョブが有効な状態のまま、アクティビティモニターの詳細ページには、更新された状態が表示されない場合があります。

回避方法: Snapshot Manager で、次のコマンドを使用して、ワークフローコンテナを再起動します。

```
docker restart flexsnap-workflow-system-0-min
flexsnap-workflow-general-0-min
```

コンテナを再起動すると、アクティビティモニターでリストアジョブが更新され、最新の状態が表示されます。

状態コード 233: 想定しない EOF が発生しました

説明: バックアップに使用するクライアント名が 255 文字を超えると表示されます。

bpdbm ログにも同じ問題を示す次のエラーメッセージが表示されます。

```
db_error_add_to_file: Length of client is too long. Got 278, but
limit is 255. read_next_image: db_IMAGEreceive() failed: text exceeded
allowed length (225)
```

メモ: これは、プライマリサーバーが RHEL の場合に発生します。

回避方法: クライアント名が 255 文字以内になるようにデータベースの名前を変更します。

Error: Broken pipe (32), premature end of file encountered EXITING with status 42, network read failed

または

状態 174: media manager - システムエラーが発生しました (media manager - system error occurred)

説明: バックアップ中に、保護計画の作成中にポリシー接頭辞の長さが許可された長さよりも長い場合に発生します。このため、カタログイメージのファイルパスの長さが 256 文字を超え、アクティビティモニターに上記のエラーメッセージが表示されて失敗します。

bpdbm ログにも同じ問題を示す次のエラーメッセージが表示されます。

```
<16> db_error_add_to_file: cannot stat(¥¥?¥C:¥Program Files¥Veritas
¥NetBackup¥db¥images ¥azure-midb-1afb87487dc04ddc8fafe453dccb7ca3+
nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+
testdb_bidinet02¥1656000000¥tmp¥catstore¥
BACKUPNOW+141a73e7-cdc4-4371-823a-f170447dba2d_
1656349831_FULL.f_imgUserGroupNames0): No such file or directory (2)
<16> ImageReadFilesFile::get_file_size: cannot stat(¥¥?¥C:¥Program
Files¥Veritas¥NetBackup¥db
¥images¥azure-midb-1afb87487dc04ddc8fafe453d
ccb7ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_
bidinet02¥1656000000¥tmp¥catstore¥BACKUPNOW+141a73e7-cdc4-4371
-823a-f170447dba2d_1656349831_FULL.f_imgUserGroupNames0): No such
file or directory (2) <16> ImageReadFilesFile::executeQuery: Cannot
copy ¥¥?¥C:¥Program
Files¥Veritas¥NetBackup¥db¥images¥azure-midb-1afb87487dc04ddc8fafe453dccb7
ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_bidinet02¥1
656000000¥tmp¥catstore¥BACKUPNOW+141a73e7-cdc4-4371-823a-f170447d
ba2d_1656349831_FULL.f_imgUserGroupNames0
```

メモ: これは、プライマリサーバーが Windows の場合に発生します。

回避策: カタログパスの長さが合計で 256 文字未満になるように、保護計画のポリシーの接頭辞名を 10 文字未満の長さにします。

状態コード 3801: 要求された操作を完了できません。(Cannot complete the requested operation.)

説明: NetBackup は、要求された操作を正常に実行できません。

推奨処置: 考えられるエラーの原因については、アクティビティモニターの詳細を参照してください。

状態コード 3817: バックアップ前操作を完了できません (Cannot complete the pre-backup operation)

説明: dbagentsutil ログにエラーメッセージ「pg_dump: error: query failed: ERROR: permission denied for table test;pg_dump: error: query was: LOCK TABLE public.test IN ACCESS SHARE MODE;Invoked operation: PRE_BACKUP failed」が表示されます。

異なる役割を持つ複数のテーブルがあるデータベースをバックアップしようとすると発生します。テーブルにデータベース所有者とは異なる所有者が 1 人以上存在し、その所有者がデータベース所有者役割のメンバーでない場合、バックアップが失敗する可能性があります。

対処方法: バックアップまたはリストアするデータベース内のすべてのテーブルにアクセスできる役割が必要です。

たとえば、2 つのテーブルがある**学校**のデータベースをバックアップしたいとします。

- **学生**テーブルの所有者は postgres です。
- **教員**テーブルの所有者は schooladmin です。

新しい役割を作成します。例: NBUbackupadmin

次のコマンドを実行して、役割を作成します。

```
postgres=> CREATE USER NBUbackupadmin WITH PASSWORD '***********';

CREATE ROLE
```

この新しい役割を postgres 役割と schooladmin 役割のメンバーに適用するには、次のコマンドを実行します。

```
postgres=> GRANT postgres TO NBUbackupadmin;

GRANT ROLE

postgres=> GRANT schooladmin TO NBUbackupadmin;

GRANT ROLE
```

メモ: データベース内のすべてのテーブルに対して、テーブルの所有者または所有者のメンバーである役割が必要です。

バックアップが状態 40 (ネットワーク接続の切断) で失敗する

説明: メディアサーバーへの接続が切断されたため、バックアップが失敗します。

推奨処置: ポリシーでチェックポイントが有効になっている場合は、バックアップジョブを再開できます。ネットワークの問題が解決したら、Web UI で未完了のバックアップジョブを選択し、[再開 (Resume)]をクリックします。ジョブは停止された時点から再開されま

す。ポリシーでチェックポイントが有効になっていない場合、ジョブは Web UI で失敗したジョブとして表示されます。

バックアップジョブがエラー[データベースのバックアップに失敗しました (Failed to backup database)]で失敗する

説明: ジョブの詳細には、次のような追加の詳細が含まれます:
ManagedIdentityCredential 認証が利用できません。要求された ID はこのリソースに割り当てられていません。割り当てられたメディアサーバーに管理対象 ID が関連付けられていません。

推奨処置: PaaS Azure SQL と管理対象インスタンスにシステムまたはユーザーの管理対象 ID を使用する場合は、メディアサーバーとスナップショットマネージャに同じ権限またはルールのセットを適用します。ユーザーの管理対象 ID を使用する場合は、同じユーザーの管理対象 ID をメディアサーバーと Snapshot Manager に接続します。

エラーコード 3842 - 対応する PaaS 資産に対して要求されたバックアップ形式はサポートされていません。(The requested backup type for the corresponding PaaS asset is unsupported.)

差分増分バックアップは、Azure SQL Server と Azure SQL 管理対象インスタンスでのみサポートされます。サポートされていないバックアップ形式を選択すると、このエラーが表示されます。

エラーコード 3843 または 3844 - CDC の無効化に失敗しました。/CDC の有効化に失敗しました。(Failed to disable CDC./Failed to enable CDC.)

CDC を有効または無効にする権限がない場合に表示されます。

回避方法: Azure 環境で CDC を有効または無効にするために必要な権限を NetBackup に付与します。

メモ: CDC を手動で有効にしないでください。CDC を有効または無効にする権限を NetBackup に付与します。

エラー: クライアントリストアの終了状態 5: 要求されたファイルのリカバリに失敗しました (the restore failed to recover the requested files) クラウドポリシーのリストアエラー (2824)

エラー: ERR - データベース [<db_name>] (名前 [<db_name>]) のリストアに失敗しました。(Failed to restore database [<db_name>] with name [<db_name>].) ERR - ファイルを開けませんでした " (Failed to open file ".) エラー番号 = 12: クライアントリストアの終了状態 5: リストアは、要求されたファイルの

リカバリに失敗しました (the restore failed to recover the requested files)

説明: リストア中に、バックアップイメージが 10.2 メディアで生成され、リストアが古い (10.2 より前の) メディアサーバーに対して行われた場合に発生します。

回避策: リストアメディアを 10.2 に変更し、古いメディアをストレージから削除します。

自動スケーリングを有効にしてバックアップイメージからリストアした後、AWS DynamoDB テーブルで自動スケーリングが有効になっていない

説明: 現在、AWS API レスポンスでは、テーブルで自動スケーリングが有効になっているかどうかは示されません。したがって、バックアップ中にこのメタデータは NetBackup にキャプチャされず、その結果、リストアされたテーブルでは自動スケーリングが有効になりません。

回避策: AWS ポータルで、リストアされた DynamoDB テーブルの自動スケーリングプロパティを手動で有効にします。

CDC が有効な Azure SQL MI 増分バックアップ: CDC が有効なデータベースを削除すると、スキーマが変更されず、増分バックアップでなく完全バックアップが実行されます。

説明: Azure SQL MI は、CDC が有効なデータベースの詳細を `msdb` スキーマ内の `cdc_jobs` テーブルに保持します。データベースが削除されると、`cdc_jobs` エントリを削除する必要があります。このエントリが `cdc_jobs` テーブルから削除されない場合があります。したがって、`cdc_jobs` テーブル内にすでに存在する同じ `db_id` を使用して新しいデータベースが作成されると、問題が発生します。

回避策: データベースを削除する場合は、削除されたデータベースのエントリを `msdb` スキーマの `cdc_jobs` テーブル内で確認します。このエントリが存在する場合は、手動で削除します。

AWS RDS: db インスタンスの詳細のフェッチ中にエラーが発生しました: DescribeDBInstances 操作の呼び出し時にエラー (SignatureDoesNotMatch) が発生しました: 署名の有効期限が切れました。(AWS RDS: Error while fetching details of db instance: An error occurred (SignatureDoesNotMatch) when calling the DescribeDBInstances operation: Signature expired.)

説明: RDS boto3 API が失敗すると、このエラーが表示されます。NetBackup は、DescribeDBInstances 操作についてこのエラーを表示します。

回避方法: メディアサーバーの日時を実際のネットワークの日時と同期します。

また、正しいプロバイダのクレデンシャルを使用しているかどうかを確認します。

ターゲット NetBackup ドメインのレプリカからのインポートが状態コード 191 で失敗する

説明: ターゲットドメインでのインポート操作が、状態コード 191: [正常に処理されたイメージはありませんでした (`No images successfully processed`)] で失敗することがあります。アクティビティモニターのジョブの詳細には、[JSON ペイロードの作成に失敗しました (`Failed to create JSON payload`)] が表示されます。

原因: ターゲットドメインにレプリケートしているイメージは、NetBackup 10.4 以前のメディアサーバーから作成されています。これには、NetBackup カタログに必要なメタデータがありません。

回避方法: 次のいずれかを実行します。

- PaaS 作業負荷に AIR 機能を使用するには、バージョン 10.4 以降のメディアサーバーを使用します。
- 10.4 メディアサーバーに EEB をインストールして、PaaS 作業負荷の AIR 機能の旧バージョンのメディアサーバーとして使用します。詳しくは、Cohesity テクニカルサポートにお問い合わせください。

Amazon Redshift の問題のトラブルシューティング

問い合わせ文字列が 100 KB を超える場合、Amazon Redshift のリストアが失敗する

説明:

これは AWS の既知の制限事項です。問い合わせ文の最大サイズは 100 KB です。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/redshift/latest/mgmt/data-api.html

Redshift データベースのリストアが正常に完了した後、ストアドプロシージャ、ビュー、関数の数がソースデータベースと同じでない場合。

回避方法:

次を実行します。

1 次の API を使用して、IA (インスタントアクセス) パスをマウントします。

```
netbackup/recovery/workloads/cloud/paas/instant-access-mounts
```

2 メディアサーバーのマウントパスに移動します。

3 マウントパスのディレクトリ階層が次の通りであることを確認します。

```
ClusterDirectory/DatabaseDirectory/DatabaseDirectory/SchemaDirectory/TableDirectory
```

4 SchemaDirectory で、ファイル StoredProcedures.json、Views.json、および Functions.json を見つけます。各ファイルには、Amazon Redshift クエリーエディタ 2 で実行できる 1 つ以上の SQL 文が含まれています。

これらの SQL ステートメントを手動で実行します。

botocore.exceptions.ClientError: ListDatabases 操作を呼び出すときにエラーが発生した (InvalidSignatureException)

説明:

AWS Redshift API を実行するシステム時刻が正しくない場合、このエラーが表示されます。ログに次のメッセージが表示されます。

```
Signature expired: 20230226T181919Z is now earlier than
20230226T181921Z (20230226T182421Z - 5 min.)"
```

回避方法:

ntpdate コマンド実行して、システム時刻を修正します。

バックアップジョブまたはリストアジョブが「NoCredentialsError: クレデンシャルが見つかりません (NoCredentialsError: Unable to locate credentials)」エラーで失敗する。

説明:

このエラーは地域が指定されていない場合に表示されます。dbagentsutil ログに次のエラーが記録されます。dbagentsutil ログは、次の場所で見つけることができます。

```
/usr/openv/netbackup/logs/
```

回避方法:

次を実行します。

1 dbagent が実行されているメディアサーバーに AWS CLI をダウンロードします。

2 次のコマンドを実行します。

```
aws configure
```

3 プロンプトが表示されたら EC2 の地域名を入力します。他のパラメータの値は指定しないでください。

Redshift データベースのバックアップとリストアが停止する

説明:

このエラーは、検出を実行する NetBackup Snapshot Manager に Redshift クラスタへのアクセス権がない場合に表示されます。flexsnap のログに次のエラーが表示されます。

```
Connect timeout on endpoint URL:
"https://redshift.us-east-2.amazonaws.com/
```

回避方法:

アクセス権がない場合、Snapshot Manager では、「Redshift サービスの VPC エンドポイント」のセキュリティグループに含まれるスナップショットマネージャに対してインバウンドルールを設定する必要があります。

AWS ポータルで、クラスタを選択します。[Properties]、[Network and security settings]、[virtual private cloud object]、[Endpoints]の順に選択します。検索フィールドで「redshift-endpoint」を検索し、VPC エンドポイント ID をクリックして[Security Groups]タブをクリックします。[Security Group ID]、[Edit Inbound rules]の順に選択して、メディアサーバーに次を追加します。

```
Type : HTTPS

Protocol : TCP

Port range : 443

Source : 10.177.77.210/32
```

* ここで、ソースはメディアサーバーインスタンスを参照します。

NetBackup Web UI からリカバリを再び実行します。

Azure Postgres の問題のトラブルシューティング

増分バックアップジョブが、上限に達したためレプリケーションスロットを作成できないというエラーで失敗する

説明:

サーバーで作成されたレプリケーションスロットの数が、構成済みの `max_replication_slot` サーバーパラメータを超えています。

回避方法:

次のいずれかを実行します。

- 未使用のレプリケーションスロットを削除します。
- サーバーパラメータの `max_replication_slots` の値を大きくします。

バックアップが、[XID 1676198 のデータファイルに書き込めません: デバイスに領域が残っていません (Could not write to data file for XID 1676198: No space left on the device)]のエラーで失敗する

説明:

WAL がいっぱいで WAL_SIZE サーバーパラメータの構成値に達しました。

回避方法:

サーバーパラメータの WAL_SIZE の値を大きくします。

Amazon RDS Custom for SQL の問題のトラブルシューティング

RDS Custom SQL オンプレミスエージェントのアクセス拒否エラー。

説明:

このエラーは、バックアップ操作中に作成されたバッチファイルを削除するときに、バックアップ後の操作で発生します。そのインスタンスでバックアップジョブが実行されていない場合は、これらのバッチファイルを手動で削除できます。