NetBackup™ Web UI クラウド管理者ガイド

リリース 10.2

VERITAS™

最終更新日: 2023-04-28

法的通知と登録商標

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

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

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

マニュアル

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

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

1

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 クラウドの資産を保護でき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	環境に Snapshot Manager をインストールします。 p.13 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.10 の「制限事項および考慮事項」を参照してください。
Snapshot Manager の構成	NetBackup で Snapshot Manager を登録します。 『NetBackup Snapshot Client 管理者ガイド』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.14 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。 Amazon の場合は、IAM ロールを使用することもできます。 p.17 の「AWS の構成の IAM ロール」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.18 の「Snapshot Manager の資産の検出」を参照してください。
保護計画の作成	保護計画を作成します。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.49 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。
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.56 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.77 の「クラウド資産のリカバリ」を参照してください。 p.77 の「クラウド資産のリカバリ」を参照してください。 p.85 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。
トラブルシューティング	p.112 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、Snapshot Manager サーバー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: Veritas 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。

NetBackup での Snapshot Manager の構成

NetBackup Web UI を使用して Snapshot Manager を追加できます。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クラウド資産を検出できます。

次の重要な点に注意してください。

- 複数の Snapshot Manager を NetBackup プライマリサーバーに関連付けることができます。ただし、1 つの NetBackup マスターサーバーに関連付けることができる Snapshot Manager は 1 つだけです。
- 複数のメディアサーバーを Snapshot Manager に関連付けることができます。NetBackup プライマリサーバーにリンクされているメディアサーバーのみを Snapshot Manager にリンクできます。
- 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 の設定

作業	説明
Snapshot Manager の追加	NetBackup で Snapshot Manager を追加するには、Snapshot Manager のクレデンシャルを追加し、証明書を検証する必要があります。p.13 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.14 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.18 の「Snapshot Manager の資産の検出」を参照してください。
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.18 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。

サードパーティ CA 証明書の構成

自己署名証明書またはサードパーティの証明書を使用して、Snapshot Manager を検証できます。

以下のポイントを考慮します。

- Windows の場合、証明書をファイルパスとして指定するか、信頼できる root 認証局にサードパーティの証明書をインストールすることができます。
- すでに追加されている Snapshot Manager の自己署名証明書をサードパーティの証明書に切り替えるには、`tpconfig` コマンドを更新するか、Snapshot Manager API を編集するか、NetBackup Web UI から行えます。

サードパーティ CA 証明書を構成するには

1. Snapshot Manager のサードパーティ証明書と秘密鍵を生成します。
2. /cloudpoint/scripts/cp_certificate_management.sh スクリプトを実行して、証明書、鍵、トラストストアを Snapshot Manager にアップロードします。
3. NetBackup で証明書ファイルを作成し、root とすべての中間 CA の証明書を pem ファイルに追加します。
4. `/cloudpoint/openv/netbackup/` にある `bp.conf` ファイルで、次のエントリを作成します。
   - ECA_TRUST_STORE_PATH = /cloudpoint/eca/trusted/cacerts.pem
   - (オプション) VIRTUALIZATION_CRL_CHECK = CHAIN
   - (オプション) ECA_CRL_PATH =/cloudpoint/eca/crl/

   メモ: CA 証明書と CRL は、トラストストアの場合は `/cloudpoint/eca/trusted/cacerts.pem`、CRL の場合は `/cloudpoint/eca/crl` に存在する必要があります。

   - ECA_CRL_PATH オプションは、外部認証局 (CA) の証明書失効リスト (CRL) が保存されているディレクトリのパスを指定します。ECA_CRL_PATH 内のすべてのファイルは DER、PEM、P7B 形式である必要があります。
   - VIRTUALIZATION_CRL_CHECK オプションは、証明書の失効状態を確認する場合にのみ必要です。デフォルトでは、VIRTUALIZATION_CRL_CHECK は無効になっています。
   - VIRTUALIZATION_CRL_CHECK オプションの有効値は、LEAF、CHAIN、DISABLE です。LEAF - CRL でリーフ証明書の失効状態が検証されます。CHAIN - CRL で証明書チェーンの証明書すべての失効状態が検証されます。

メモ: 証明書は、リーフ、中間、root の順序でアップロードする必要があります。証明書が正しい順序でアップロードされないと、Snapshot Manager が動作しないことがあります。

5 Snapshot Manager を NetBackup に追加するか、`tpconfig` コマンドを実行することにより、NetBackup にすでに追加されている Snapshot Manager の証明書を更新します。

Snapshot Manager の追加

NetBackup Web UI を使用して Snapshot Manager を追加できます。Snapshot Manager のクレデンシャルを入力し、証明書を検証する必要があります。

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 左側の[クラウド (Cloud)]をクリックします。

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 FDQN 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 [検証 (Validate)]をクリックします。

7 [証明書の検証 (Validate certificate)]ダイアログボックスで、[承認 (Accept)]をクリックします。

8 Snapshot Manager のインストール時に指定した Snapshot Manager のクレデンシャルを入力します。

9 [保存 (Save)]をクリックします。

メモ: NetBackup のセキュリティレベルが[最高 (Very High)]に設定されている場合、追加のフィールド[トークン (Token)]が表示され、標準ホストトークンを指定できます。これは、Snapshot Manager で NetBackup 証明書を生成するために必要です。トークンの生成に必要な追加のセキュリティ権限を要求する場合は、セキュリティ管理者またはバックアップ管理者にお問い合わせください。

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 クラウド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. 左側の[クラウド (Cloud)]をクリックします。
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: System managed identity	Azure の Snapshot Manager ホストでシステム管理 ID を有効にします。 **メモ:** システムの管理対象 ID にロールを割り当てます。
	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。
	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:*	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。
	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 **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。	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。
	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。
	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。

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。

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。

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.14 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。

開始前に次の点を確認してください。

- IAM ロールは AWS で構成されます。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。
- NetBackup と Snapshot Manager を最新バージョンにアップグレードした後、クレデンシャルを更新する必要があります。次のコマンドを実行します。

```
tpconfig -update -snapshot_manager <snapshot manager host>
-snapshot_manager_user_id <snapshot manager user ID>
-manage_workload <workload type> -security_token <security token>
```

メモ: アップグレード後、クレデンシャルは IAM ロールのみをサポートするように更新されます。

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。

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 マスター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 マスター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. 左側の[クラウド (Cloud)]をクリックします。
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、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 マスターサーバーと 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。これは実際に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. 左側の[クラウド (Cloud)]をクリックします。
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. 左側の[クラウド (Cloud)]をクリックします。
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 の編集

Snapshot Manager のクレデンシャルを更新できます。ただし、Snapshot Manager のホスト名、IP アドレス、またはポートは編集できません。

Snapshot Manager を編集するには

1. 左側の[クラウド (Cloud)]をクリックします。
2. [Snapshot Manager]タブをクリックします。
3. Snapshot Manager の横のメニューから[編集 (Edit)]をクリックします。

   Snapshot Manager のクレデンシャルのみを編集できます。クレデンシャルを更新するには、まず証明書を確認する必要があります。
4. クレデンシャルを更新します。
5. [トークン (Token)]フィールドに、Snapshot Manager の再発行トークンを入力します。
6. [保存 (Save)]をクリックします。

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. 左側の[クラウド (Cloud)]をクリックします。
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
- 管理対象の Kubernetes クラスタを使用する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。

インテリジェントクラウドグループの管理

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、またはボリュームを選択し、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。

インテリジェントクラウドグループの作成

インテリジェントクラウドグループを作成するには

1. 左側の[クラウド (Cloud)]をクリックします。
2. [インテリジェントグループ (Intelligent groups)]タブ、[+ 追加 (+ Add)]の順にクリックします。
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、クラウドインテリジェントグループは領域全体の資産を保護します。

---

5 ［資産タイプ (Asset type)］を選択します。

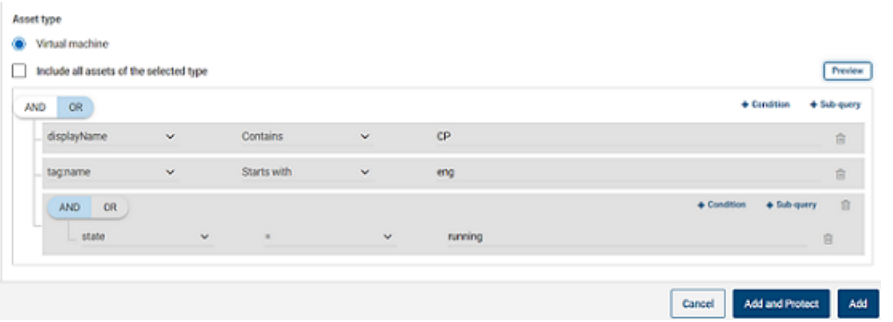
6 その後、次のいずれかを実行します。

- ［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するために［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.24 の「インテリジェントクラウド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 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。

インテリジェントクラウド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	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。

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。

インテリジェントクラウドグループの削除

インテリジェントクラウドグループを削除するには

1. 左側の[クラウド (Cloud)]をクリックします。
2. [インテリジェントグループ (Intelligent groups)]タブで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インテリジェントクラウドグループの保護

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.27 の「NetBackup 9.1 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. 左側の[クラウド (Cloud)]をクリックします。
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、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 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 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。その場合も、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 左側の[クラウド (Cloud)]をクリックします。

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。

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。

- クラウド資産に対する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)。

ユーザーは、クリーンアップ期間を更新し、`bp.conf` ファイルを使用して資産に特定のフィルタ基準を指定することで、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

ユーザーは属性に基づいてカスタムフィルタを定義できます。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. 左側の[クラウド (Cloud)]をクリックします。
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、属性に基づいて資産を[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)]タブに一覧表示するように、カスタムフィルタを定義します。

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。

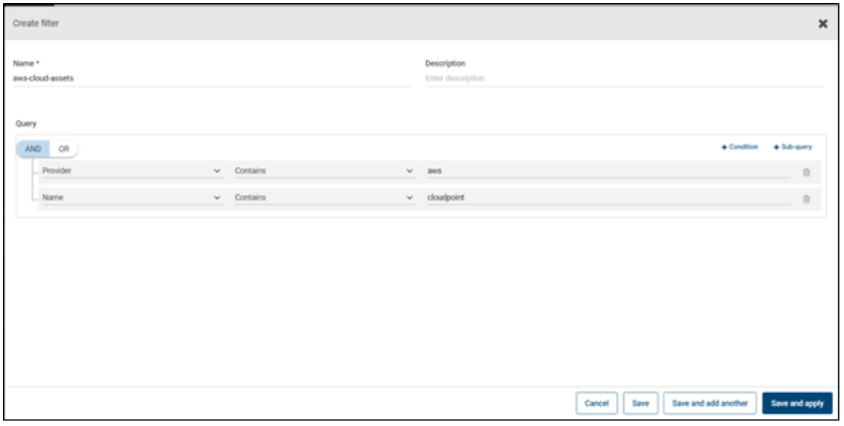
パラメータ	説明
名前 (Name)	フィルタの名前。
説明 (Description)	フィルタの説明を入力します。
問い合わせ (Query)	特定の条件を満たす資産のみを選択するには、独自の問い合わせを作成します。

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.24 の「インテリジェントクラウド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 1-5 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。
`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 1-6 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。

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の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.14 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。

リソースグループを使用した Microsoft Azure リソースの保護について

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 1-7 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	選択されていない	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	選択されていない	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 1-8　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. 保存して、バックアップを再試行します。

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 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 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。

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、AWS、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 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.63 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。
- 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.49 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。

メモ: NetBackup ではスナップショットからの個別リストアのみがサポートされるため、[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、個別リカバリオプションは機能しません。同様に、[バックアップのみを保持 (Keep Backup Only)]を選択した場合、AWS スナップショットレプリケーション機能は動作しません。

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、個別リカバリは利用できません。

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、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。

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。

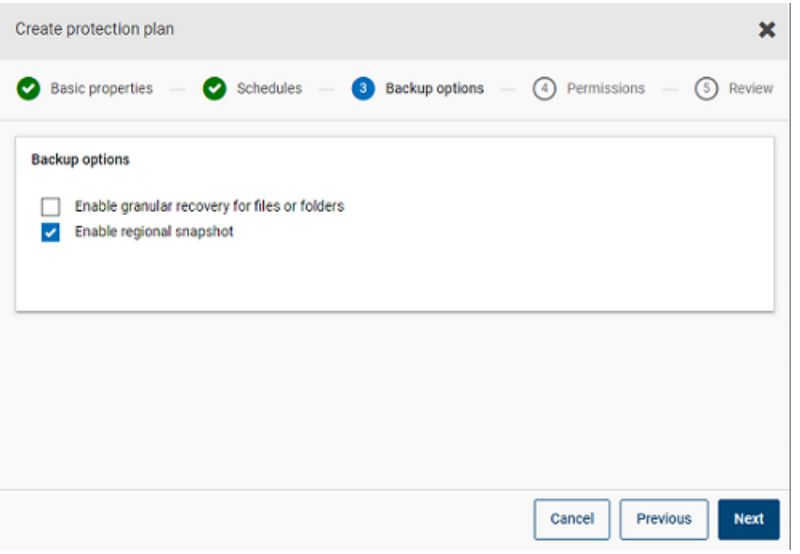
クラウド作業負荷のバックアップオプション

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、取得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。

Google Cloud の地域別スナップショット

保護計画の作成中に、Google Cloud 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。



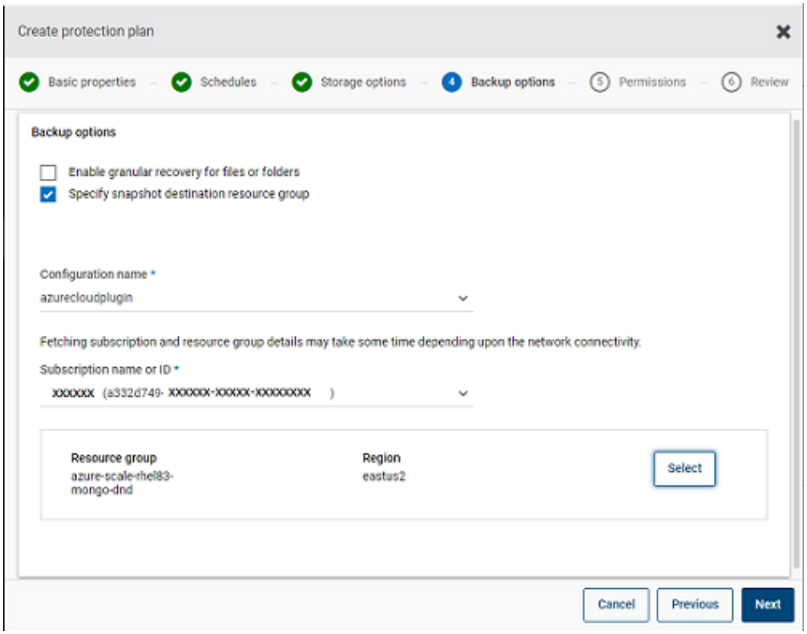
Azure および Azure Stack Hub のスナップショットの宛先リソースグループ

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。

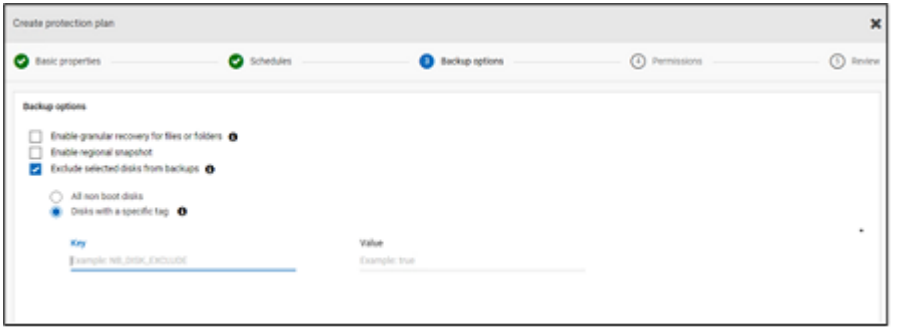
- 保護計画で指定された宛先リソースグループ
- プラグインの構成で指定されている、接頭辞が付いたリソースグループ (Azure のみ)
- 資産が存在するリソースグループ (宛先リソースグループまたは接頭辞が付いたリソースグループが NetBackup で指定されていない場合)



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。
- サポート対象外のファイルシステムがディスク上に構成されていて、ユーザーがそのディスクをスナップショットから除外する必要がある場合、サポート対象外のファイルシステムを含むディスクを除外すると、スナップショットはクラッシュ整合スナップショットであり続けます。
- ユーザーは、ディスクを除外する場合、`/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
- ユーザーは、クラウドプロバイダからタグに変更が加えられたら、資産が正しく検出されていることを確認する必要があります。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ユーザーがタグを接続した場合、そのタグは除外の対象として考慮されません。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、ユーザーが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。

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に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

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。
- アカウント間のレプリケーションの場合、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。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、同じ領域の別のアカウント「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詳しく説明します。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.13 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.42 の「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トリガし、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.20 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 にログオンします。
   - 左側で、[作業負荷 (Workloads)]の[クラウド (Cloud)]をクリックします。[仮想マシン (Virtual machines)]タブで、リカバリするマシンをクリックします。

- [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.77 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トリガします。

ターゲット領域からソース領域への再リストア

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トリガして、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.20 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トリガします。

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、CP1 サーバーに Snapshot Manager エージェントを登録します。

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 1-9 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 1-10 別のアカウントの同じ地域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 1-11 別のアカウントの異なる地域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

クラウドの仮想マシン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。

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、Veritas Snapshot Manager のマニュアルで、プラグイン構成の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。『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 バックアップ管理者ガイド』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。

PaaS 資産の保護

PaaS 資産は、NetBackup で検出した後に管理できます。資産は、クラウド作業負荷の下の[PaaS]タブと[アプリケーション (Applications)]タブに表示されます。[アプリケーション (Applications)]タブには RDS 資産が表示され、[PaaS]タブには RDS 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 1-12 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 管理対象インスタンス、SQL、MariaDB、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 管理対象インスタンス - Azure Arc Azure PostgreSQL - HyperScale (Citus) サーバーグループと Azure Arc 対応 PostgreSQL HyperScale
AWS	RDS SQL、RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS Aurora MySQL、RDS Aurora PostgreSQL、および DynamoDB。
GCP	Cloud SQL for PostgreSQL、Cloud SQL for MySQL

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 1-13 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すべての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。

表 1-14 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
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

MySQL 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。

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。

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 メディアサーバーとプライマリサーバーの一部としてパッケージ化されており、それらを手動でインストールする必要はありません。

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。

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

メモ: MySQL クライアントユーティリティの推奨バージョンは 8.0.31 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

メモ: `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: 16.0.6296.0) 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/msodbcsql17-17.10.2.1-1.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。

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`

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。

Postgres クライアントユーティリティのインストール

メモ: Postgres クライアントユーティリティの推奨バージョンは 14.6 です。

ダウンロード場所	RHEL 7	https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-7-x86_64/
	RHEL 8	https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-8-x86_64/
	RHEL 9	https://download.postgresql.org/pub/repos/yum/14/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 postgresql14-libs-14.6-1PGDG.rhel7.x86_64.rpm`
2. `rpm -ivh postgresql14-14.6-1PGDG.rhel7.x86_64.rpm`

メモ: RHEL 8 と 9 上の `postgresql14-14.6-1PGDG.rhel8.x86_64.rpm` には、`lz4` 圧縮パッケージと `libicu` が必要です。

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 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 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。

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。

すべてのデータベースについて

- 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。
- プロバイダ全体のすべてのデータベースでデフォルトポートのみがサポートされています。カスタムポートで構成された作業負荷インスタンスはサポートされていません。
- 「#」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。
- マルチバイト文字または英語以外の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 を実行していて、10.1.1 より古い旧バージョンのメディアサーバーが含まれるプライマリサーバーではサポートされていません。
- 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.91 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 10.2 では、管理対象 ID ベースの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 を使用して作成された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。

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、`-no-owner` および `-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。
- GCP PostgreSQL 作業負荷に対してサーバーレベルで SSL (Secure Sockets Layer) 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。
- 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ていません。
- リストアワークフローのデータベース名では、&、(、)、<、>、¥、|、/、;、`、'、" の各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。

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。

AWS RDS SQL の場合

- AWS RDS SQL の Express と Web のエディションのみがサポートされます。

- 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。
- Amazon RDS のデータ管理タイプのみがサポートされます。データ管理タイプ RDS カスタムは、AWS RDS SQL インスタンスエディションではサポートされません。

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 10.2 以降で取得されたバックアップは、10.2 より前のバージョンを使用してリストアできません。
- 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 SQL と SQL Managed Instance の場合

- 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。tempdb の古いエントリは、Azure クラウドポータルから削除されません。これは手動で削除する必要があります。
- 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、必要に応じて、リストアを開始する前にターゲットサーバーの AAD 管理者権限を次に対して割り当てる必要があります。
  - 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 の増分バックアップの場合

- CDC (変更データキャプチャ) は、S3 以上のデータベース層でのみ有効にできます。サブコア (Basic、S0、S1、S2) の Azure SQL データベースは CDC ではサポートされません。

- 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。完全バックアップと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。
- 増分バックアップは NetBackup バージョン 10.2 以降のメディアサーバーでのみ実行できることに注意してください。
- クラウドサービスに使用されるユーザー ID には、CDC を有効または無効にする権限が必要です。この権限がないと、次のようなエラーが表示されます。3842: [CDC の有効化に失敗しました。(Failed to enable CDC.)]および 3844: [CDC の無効化に失敗しました。(Failed to disable CDC.)]。
- 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。cdc という用語は、システムで使用するために予約されています。
- Standard または Enterprise 以外のエディションにリストアする場合、CDC には SQL Server Standard エディションまたは Enterprise エディションが必要なため、処理はブロックされます。エラーメッセージ 932 が表示されます。
- 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。

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)。この問題の回避方法として、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、削除済みの資産を 24 時間ごとに削除します。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.13 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.14 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.18 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、検出されたすべての Azure PostgreSQL、MariaDB、SQL Managed Instance、SQL、MySQL、GCP Cloud SQL for PostgreSQL、Cloud SQL for MySQL、または AWS Dynamo DB 資産が、[クラウド (Cloud)]作業負荷の[PaaS]タブに表示されます。

   検出されたすべての AWS RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS SQL および AuroraDB 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)]の[クラウド (Cloud)]をクリックします。
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。

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 作業負荷に接続可能な RHEL メディアサーバーである必要があります。

   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.71 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: 必要な権限を持つ IAM ロールがアタッチされた状態で、クラウド内に Snapshot Manager が配備されている場合。また、メディアサーバーを同じクラウド環境に配備し、同じ IAM ロールを関連付ける必要があります。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。

       - 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。

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。［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 *.* TO `iamuser`@'%' WITH GRANT OPTION;

- PostgreSQL の場合、サーバー下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 postgres 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。

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]、[Azure Active Directory]、[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 を AAD 管理者として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。Active Directory ユーザー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

- ユーザーを作成するために MySQL サーバー用 AAD 管理者を構成するには、[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 を使用してログイ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インします。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

- ユーザーを作成するために PostgreSQL サーバー用 AAD 管理者を構成するには、[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、権限を付与します。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。

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。

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.69 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.69 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。

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。

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。

メモ: Azure SQL データベース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。

2

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、レプリカコピー、バックアップコピー、または複製コピーから、AWS、Azure、Azure Stack、GCP VM の資産をリストアできます。

VM のリストア中、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
- Azure の場合: ネットワークセキュリティグループを選択
- AWS の場合: セキュリティグループを選択

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
- VM とディスクに対して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 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

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 2-1 Azure、Azure Stack、GCP、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	GCP と AWS	Azure	Azure Stack	GCP と AWS
VM の表示名を変更する	Y	Y	Y	Y	Y	Y
VM の電源状態を変更する	Y	Y	Y	Y	Y	Y
タグの関連付けを削除する	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

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	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

仮想マシンのリカバリ

VM をリカバリするには

1. 左側の[クラウド (Cloud)]をクリックします。
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 のみ)。
- ［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 のみ)。
- ［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 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。

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。

- バックアップ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)］の近く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。
  ユーザーは、AWS、Azure、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。
- (*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。

ユーザーは、AWS、Azure、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。

リカバリの状態コードについて詳しくは、NetBackup 管理者に問い合わせるか、次の場所から入手できる『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. 左側の[クラウド (Cloud)]をクリックします。
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. 左側の[クラウド (Cloud)]をクリックします。
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。

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 2-2 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。

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。

メモ: 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。また、Azure Stack と 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. 左側の[クラウド (Cloud)]をクリックします。
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。

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。AWS RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS AuroraDB および RDS SQL Server 資産は[アプリケーション (Applications)]タブから、その他すべての 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 10.2 から、MySQL データベースのデータ/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。

インスタントアクセスリカバリを実行する前に、プライマリサーバーの `bp.conf` ファイルに `MEDIA_SERVER_POD_CIDR` キーを追加します。AKS または EKS 環境に配備された NetBackup の場合は、値をカンマ区切り値としてメディアサーバーポッドのサブネットに設定します。例: MEDIA_SERVER_POD_CIDR=10.0.0.0/8, 10.0.0.0/16

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.69 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。

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. 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。
6. (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。
7. (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。
8. (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.69 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。
9. [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. 左側の[クラウド (Cloud)]をクリックします。
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 時間を使用して、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 左側の[クラウド (Cloud)]をクリックします。

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.86 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。

3

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。スナップショットを作成し、スナップショットをバックアップしてリストアできるだけでなく、個々のファイルと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 によってバックアップのインデックス付けが完了している場合にのみ、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。

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 3-1　　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。
■ ファイルまたはフォルダのリストア ■ ボリュームのリストア **メモ:** ボリュームのリストアはバックアップコピーではサポートされません。	ファイル、フォルダまたはボリューム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 3-2　　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	10.2

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 7.x および 8.x
Snapshot Manager ホスト OS	■ RHEL 7.x 以降、RHEL 8.6 ■ Ubuntu 18.04 LTS および 20.04 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
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
保護対象の Snapshot Manager エージェントホスト	■ Linux OS: RHEL 7.x および RHEL 8.2、8.4、8.5 ■ 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:** Google Cloud Platform 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。

- (スナップショットにのみ適用可能)
  - (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。
  - Amazon AWS: Snapshot Manager ホストと接続された VM は、同じアカウントおよび地域内にある必要があります。
  - Google Cloud Platform: Snapshot Manager ホストと接続された VM は同じプロジェクトにある必要があります。

- 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。
- 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。

- 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.95 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。Windows プラットフォームの場合は、インデックス付け可能な仮想マシンでポート 135、445 および動的/固定 WMI-IN ポートを構成します。
- スナップショットの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。
  - サポート対象の NetBackup および Snapshot Manager バージョン 10.2 以降を用意します。
  - 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 (バージョンは 10.2 以降であることが必要) からリストアされる場合にのみ機能します。
  - 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。
  - 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 へのアクセスに対して MSDP ストレージサーバーへのアクセス権が必要です。
- Windows ターゲットは次のようにする必要があります。
  - (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、(インスタントアクセス共有をエクスポートしている) 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。

    MSDP サーバーで、`smbpasswd -a <username>` コマンドを実行して Samba クレデンシャルを生成します。

    上記のユーザー名と生成されたパスワードを使用して、MSDP サーバーの DNS 名または IP を Windows クレデンシャルマネージャに追加します。

    ユーザーが MSDP サーバーに存在しない場合、コマンド `smbpasswd` は失敗します。そのため、最初に `useradd <username>` コマンドを使用してユーザーを追加してから、`smbpasswd` コマンドを使用します。
  - (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る必要があります。

  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。

  `/usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh` 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。

制限事項および考慮事項

個別リストアに関して、次の重要な点に注意してください。

- 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。
- 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。
- 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、概略は空白になります。
- アクティビティモニターの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。
- 一時的なストレージデバイスは、スナップショットの実行時には無視されます。(例: 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) これらのデバイスはインデックス処理でも無視されます。
- LDM ディスクで作成されたファイルシステムは、ホスト整合スナップショットの作成およびインデックス付け処理中には無視されます。

- 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 (GRT) またはシングルファイルリストア (SFR) 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、AWS クラウド、および GCP に対して実行でき、既存のマウントベースのインデックス付けで実行されます。
- 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。
- Snapshot Manager は、実行可能なインデックスジョブの数を NetBackup に伝えます。NetBackup はその後、要求をスロットルします。デフォルトでは、インデックスジョブの数は 2 に初期化されています。Snapshot Manager ホスト機能の検出後、利用可能なディスクスロットの数に増加します。ただし、flexsnap.conf ファイルにあるインデックス付けに関する max_jobs=<value> の値を更新して、この制限を上書きできます。
- Snapshot Manager ホストは、クラウドプロバイダによって適用されるディスクスロットの数を制限します。NetBackup は、Snapshot Manager に対するインデックス付け要求をスロットルします。クラウド資産の検出処理中にこの要求を達成するため、NetBackup は Snapshot Manager ホスト機能をフェッチします。これらの機能には、インデックスジョブの最大数のパラメータが含まれています。このパラメータは、Snapshot Manager および NetBackup のインデックスジョブキューに送信される要求を制限するために使用されます。デフォルトでは、並列インデックス付けジョブの最大数は 2 です。ただし、クラウドプラグインが Snapshot Manager ホストを検出するように構成されると、機能 API は接続ポイントと利用可能なリソースに基づいて最大ジョブ数をフェッチします。Snapshot Manager ホストの config ファイルに `indexing max_jobs=x` エントリを追加して、制限を設定できます。Snapshot Manager ホストがその機能を上回る数のインデックス付け要求を受信した場合、要求はキューに投入されます。
- 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。

- リカバリポイントでファイルまたはフォルダを参照して追加するときに、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。

  たとえば、ディスクが /mnt1/mnt2 にマウントされ、/mnt1 は「/」配下のディレクトリ、mnt2 は mnt1 内のマウントポイントである場合、「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。高いバージョンから低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。
- スナップショットのバックアップからの単一ファイルリストアでは、次の制限事項を考慮してください。
  - ソースホストが Linux でターゲットホストが Windows の場合にファイルまたはフォルダをリストアする場合
    - 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。
    - 選択したファイルまたはフォルダに symlink がリストア用に存在する場合、その symlink はリストアされません。
  - 元の場所のリストアの場合、コピー前の利用可能なサイズチェックがスキップされます。

- 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。
- 部分的なリストアが成功した場合に保持されるライブマウントは、メディアサーバーまたは PureDisk Deduplication Engine および Veritas 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、保持期間の期限が切れる前に削除または期限切れになります。
- メディアサーバーが 10.2 にアップグレードされていない場合、NetBackup Snapshot Manager に接続するために 10.2 のマスターサーバーが使用されます。
- インデックス処理後のウィンドウの接合点は、[ファイルを追加 (Add files)]にボリューム {4e3f8396-490a-400a-8abf-5579cafd4c0f} のような形式として表示されます。バックアップからの単一ファイルのリストア操作に対する[ファイルを追加 (Add files)]で接合点が選択されている場合、[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。

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、Google Cloud Platform、および Amazon 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. 左側の[クラウド (Cloud)]をクリックします。
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、特定の種類のコピーに対して[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)]ダイアログボックスで、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 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)]ダイアログボックス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。これにより、ハードリンクファイルのコピーに失敗します。

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. 左側の[クラウド (Cloud)]をクリックします。
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、ボリュームをリストアする 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 からリストアする場合、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。

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トリガすると、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、ユーザーのログイ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。それ以外の場合は、Microsoft 社が提供する次の文書に記載されている手順を実行します。

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:

シングルファイルリストア用に参照しているときに、Snapshot Manager でサポートされていないファイルまたはフォルダの一覧表示を回避するには、NetBackup マスターサーバーの `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おらず、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領域を考慮します。しかし、ファイルをコピーしようとすると、概略レポートに記録された領域エラーで失敗します。次に例を示します。

```
 /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。

このような部分的なリカバリの場合、作成されたインスタンスのアクセスは削除されず、以降 24 時間利用可能になります。

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 キーを設定することで構成できます。(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。
- ディスク管理のダイアログボックスにある[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。
- [ドライブ文字またはパスを追加 (Add Drive Letter or Path)]ダイアログボックスで、[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。
- 上記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単一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。 ■ **パス/ファイル:** /tmp/flexsnap-agentless-onhost.log ■ /var/log/flexsnap/restore/granular-restore-*	Snapshot Manager での単一ファイルの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

問題/エラー	説明	回避方法
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、構成されたエージェントとターゲット仮想マシンが接続状態であ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 ターゲットマシンに NFS クライアントをインストールせずにソース Linux VM からターゲット Windows VM にファイルとフォルダをリストアする場合、次のエラーが表示されてリカバリが部分的に成功します。 `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 ターゲットマシンに NFS クライアントをインストールします。
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 の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。	次の事前チェックスクリプトを使用して、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。 `/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。	ボリューム数を減らして、ファイルとフォルダをリストアします。
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 が有効になっている場合。	MSDP がインストールされているメディアサーバーで FIPS を無効にするか、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 では処理ができません。

回避方法:

ディスクを初期化し、VM をバックアップし、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。

4

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
- 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

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。

- 「構成用のログファイル」
- 「スナップショット作成のログファイル」
- 「リストア操作のログファイル」
- 「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.10 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 4-1　　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 に登録する方法の 1 つです。	Windows の場合 NetBackup install path/volmgr/debug/tpcommand UNIX の場合 `/usr/openv/volmgr/debug/tpcommand`

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/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`*`/path/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 4-2　　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`

プロセス	ログ

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 4-3 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`
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`

プロセス	ログ
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 4-4

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
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 4-5 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。

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に使用している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 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

説明: バックアップ中に使用されたクライアント名が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。

回避方法: ファイルパスの長さが 256 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。

状態コード: 3801 要求された操作を完了できません。

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

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。ユーザー管理 ID を使用する場合は、同じユーザー管理 ID をメディアサーバーとスナップショットマネージャに接続します。

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 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。(Failed to disable 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。

説明: 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。