

NetBackup™ Web UI クラウド 管理者ガイド

リリース 10.0

VERITAS™

最終更新日: 2022-04-27

法的通知と登録商標

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

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から入手できます。

<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

第 1 章	クラウド資産の管理と保護	6
	クラウド資産の保護について	7
	制限事項および考慮事項	9
	NetBackup での CloudPoint サーバーの構成	9
	サードパーティ CA 証明書の構成	10
	CloudPoint サーバーの追加	12
	CloudPoint サーバーのクラウドプロバイダの追加	13
	メディアサーバーと CloudPoint サーバーの関連付け	16
	CloudPoint サーバーの資産の検出	17
	CloudPoint サーバーの編集	18
	CloudPoint サーバーの有効化または無効化	19
	(オプション) CloudPoint 拡張機能の追加	19
	インテリジェントクラウドグループの管理	19
	インテリジェントクラウドグループの作成	20
	インテリジェントクラウドグループの削除	23
	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	24
	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	26
	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	27
	クラウド資産のクリーンアップ	27
	AWS と Azure の政府向けクラウドサポート	28
	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	29
	開始する前に	30
	制限事項および考慮事項	30
	リソースグループの構成と結果について	30
	リソースグループの権限のトラブルシューティング	34
	クラウド作業負荷のための NetBackup アクセラレータ	34
	NetBackup アクセラレータが仮想マシンと連携する仕組み	35
	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)	36
	アクセラレータバックアップおよび NetBackup カタログ	37
	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	37
	クラウド作業負荷のバックアップスケジュールの構成	38
	クラウド作業負荷のバックアップオプション	40
	スナップショットレプリケーション	43

	AWS スナップショットレプリケーションの構成	44
	AWS スナップショットレプリケーションの使用	46
	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	49
	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	51
	PaaS 資産の検出	52
第 2 章	NetBackup Web ユーザーインターフェースの概要	54
第 3 章	クラウド資産のリカバリ	55
	クラウド資産のリカバリ	55
	クラウド資産のロールバックリカバリの実行	62
	PaaS 資産のリカバリ	63
第 4 章	NetBackup の監視	66
第 5 章	個別リストアの実行	67
	個別リストアについて	67
	サポート対象の環境リスト	68
	サポートされているファイルシステムのリスト	69
	開始する前に	70
	制限事項および考慮事項	71
	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	73
	クラウド仮想マシンでのボリュームのリストア	75
	LVM を含むボリュームリストア後の手順の実行	76
	トラブルシューティング	78
第 6 章	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	79
	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	79
	PaaS の作業負荷のリカバリに関する問題のトラブルシューティング	83

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
- 制限事項および考慮事項
- **NetBackup** での **CloudPoint** サーバーの構成
- インテリジェントクラウドグループの管理
- 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
- クラウド資産のクリーンアップ
- **AWS** と **Azure** の政府向けクラウドサポート
- 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
- クラウド作業負荷のための **NetBackup** アクセラレータ
- クラウド作業負荷のバックアップスケジュールの構成
- クラウド作業負荷のバックアップオプション
- スナップショットレプリケーション
- **AWS** スナップショットレプリケーションの構成
- **AWS** スナップショットレプリケーションの使用
- 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
- 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
- **PaaS** 資産の検出

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、CloudPoint 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。8.3 以降、CloudPoint 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。
CloudPoint の配備	環境内に CloudPoint をインストールします。 p.12 の「 CloudPoint サーバーの追加 」を参照してください。 CloudPoint と NetBackup の制限事項を確認します。 p.9 の「 制限事項および考慮事項 」を参照してください。
NetBackup 管理コンソールを使用した、CloudPoint サーバーの構成	NetBackup で CloudPoint サーバーを登録します。 『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.13 の「 CloudPoint サーバー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.16 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	<p>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。</p> <p>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。</p> <p>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> <p>p.17 の「CloudPoint サーバーの資産の検出」を参照してください。</p>
保護計画の作成	<p>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。</p> <p>『NetBackup Web UI 管理者ガイド』を参照してください。</p> <p>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.44 の「AWS スナップショットレプリケーションの構成」を参照してください。</p>
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	<p>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。</p> <p>『NetBackup Web UI 管理者ガイド』を参照してください。</p> <p>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.51 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。</p>
クラウド資産のリカバリ	<ul style="list-style-type: none"> ■ 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.55 の「クラウド資産のリカバリ」を参照してください。 p.62 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>p.79 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。</p>

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。

- **CloudPoint** ホストエン트리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 **CloudPoint** イメージはリカバリできません。
- **CloudPoint** の機能について詳しくは、『**Veritas CloudPoint Install and Upgrade Guide**』を参照してください。
- 以前にインストールした **CloudPoint** がある場合、**CloudPoint** 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。
CloudPoint サーバーを再インストールした場合は、**CloudPoint** 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、**CloudPoint** はポート **443** で構成されます。
- **CloudPoint** 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。
- **CloudPoint** サーバーでは、拡張監査はサポートされません。このため、ルート以外の **NetBackup** 管理者権限を使用して **CloudPoint** サーバーを追加または更新する場合、監査中にユーザーはルートとして表示されます。
- **CloudFormation** テンプレートを使用して **CloudPoint** を配備する場合、コマンドを使用して **CloudPoint** 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。

NetBackup での CloudPoint サーバーの構成

NetBackup Web UI を使用して **CloudPoint** サーバーを追加できます。8.3 以降、**CloudPoint** サーバーは、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 **CloudPoint** サーバーを **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 **CloudPoint** サーバーは 1 つだけです。
- 複数のメディアサーバーを **CloudPoint** サーバー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 **CloudPoint** サーバーにリンクできます。

- **CloudPoint** インターフェースで操作しなくても、**CloudPoint** 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、**CloudPoint** 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。**CloudPoint** 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 **CloudPoint** 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 CloudPoint サーバーの構成

タスク	説明
CloudPoint サーバーの追加	NetBackup で CloudPoint サーバーを追加するには、 CloudPoint サーバー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.12 の「 CloudPoint サーバーの追加 」を参照してください。
クラウドプロバイダの追加	CloudPoint サーバー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.13 の「 CloudPoint サーバーのクラウドプロバイダの追加 」を参照してください。
CloudPoint サーバーの資産の検出	CloudPoint サーバーの資産を検出できません。p.17 の「 CloudPoint サーバーの資産の検出 」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 CloudPoint サーバーに関連付ける必要があります。p.16 の「 メディアサーバーと CloudPoint サーバーの関連付け 」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、**CloudPoint** サーバーを検証できます。

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、信頼できるルート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 **CloudPoint** サーバー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、**CloudPoint** サーバー 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 **CloudPoint** サーバー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 **CloudPoint** サーバーにアップロードします。
- 3 **NetBackup** で証明書ファイルを作成し、ルートとすべての中間 **CA** の証明書を `pem` ファイルに追加します。
- 4 `/cloudpoint/openssl/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、ルート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、**CloudPoint** が動作しないことがあります。

- 5 **NetBackup** に **CloudPoint** サーバーを追加するか、`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 **CloudPoint** サーバーの証明書を更新します。

CloudPoint サーバーの追加

NetBackup Web UI を使用して CloudPoint サーバーを追加できます。CloudPoint サーバーのクレデンシアルを入力し、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、CloudPoint と NetBackup サーバー間に双方向の接続が必要です。

CloudPoint サーバーを追加するには

- 1 左側の [クラウド (Cloud)] をクリックします。
- 2 [CloudPoint サーバー (CloudPoint server)] タブをクリックします。
- 3 [追加 (Add)] をクリックします。
- 4 [CloudPoint サーバー (CloudPoint server)] フィールドに、次のいずれかを入力します。
 - CloudPoint サーバーのホスト名または IP アドレス。
ホスト名または IP アドレスは、CloudPoint のインストール中に CloudPoint 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、CloudPoint サーバーの FDQN を入力します。
- 5 [ポート (Port)] フィールドに CloudPoint サーバー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 CloudPoint のインストール時に指定した CloudPoint のサーバークレデンシアルを入力します。
- 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、CloudPoint 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。

CloudPoint サーバー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、CloudPoint サーバーは、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。

CloudPoint サーバー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 望ましい CloudPoint サーバーを選択します。

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	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。
	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。
	AAD を使用:	CloudPoint 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>.<EQDN>
	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:	CloudPoint 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>.<EQDN>	

クラウドプロバイダ	パラメータ	説明
	テナント ID (Tenant ID)	アプリケーションを作成した AAD ディレクトリの ID。
	クライアント ID (Client ID)	アプリケーション ID。
	シークレットキー (Secret Key)	アプリケーションのシークレットキー。
	認証リソースの URL (省略可能) (Authentication Resource URL (optional))	認証トークンの送信先の URL。
Amazon AWS	アクセスキー (Access key)	アクセスキー ID をシークレットアクセスキーと共に指定すると、AWS API との通信が CloudPoint に許可されます。
メモ: CloudPoint サーバーが 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。	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。
	Google Cloud Platform	プロジェクト ID (Project ID)
	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。
	ゾーン (Zones)	プロバイダが動作するゾーンのリスト。

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

CloudPoint 管理サーバー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.13 の「[CloudPoint サーバー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 CloudPoint Install and Upgrade Guide](#)』を参照してください。
- NetBackup と CloudPoint 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。tpconfig -update コマンドを実行します。

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 CloudPoint 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 CloudPoint 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 CloudPoint 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 CloudPoint サーバーの関連付け

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 CloudPoint サーバー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。CloudPoint サーバー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。

メディアサーバーを CloudPoint サーバーに関連付けるには

- 1 左側の[クラウド (Cloud)]をクリックします。
- 2 [CloudPoint サーバー (CloudPoint server)]タブをクリックします。
- 3 CloudPoint サーバーの横のメニューで[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、CloudPoint サーバーと関連付ける 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。

CloudPoint サーバーの資産の検出

CloudPoint サーバー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 CloudPoint から資産データを、CloudPoint 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。CloudPoint サーバーを無効にすると、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手動でトリガしたり、CloudPoint サーバーで検出をトリガして、CloudPoint サーバー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 CloudPoint サーバーに対して資産の増分検出を定期的に行い、前回の検出と今回の検出の間に発生した資産の追加、削除、修正などの変更のみを検出します。

メモ: 正確に増分を検出し、検出の問題を回避するため、NetBackup プライマリサーバーと CloudPoint サーバー上で、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、CloudPoint サーバー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、CloudPoint サーバーからの特定時点のデータをフェッチするだけです。

CloudPoint サーバー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 [CloudPoint サーバー (CloudPoint server)]タブをクリックします。
- 3 CloudPoint サーバーの横のメニューで[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 [CloudPoint サーバー (CloudPoint server)]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 CloudPoint サーバーの 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 CloudPoint サーバーの資産と同期されます。

CloudPoint サーバーの自動検出間隔の変更

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。

CloudPoint サーバーの編集

CloudPoint サーバーのクレデンシャルを更新できます。ただし、CloudPoint サーバーのホスト名、IP アドレス、またはポートを編集することはできません。

CloudPoint サーバーを編集するには

- 1 左側の[クラウド (Cloud)]をクリックします。
- 2 [CloudPoint サーバー (CloudPoint server)]タブをクリックします。
- 3 CloudPoint サーバーの横のメニューで[編集 (Edit)]をクリックします。
CloudPoint サーバー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、CloudPoint サーバー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。

CloudPoint サーバーの有効化または無効化

必要に応じて、CloudPoint サーバーを有効または無効にできます。CloudPoint サーバーを無効にすると、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。

CloudPoint サーバー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 [CloudPoint サーバー (CloudPoint server)]タブをクリックします。
- 3 CloudPoint サーバーの状態に基づいて、[有効化 (Enable)]または[無効化 (Disable)]を選択します。

メモ: CloudPoint サーバーを無効化すると、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リプト解除するか、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) CloudPoint 拡張機能の追加

CloudPoint 拡張機能の目的は、パフォーマンス容量がピーク時に CloudPoint サーバー上で多数の要求を同時に実行するため、CloudPoint 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 CloudPoint 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、CloudPoint ホストの処理容量を増加できます。

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

サポート対象の CloudPoint 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 CloudPoint インストール/アップグレードガイド](#)』の「CloudPoint 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。
- 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.22 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:

The screenshot shows the 'Asset type' section with 'Virtual machine' selected. Below it, there is a search query builder interface. The query is built using AND/OR logic. The first condition is 'displayName Contains CP'. The second condition is 'tagName Starts with eng'. The third condition is 'state = running'. The interface includes buttons for 'Preview', 'Cancel', 'Add and Protect', and 'Add'.

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じ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、その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、**NetBackup 9.1** へのアップグレード後に、自動的に新しいプロバイダ固有の形式に変換されます。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、プロバイダごとに別々の 2 つの計画に変換されます。

p.25 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。セクション。

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)
 - 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。
- 資産がサブスクリ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リブ解除され、変換された保護計画にサブスクリブされます。
 - 新しい資産は古い保護計画にサブスクリブできません。
 - [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。ただし、変換時にいずれか1つのクラウドプロバイダの資産サブスクリプションを保持するように保護計画が更新された場合を除きます。
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。サブスクライブ解除に失敗した資産の変換は、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 CloudPoint サーバーで削除されません)。

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/opensv/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'"  
    }  
  }  
}
```

AWS と Azure の政府向けクラウドサポート

8.3 以降の CloudPoint は、アマゾンウェブサービスおよび Microsoft Azure の米国政府向けクラウドの作業負荷を検出できます。CloudPoint サーバーが 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 CloudPoint 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 CloudPoint ホストで、パブリッククラウドと政府向けクラウドを組み合わせた使用できません。

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。

CloudPoint 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

アマゾンウェブサービス

Microsoft Azure

GovCloud (米国) 地域

- us-gov-east-1
- us-gov-west-1

- US Gov アリゾナ
- US Gov テキサス
- US Gov バージニア

AWS と Microsoft Azure の構成について詳しくは、p.13 の「[CloudPoint サーバー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>

CloudPoint 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。CloudPoint 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 1-5 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。

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。 <ul style="list-style-type: none"> ■ 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。
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。 <ul style="list-style-type: none"> ■ 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 1-6 構成例

条件	構成	結果
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>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。</p>
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>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。</p>
<ul style="list-style-type: none"> ■ 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で作成されている。 	<ul style="list-style-type: none"> ■ 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。 	<p>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。</p>
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>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。</p>

条件	構成	結果
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>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 で作成されません。</p>
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>スナップショットは作成されず、ジョブは失敗します。</p>
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>スナップショットは作成されず、ジョブは失敗します。</p>

条件	構成	結果
<ul style="list-style-type: none"> ■ 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。 	<ul style="list-style-type: none"> ■ 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。 	<p>スナップショットは作成されず、ジョブは失敗します。</p>

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. [アクセス制御 (IAM)] をクリックします。
4. [役割の割り当ての追加 (Add Role Assignment)] をクリックします。
5. [所有者としての役割 (Role as Owner)]、[ユーザーとしてアクセスを割り当て (Assign Access to as User)]、[アプリケーション (Application)] (API 呼び出しのため、CloudPoint 用に作成) を選択します。
6. 保存して、バックアップを再実行します。

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済みます。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。
- CloudPoint サーバーの I/O を低減します。
- CloudPoint サーバーの CPU 負荷を低減します。

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ツ (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。

```
bpbbackup -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 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 [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。
- 5 [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

トのレプリケーションについて詳しくは、p.44 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。

- 6 『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、CloudPoint サーバー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処理は現在、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、CloudPoint サーバーの `/cloudpoint/opencv/dm/datamover.<datamover-id>/netbackup/logs` フォルダにあります。

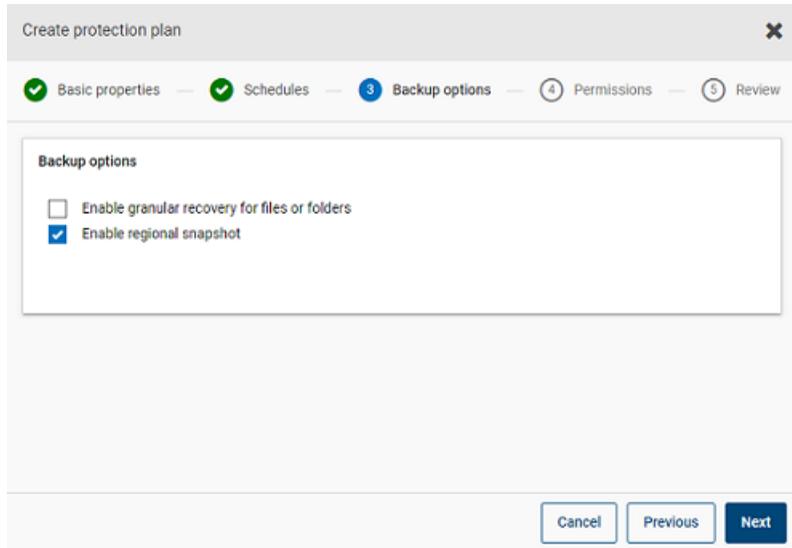
メモ: VM が接続状態ではない場合、VM のバックアップは続行し、バックアップジョブは部分的に成功とマークされます。この場合、VM が接続されていないとインデックス処理を利用できないので、個々のファイルまたはフォルダをリストアできません。

クラウド作業負荷のバックアップオプション

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。



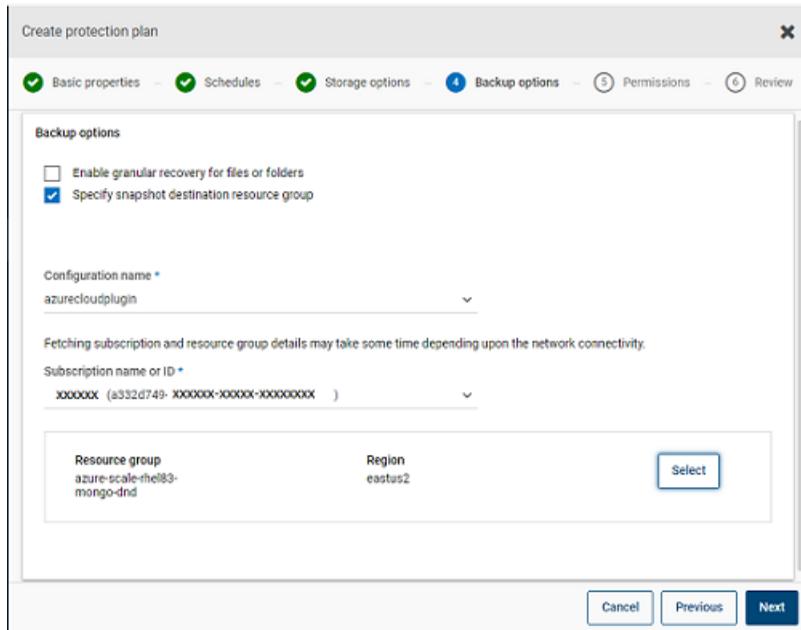
Azure および Azure Stack Hub のスナップショットの宛先リソースグループ

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。

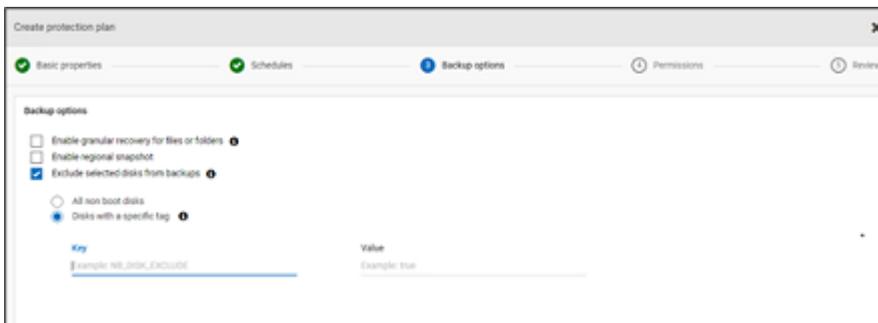
- 保護計画で指定された宛先リソースグループ
- プラグインの構成で指定されている、接頭辞が付いたリソースグループ (Azure のみ)
- 資産が存在するリソースグループ (宛先リソースグループまたは接頭辞が付いたリソースグループが NetBackup で指定されていない場合)



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しても、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 CloudPoint 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](#) に関する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](#) に関する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 CloudPoint 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 CloudPoint 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。**CloudPoint** サーバーは、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。
- CloudPoint サーバーで検出された資産は、同じ CloudPoint サーバー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、CloudPoint サーバー「CP1」で検出された資産は、CloudPoint サーバー「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™ CloudPoint

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 で CloudPoint サーバー (CP1) を追加します。p.12 の「[CloudPoint サーバーの追加](#)」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.38 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 CloudPoint サーバー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.19 の「[CloudPoint サーバー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 CloudPoint サーバー (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 コンソールにログオンします。
 - 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.55 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 CloudPoint 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 CloudPoint 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.19 の「CloudPoint サーバー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 CloudPoint 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 CloudPoint 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 1-7 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 1-8 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 1-9 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：

- **MongoDB と 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 CloudPoint 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 資産の検出

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: PaaS 資産は NetBackup の保護計画に追加できません。

PaaS 資産を検出するには

- 1 CloudPoint サーバーを追加します。p.12 の「[CloudPoint サーバーの追加](#)」を参照してください。
- 2 Microsoft Azure をプロバイダとして追加します。p.13 の「[CloudPoint サーバー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.17 の「[CloudPoint サーバーの資産の検出](#)」を参照してください。

検出が完了すると、[クラウド (Cloud)]作業負荷の[PaaS]タブで、Azure SQL データベースと Azure SQL 管理対象データベースについて検出されたすべての資産を検索できます。

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。

NetBackup Web ユーザー インターフェースの概要

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](#)
- [クラウド資産のロールバックリカバリの実行](#)
- [PaaS 資産のリカバリ](#)

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 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、異なる領域、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。

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

- CloudPoint サーバーとの接続とクラウドクレデンシャルの検証

PaaS 資産のリカバリ前チェックについて

PaaS 資産のリカバリ前チェックでは、次の項目が確認されます。

- 有効な Azure SQL データベースの表示名。同じ表示名のデータベースは他に存在できません。
- Azure の有効なリストアポイント。リストアポイントは、最も古いリカバリポイント以降で、現在の時刻以前でなければなりません。
- Azure の有効な管理対象インスタンス。指定した管理対象インスタンスが存在する必要があります。管理対象インスタンスが存在する場合は、その SQL データベースの表示名のみが検証されます。これは、Azure SQL の管理対象データベースのリカバリポイントにのみ適用されます。

クラウド資産のリストアでサポートされるパラメータ

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

表 3-1 Azure および Azure Stack 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		バックアップコピー		
	Azure	Azure Stack	Azure	Azure Stack	AWS
VM の表示名を変更する	Y	Y	Y	Y	Y
VM の電源状態を変更する	Y	Y	Y	Y	Y

タグの関連付けを削除する	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
サブスクリプションID			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	Y

ディ
スク
のリ
ゾー
スグ
ルー
プを
変更
する

表 3-2 AWS と GCP のスナップショットコピーでサポートされるパラメータ

パラメータ	AWS	GCP
VM の表示名を変更する	Y	Y
VM の電源状態を変更する	Y	Y
タグの関連付けを削除する	Y	Y
異なるネットワークにリストアする	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、別の領域にリストアするには[領域 (Region)]を選択します。その領域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。
 - スナップショットコピーをリストアする場合は、[ネットワーク構成 (Network configuration)]の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、その領域で利用可能なネットワークが表示されます。
- [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。

- 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 Google Cloud Platform 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。

シナリオ	処理
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する (NetBackup Web UI のクラウド作業負荷にある [ボリューム (Volumes)] タブから)	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。
クラッシュ整合スナップショットから VM をリストアする (読み取り専用ディスクを使用) (NetBackup Web UI のクラウド作業負荷にある [仮想マシン (Virtual Machines)] タブから)	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間、「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

アプリケーション整合スナップショットから VM をリストアする (読み取り専用ディスクを使用) (NetBackup Web UI のクラウド作業負荷にある [仮想マシン (Virtual Machines)] タブから)

処理

「読み取り専用」ディスクを複数の VM に接続できる場合でも、検出できるのは 1 つの VM のみです。

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。

```
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 に対してスナップショットが成功する場合としない場合がありますが、他の 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.Flow: create snapshot  
(test-win) of host linux-1(len=4) '  
requires  
['snap_google-gcp-us-west2-b-7534340043132122994']  
but no other entity produces said  
requirements\nMissingDependencies
```

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

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 [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。
- 5 [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。

- 6 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/ja-jp/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。
- 7 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。
- 8 [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/ja-jp/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。

- 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が属する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 CloudPoint 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。

NetBackup の監視

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](#)
- [サポート対象の環境リスト](#)
- [サポートされているファイルシステムのリスト](#)
- [開始する前に](#)
- [制限事項および考慮事項](#)
- [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でのボリュームのリストア](#)
- [LVM を含むボリュームリストア後の手順の実行](#)
- [トラブルシューティング](#)

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。

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 5-1 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)]、[CloudPoint サーバー (CloudPoint servers)]、[CloudPoint サーバー (CloudPoint servers)]、[処理 (Actions)]、[検出 (Discover)] の順に選択します。
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またはボリュームのリストア	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 5-2 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	10.0
NetBackup バックアップホスト OS	RHEL 7.x および 8

アプリケーション	バージョン
CloudPoint ホスト OS	<ul style="list-style-type: none"> ■ RHEL 7.x 以降、RHEL 8.4 および 8.5 ■ Ubuntu 18.04 LTS および 20.04 LTS <p>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。</p>
クラウドプロバイダ	<ul style="list-style-type: none"> ■ アマゾンウェブサービス ■ Microsoft Azure ■ Microsoft Azure Stack Hub ■ Google Cloud Platform
CloudPoint またはエージェントインスタンスタイプ	<ul style="list-style-type: none"> ■ 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 CloudPoint エージェントホスト	<ul style="list-style-type: none"> ■ 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: RHEL 8.3 および 8.2 エージェントホストの個別リストアは、CloudPoint が RHEL 8.3 に配備されている場合にのみサポートされます。	<ul style="list-style-type: none"> ■ ext3 ■ ext4 ■ xfs 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ GPT ■ MBR

メモ: 一貫性のある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。個別リストアを使用にして保護されるように構成された **CloudPoint** サーバーと **VM** には、次の要件があります。

- (Microsoft Azure と Azure Stack Hub) 接続された **VM** と同じサブスクリプションおよび地域内に **CloudPoint** 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 **CloudPoint** ホストを配備する必要があります。
- **Amazon AWS:** **CloudPoint** 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:** **CloudPoint** 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。
- **CloudPoint** ホストが配備されている領域の資産を保護するために、クラウドプラグインを構成する必要があります。
- ホストは接続状態である必要があります。また、必須のサポート構成になっている必要があります。
- ホストは、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 **CloudPoint** 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.69 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 **CloudPoint** 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。
- 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。

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。
- (GCP にのみ該当) 利用可能なデータディスクの接続ポイントの数は、CloudPoint ホストにおけるインスタンスの種類ごとのディスクスロット数の合計から **1** を引いた数です。この **1** つの接続ポイントは **CloudPoint** メタデータボリュームが使用します。
- Amazon AWS インスタンスストアボリュームや Microsoft Azure 一時ディスクなどの揮発性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。これらのデバイスは、インデックス付け処理でも無視されます。
- LDM ディスクで作成され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、CloudPoint 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、AzureStack、AWS クラウド (GCP を除く) 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せん。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。
- **CloudPoint** 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。**CloudPoint** 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。
- **CloudPoint** 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、**CloudPoint** 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 **CloudPoint** 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、**CloudPoint** 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 **CloudPoint** 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。**CloudPoint** 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。**CloudPoint** 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。
- インデックス付け操作の進行中に、ファイル、ディレクトリ、または他のエントリのクローラで **OS** エラーが発生した場合、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。
- リカバリポイントからファイルまたはフォルダを追加したときに左側のパネルのツリーにマウントポイントが表示されない場合は、次の理由が考えられます。
 - 「/」(ルートファイルシステム) が **LVM** 上にある
 - マウントポイントが「/」(ルートファイルシステム) 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。
- ドライブ (ソース) を代替フォルダ (ターゲット) にリストアする際、ユーザーグループは、書き込み権限がないため、新しく作成されたフォルダで書き込み操作を実行できません。
- 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。

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の右上で、[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。
- 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もできます。レプリケーションの場合は、[リカバリ (Recover)]をクリックし、[ファイルとフォルダをリストアする (Restore files and folders)]を選択します。
- 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の手順で、[ターゲット VM (Target VM)]リストから 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。
- 14 [リストア済みファイル (Files restored)]オプションで、次のいずれかのオプションを選択します。
- すべてを元のディレクトリにリストア (Restore everything to the original directory)
 - すべてを異なるディレクトリにリストア (Restore everything to a different directory)
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。
- 15 [次へ (Next)]をクリックします。
- 16 リカバリオプションの手順で、必要なオプションを選択します。
- 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 (Overwrite existing files)
適切な権限を所有している必要があります。
 - ([すべてを異なるディレクトリにリストア (Restore everything to a different directory)]オプションを選択した場合) ハードリンクの新しいファイルを作成 (Create new files for hard links)

- 17 [次へ (Next)]をクリックします。
- 18 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。

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。

LVM を含むボリュームリストア後の手順の実行

LVM ボリュームのボリュームリストア後の手順を実行できます。

メモ: SFR (シングルファイルリストア) または GRT (個別リストア) およびアプリケーションリストアは、インストールされているエージェントを介して実行されます。ただし、ボリュームリカバリでは、リカバリの成功後に関連ファイルシステムをオンラインにする必要があります。

ボリュームリストア後の手順を実行するには

- 1 コマンドを実行して、ホストに新しく接続されたポストボリュームをすべて表示します。
PVS

重複する PV がある (上記のコマンドで警告が表示される) 場合は、次のコマンドを実行します。

```
vgimportclone --import /dev/<Device1> /dev/<Device2> ...  
--basevgname <NewVGName>
```

または、ホストで新しく作成されたボリュームグループ (VG) を確認します。新しい VG が表示されない場合は、次のコマンドを使用して VG をインポートします。新しい VG は <NewVGName> として検出されます。

```
vgimport -a  
  
vgs
```

- 2 次のコマンドを実行して、すべての論理ボリューム (新旧) を一覧表示します。

```
lvs <NewVGName>
```

- 3 <NewVGName> に属するすべての LV を有効化します。

```
lvchange --activate y /dev/mapper/<NewVGName>-<LVName1>  
  
lvchange --activate y /dev/mapper/<NewVGName>-<LVName2>  
  
lvchange --activate y /dev/mapper/<NewVGName>-<LVNameN>
```

- 4 認証され、新しく有効化された LV の UUID とファイルシステムを特定します。

```
blkid -p /dev/mapper/<NewVGName>-<LVName1>

Output: /dev/mapper/<NewVGName>-<LVName1>:
UUID="2a4bdc14-b5eb-4ee6-b876-ebdcb66c55d9"
BLOCK_SIZE="4096"TYPE="xfs" USAGE="filesystem"

blkid -p /dev/mapper/<OldVGName>-<LVName1>

Output: /dev/mapper/<OldVGName>-<LVName1>:
UUID="2a4bdc14-b5eb-4ee6-b876-ebdcb66c55d9"
BLOCK_SIZE="4096"TYPE="xfs" USAGE="filesystem"
```

- 5 UUID が同じ場合は、次のように変更する必要があります。

ファイルシステム 手順

```
xfs          mkdir <NewMountPoint>

             mount -o nouuid /dev/mapper/<NewVGName>-<LVName1>
             <NewMountPoint>

             umount <NewMountPoint>

             xfs_admin -U generate
             /dev/mapper/<NewVGName>-<LVName1>

             mount /dev/mapper/<NewVGName>-<LVName1>
             <NewMountPoint>

ext2 / ext3/ ext4  mkdir<NewMountPoint>

                 tune2fs -U random
                 /dev/mapper/<NewVGName>-<LVName1>

                 mount /dev/mapper/<NewVGName>-<LVName1>
                 <NewMountPoint>
```

- 6 UUID が異なる場合は、次のコマンドを実行します。

```
mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>
```

トラブルシューティング

Microsoft Azure クラウドのスナップショットリストア処理のトラブルシューティング

同じ VM で後続の 2 回のリストア操作をトリガすると、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、<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-ssh-connection> のトピックに記載されている手順を実行します。

サポート対象外のファイルとフォルダのフィルタ処理

CloudPoint 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、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=<process 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、CloudPoint 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 プライマリサーバーの bp.conf ファイルで次のフラグを設定して CP DISKMAP チェックを有効にします。

```
CP_DISKMAP_CHECK = true/yes
```

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.9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。

CloudPoint ログファイルを表示するには、『[NetBackup CloudPoint インストールおよびアップグレードガイド](#)』の CloudPoint 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 6-1 構成用のログファイル

プロセス	ログ
<p>tpconfig</p> <p>tpconfig コマンドは、CloudPoint を NetBackup に登録する方法の 1 つです。</p>	<p>Windows の場合</p> <p>NetBackup install path/volmgr/debug/tpcommand</p> <p>UNIX の場合</p> <p>/usr/opensv/volmgr/debug/tpcommand</p>
<p>nbwebservice</p> <p>プラグインは、NetBackup REST API を使用して構成します。</p>	<p>Windows の場合</p> <p>NetBackup install path/webserver/logs</p> <p>UNIX の場合</p> <p>/usr/opensv/wmc/webserver/logs</p> <p>/usr/opensv/logs/nbwebservices</p>
<p>nbemm</p> <p>nbemm は、CloudPoint サーバーとプラグインの情報を EMM データベースに格納します。</p>	<p>Windows の場合</p> <p>NetBackup install path/path/logs/nbemm</p> <p>UNIX の場合</p> <p>/usr/opensv/logs/nbemm</p>

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 6-2 資産検出のログファイル

プロセス	ログ
<p>ncfnbcs</p> <p>検出が完了したかどうかを確認します。</p>	<p>Windows の場合</p> <p>NetBackup install path/bin/vxlogview -o 366</p> <p>UNIX の場合</p> <p>/usr/opensv/netbackup/bin/vxlogview -o 366</p>
<p>Picloud</p> <p>検出操作の詳細を提供します。</p>	<p>Windows の場合</p> <p>NetBackup install path/bin/vxlogview -i 497</p> <p>UNIX の場合</p> <p>/usr/opensv/netbackup/bin/vxlogview -i 497</p>

プロセス	ログ
<p>nbwebservice</p> <p>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。</p> <p>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。</p>	<p>Windows の場合</p> <p>NetBackup install path/webserver/logs</p> <p>UNIX の場合</p> <p><code>/usr/opensv/wmc/webserver/logs</code></p> <p><code>/usr/opensv/logs/nbwebservices</code></p>

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 6-3 スナップショット作成のログファイル

プロセス	ログ
<p>nbpem</p> <p>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。</p>	<p>Windows の場合</p> <p>NetBackup install path/bin/vxlogview -o 116</p> <p>UNIX の場合</p> <p><code>/usr/opensv/netbackup/bin/vxlogview -o 116</code></p>
<p>nbjm</p> <p>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。</p>	<p>Windows の場合</p> <p>NetBackup install path/bin/vxlogview -o 117</p> <p>UNIX の場合</p> <p><code>/usr/opensv/netbackup/bin/vxlogview -o 117</code></p>
<p>nbcs</p> <p>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。</p>	<p>Windows の場合</p> <p><i>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</i></p> <p>UNIX の場合</p> <p><code>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</code></p> <p>nbcs ログは次の場所から入手できます。</p> <p>Windows の場合</p> <p>NetBackup install path/logs/ncfnbcs</p> <p>UNIX の場合</p> <p><code>/usr/opensv/logs/ncfnbcs</code></p>

プロセス	ログ
<p>nbrb</p> <p>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、CloudPoint サーバー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。</p>	<p>Windows の場合</p> <p><code>NetBackup install path/bin/vxlogview -o 118</code></p> <p>UNIX の場合</p> <p><code>/usr/opensv/netbackup/bin/vxlogview -i 118</code></p>

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 6-4

プロセス	ログ
<p>nbwebservice</p> <p>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。</p>	<p>Windows の場合</p> <p><code>NetBackup install path/webserver/logs</code></p> <p>UNIX の場合</p> <p><code>/usr/opensv/wmc/webserver/logs</code></p> <p><code>/usr/opensv/logs/nbwebservices</code></p>
<p>bprd</p> <p>NetBackup REST API は、リストアを開始するために bprd と通信します。</p>	<p>Windows の場合</p> <p><code>NetBackup install path/netbackup/logs</code></p> <p>UNIX の場合</p> <p><code>/usr/opensv/netbackup/logs/bprd</code></p>
<p>ncfnbcs</p> <p>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。</p>	<p>Windows の場合</p> <p><code>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</code></p> <p>UNIX の場合</p> <p><code>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</code></p>

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 6-5 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/opensv/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/opensv/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 の作業負荷のリカバリに関する問題のトラブルシューティング

エラー 150: 管理者から終了が要求されました (Error 150: Termination requested by administrator)

説明: これは、アクティビティモニターから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でデータベース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 **CloudPoint** 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: **CloudPoint** サーバーで、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。