NetBackup™ Web UI クラウド管理者ガイド

リリース 9.0

VERITAS™

NetBackup Web UI クラウド管理者ガイド

最終更新日: 2021-02-01

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

NetBackup Web ユーザーインターフェースの概要

この章では以下の項目について説明しています。

NetBackup Web UI について

NetBackup Web ユーザーインターフェースは、次の機能を提供します。

- Chrome や Firefox などの Web ブラウザからマスターサーバーにアクセスする機能。Web UI でサポートされるブラウザについて詳しくは、NetBackup ソフトウェア互換性リストを参照してください。
  NetBackup Web UI は、ブラウザによって動作が変わる場合があります。日付選択などの一部の機能は、一部のブラウザでは利用できないことがあります。こうした違いは、NetBackup の制限によるものではなく、ブラウザの機能によるものです。
- 重要な情報の概要を表示するダッシュボード。
- 役割ベースのアクセス制御 (RBAC) により、管理者は NetBackup へのユーザーアクセスを構成し、セキュリティ、ストレージ管理、または作業負荷の保護などのタスクを委任できます。
- NetBackup セキュリティ設定、証明書、API キー、ユーザーセッションの管理。
- 資産の保護は、保護計画、ジョブ管理、資産の保護状態の可視性を通じて実現します。また、ポリシー管理は、限られた数のポリシー形式でも利用できます。

- 作業負荷管理者は、保護計画を作成し、SLO を満たす保護計画に資産をサブスクライブし、保護状態を監視し、仮想マシンのセルフサービスリカバリを実行できます。Web UI は次の作業負荷をサポートします。
  - クラウド
  - Microsoft SQL Server
  - Oracle
  - Red Hat Virtualization (RHV)
  - VMware
- 使用状況レポートは、マスターサーバー上のバックアップデータのサイズを追跡します。また、Veritas NetInsights コンソールに簡単に接続して、NetBackup ライセンスを表示および管理できます。

メモ: NetBackup Web UI は、1280x1024 以上の画面解像度で最適に表示されます。

NetBackup Web UI のアクセス制御

NetBackup では、役割ベースのアクセス制御を使用して Web UI へのアクセス権を付与します。アクセス制御は、役割を通じて実行されます。

- 役割は、ユーザーが実行できる操作と、作業負荷資産、保護計画、またはクレデンシャルに必要なアクセス権を定義します。単一のユーザーに複数の役割を設定でき、ユーザーアクセスを完全かつ柔軟にカスタマイズできます。
- RBAC は、Web UI と API でのみ利用可能です。
  NetBackup のその他のアクセス制御方法は、拡張監査 (EA) を除いて、Web UI と API ではサポートされません。

NetBackup ジョブおよびイベントの監視

NetBackup Web UI を使用すると、管理者はより簡単に NetBackup 操作とイベントを監視し、注意が必要な問題を特定できます。

- ダッシュボードには、NetBackup ジョブ、証明書、トークン、セキュリティイベント、使用状況レポートの概要が表示されます。
  表示されるダッシュボードウィジェットは、ユーザーの RBAC の役割と権限によって異なります。
- ジョブが失敗したときに管理者が通知を受信するように電子メール通知を設定できます。NetBackup は、受信電子メールを受け取ることができる任意のチケットシステムをサポートします。

保護計画: スケジュール、ストレージ、およびストレージオプションを一元的に構成する場所

保護計画には、次の利点があります。

- バックアップのスケジュールに加えて、保護計画には、レプリケーションと長期保持のスケジュールも含めることができます。
- 利用可能なストレージから選択するときに、そのストレージで利用可能な追加機能を確認できます。
- デフォルトの作業負荷管理者は、バックアップ処理時間帯やバックアップ保持期間などの保護計画を作成して管理できます。
  役割の権限について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。
- デフォルトの作業負荷管理者は、資産またはインテリジェントグループを保護するために使用する保護計画を選択できます。

セルフサービスリカバリ

NetBackup Web UI を使用すると、作業負荷管理者が VM またはデータベースを簡単にリカバリできるようになります。インスタントアクセス機能をサポートする作業負荷の場合、ユーザーはスナップショットをマウントして、VM のファイルやデータベースにすぐにアクセスできます。

用語

次の表では、新しい Web ユーザーインターフェースで導入された概念と用語について説明します。

表 1-1 Web ユーザーインターフェースの用語および概念

用語	定義
管理者	NetBackup と、NetBackup Web UI を含むすべてのインターフェースに対する完全なアクセス権を持つユーザーです。ルート、管理者、拡張監査のすべてのユーザーは、NetBackup の完全なアクセス権を持ちます。NetBackup Web UI の各ガイドでは、*NetBackup 管理者*という用語は、NetBackup への完全なアクセス権を持つユーザーも指しますが、通常は NetBackup 管理コンソールのユーザーを指します。 *「役割」*も参照してください。
資産グループ	*「インテリジェントグループ」*を参照してください。
資産	物理クライアント、仮想マシン、データベースアプリケーションなどの保護対象データです。

用語	定義
今すぐバックアップ	資産のバックアップをすぐに作成します。NetBackup は、選択した保護計画を使用して資産の完全バックアップを 1 回のみ実行します。このバックアップは、スケジュールバックアップには影響しません。
従来のポリシー	NetBackup Web UI では、レガシーポリシーが資産を保護することを示します。レガシーポリシーは、NetBackup 管理コンソールで作成します。
外部証明書	NetBackup 以外のあらゆる CA から発行されたセキュリティ証明書です。
インテリジェントグループ	指定した条件 (クエリー) に基づいて、NetBackup が保護対象資産を自動的に選択することを可能にします。インテリジェントグループは、本番環境の変更が含まれるように、自動的に最新の状態に維持されます。これらのグループは、資産グループとも呼ばれます。 VMware と RHV の場合、[インテリジェント VM グループ (Intelligent VM groups)]タブにこれらのグループが表示されます。
インスタントアクセス	NetBackup バックアップイメージから作成したインスタントアクセス VM やデータベースはほとんど瞬時に利用可能になるため、ほぼゼロのリカバリ時間目標を達成できます。NetBackup は、バックアップストレージデバイスにスナップショットを直接マウントし、そのスナップショットを通常の VM またはデータベースとして扱います。
NetBackup 証明書	NetBackup CA から発行されたセキュリティ証明書です。
保護計画	保護計画は、バックアップを実行するタイミング、バックアップの保持期間、使用するストレージ形式を定義します。保護計画を設定したら、資産を保護計画にサブスクライブできます。
RBAC	役割ベースのアクセス制御です。管理者は、RBAC で設定されている役割を通じて、NetBackup Web UI へのアクセスを委任または制限できます。 注意: RBAC で設定した役割は、NetBackup 管理コンソールまたは CLI へのアクセスを制御しません。
役割	RBAC の場合、ユーザーが実行できる操作と、ユーザーがアクセスできる資産やオブジェクトを定義します。たとえば、特定のデータベースのリカバリを管理する役割と、バックアップおよびリストアに必要なクレデンシャルを設定できます。
ストレージ	データのバックアップ、レプリケート、または複製 (長期保持用) 対象となるストレージです。

用語	定義
保護計画にサブスクライブする	保護計画にサブスクライブする資産または資産グループを選択する処理です。資産は、保護計画のスケジュールに従って保護されます。Web UI では、*サブスクライブ*を「保護の追加」とも表記します。
保護計画からサブスクライブ解除する	*サブスクライブ解除*は、保護を解除する処理、または計画から資産や資産グループを削除する処理を指します。
作業負荷 (Workload)	資産のタイプです。たとえば、VMware、RHV、またはクラウドです。

NetBackup Web UI へのサインイン

権限を持つユーザーは、NetBackup Web UI を使用して、NetBackup マスターサーバーに Web ブラウザからサインインできます。利用可能なサインインオプションは次のとおりです。

- 「ユーザー名とパスワードでサインインする」
- 「証明書またはスマートカードでサインインする」
- 「シングルサインオン (SSO) でサインインする」

ユーザー名とパスワードでサインインする

認可済みのユーザーのみが NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

ユーザー名とパスワードを使用して NetBackup マスターサーバーにサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*masterserver*/webui/login

   masterserver は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。

2. クレデンシャルを入力して、[サインイン (Sign in)]をクリックします。

   次に例を示します。

ユーザーの種類	使用する形式	例
ローカルユーザー	*username*	jane_doe
Windows ユーザー	*DOMAIN¥username*	WINDOWS¥jane_doe
UNIX ユーザー	*username@domain*	john_doe@unix

証明書またはスマートカードでサインインする

権限を持つユーザーである場合は、スマートカードまたはデジタル証明書を使用して NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

スマートカードにないデジタル証明書を使用するには、まずブラウザの証明書マネージャに証明書をアップロードする必要があります。詳しくはブラウザのマニュアルで手順を参照するか、証明書管理者にお問い合わせください。

証明書またはスマートカードでサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*masterserver*/webui/login

   masterserver は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。

2. ［証明書またはスマートカードでサインイン (Sign in with certificate or smart card)］をクリックします。
3. ブラウザにプロンプトが表示されたら、証明書を選択します。

シングルサインオン (SSO) でサインインする

NetBackup 環境内で SAML が ID プロバイダとして設定されている場合、シングルサインオン (SSO) オプションを使用して NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

SSO を使用して NetBackup マスターサーバーにサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*masterserver*/webui/login

   masterserver は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。

2. ［シングルサインオンでサインイン (Sign in with single sign-on)］をクリックします。
3. 管理者が指示する手順に従ってください。

   以降のログオンでは、NetBackup によって自動的にマスターサーバーへのサインインが行われます。

NetBackup Web UI からのサインアウト

NetBackup は、24 時間 (ユーザーセッションで許可される最大時間) 後に Web UI からの自動サインアウトを強制的に実行します。その時間が経過すると、NetBackup は再びサインインを要求します。また、使用するサインインオプション (ユーザー名とパスワード、

スマートカード、またはシングルサインオン (SSO)) を変更する場合にもサインアウトできます。

NetBackup Web UI からサインアウトするには

- 右上で、プロファイルアイコン、[サインアウト (Sign out)]の順にクリックします。

2

監視と通知

この章では以下の項目について説明しています。

NetBackup ダッシュボード

NetBackup ダッシュボードは、組織内のロールに関連する詳細情報のクイックビューを提供します。

表 2-1 NetBackup ダッシュボード

ダッシュボードウィジェット	説明
ジョブ	アクティブジョブやキューに投入済みのジョブの数、試行されたジョブや完了したジョブの状態などのジョブ情報を一覧表示します。
証明書	環境内の NetBackup のホスト ID ベースのセキュリティ証明書または外部証明書に関する情報を表示します。 外部証明書では、NetBackup 8.2 以降のホストに関する次の情報が表示されます。 ■ ホストの合計。ホストの合計数です。ホストはオンラインになっており、NetBackup マスターサーバーと通信できる必要があります。 ■ 不明。外部証明書が登録されていないホストの数です。 ■ 有効。外部証明書が登録されているホストの数です。 ■ 期限切れ。期限切れの外部証明書を持つホストの数です。
トークン	環境内の認証トークンに関する情報を表示します。

ダッシュボードウィジェット	説明
セキュリティイベント	[アクセス履歴 (Access history)]ビューには、ログオンイベントのレコードが含まれます。[監査イベント (Audit events)]ビューには、ユーザーが NetBackup マスターサーバーで開始したイベントが含まれます。
使用状況レポート	組織内の NetBackup マスターサーバーのバックアップデータのサイズを一覧表示します。このレポートは、容量ライセンスを追跡するために役立ちます。右上のドロップダウンリストを使用して、表示する期間とビューを選択します。サーバー名をクリックして、そのサーバーの特定の詳細を表示します。

ジョブの監視

[ジョブ (Jobs)]ノードを使用して、NetBackup 環境のジョブを監視し、特定のジョブの詳細を表示します。

ジョブを監視するには

1. 左側で、[アクティビティモニター (Activity monitor)]>[ジョブ (Jobs)]をクリックします。
2. 表示するジョブの名前をクリックします。

   [概要 (Overview)]タブで、ジョブに関する情報を表示します。

   - [ファイルリスト (File List)]には、バックアップイメージに含まれているファイルが表示されます。
   - [状態 (Status)]セクションには、ジョブに関連する状態と状態コードが表示されます。状態コード番号をクリックすると、この状態コードについてのベリタスナレッジベースの情報が表示されます。
     『NetBackup 状態コードリファレンスガイド』を参照してください。
3. [詳細 (Details)]タブをクリックして、ジョブについて記録された詳細を表示します。ドロップダウンメニューを使用して、エラーの種類によってログをフィルタできます。

   p.14 の「ジョブリストのジョブフィルタ」を参照してください。

ジョブリストのジョブフィルタ

特定の状態のジョブを表示するために、ジョブをフィルタできます。たとえば、実行中のジョブまたは一時停止中のジョブをすべて表示できます。

ジョブリストをフィルタするには

1. [ジョブ (Jobs)]をクリックします。
2. ジョブリストの上にある[フィルタ (Filter)]オプションをクリックします。

3 [フィルタ (Filter)]ウィンドウでフィルタオプションを選択すると、表示されるジョブが動的に変わります。フィルタオプションは次のとおりです。

- すべて (All)
- 有効 (Active)
- 完了 (Done)
- 失敗 (Failed)
- 未完了 (Incomplete)
- 部分的に成功 (Partially Successful)
- キューへ投入済み (Queued)
- 成功 (Successful)
- 一時停止 (Suspended)
- 再試行を待機中 (Waiting for Retry)

4 [フィルタの適用 (Apply Filters)]をクリックします。

5 選択したフィルタを解除するには、[すべて消去 (Clear All)]をクリックします。

3

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、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。9.0 以降のバージョンでは、CloudPoint で、ネットワーク通信チャネルに IPv6 を使用する資産を保護できるようになりました。IPv6 は、AWS 商用リージョンと AWS Gov Cloud (米国) でのみサポートされます。Azure 商用クラウド、Azure Gov クラウド、GCP ではサポートされません。

次の表では、タスクについて説明します。

表 3-1 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にお問い合わせください。 『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.32 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.18 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。 『Veritas 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.33 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.35 の「AWS の構成の IAM ロール」を参照してください。
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.25 の「NetBackup サーバーの CLOUD_AUTODISCOVERY_INTERVAL オプション」を参照してください。

タスク	説明
スナップショットのみの保護計画の作成	スナップショットのみの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.26 の「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.28 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.38 の「クラウド資産の元の場所へのリカバリ」を参照してください。 p.39 の「クラウド資産の代替の場所へのリカバリ」を参照してください。 p.39 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。 『 コマンドリファレンスガイド』を参照してください。 http://www.veritas.com/docs/DOC5332NetBackup
トラブルシューティング	p.41 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

クラウドワークロードを保護するときは、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 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。
- CloudPoint freemium バージョンとの NetBackup 統合はサポートされません。
- 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。
- ポート 0 を使用して CloudPoint サーバーを構成する場合は、デフォルト値が使用されます。
- 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 8.3 は、Ubuntu 18.04 以降または RHEL のオペレーティングシステムにインストールされている場合のみ IPv6 をサポートします。Ubuntu 16.04 を使用している場合は、最初に OS を Ubuntu 18.04 にアップグレードして IPv6 を使用する必要があります。
- 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。

AWS と Azure の政府向けクラウドサポート

8.3 以降の CloudPoint は、Amazon Web Services 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。

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	GovCloud (米国) 地域
Amazon Web Services	■ 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

AWS と Microsoft Azure の構成について詳しくは、p.33 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。https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal を参照してください。

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。

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 3-2　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。 ■ 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。 ■ 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 3-3　　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。
■ 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。

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 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。
■ 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。

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 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. [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、バックアップを再試行します。

NetBackup サーバーの CLOUD_AUTODISCOVERY_INTERVAL オプション

このオプションは、NetBackup がクラウド資産を検出して NetBackup に表示するために、CloudPoint サーバーをスキャンする頻度を制御します。

表 3-4 CLOUD_AUTODISCOVERY_INTERVAL 情報

使用方法	説明
使用する場所	NetBackup マスターサーバー上。
使用方法	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。 **メモ:** これらのコマンドでは、NetBackup マスターサーバーの管理者権限が必要です。詳しくは、NetBackup 管理者にお問い合わせください。 デフォルトは 2 時間です。最小値は 2 時間で、最大値は 1 年です。 次の形式を使用します。 CLOUD_AUTODISCOVERY_INTERVAL = 秒数 例: CLOUD_AUTODISCOVERY_INTERVAL = 100000 このエントリは、設定ファイルで一度のみ表示されます。 **メモ:** このオプションを変更した後、NetBackup サービスを停止して再起動します。

スナップショットレプリケーションの構成

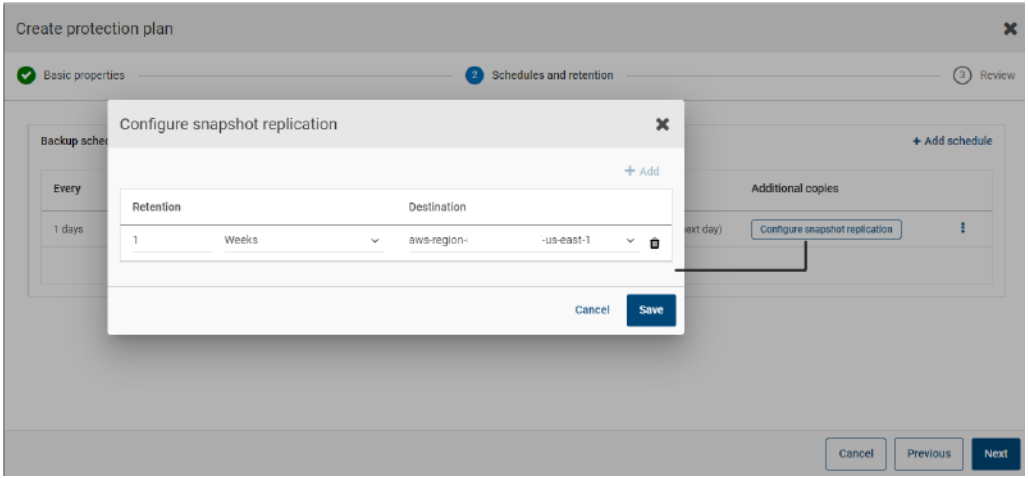
スナップショットクラウド資産をプライマリの場所からリモートやセカンダリの場所にレプリケートできます。スナップショット管理サーバー (CloudPoint) は、領域間およびアカウント間のレプリケーションをサポートしています。スナップショットレプリケーションを使用すると、次を実現できます。

- 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、Amazon Web Services 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。

- 1 つの保護計画で、1 つの宛先領域へのレプリケーションのみがサポートされます。
- 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。

- スナップショット管理サーバーで検出された資産は、同じスナップショット管理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、スナップショット管理サーバー「CP1」で検出された資産は、スナップショット管理サーバー「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、Amazon Web Services 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。

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 の作業負荷の場合、代替の場所を検出する必要がありますが、接続したり構成したりしないでください。
- Oracle の作業負荷の場合、代替の場所を検出し、構成する必要がありますが、接続しないでください。

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[VM の接続 (Connect VM)]をクリックします。
   - クレデンシャルを入力します。
   - [接続 (Connect)]をクリックします。
   - 仮想マシンが接続されると、仮想マシンの状態が[構成 (Configure)]に更新されます。

   メモ: Microsoft SQL Server の場合、この処理を手動で実行する必要があります。Veritas CloudPoint のドキュメントで、Windows ベースのオンホストのエージェントの構成に関するトピックを参照してください。次回の検出サイクル後に、仮想マシンの状態が[構成 (Configure)]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[クレデンシャルの編集 (Edit credentials)]をクリックします。
3. クレデンシャルを更新し、[接続 (Connect)]をクリックします。

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。

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るようになりました。9.0 以降では、CloudPoint は、Amazon Web Services および Microsoft AZURE US Government 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 マスター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 マスター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。

次の表では、基になるタスクについて説明します。

表 3-5 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.32 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.33 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す。p.36 の「CloudPoint サーバーの資産の検出」を参照してください。

タスク	説明
メディアサーバーの関連付け	メディアサーバーにスナップショットをオフロードしてワークフローをリストアするには、メディアサーバーを CloudPoint サーバーに関連付ける必要があります。p.36 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、証明書と鍵を 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. bp.conf ファイルで、次のエントリを作成します。
   - ECA_TRUST_STORE_PATH = /certificate.pem
   - (オプション) VIRTUALIZATION_CRL_CHECK = CHAIN
   - (オプション) ECA_CRL_PATH = /crls

   メモ:

   - 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 pem 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。

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。

メモ: 証明書のアップロード順序は次のとおりです。

- リーフ証明書
- 中間証明書
- ルート証明書

証明書が正しい順序でアップロードされていないと、CloudPoint が動作しないことがあります。

CloudPoint サーバーの追加

NetBackup 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ャルを入力し、証明書を検証する必要があります。

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 サーバー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。

CloudPoint サーバーのクラウドプロバイダの追加

AWS (Amazon Web Services)、GCP (Google Cloud Platform)、Microsoft Azure クラウドプロバイダ上の資産を保護できます。9.0 以降では、CloudPoint は、Amazon Web Services および Microsoft AZURE US Government 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 [CloudPoint サーバー (CloudPoint server)]タブをクリックします。

3 [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。

4 [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。

5 望ましい CloudPoint サーバーを選択します。

6 [保存 (Save)]をクリックします。

7 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。
Amazon AWS **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。	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。
	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` 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` JSON ファイルに記載されています。
	秘密鍵 (Private Key)	秘密鍵。`private_key` 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。

8 ［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。

9 ［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

スナップショット管理サーバー (CloudPoint) 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.33 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。詳しくは、Amazon Web Services 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。

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. [詳細設定 (Advanced settings)]ダイアログボックスで、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 サーバーにクラウドプロバイダを構成した後、資産を検出し、保護計画を割り当てることができます。この操作の一環として、最初に CloudPoint サーバーでクラウド検出がトリガされます。CloudPoint サーバーは、クラウドのすべての資産を検出します。CloudPoint サーバーの検出が完了すると、NetBackup の資産が CloudPoint サーバーが検出した資産で更新されます。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ます。

メモ: CloudPoint の検出は、30 分でタイムアウトします。CloudPoint サーバーによる検出は、30 分以上かかると最初の検出操作がタイムアウトします。ただし、2 回目の検出操作が続行され、NetBackup 資産は CloudPoint サーバーが検出した資産で更新されます。

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。

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. [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。

4

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。

クラウド資産の元の場所へのリカバリ

Google Cloud Platform の場合、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、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。

クラウド資産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. クラウド資産タイプに応じて、[仮想マシン (Virtual Machine)]、[アプリケーション (Applications)]、[ボリューム (Volumes)]タブのいずれかをクリックします。

   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。
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。

クラウド資産の代替の場所へのリカバリ

注意事項

- Google Cloud Platform 用のクラウド資産は、代替の場所にリストアできません。
- レプリケートした EC2 インスタンスのコピーを代替の場所にリストアするには、レプリケーション元とレプリケーション先の領域でキー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キーペアと一貫性がある新しいキーペアをレプリケーション先の領域で作成してください。

クラウド資産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. クラウド資産タイプに応じて、[仮想マシン (Virtual Machine)]、[アプリケーション (Applications)]、[ボリューム (Volumes)]タブのいずれかをクリックします。

   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。
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。

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。元の場所や代替の場所へのリストアとは異なり、リストアされたイメージの新しい複製は作成されませんが、リストア元の既存のデータは置き換えられます。

メモ: スナップショットレプリカはロールバックできません。

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. サポート対象のクラウド資産タイプで、[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。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. リカバリするイメージで、[リカバリ (Recover)]、[ロールバック (Rollback)]の順にクリックします。
6. [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。
7. 左側の[ジョブ (Jobs)]をクリックして、ジョブ状態を表示します。

5

クラウド資産の保護とリカバリのトラブルシューティング

この章では以下の項目について説明しています。

クラウドの作業負荷の保護に関する問題のトラブルシューティング

クラウド資産の保護で発生する問題のトラブルシューティングを行うには、次のログファイルを確認します。

- 「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.18 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、『Veritas NetBackup CloudPoint Install and Upgrade Guide』の「CloudPoint logs」を参照してください。

構成用のログファイル

クラウド構成の問題のトラブルシューティングを行うには、次のログを使用します。

表 5-1 構成用のログファイル

プロセス	ログ
tpconfig tpconfig コマンドは、CloudPoint 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、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。	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 5-2 資産検出のログファイル

プロセス	ログ
ncfnbcs 検出が完了したかどうかを確認します。	Windows の場合 NetBackup install path/bin/vxlogview –o 400 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -o 400
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 5-3　　スナップショット作成のログファイル

プロセス	ログ
nbpem 特定のジョブの nbpem PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 NetBackup install path/bin/vxlogview –o 116 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -o 116
nbjm 特定のジョブの nbjm PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 NetBackup install path/bin/vxlogview –o 117 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -o 117
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、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。	Windows の場合 *NetBackup install path*/bin/vxlogview –o 118 UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 118

リストア操作のログファイル

リストアの問題のトラブルシューティングを行うには、次のログを使用します。

表 5-4

プロセス	ログ
nbwebservice スナップショットのリストア操作は、NetBackup REST API によってトリガされます。	Windows の場合 NetBackup install path/webserver/logs UNIX の場合 /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices
bprd NetBackup REST API は、リストアを開始するために bprd と通信します。	Windows の場合 NetBackup install path/netbackup/logs UNIX の場合 /usr/openv/netbackup/logs/bprd
ncfnbcs 特定のジョブの nbcs PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 *NetBackup install path*/bin/vxlogview –i 366 –P *nbcs_process_id* UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id

スナップショットの削除のログファイル

スナップショットの削除の問題のトラブルシューティングを行うには、次のログを使用します。

表 5-5 スナップショットの削除のログファイル

プロセス	ログ
bpdm スナップショットの削除またはクリーンアップ操作は、bpdm によってトリガされます。	Windows の場合 NetBackup install path/netbackup/logs UNIX の場合 /usr/openv/netbackup/logs/bpdm
ncfnbcs 特定のジョブの nbcs PID は、NetBackup アクティビティモニターで利用可能です。	Windows の場合 *NetBackup install path*/bin/vxlogview -i 366 -P *nbcs_process_id* UNIX の場合 /usr/openv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id

6

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 6-1 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 6-2 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	9.0
NetBackup バックアップホスト OS	RHEL 7.x
CloudPoint ホスト OS	■ RHEL 7x 以降 ■ Ubuntu 18.04 LTS および 16.04 LTS

アプリケーション	バージョン
クラウドプロバイダ	■ Amazon Web Services ■ Microsoft Azure ■ Google Cloud Platform **メモ:** 個別リストアは、Google Cloud Platform の Windows 環境ではサポートされません。
CloudPoint 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 ■ Google Cloud Platform: n1.Standard2 以降
保護対象の CloudPoint エージェントホスト	■ Linux OS: RHEL 7.7 および 7.6 ■ Windows OS のバージョン: 2016 および 2012 **メモ:** 個別リストアは、RHEL 8.X プラットフォームではサポートされません。

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:** 個別リストアは、RHEL 8.X プラットフォームではサポートされません。	■ 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: 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。

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: CloudPoint ホストと接続された VM は、同じサブスクリプションおよび地域内にある必要があります。
- 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。
- 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。
- 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。fsConsistent フラグを使用すると、ホスト上のファイルシステムを CloudPoint によってスナップできるようになり、indexable フラグによってホストのインデックス付けが可能になります。fsConsistent フラグが true に設定されている場合にのみ、indexable フラグを true に設定できます。
- 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.48 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。
- エージェントレスリストアの場合は、エージェント接続のために、インデックス付け可能な仮想マシンでポート 22 を設定する必要があります。
- オンホストリストアの場合、ポート 5671 と 3389 (RDP) は、エージェント接続用のターゲット仮想マシンで開いている必要があります。RDP は構成にのみ使用され、省略可能です。
- 個別リストアを実行するための適切な権限があることを確認します。『NetBackup Web UI 管理者ガイド』を参照してください。
- 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。
- CloudPoint がサポートするインデックス付けジョブの最大数は、次の条件に基づいて制限されます。
  - CloudPoint ホストで利用可能なデータディスクの接続ポイントの数から 1 を減算した数およびインスタンスの種類。CloudPoint メタデータボリュームは、この 1 つの接続ポイントを使用します。
  - CloudPoint マシンの CPU またはメモリのリソースの可用性。
- 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。
- LVM または LDM ディスクで作成されたファイルシステムは、ファイルシステムの一貫性のあるスナップショットの作成およびインデックス付け中には無視されます。
- 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ルで 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。
- アプリケーションおよびディスクのリストアは、RHEL 8.2 から RHEL 8.2 ターゲットでのみサポートされています。
- 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。
- 個別リストアは、RHEL 8.x プラットフォームではサポートされません。
- 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。

クラウド仮想マシン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 と Google Cloud Platform 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[VM の接続 (Connect VM)]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と、2 つのインデックス付けジョブが完了した後、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、[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。

Microsoft Azure 固有の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。