

# NetBackup™ Web UI クラウド 管理者ガイド

リリース 8.2

**VERITAS™**

# NetBackup Web UI クラウド管理者ガイド

最終更新日: 2019-06-28

## 法的通知と登録商標

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、NetBackup は Veritas Technologies LLC または同社の米国とその他の国における関連会社の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、サードパーティの所有物であることをベリタスが示す必要のあるサードパーティソフトウェア（「サードパーティプログラム」）が含まれている場合があります。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。このベリタス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 は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については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。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202、「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となります。業務用またはホスト対象サービスとしてベリタスによって提供されている場合でも同様です。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世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供

されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の Web サイトにアクセスしてください。

[https://www.veritas.com/support/ja\\_JP.html](https://www.veritas.com/support/ja_JP.html)

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

既存のサポート契約に関する質問については、次に示す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。

世界全域 (日本を除く)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan (日本)

[CustomerCare\\_Japan@veritas.com](mailto: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 ページに最終更新日付が記載されています。最新のマニュアルは、次のベリタス 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](mailto:NB.docs@veritas.com)

次のベリタスコミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

<http://www.veritas.com/community/ja>

## ベリタスの Service and Operations Readiness Tools (SORT) の表示

ベリタスの Service and Operations Readiness Tools (SORT) は、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](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# 目次

<b>第 1 章</b>	<b>NetBackup Web ユーザーインターフェースの概要</b>	5
	NetBackup Web ユーザーインターフェースについて	5
	用語	7
	NetBackup Web UI へのサインイン	9
<b>第 2 章</b>	<b>クラウド資産の管理</b>	11
	クラウド資産の保護について	11
	制限事項および考慮事項	13
	NetBackup での CloudPoint サーバーの登録	14
	クラウドプロバイダ向けの構成	15
	AWS の構成の IAM ロール	16
	スナップショットレプリケーションの構成	16
	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	18
	クラウド資産検出間隔の設定	20
	クラウド資産の元の場所へのリカバリ	21
	クラウド資産の代替の場所へのリカバリ	21
	クラウド資産のロールバックリカバリの実行	22
	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	23

# 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 ユーザーインターフェースについて](#)
- [用語](#)
- [NetBackup Web UI へのサインイン](#)

## NetBackup Web ユーザーインターフェースについて

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。
- 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、バックアップ管理、または作業負荷の保護に関連するタスクを委任できます。
- NetBackup セキュリティ管理者は、NetBackup のセキュリティ、証明書、RBAC、API キー、ユーザーセッション、ロックされている NetBackup ユーザーアカウントを管理できます。
- バックアップ管理者は、サービスレベル目標 (SLO) を満たすために保護サービスを提供します。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。

- 作業負荷管理者は、**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
  - 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 Smart Meter 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。

## 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。このアクセス制御には、ユーザーが実行できるタスクと、ユーザーが表示および管理できる資産が含まれています。アクセス制御は、アクセスルールを通じて実行されます。

- アクセスルールは、ユーザーまたはユーザーグループに、役割とオブジェクトグループを関連付けます。役割は、ユーザーが持つアクセス権を定義します。オブジェクトグループでは、ユーザーがアクセスできる資産と **NetBackup** オブジェクトを定義します。単一のユーザーまたはグループに複数のアクセスルールを作成でき、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。
- **NetBackup** には、デフォルトの役割が 3 つ用意されています。ユーザーのニーズに最も適した役割を選択するか、そのユーザーの要件を満たすためのカスタムの役割を作成します。
- オブジェクトグループを使用して、資産やアプリケーションサーバーのグループを定義したり、ユーザーが表示または管理できる保護計画を示します。たとえば、特定の **VMware** アプリケーションサーバーを使用してオブジェクトグループを作成して、**VMware** 管理者向けアクセス権を付与できます。**VMware** 管理者が **VMware** 資産を保護するために選択できる特定の保護計画を、オブジェクトグループに追加することもできます。
- **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** アクセス制御 (**NBAC**) が有効な場合は、**Web UI** を使用できません。

## NetBackup ジョブおよびイベントの監視

NetBackup Web UI を使用すると、セキュリティ管理者やバックアップ管理者は、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。

- **NetBackup** セキュリティ管理者は、ダッシュボードを使用して、セキュリティ証明書や監査イベントの状態を参照できます。

- バックアップ管理者は、ダッシュボードを使用することで、NetBackup ジョブの状態を参照できます。ジョブが失敗したときに通知を受信するために、電子メール通知を構成することもできます。NetBackup では、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。
- オンプレミスストレージまたはスナップショットストレージを簡単に選択できます。
- 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。
- バックアップ管理者は、保護計画を作成して管理します。つまり、バックアップのスケジュールとストレージの責任を負います。
- 作業負荷管理者は、主に資産またはインテリジェントグループを保護するための保護計画を選択します。ただし、バックアップ管理者は、必要に応じて保護計画に資産をサブスクライブすることもできます。

## セルフサービスリカバリ

NetBackup Web UI は、VM のリカバリを簡略化します。VMware の場合、インスタントアクセス機能を使用して、VM のスナップショットをマウントし、そのファイルにすぐにアクセスできます。ファイルをローカルホストにダウンロードしたり、ファイルを元の VM にリストアしたりできます。

# 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
アクセスルール	RBAC は、ユーザーまたはユーザーグループ、役割またはアクセス権、ユーザーまたはユーザーグループがアクセスできるオブジェクトグループを定義します。ユーザーまたはグループには、複数のアクセスルールを設定できます。

用語	定義
管理者	<p>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 に対して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。</p> <p>「役割」も参照してください。</p>
資産グループ	<p>「インテリジェントグループ」を参照してください。</p>
資産	<p>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。</p>
従来のポリシー	<p>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。</p>
外部証明書	<p>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。</p>
インテリジェントグループ	<p>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。</p> <p>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。</p>
オブジェクトグループ	<p>RBAC の場合、ユーザーがアクセスすることを許可された資産のコレクション、保護計画、サーバー、その他のリソースを指します。</p>
NetBackup 証明書	<p>NetBackup CA から発行されたセキュリティ証明書。</p>
保護計画	<p>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。</p>
RBAC	<p>役割ベースのアクセス制御です。管理者は、RBAC で構成されているアクセスルールを通じて、NetBackup Web UI へのアクセスを委任または制限できます。</p> <p>注意: RBAC で構成したルールは、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。Web UI は、NetBackup アクセス制御 (NBAC) ではサポートされておらず、NBAC が有効になっている場合は使用できません。</p>

用語	定義
役割	RBAC の場合、ユーザーが持つことができる権限を定義します。 NetBackup にはシステム定義の役割が 3 つあり、ユーザーがセキュリティ、保護計画、バックアップを管理したり、作業負荷資産を管理したりすることを可能にします。
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。クラウドの作業負荷に対しては、スナップショットストレージが使用されます。
サブスクリプション、保護計画に対して	資産または資産グループを保護する保護計画を選択する処理です。関連付けられた資産は、計画のスケジュールとストレージの設定に従って保護されます。Web UI では、サブスクリプションを「保護の追加」とも表記します。
保護計画からサブスクリプション解除する	サブスクリプション解除は、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。
ワークフロー	NetBackup Web UI を使用して完了できるエンドツーエンドプロセスです。たとえば、NetBackup 8.1.2 以降では、VMware とクラウドの資産を保護およびリカバリできます。

## 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」

### ユーザー名とパスワ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、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。

NetBackup Web UI 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	<code>username</code>	<code>root</code>
ドメインユーザー	<code>DOMAIN\username</code>	<code>WINDOWS\Administrator</code>

## 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。

# クラウド資産の管理

この章では以下の項目について説明しています。

- [クラウド資産の保護について](#)
- [制限事項および考慮事項](#)
- [NetBackup での CloudPoint サーバーの登録](#)
- [クラウドプロバイダ向けの構成](#)
- [スナップショットレプリケーションの構成](#)
- [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](#)
- [クラウド資産検出間隔の設定](#)
- [クラウド資産の元の場所へのリカバリ](#)
- [クラウド資産の代替の場所へのリカバリ](#)
- [クラウド資産のロールバックリカバリの実行](#)
- [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。

次の表では、タスクについて説明します。

表 2-1 クラウド資産に対する保護の構成

作業	説明
<p>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。</p>	<p>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。</p> <p>『<a href="#">NetBackup Web UI セキュリティ管理者ガイド</a>』を参照してください。</p> <p><b>メモ:</b> 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。</p>
<p>CloudPoint の配備</p>	<p>環境内に CloudPoint をインストールします。</p> <p>『<a href="#">Veritas CloudPoint 管理者ガイド</a>』を参照してください。</p> <p>CloudPoint と NetBackup の制限事項を確認します。</p> <p>p.13 の「<a href="#">制限事項および考慮事項</a>」を参照してください。</p>
<p>NetBackup 管理コンソールを使用した、CloudPoint サーバーの構成</p>	<p>NetBackup で CloudPoint サーバーを登録します。</p> <p>p.14 の「<a href="#">NetBackup での CloudPoint サーバーの登録</a>」を参照してください。</p>
<p>構成の追加</p>	<p>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。</p> <p>必要なクラウドプロバイダに対して、クラウドアカウントを追加 (クラウドプラグインを構成) する必要があります。プロバイダごとに複数の構成を作成できます。p.15 の「<a href="#">クラウドプロバイダ向けの構成</a>」を参照してください。</p> <p>Amazon の場合は、IAM ロールを使用することもできます。p.16 の「<a href="#">AWS の構成の IAM ロール</a>」を参照してください。</p>
<p>資産の検出</p>	<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 4 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.20 の「<a href="#">クラウド資産検出間隔の設定</a>」を参照してください。</p>

作業	説明
スナップショットのみの保護計画の作成	<p>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。</p> <p>『<a href="#">NetBackup Web UI バックアップ管理者ガイド</a>』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.16 の「<a href="#">スナップショットレプリケーションの構成</a>」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>『<a href="#">NetBackup Web UI バックアップ管理者ガイド</a>』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.18 の「<a href="#">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</a>」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"> <li>■ 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.21 の「<a href="#">クラウド資産の元の場所へのリカバリ</a>」を参照してください。</li> <li>■ p.21 の「<a href="#">クラウド資産の代替の場所へのリカバリ</a>」を参照してください。</li> <li>■ p.22 の「<a href="#">クラウド資産のロールバックリカバリの実行</a>」を参照してください。</li> <li>■ 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。</li> </ul> <p><b>メモ:</b> リストアに bprestore CLI を使用しないでください。</p> <p>『<a href="#">NetBackup コマンドリファレンスガイド</a>』を参照してください。</p>
トラブルシューティング	<p>p.23 の「<a href="#">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</a>」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 管理者ガイド』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。
- スナップショットまたはリストアジョブが失敗した場合、クラウドのターゲット上のデータを手動でクリーンアップ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。

## NetBackup での CloudPoint サーバーの登録

次の方法のいずれかを使って CloudPoint サーバーを登録できます。

- NetBackup 管理コンソールの使用。  
『NetBackup Snapshot Client 管理者ガイド』を参照してください。
- `-tpconfig` コマンドの使用。  

```
tpconfig -add -cloudpoint_server cloudpoint_server_name  
-cloudpoint_server_user_id user_ID [-requiredport IP_port_number]
```

『NetBackup コマンドリファレンスガイド』を参照してください。

NetBackup で CloudPoint サーバーを構成するには、次のようにします。

- 特定の NetBackup 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。  
メディアサーバーの関連付けは、`tpconfig` コマンドラインを使用した場合にのみサポートされます。  

```
tpconfig -update -cloudpoint_server cloudpoint_server_name  
-add_media_server media_server
```

複数のメディアサーバーを関連付けるには、コマンドを複数回実行する必要があります。メディアサーバーは、バージョン 8.1.2 以降でなければなりません。メディアサーバーを関連付けない場合は、NetBackup マスターサーバーが使用されます。

- クラウドプラグインを構成するときは、マスターサーバーに登録されているすべての CloudPoint サーバー間で、地域が他のプラグインと重複していないことを確認します。

## クラウドプロバイダ向けの構成

NetBackup がサポートするすべてのクラウドプロバイダは、NetBackup 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。

### クラウドプロバイダ向けの構成を追加するには

- 1 左側の[クラウド (Cloud)]をクリックします。
- 2 [プロバイダ (Providers)]タブをクリックします。  
NetBackup がサポートするクラウドプロバイダが表示されます。
- 3 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)]ペインで、接続と認証の詳細を入力します。
- 5 [保存 (Save)]をクリックします。

### クラウドプロバイダの構成を編集するには

- 1 左側の[クラウド (Cloud)]をクリックします。
- 2 [プロバイダ (Providers)]タブをクリックします。  
NetBackup がサポートするクラウドプロバイダが表示されます。
- 3 構成を更新するクラウドプロバイダの下にある[構成 (Configuration)]をクリックします。
- 4 リストから、更新する構成をダブルクリックします。
- 5 [構成の追加 (Add Configuration)]ペインで、接続と認証の詳細を更新します。
- 6 [保存 (Save)]をクリックします。

### クラウドプロバイダの構成を無効にするには

- 1 左側の[クラウド (Cloud)]をクリックします。
- 2 [プロバイダ (Providers)]タブをクリックします。サポート対象のクラウドプロバイダが表示されます。
- 3 構成を無効にするクラウドプロバイダの下にある[構成 (Configuration)]をクリックします。
- 4 リストから削除する構成を選択します。
- 5 [無効化 (Disable)]をクリックします。

## 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.15 の「クラウドプロバイダ向けの構成」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、[Veritas CloudPoint のドキュメント](#)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。詳しくは、[Veritas CloudPoint のマニュアル](#)を参照してください。  
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。

## スナップショットレプリケーションの構成

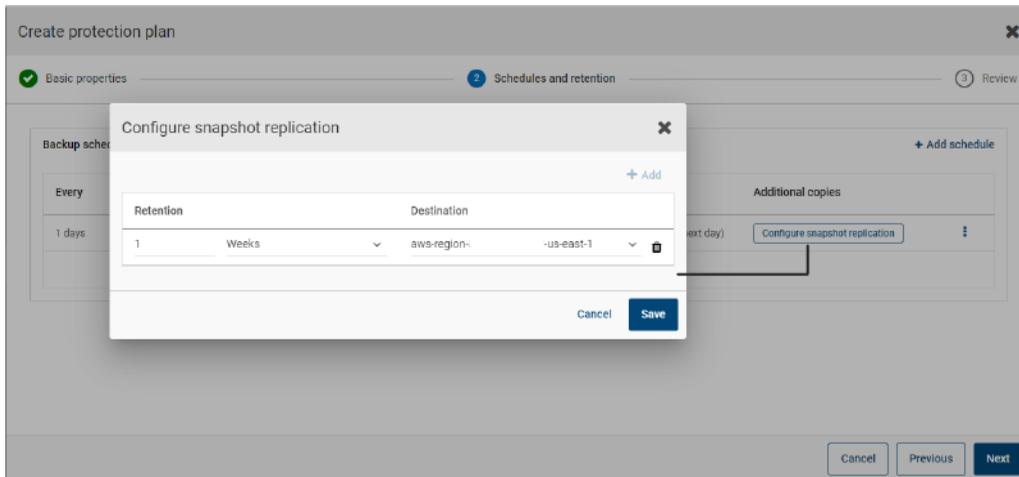
スナップショットクラウド資産をプライマリの場所からリモートやセカンダリの場所にレプリケートできます。スナップショット管理サーバー (CloudPoint) は、領域間およびアカウント間のレプリケーションをサポートしています。スナップショットレプリケーションを使用すると、次を実現できます。

- 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。

## 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 については、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。

# クラウド資産検出間隔の設定

資産検出間隔は、資産を検出して NetBackup に追加する頻度です。

## VM のクラウド資産検出間隔の設定

デフォルトでは、VM の資産検出は 4 時間ごとに行われます。この間隔は時間を表し、1 ~ 23 の間で設定できます。値は、整数で指定する必要があります。

クラウド資産の検出間隔を構成するには

1 適切な構成オプションを選択します。

- Windows

検出間隔は、nbsetconfig コマンドを使用して構成できます。

例

```
nbsetconfig nbsetconfig>  
CLOUD_DISCOVERY_INTERVAL = 2
```

このコマンドのディレクトリパスは、install\_path¥NetBackup¥bin¥ です。

『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

- UNIX

/usr/opensv/netbackup/bp.conf ファイル内の CLOUD\_DISCOVERY\_INTERVAL パラメータを設定します。

2 nbdisco サービスを再起動します。

資産検出は、サービスの再起動後にトリガされます。

## ホストアプリケーションのクラウド資産の検出間隔の構成

デフォルトでは、ホストアプリケーションの資産検出は 15 時間ごとに行われます。この間隔は分を表し、15 から 45 までの間で構成できます。値は、整数で指定する必要があります。

ホストアプリケーションのクラウド資産の検出間隔を構成するには

1 適切な構成オプションを選択します。

- Windows

検出間隔は、nbsetconfig コマンドを使用して構成できます。

例

```
nbsetconfig nbsetconfig>  
CLOUD_HOSTED_APP_DISCOVERY_INTERVAL = 15
```

このコマンドのディレクトリパスは、install\_path¥NetBackup¥bin¥ です。

『[NetBackup コマンドリファレンスガイド](#)』を参照してください。

- UNIX

/usr/opensv/netbackup/bp.conf ファイル内の  
CLOUD\_HOSTED\_APP\_DISCOVERY\_INTERVAL パラメータを設定します。

- 2 nbdisco サービスを再起動します。  
資産検出は、サービスの再起動後にトリガされます。  
指定した間隔の経過後にホストアプリケーションの検出がトリガされます。

## クラウド資産の元の場所へのリカバリ

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、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)]、[元の場所にリストア (Restore to original location)]の順にクリックします。
- 6 [OK]をクリックします。
- 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。

## 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、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)]、[代替の場所にリストア (Restore to alternate location)]の順にクリックします。
- 6 クラウド資産をリストアする場所を入力します。
- 7 [リカバリの開始 (Start Recovery)]をクリックします。
- 8 左側の[ジョブ (Jobs)]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。

## 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.13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。

### 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 2-2 構成用のログファイル

プロセス	Logs
tpconfig tpconfigコマンドは、CloudPointをNetBackupに登録する方法の1つです。	Windows <i>NetBackup install</i> <i>path/volmgr/debug/tpcommand</i>  UNIX <i>/usr/opensv/volmgr/debug/tpcommand</i>

プロセス	Logs
<b>nbwebservice</b> プラグインは、NetBackup REST API を使用して構成します。	Windows <code>NetBackup install path/webserver/logs</code> UNIX <code>/usr/opensv/wmc/webserver/logs</code> <code>/usr/opensv/logs/nbwebservices</code>
<b>nbemm</b> 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 <code>NetBackup install path/bin/vxlogview -o 111</code> UNIX <code>/usr/opensv/netbackup/bin/vxlogview -o 111</code>

## 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 2-3 資産検出のログファイル

プロセス	Logs
<b>nbdisco</b> 検出が完了したかどうかを確認します。	Windows <code>NetBackup install path/bin/vxlogview -o 400</code> UNIX <code>/usr/opensv/netbackup/bin/vxlogview -o 400</code>
<b>Picloud</b> 検出操作の詳細を提供します。	Windows <code>NetBackup install path/bin/vxlogview -i 497</code> UNIX <code>/usr/opensv/netbackup/bin/vxlogview -i 497</code>
<b>nbwebservice</b> 検出操作に含まれる資産 DB ワークフローについての詳細を取得できます。 <b>メモ:</b> 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 <code>NetBackup install path/webserver/logs</code> UNIX <code>/usr/opensv/wmc/webserver/logs</code> <code>/usr/opensv/logs/nbwebservices</code>

## 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 2-4 スナップショット作成のログファイル

プロセス	Logs
<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</p> <p><i>NetBackup install path/bin/vxlogview -o 116</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/bin/vxlogview -o 116</i></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</p> <p><i>NetBackup install path/bin/vxlogview -o 117</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/bin/vxlogview -o 117</i></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</p> <p><i>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i></p> <p>nbcs ログは次の場所から入手できます。</p> <p>Windows</p> <p><i>NetBackup install path/logs/ncfnbcs</i></p> <p>UNIX</p> <p><i>/usr/opensv/logs/ncfnbcs</i></p>
<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</p> <p><i>NetBackup install path/bin/vxlogview -o 118</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/bin/vxlogview -i 118</i></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 2-5

プロセス	Logs
<p><b>nbwebservice</b></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</p> <p><i>NetBackup install path/webserver/logs</i></p> <p>UNIX</p> <p><i>/usr/opensv/wmc/webserver/logs</i></p> <p><i>/usr/opensv/logs/nbwebservices</i></p>
<p><b>bprd</b></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</p> <p><i>NetBackup install path/netbackup/logs</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/logs/bprd</i></p>
<p><b>ncfnbcs</b></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</p> <p><i>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i></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 2-6 スナップショットの削除のログファイル

プロセス	Logs
<p><b>bpdm</b></p> <p>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。</p>	<p>Windows</p> <p><i>NetBackup install path/netbackup/logs</i></p> <p>UNIX</p> <p><i>/usr/opensv/netbackup/logs/bpdm</i></p>

プロセス	Logs
<p><b>ncfnbcs</b></p> <p>特定のジョブの <b>nbcs</b> PID は、<b>NetBackup</b> アクティビティモニターで利用可能です。</p>	<p><b>Windows</b></p> <pre>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</pre> <p><b>UNIX</b></p> <pre>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</pre>