

NetBackup™ Web UI VMware 管理者ガイド

リリース 9.1

最終更新日: 2021-07-20

法的通知と登録商標

Copyright © 2021 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

目次

第 1 章	NetBackup Web ユーザーインターフェースの概要	7
	NetBackup Web UI について	7
	用語	9
	NetBackup Web UI へのサインイン	10
	NetBackup Web UI からのサインアウト	12
第 2 章	NetBackup の監視	13
	NetBackup ダッシュボード	13
	ジョブの監視	13
	ジョブリストのジョブフィルタ	14
第 3 章	VMware サーバーの管理	15
	VMware サーバーの追加	15
	VMware サーバーのクレデンシャルの検証と更新	17
	VMware サーバーの参照	18
	VMware サーバーの削除	18
	インテリジェント VM グループの作成	19
	インテリジェント VM グループの削除	26
	VMware アクセスホストの追加	26
	VMware アクセスホストの削除	27
	VMware リソース形式のリソース制限の変更	27
	VMware 資産の自動検出の間隔の変更	28
	VMware サーバーの資産の手動での検出	29
第 4 章	VM の保護	31
	Web UI での VMware ポリシーの操作	31
	VM またはインテリジェント VM グループの保護	32
	VMware バックアップを使用した SQL Server データの保護	33
	VMware 資産の保護設定の編集	34
	スケジュールと保持	35
	バックアップオプション (Backup options) と詳細オプション (Advanced options)	35
	バックアップからのディスクの除外	36

	スナップショットの再試行オプション (Snapshot retry options)	37
	VM またはインテリジェント VM グループの保護の解除	38
	VM またはインテリジェント VM グループの保護状態の表示	38
第 5 章	インスタントアクセス	40
	インスタントアクセス VM の作成	40
	VM バックアップイメージからのファイルとフォルダのリストア	42
	VM バックアップイメージからのファイルとフォルダのダウンロード	44
	インスタントアクセス機能を使用する前の考慮事項	45
	インスタントアクセス Build Your Own (BYO)	47
	インスタントアクセス Build Your Own (BYO) の前提条件	47
	インスタントアクセス Build Your Own (BYO) のハードウェア構成の必 要条件	49
	よく寄せられる質問	49
第 6 章	インスタントロールバック	53
	インスタントロールバックの前提条件	53
	インスタントロールバック機能を使用する前の考慮事項	53
	VM バックアップイメージからのインスタントロールバック	54
第 7 章	継続的なデータ保護	56
	継続的なデータ保護について	56
	前提条件	57
	CDP 用の容量ベースのライセンス	58
	CDP の構成	59
	CDP ゲートウェイの定義	59
	サイズ変更の注意事項	60
	CDP の並列実行バックアップジョブの制限	62
	完全同期の制御	63
	CDP ジョブの監視	64
	CDP でのアクセラレータの使用	67
	CDP で保護されている VM のリカバリ	67
	CDP のトラブルシューティング	68
第 8 章	VM のリカバリ	70
	VM のリカバリ	70
	VMware エージェントレスリストアについて	76
	VMware エージェントレスリストアの前提条件と制限事項	77
	VMware エージェントレスリストアによるファイルとフォルダのリカバリ	78
	制限されたリストアモードについて	79

第 9 章	VMware の操作のトラブルシューティング	81
	VMware サーバーの追加エラー	82
	VMware サーバーを参照するときに発生するエラー	82
	新たに検出された VM の状態のエラー	83
	インスタントアクセス VM からファイルをダウンロードするときに発生するエ ラー	84
	除外された仮想ディスクのバックアップとリストアのトラブルシューティング	85
	複数のデータストアを使用した仮想マシンのリストアが失敗する	87
	リカバリ先を変更したときに発生したエラー	87

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](#)
- [用語](#)
- [NetBackup Web UI へのサインイン](#)
- [NetBackup Web UI からのサインアウト](#)

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 ブラウザからプライマリ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、作業負荷の保護のタスクを委任できます。
- 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。

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。ポリシー形式の詳細を参照できます。

- 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、資産のセルフサービスリカバリを実行できます。

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、Web UI でユーザーがアクセスできる機能を定義します。たとえば、作業負荷の資産、保護計画、またはクレデンシャルへのアクセスなどがあります。
- 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 ジョブの監視

NetBackup Web UI を使用すると、管理者はより簡単に NetBackup ジョブの操作を監視し、注意が必要な問題を特定できます。

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。

- デフォルトの作業負荷管理者は、資産を保護するために使用する保護計画を選択できます。
- 必要な RBAC 権限を使用して、作業負荷管理者は、使用されているバックアップスケジュールやストレージを含む保護計画を作成して管理できます。
- 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。

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、その作業負荷に適用可能な VM、データベース、その他の資産形式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、Web ユーザーインターフェースの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
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。
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。
インテリジェントグループ	指定した条件 (問い合わせ) 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。 [インテリジェント VM グループ (Intelligent VM groups)] タブまたは [インテリジェントグループ (Intelligent 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	注意: インスタントアクセスは、一部の作業負荷でのみサポートされます。 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。
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。役割の管理者は、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 では、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アルを設定できます。

用語	定義
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。
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、AHV、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 プライマリサーバーに 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** プライマリ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://primaryserver/webui/login`

`primaryserver` は、サインインする **NetBackup** プライマリ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>jane_doe</code>
Windows ユーザー	<code>DOMAIN\username</code>	<code>WINDOWS\jane_doe</code>
UNIX ユーザー	<code>username@domain</code>	<code>john_doe@unix</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://primaryserver/webui/login`

`primaryserver` は、サインインする **NetBackup** プライマリ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** プライマリ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://primaryserver/webui/login`

primaryserver は、サインインする **NetBackup** プライマリ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** によって自動的にプライマリ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、プロフィールアイコン、[サインアウト (Sign out)]の順にクリックします。

NetBackup の監視

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](#)
- [ジョブの監視](#)
- [ジョブリストのジョブフィルタ](#)

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	実行中の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。

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ペ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。

VMware サーバーの管理

この章では以下の項目について説明しています。

- VMware サーバーの追加
- VMware サーバーのクレデンシャルの検証と更新
- VMware サーバーの参照
- VMware サーバーの削除
- インテリジェント VM グループの作成
- インテリジェント VM グループの削除
- VMware アクセスホストの追加
- VMware アクセスホストの削除
- VMware リソース形式のリソース制限の変更
- VMware 資産の自動検出の間隔の変更
- VMware サーバーの資産の手動での検出

VMware サーバーの追加

ここでは、VMware サーバーとそのクレデンシャルを追加する手順を示します。

VMware サーバーとそのクレデンシャルを追加するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[VMware サーバー (VMware servers)]タブをクリックします。

このタブには、アクセスできる vCenter Server と ESXi Server が表示されます。

- 2 [追加 (Add)]をクリックしてサーバーを追加します。

- 3 サーバー形式を選択し、ホスト名とクレデンシヤルを入力します。
- 4 [検証用バックアップホスト (Backup host for validation)]を選択します。

メモ: VMware のクレデンシヤルを追加または更新した場合も、VMware サーバーの検出が自動的に開始されます。要求でバックアップホストの情報を指定すると、検出の実行に加えて、クレデンシヤルの検証にもその情報が使用されます。検出の場合、バックアップホストとして動作する NetBackup メディアサーバーまたはクライアントでサポートされる最小バージョンは、NetBackup 8.1.2 です。古いバージョンでは、バックアップホストのクレデンシヤルは正常に検証されますが、VMware サーバーの検出に失敗します。

- 5 接続に使用する[ポート (Port)]番号を指定します。

VMware サーバーでデフォルトのポート番号が変更されていない場合、ポートの指定は不要です。異なるポートを使用するように VMware サーバーが構成されている場合、そのポート番号を指定してください。

- 6 [保存 (Save)]をクリックします。

重要!

サーバーのクレデンシヤルが Web UI や API で追加または更新されると、vCenter または ESXi Server の VM とその他のオブジェクトの検出が開始されます。ただし、UI にはサーバーの VM とその他のオブジェクトがすぐに表示されない場合があります。それらは VMware サーバーの検出プロセスが完了した後に表示されます。検出は設定された間隔でも実行されます(デフォルトの間隔は 8 時間です)。

VMware サーバーのオブジェクトの自動検出を異なる間隔で実行する方法については、次の情報を参照してください。

p.28 の「[VMware 資産の自動検出の間隔の変更](#)」を参照してください。

- 7 別の VMware サーバーの NetBackup クレデンシヤルを入力するには、[追加 (Add)]をクリックします。

発生する可能性がある問題のトラブルシューティングについては、次の情報を参照してください。

p.82 の「[VMware サーバーの追加エラー](#)」を参照してください。

p.82 の「[VMware サーバーを参照するときに発生するエラー](#)」を参照してください。

p.83 の「[新たに検出された VM の状態のエラー](#)」を参照してください。

VMware サーバーのクレデンシャルの検証と更新

VMware のクレデンシャルを検証するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[VMware サーバー (VMware servers)]タブをクリックします。
- 2 1 つのサーバーのクレデンシャルを検証するには、その VMware サーバーを特定して選択します。複数のサーバーのクレデンシャルを同時に検証するには、それらの VMware サーバーを特定して選択します。次に、該当するサーバーの行で[検証 (Validate)]をクリックします。

選択した VMware サーバーの現在のクレデンシャルが NetBackup で検証されます。

クレデンシャルが有効でない場合、NetBackup では[クレデンシャル (Credentials)]に[無効 (Invalid)]と表示されます。VMware サーバーのクレデンシャルを更新するには、次の手順を実行します。

VMware サーバーのクレデンシャルを更新するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[VMware サーバー (VMware servers)]タブをクリックします。
- 2 VMware サーバーを特定します。
- 3 [処理 (Actions)]、[クレデンシャルの管理 (Manage credentials)]の順に選択します。
- 4 クレデンシャルを必要に応じて更新します。

メモ: VMware のクレデンシャルを追加または更新した場合も、VMware サーバーの検出が自動的に開始されます。要求でバックアップホストの情報を指定すると、検出の実行に加えて、クレデンシャルの検証にもその情報が使用されます。検出の場合、バックアップホストとして動作する NetBackup メディアサーバーまたはクライアントでサポートされる最小バージョンは、NetBackup 8.1.2 です。古いバージョンでは、バックアップホストのクレデンシャルは正常に検証されますが、VMware サーバーの検出に失敗します。

- 5 [保存 (Save)]をクリックします。

選択した VMware サーバーの更新後のクレデンシャルが NetBackup で検証されます。

VMware サーバーの参照

vCenter Server とスタンドアロンの ESXi Server を参照して、VM を特定し、保護計画やリカバリポイントなどの詳細を表示できます。

VMware サーバーを参照するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 [VMware サーバー (VMware servers)]をクリックして、検索を開始します。

リストには、アクセス権を持つ vCenter Server とスタンドアロンの ESXi Server の名前と種類が含まれます。[検出の状態 (Discovery Status)]と[前回の検出の試行 (Last discovery attempt)]を確認すると、サーバーの VM やその他のオブジェクトが正常に検出されたかどうかを確認できます。

サーバーを見つけるには、検索フィールドに文字列を入力します。

- 3 サーバーをクリックしてドリルダウンを開始します。
上向き矢印をクリックすると、より高いレベルに移動して戻れます。
- 4 VM をクリックすると、保護状態、リカバリポイント、リストアアクティビティが表示されます。
- 5 計画に VM をサブスクライブするには、[保護の追加 (Add protection)]をクリックします。

VMware サーバーの削除

ここでは、NetBackup から VMware サーバーを削除する手順を示します。

VMware サーバーを削除するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[VMware サーバー (VMware servers)]タブをクリックします。

このタブには、アクセス権を持つ vCenter Server とスタンドアロンの ESXi Server の名前と種類が表示されます。[検出の状態 (Discovery Status)]と[前回の検出の試行 (Last discovery attempt)]を確認すると、サーバーの VM やその他のオブジェクトが最後にいつ検出されたかも確認できます。

- 2 VMware サーバーを特定します。

- 3 [処理 (Actions)]、[削除 (Delete)]の順に選択します。

メモ: VMware サーバーを削除すると、そのサーバーに関連付けられているすべての仮想マシンの保護が行われなくなります。既存のバックアップイメージのリカバリは引き続き可能ですが、このサーバーへの VM のバックアップは失敗します。

- 4 VMware サーバーを削除してもよいことを確認したら、[削除 (Delete)]をクリックします。

インテリジェント VM グループの作成

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 VM グループを作成できます。NetBackup は、問い合わせに基づいて自動的に仮想マシンを選択し、それらをグループに追加します。その後、グループに保護を適用できます。インテリジェントグループでは、VM 環境内の変更が自動的に反映されるため、グループ内の VM 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。

メモ: VMware サーバーの VM の検出が、自動検出の間隔に従って設定された間隔で実行されます (デフォルトの間隔は 8 時間です)。問い合わせが選択できる状態になるには、Web UI が各サーバー上の VM を検出する必要があります。VMware サーバーが Web UI に最近追加された場合、その VM は検出されない可能性があります。このオプションについて詳しくは、次の情報を参照してください。

p.28 の「[VMware 資産の自動検出の間隔の変更](#)」を参照してください。

VM をすぐに検出する方法については、次の情報を参照してください。

p.29 の「[VMware サーバーの資産の手動での検出](#)」を参照してください。

インテリジェント VM グループを作成するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 [インテリジェント VM グループ (Intelligent VM 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 適切な VMware サーバーを選択します。
- 5 次のいずれかを実行します。
 - [すべての VM を含める (Include all VMs)]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 vCenter または ESXi に現在あるすべての VM 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 VM 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。
- 6 条件を追加するには、ドロップダウンを使用してキーワードと演算子を選択し、値を入力します。

この手順の後に、オプションについて説明します「[インテリジェント VM グループ作成のための問い合わせオプション](#)」。

こちらに例もあります。「[問い合わせの例](#)」

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、条件のキーワード、演算子、値を選択します。次に例を示します。

The screenshot shows a query builder interface with two conditions. At the top, there are buttons for 'AND' and 'OR'. To the right are links for '+ Condition' and '+ Sub-query'. The first condition has the keyword 'displayName', the operator 'Contains', and the value 'prod'. The second condition has the keyword 'tag', the operator '=', and the value 'eng'. Each condition has a trash icon on the right.

必要に応じて、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。次に例を示します。

The screenshot shows a query builder interface with a main condition and a sub-query. The main condition has the keyword 'displayName', the operator 'Contains', and the value 'prod'. Below it is a sub-query box. Inside the sub-query box, there are buttons for 'AND' and 'OR'. To the right are links for '+ Condition' and '+ Sub-query'. The sub-query has the keyword 'cluster', the operator 'Starts with', and the value 'clust'. Each condition has a trash icon on the right.

- 7 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仮想マシン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ときに問い合わせが選択する VM が、プレビューに現在表示されているものと同一でなくなる可能性があります。

- 8 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。

保存して保護計画に追加するには、[追加と保護 (Add and protect)]をクリックして計画を選択し、[保護する (Protect)]をクリックします。

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 VM を選択するときに、問い合わせオプションでは大文字小文字が区別されます。[仮想マシン (Virtual machine)]で、グループに選択されていない VM をクリックすると、[仮想マシングループのメンバー (Member of virtual machine groups)]フィールドは none になります。

ただし、保護計画にグループを追加したときに、保護計画のバックアップが実行されると、一部の問い合わせオプションは、大文字と小文字が区別されないものとして扱われます。その結果、同じ VM がグループに含められてバックアップされる場合があります。

各オプションの大文字小文字関連の動作は、「[インテリジェント VM 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。

インテリジェント VM グループ作成のための問い合わせオプション

インテリジェント VM グループについては、次の点に注意してください。

- [インテリジェント VM グループ (Intelligent VM 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、問い合わせに一致する正確な VM のリストが NetBackup Web UI に表示されないことがあります。ただし、バックアップ中は、VM の属性が英語以外でも、正しい VM が選択されます。
- 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) 資産を含む資産が返されます。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。
- インテリジェント VM グループのサーバーが更新されると、インテリジェントグループが新しいサーバー名前空間に登録されるため、そのインテリジェントグループに設定されているすべての既存のアクセス定義は削除されます。更新されたインテリジェントグループに新しいアクセス定義を追加する必要があります。

表 3-1 問い合わせキーワード

キーワード	説明	保護計画の実行時に大文字と小文字が区別される
annotation	vSphere Client の VM の注釈に追加されるテキスト。	はい
connectionState	ESX Server への VM 接続の状態。たとえば、仮想マシンの ESX Server が停止している場合、その仮想マシンは接続されていません。	いいえ
cluster	VM が存在するクラスター (ESXi Server のグループ) の名前。	いいえ
datacenter	データセンターの名前。	いいえ
datacenterPath	データセンターへのパスを定義するフォルダの構造。フィルタリングの基準にするデータセンター名が環境で一意でない場合にこのオプションを使います。	はい
datastore	データストアの名前。	はい
displayName	VM の表示名。	はい
host	ESXi Server の名前。ESXi ホスト名は vCenter Server で定義された名前と一致する必要があります。	いいえ
dnsName	vSphere Client の VM の DNS 名。	いいえ
guestOS	vSphere Client に記録される VM のゲスト OS の種類。	はい
hostName	IP アドレスの逆引きから導かれる VM 名。	いいえ
instanceUuid	VM のインスタンス UUID。 例: 501b13c3-52de-9a06-cd9a-ecb23aa975d1	いいえ
networkName	ネットワークスイッチ (ESX Server 上) または分散スイッチの名前。	いいえ
powerState	VM の電源状態。	いいえ
tag	VM のタグの名前。	はい
template	VM が仮想マシンテンプレートかどうかを示します。	いいえ
version	仮想マシンの VMware バージョン。例: vmx-04、vmx-07、vmx-08。	はい
vmFolder	VM フォルダ (データセンター内の) の名前。VM が格納されているフォルダのパスも含みます。 p.25 の「 VMFolder の例 」を参照してください。	いいえ

キーワード	説明	保護計画の実行時に大文字と小文字が区別される
vmxDatastore	VMX データストアの名前 (VMX ディレクトリや構成データストアと呼ばれることもあります)。	はい
vmxDatastoreType	VMX データストアの形式。値は NFS または VMFS です。	いいえ

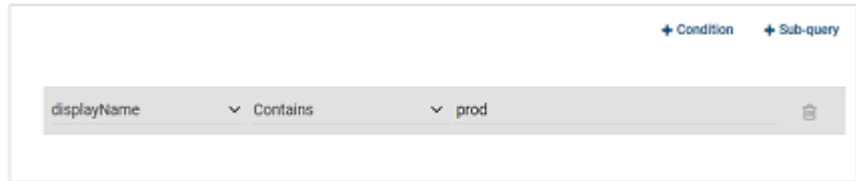
問い合わせ演算子

表 3-2 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。 たとえば、入力した値が「box」の場合、このオプションは文字列「box_car」と一致しますが、「flatbox」とは一致しません。
Ends with	文字列の末尾に値が出現する場合に一致します。 たとえば、入力した値が「dev」の場合、このオプションは文字列「01dev」と一致しますが、「01dev99」または「devOP」とは一致しません。
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。 たとえば、入力した値が「dev」の場合、このオプションは「01dev」、「01dev99」、「devOP」、「development_machine」などの文字列と一致します。
=	入力した値にのみ一致します。 たとえば、入力した値が「VMTest27」の場合、このオプションは「VMtest27」(大文字小文字が同じ) とは一致しますが、「vmtest27」、「vmTEST27」、または「VMtest28」とは一致しません。
!=	入力した値と等しくない任意の値と一致します。

問い合わせの例

この例の問い合わせは、表示名に prod が含まれるすべての VM をグループに追加します。

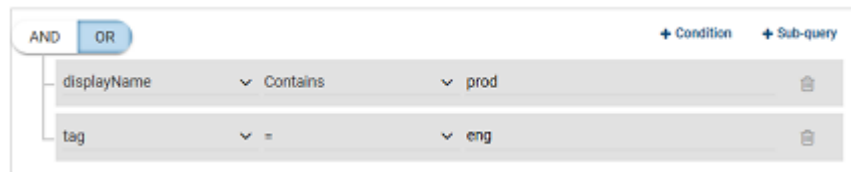


問い合わせの効果を変更するには、[条件 (Condition)]をクリックし、[AND]または[OR]をクリックして、条件のキーワード、演算子、値を選択します。例:



この例では、**AND** を使用して問い合わせの範囲を絞り込みます。表示名に prod が含まれ、eng という名前のタグを持つ **VM** のみが選択されます。**VM** の表示名に prod が含まれず、eng という名前のタグがない場合、その **VM** はグループに追加されません。

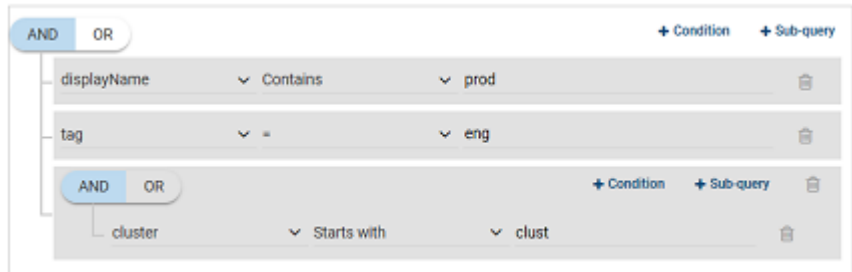
問い合わせの範囲を広げるには、[OR]を使用します。



この例では、[OR]が設定されているため、問い合わせでグループに次の **VM** が追加されます。

- 表示名に prod が含まれる **VM** (タグに関係なく)。
- eng という名前のタグを持つ **VM** (表示名に関係なく)。

必要に応じて、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。例:



この例では、サブクエリーを使用して問い合わせの範囲をさらに絞り込みます。表示名に prod を含み、eng という名前のタグを持つ VM のうち、clust で始まるクラスタに含まれている VM のみが選択されます。

VMFolder の例

たとえば、次の VM フォルダに合計で 65 個の VM が含まれていると想定します。

vm¥VM_backup_prod1 (5 個の VM を含む)

vm¥VM_backup_prod1¥cluster1 (10 個の VM を含む)

vm¥VM_backup_prod2 (50 個の VM を含む)

vm¥VM_backup_prod1 の VM を含め、cluster1 またはその他のフォルダの VM は除外する場合は、次のように指定します。

```
VMFolder Equal "vm¥VM_backup_prod1"
```

vm¥VM_backup_prod1 の VM とそのサブフォルダ cluster1 を含めるには、次のように指定します。

```
VMFolder Equal "vm¥VM_backup_prod1"
```

または

```
VMFolder StartsWith "vm¥VM_backup_prod1"
```

注意: 最初のバックスラッシュは、続くバックスラッシュがリテラル文字として解釈されるようにするためのエスケープ文字です。

65 個のすべての VM を含めるには、VMFolder StartsWith "vm¥VM_backup_prod" のように指定します。

注意: vm¥VM_backup_prod で始まるパス内にあるすべての VM が含まれます。

インテリジェント VM グループの削除

インテリジェント VM グループを削除するには、次の手順を使用します。

インテリジェント VM グループを削除するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 [インテリジェント VM グループ (Intelligent VM 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てスクロールダウンし、鍵の記号をクリックして、[サブスクライブ解除 (Unsubscribe)]をクリックします。
- 5 [削除]をクリックします。

VMware アクセスホストの追加

NetBackupでは、VMware アクセスホストと呼ばれる特別なホストを使用します。これは仮想マシンに代わってバックアップを実行する NetBackup クライアントです。アクセスホストは、NetBackup マスターサーバーまたはクライアントソフトウェアがインストールされる唯一のホストです。仮想マシンでは、NetBackup クライアントソフトウェアは不要です。ただし、アクセスホストは、仮想マシンのデータストアにアクセスする必要があります。アクセスホストはデータストアからデータを読み込み、ネットワーク経由でデータをメディアサーバーに送信します。

VMware アクセスホストは、以前は VMware バックアップホストまたは VMware バックアッププロキシサーバーと呼ばれていました。アクセスホストは、リストアを実行する場合はリカバリホストと呼ばれます。

メモ: 追加するすべてのアクセスホストに、NetBackup のメディアサーバーソフトウェアまたはクライアントソフトウェアがインストールされていることを確認してください。

VMware アクセスホストを追加するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[仮想マシン (Virtual machines)]タブをクリックします。
- 2 右側で[VMware 設定 (VMware settings)]、[アクセスホスト (Access hosts)]の順に選択します。

NetBackup でこれまでに追加されたすべてのアクセスホストが一覧表示されます。
- 3 [追加 (Add)]をクリックします。
- 4 アクセスホストの名前を入力し、[追加 (Add)]をクリックします。

VMware アクセスホストの削除

VMware アクセスホストを削除するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[仮想マシン (Virtual machines)]タブをクリックします。
- 2 右側で[VMware 設定 (VMware settings)]、[アクセスホスト (Access hosts)]の順に選択します。

NetBackup でこれまでに追加されたすべてのアクセスホストが一覧表示されます。

- 3 VMware アクセスホストを特定し、削除アイコンをクリックします。
- 4 内容を確認したら、[削除 (Delete)]をクリックします。

VMware リソース形式のリソース制限の変更

VMware リソース形式で同時に実行できるバックアップの数は、VMware リソース制限で制御されます。これらの設定は、現在選択しているプライマリサーバーのすべての NetBackup ポリシーに適用されます。

VMware リソース形式のリソース制限を変更するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 右上で[VMware 設定 (VMware settings)]、[リソース制限 (Resource limits)]の順に選択します。

各リソースのデフォルト値は 0 (制限なし) です。

- 3 変更する VMware リソース形式を選択し、[編集 (Edit)]を選択します。

メモ: [スナップショット (Snapshot)]のリソース制限は、他のリソース形式のものとは異なります。この設定は、スナップショットの作成や削除など、vCenter ドメインにおけるスナップショットのみに関する同時操作の数を制限します。この制限が適用されるのは、バックアップのスナップショット作成フェーズとスナップショット削除フェーズのみです。同時バックアップジョブの数は制御されません。この[スナップショット (Snapshot)]の制限は、複数のスナップショット操作が vCenter Server に与える影響を制御する場合に有効です。特定の vCenter を追加すると、その vCenter についてはグローバルなスナップショット設定が上書きされます。

4 次のオプションを選択します。

VMware リソース形式のグローバル制限を設定 [グローバル (Global)] 設定を特定して、適用する [制限 (Limits)] の値を選択します。

この値により、リソース形式で実行される同時バックアップ数が制限されます。

特定の VMware リソースの制限を設定します。 [追加 (Add)] をクリックします。

リストから、リソースを選択します。

適用する [制限 (Limits)] の値を選択します。

この値により、選択したリソースで実行される同時バックアップ数が制限されます。

5 [保存 (Save)] をクリックします。

[制限 (Limits)] には、リソース形式で実行できる同時バックアップの数が表示されます。これはグローバル制限の値です。[上書き (Override)] の値には、グローバル制限と異なる制限があるリソースの数が表示されます。

すべての VMware リソースのリソース制限をリセットする

すべての VMware リソースのリソース制限をリセットするには

- ◆ [デフォルト値に戻す (Reset default values)] をクリックすると、すべての上書きが削除され、グローバルな VMware リソース制限がすべてデフォルト値に設定されます。

VMware 資産の自動検出の間隔の変更

VMware 資産の自動検出は一定の間隔で実行されます。デフォルトの間隔は 8 時間です。自動検出の間隔を変更する手順は次のとおりです。

VM 資産の自動検出の間隔を変更するには

- 1 左側で [作業負荷 (Workloads)]、[VMware] の順にクリックし、[仮想マシン (Virtual machines)] タブをクリックします。
- 2 右側で [VMware 設定 (VMware settings)]、[自動検出 (Autodiscovery)] の順に選択します。

- 3 [間隔 (Frequency)]、[編集 (Edit)]の順に選択します。
- 4 NetBackup で VMware 資産の自動検出を実行する間隔を上下の矢印を使用して選択します。次に、[保存 (Save)]をクリックします。

選択できる範囲は 1 時間から 24 時間までです。自動検出の間隔を分または秒単位で設定する場合や自動検出を無効にする場合は、VMware 自動検出 API を使用する必要があります。

VMware サーバーの資産の手動での検出

ここでは、最近追加された資産を表示して保護できるように、VMware サーバーの資産を手動で検出する手順を示します。

メモ: サーバーのクレデンシャルが Web UI や API で追加または更新されると、vCenter または ESXi Server の VM とその他のオブジェクトの自動検出が開始されます。ただし、UI にはサーバーの VM とその他のオブジェクトがすぐに表示されない場合があります。それらは VMware サーバーの検出プロセスが完了した後に表示されます。検出は `VMWARE_AUTODISCOVERY_INTERVAL` オプションで設定された間隔でも実行されます (デフォルトの間隔は 8 時間です)。このオプションについて詳しくは、次の情報を参照してください。

p.28 の「[VMware 資産の自動検出の間隔の変更](#)」を参照してください。

VMware サーバーの資産を手動で検出するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックし、[VMware サーバー (VMware servers)]タブをクリックします。

このタブには、アクセス権を持つ vCenter Server とスタンドアロンの ESXi Server の名前と種類が表示されます。[検出の状態 (Discovery Status)]と[前回の検出の試行 (Last discovery attempt)]を確認すると、サーバーの VM やその他のオブジェクトが最後にいつ検出されたかも確認できます。

- 2 VMware サーバーを特定して選択します。
- 3 [処理 (Actions)]、[検出 (Discover)]の順に選択します。

VMware サーバーのクレデンシャルが無効な場合、検出操作に失敗することがあります。クレデンシャルを検証および更新する方法については、次の情報を参照してください。

p.17 の「[VMware サーバーのクレデンシャルの検証と更新](#)」を参照してください。

VM およびインテリジェント VM グループの保護状態について詳しくは、次の情報を参照してください。

p.38 の「[VM またはインテリジェント VM グループの保護状態の表示](#)」を参照してください。

p.83 の「[新たに検出された VM の状態のエラー](#)」を参照してください。

VM の保護

この章では以下の項目について説明しています。

- [Web UI での VMware ポリシーの操作](#)
- [VM またはインテリジェント VM グループの保護](#)
- [VMware 資産の保護設定の編集](#)
- [VM またはインテリジェント VM グループの保護の解除](#)
- [VM またはインテリジェント VM グループの保護状態の表示](#)

Web UI での VMware ポリシーの操作

NetBackup 管理コンソールと NetBackup Web UI の両方で、新しい VMware ポリシーを追加したり、既存の VMware ポリシーを管理したりできます。

両方のインターフェースで VMware ポリシーの機能は同じですが、いくつか違いがあります。

	NetBackup Web UI	NetBackup 管理コンソール
問い合わせビルダーキーワード	問い合わせビルダーで OData キーワードを使用する必要があります。	問い合わせビルダーで VIP キーワードを使用する必要があります。
VM の検出と更新	VMware サーバー資産を手動で検出または更新する方法が、Web UI では異なります。 p.29 の「VMware サーバーの資産の手動での検出」を参照してください。 また、VMware サーバーを参照する前など、VMware サーバー資産の検出を更新する場合にもこの手順を使用します。	VM を参照するときに VMware サーバー資産を手動で検出するには、[更新 (Refresh)] ボタンを使用します。

最終更新日の情報

NetBackup Web UI

VMware サーバーの検出に関する[最終更新日時 (Last update)]の情報は、[仮想マシンの参照 (Browse for virtual machines)]ダイアログボックスで VMware サーバーごとに一覧表示されます。[作業負荷 (Workloads)]、[VMware]、[VMware サーバー (VMware servers)]の順にクリックすると、各サーバーの[検出の状態 (Discovery status)]と[前回の検出の試行 (Last discovery attempt)]も一覧表示されます。

NetBackup 管理コンソール

VMware ポリシーの[クライアント (Client)]タブの[仮想マシンの参照 (Browse for virtual machines)]ダイアログで、[最終更新日時 (Last update)]を表示します。この情報は、各 VMware サーバーではなく、選択した vCenter 内の VMware サーバーの最終更新日時に関係しています。

メモ: VMware ポリシーについての詳細は、このガイドには含まれていません。VMware ポリシーの完全なマニュアルについては、『[NetBackup for VMware 管理者ガイド](#)』を参照してください。

Web UI で VMware ポリシーを追加または変更するには

- 1 左側で[保護 (Protection)]、[ポリシー (Policies)]の順にクリックします。
- 2 VMware ポリシーを変更するには、リストからそのポリシーを選択します。
ポリシーを追加するには、[追加 (Add)]をクリックして[ポリシー名 (Policy name)]を入力し、[ポリシー形式 (Policy type)]ドロップダウンリストから[VMware]を選択します。
- 3 NetBackup 管理コンソールで、すべての必須フィールドに入力します。
- 4 [作成 (Create)]をクリックして、新しいポリシーを保存します。
既存のポリシーに対する変更を保存するには、[保存 (Save)]をクリックします。

VM またはインテリジェント VM グループの保護

次の手順を使用して、資産 (VM またはインテリジェント VM 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。

VM または VM グループを保護するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 [仮想マシン (Virtual machine)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM または VM 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 必要な役割の権限を持っている場合は、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)
バックアップが行われるタイミングと、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)
バックアップ、スナップショットオプション、除外オプションで使用するサーバーまたはホストを調整します。
 - 詳細オプション (Advanced Options)
保護計画の詳細オプションを変更するか、有効にします。
- 5 [保護 (Protect)]をクリックします。
[仮想マシン (Virtual machines)]または[インテリジェント VM グループ (Intelligent VM groups)]に、選択の結果が表示されます。

VMware バックアップを使用した SQL Server データの保護

次の手順を使用して、SQL Server データを含む VM 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。

VMware バックアップを使用して SQL Server データを保護するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 [仮想マシン (Virtual machine)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM または VM 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 必要な役割の権限を持っている場合は、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)
バックアップが行われるタイミングと、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)
バックアップ、スナップショットオプション、除外オプションで使用するサーバーまたはホストを調整します。
 - 詳細オプション (Advanced Options)
保護計画の詳細オプションを変更するか、有効にします。
- 5 [保護 (Protect)]をクリックします。
- [仮想マシン (Virtual machines)]または[インテリジェント VM グループ (Intelligent VM groups)]に、選択の結果が表示されます。

VMware 資産の保護設定の編集

必要な役割の権限がある場合は、スケジュールやその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。

- p.35 の「[スケジュールと保持](#)」を参照してください。
- p.35 の「[バックアップオプション \(Backup options\)](#)と[詳細オプション \(Advanced options\)](#)」を参照してください。

VMware 資産の保護設定を編集するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 次のいずれかを実行します。

VM の設定の編集

- [仮想マシン (Virtual machines)]タブで、編集する VM をクリックします。

インテリジェントグループの設定の編集

- [インテリジェント VM グループ (Intelligent VM groups)]タブで、編集するグループをクリックします。

- 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 必要な役割の権限を持っている場合は、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。
p.35 の「[スケジュールと保持](#)」を参照してください。
 - バックアップオプション (Backup options)と[詳細オプション \(Advanced options\)](#)

p.35 の「バックアップオプション (Backup options) と詳細オプション (Advanced options)」を参照してください。

5 「保護 (Protect)」をクリックします。

スケジュールと保持

必要な RBAC 権限がある場合、資産を保護計画にサブスクライブするときに次の設定を調整できます。

表 4-1

オプション	説明
開始時間帯 (Start window)	バックアップを開始できる時間帯を設定します。

バックアップオプション (Backup options) と詳細オプション (Advanced options)

ユーザーは、保護計画にサブスクライブするときに次の設定を調整できます。

バックアップオプション

表 4-2 保護計画のバックアップオプション

オプション	説明
バックアップに使用するサーバーまたはホストを選択する	仮想マシンに代わってバックアップを実行するホスト。[Automatic (自動)]を選択すると、ストレージユニットに基づいて、NetBackup にメディアサーバーを選択させることができます。または、ユーザーがリストから別のホストを選択できます。これらのホストは、環境内のその他のメディアサーバーか、アクセスホストとして構成されているホストです。
スナップショットが存在する場合は次の処理を実行します。(If a snapshot exists, perform the following action)	NetBackup が仮想マシンバックアップの新しいスナップショットを作成する前に、スナップショットが見つかったときに NetBackup が適用する処理を指定します。たとえば、いずれかのスナップショットが存在する場合、バックアップの停止を選択できます。スナップショットが自動的に削除されなければ、最終的に仮想マシンのパフォーマンスが低下することがあります。削除されていないスナップショットが存在すると、ディスク容量不足によりリストアに失敗する場合があります。
選択した仮想ディスクをバックアップから除外 (Exclude selected virtual disks from backups)	バックアップから除外する仮想ディスクを指定します。 p.36 の「バックアップからのディスクの除外」を参照してください。

詳細オプション

表 4-3 保護計画の詳細オプション

オプション	説明
仮想マシンの静止を有効にする (Enable virtual machine quiesce)	デフォルトで、仮想マシンの I/O は NetBackup がスナップショットを作成する前に静止します。ほとんどの場合、このデフォルトを使用する必要があります。ファイルのアクティビティを静止しないと、スナップショットのデータの一貫性は保証されません。静止を無効にすると、一貫性を保つためバックアップデータを分析する必要があります。
仮想マシンバックアップからのアプリケーションデータのリストアを許可する (Allow the restore of application data from virtual machine backups)	このオプションは、仮想マシンの完全バックアップからのアプリケーションデータのリストアをユーザーに許可します。 Microsoft Exchange Server または Microsoft SharePoint Server の NetBackup 8.3 以前のアプリケーションデータは、NetBackup の[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] インターフェースでリストアする必要があります。Microsoft SQL Server のデータは、NetBackup MS SQL Client を使用してリストアする必要があります。詳しくは、NetBackup データベースエージェントのマニュアルを参照してください。
トランスポートモード (Transport mode)	バックアップに使用するトランスポートモードまたはデータストアからデータを読み取る方法を指定します。トランスポートモードについて詳しくは、仮想化環境のベンダーのマニュアルを参照してください。
スナップショットの再試行オプション (Snapshot retry options)	p.37 の「スナップショットの再試行オプション (Snapshot retry options)」を参照してください。

バックアップからのディスクの除外

仮想ディスクの除外オプションはバックアップのサイズを減らすことができますが、使用には注意が必要です。これらは複数の仮想ディスクを備えている仮想マシン専用です。

表 4-4 仮想ディスクの除外オプション

除外オプション	説明
すべてのブートディスク (All boot disks)	ブートディスクを再作成する別の手段がある場合に、このオプションを検討します。 仮想マシンのブートディスクはバックアップには含まれません。その他のディスクはバックアップされます。注: データファイルはリストアされたデータディスクで利用可能です。ただし、このバックアップからリストアされる仮想マシンは起動できません。

除外オプション	説明
すべてのデータディスク (All data disks)	データディスクをバックアップする個別の保護計画がある場合にのみ、このオプションを検討してください。 仮想マシンのデータディスクはバックアップに含まれません。ブートディスクのみバックアップされます。注: 仮想マシンがバックアップからリストアされる時、データディスクの仮想マシンデータは失われるか不完全になる可能性があります。
カスタム属性に基づいてディスクを除外する (Exclude disks based on a custom attribute)	カスタム属性を使用した、バックアップから除外するディスクの制御を VMware 管理者に許可する場合、このオプションを使用します。 属性には、除外するディスクのデバイスコントローラの値をカンマで区切って指定する必要があります。たとえば、scsi0-0, ide0-0, sata0-0, nvme0-0 などです。この属性のデフォルト値は NB_DISK_EXCLUDE_DISK です。または、独自の値を選択できます。任意の差分バックアップ間でカスタム属性値にディスクを追加すると、それらのディスクは次のバックアップから除外されます。 VMware 管理者は、VMware インターフェースを使用して、除外するディスクに属性を適用する必要があります。『NetBackup Plug-in for VMware vSphere Web Client ガイド』または『NetBackup Plug-in for VMware vSphere Client (HTML5) ガイド』を参照してください。
除外する特定のディスク (Specific disks to be excluded)	ディスクの仮想デバイスノードを表すディスク形式、コントローラ、LUN を指定して特定のディスクを除外するには、このオプションを使用します。追加のディスクを指定するには、[追加 (Add)] をクリックします。 任意の差分バックアップ間でコントローラを追加すると、それらのディスクは次のバックアップから除外されます。

スナップショットの再試行オプション (Snapshot retry options)

ほとんどの環境では、スナップショットの再試行オプションのデフォルト値は適切です。仮想マシンのサイズと VMware サーバーの処理負荷に基づいてこれらの設定を調整すると役立つ場合があります。

表 4-5 スナップショットの再試行オプション (Snapshot retry options)

オプション	説明
スナップショットの最大試行回数 (Maximum number of times to retry a snapshot)	スナップショットを再試行する回数。
スナップショットの完了までの最長時間 (Maximum length of time to complete a snapshot)	スナップショット操作が完了するまでの分単位の時間。スナップショットが完了しない場合、タイムアウトを強制するためにこのオプションで特定の期間を設定します。後でスナップショットを再試行するには、[スナップショットを再試行するまでに待機する最長時間 (Maximum length of time to wait before a snapshot is retried)] 設定を使用します。

オプション	説明
スナップショットを再試行するまでに待機する最長時間 (Maximum length of time to wait before a snapshot is retried)	スナップショットが再試行されるまでの秒単位の待機時間。

VM またはインテリジェント VM グループの保護の解除

VM またはインテリジェント VM グループのサブスクリプションを、保護計画から解除できます。資産のサブスクリプションが解除されると、バックアップは実行されなくなります。

メモ: 保護計画から資産のサブスクリプションを解除するときに、Web UI で、資産に従来のポリシーが表示される可能性があります。この状況は、保護計画に資産がサブスクリプションされており、その資産に対してバックアップが実行される場合に発生することがあります。資産は、有効なバックアップイメージを持ったまま、保護計画からサブスクリプション解除されます。Web UI には従来のポリシーが表示されますが、資産を保護する有効なポリシーがない場合もあります。

VM またはインテリジェント VM グループの保護を解除するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 [仮想マシン (Virtual machines)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM またはインテリジェント VM グループをクリックします。
- 3 [保護の削除 (Remove protection)]、[はい (Yes)]の順にクリックします。
[仮想マシン (Virtual machines)]または[インテリジェント VM グループ (Intelligent VM groups)]で、資産が[保護されていません (Not protected)]と表示されます。

VM またはインテリジェント VM グループの保護状態の表示

VM またはインテリジェント VM グループの保護に使用される保護計画を表示できます。

VM またはインテリジェント VM グループの保護状態を表示するには

- 1 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。
- 2 必要に応じて、[仮想マシン (Virtual machines)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブを選択します。

メモ: 資産タイプフィルタを使用せずに、資産タイプ全体で資産をソートすると、資産タイプ (仮想マシンとインテリジェント VM グループ) 別にグループ化された結果が返され、各資産タイプ内でソートされます。

- 3 VM またはインテリジェント VM グループをクリックします。

[保護 (Protection)]タブは、資産がサブスクライブされている計画の詳細を表示します。

メモ: 資産のバックアップが完了しているにもかかわらず状態が未完了と表示される場合は、次の情報を参照してください。

p.83 の「[新たに検出された VM の状態のエラー](#)」を参照してください。

- 4 資産が保護されていない場合、[保護の追加 (Add protection)]をクリックして保護計画を選択します。

p.32 の「[VM またはインテリジェント VM グループの保護](#)」を参照してください。

インスタントアクセス

この章では以下の項目について説明しています。

- [インスタントアクセス VM の作成](#)
- [VM バックアップイメージからのファイルとフォルダのリストア](#)
- [VM バックアップイメージからのファイルとフォルダのダウンロード](#)
- [インスタントアクセス機能を使用する前の考慮事項](#)
- [インスタントアクセス Build Your Own \(BYO\)](#)

インスタントアクセス VM の作成

NetBackup バックアップイメージから、インスタントアクセス VM を作成できます。仮想マシンは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 は仮想マシンのスナップショットをバックアップストレージデバイスに直接マウントするため、ESXi ホストまたはクラスターはスナップショットを通常の仮想マシンとして扱えます。

マウントされた VM のスナップショットは、さまざまな目的に使用できます。次に例を示します。

- VM からのファイルのリカバリ、または **vmdk** ファイルのコピー。
- パッチのテストなど、VM でのテストの実行。
- トラブルシューティングまたはディザスタリカバリ。
- アプリケーションの検証。

メモ: この機能は、NetBackup Appliance、NetBackup Virtual Appliance、Flex Appliance、BYO (Build Your Own) サーバーでサポートされています。この機能では、NetBackup バックアップイメージがメディアサーバー重複排除プール (MSDP) ストレージデバイスに格納されることが必要です。インスタントアクセス VM の使用については、次の情報を参照してください。

p.45 の「[インスタントアクセス機能を使用する前の考慮事項](#)」を参照してください。

インスタントアクセス VM を作成するには

- 1 左側の[VMware]をクリックします。
- 2 VM を特定してクリックします。
- 3 [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は、各イメージのバックアップタイムスタンプ付きで各行に表示されます。
- 4 インスタントアクセスを使用したリカバリのオプションがあるイメージまたはイメージのコピーで、[リカバリ (Recover)]、[インスタントアクセス仮想マシンの作成 (Create instant access virtual machine)]の順にクリックします。
- 5 リカバリの設定を確認し、必要に応じて変更します。

[リカバリオプション (Recovery options)]に注意してください。

既存の仮想マシンの上 同じ表示名を持つ VM が宛先にある場合、リカバリが始まる前にその書きを許可する (Allow overwrite of existing virtual machine) の VM を削除する必要があります。そうしないと、リカバリは失敗します。

プロビジョニング後に リカバリが完了すると、VM の電源が自動的にオンになります。
電源をオン (Power on after provisioning)

vMotion の有効化 (Enable vMotion) VM の作成後に VM の移行を開始し、VM の移行の進捗を表示します。

メモ: NetBackup 8.1.2 ストレージサーバーの場合、vMotion オプションは、有効になっていても使用されません。

- 6 [作成 (Create)]をクリックします。

NetBackup では、VM バックアップイメージのスナップショットを作成し、インスタントアクセスマウントポイントを作成します。イメージのスナップショットは、[インスタントアクセス仮想マシン (Instant access virtual machines)]タブに表示されます。VM を ESXi Server の他の VM と同じように使用できるようになりました。

- 7 リストアされた VM について詳しくは、[インスタントアクセス仮想マシン (Instant access virtual machines)] タブの下にある VM をクリックし、[詳細の表示 (View details)] をクリックします。
- 8 VM での作業が終了したら、マウントされている VM のスナップショットを削除するために [削除 (Delete)] をクリックできます。VM が ESXi Server から削除されます。

メモ: vMotion を有効にしている場合、その処理が正常に完了した後は、VM を削除するとマウントされた共有のみが削除されます。この VM は別のデータストアに移行されるため、ESXi Server で VM を引き続き利用できます。

VM バックアップイメージからのファイルとフォルダのリストア

VM のインスタントアクセスイメージを参照して、ファイルとフォルダをリストアできます。

メモ: インスタントアクセス VM の使用については、次の情報を参照してください。

p.45 の「[インスタントアクセス機能を使用する前の考慮事項](#)」を参照してください。

VM バックアップイメージからファイルとフォルダをリストアするには

- 1 左側の [VMware] をクリックします。
- 2 VM を特定してクリックします。
- 3 [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。
- 4 インスタントアクセスを使用したリカバリのオプションがあるイメージまたはイメージのコピーで、[リカバリ (Recover)]、[ファイルとフォルダを復元する (Restore files and folders)] の順にクリックします。

NetBackup は、バックグラウンドでインスタントアクセスマウントポイントを作成します。

- 5 ファイルを選択し、[リストへの追加 (リストアリストに追加)]をクリックします。
フォルダをクリックしてドリルダウンします。階層の上位レベルに移動して戻るには、フォルダのパスを使用します。

yygvm004-win10 / C / \$WINDOWS.~BT / Drivers

ファイルを検索するにはファイル名を入力します。

リストアリストには、選択したファイルとフォルダについて、各ファイルの場所とサイズが表示されます。

- 6 リストア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)
 - ターゲット VM (デフォルトは元の VM) の名前とそのターゲット VM のユーザー名およびパスワードを入力します。
 - すべてを異なるディレクトリにリストア (Restore everything to a different directory)
 - [リストア用ディレクトリ (Directory for restore)]に、リストア先のパスを入力します。

メモ: ストレージサーバーが NetBackup 8.1.2 の場合は、[親フォルダのパス (Parent Folder Path)]ではなく、[単一ファイルの絶対パス (Single File Full Path)]に入力します。

- [既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]
チェックボックスにチェックマークを付けると、すべてのファイルが 1 つのディレクトリにリストアされます。

メモ: ストレージサーバーが NetBackup 8.1.2 の場合、リストア時にこのオプションが自動的に使用されます。

- ターゲット VM (デフォルトは元の VM) の名前とそのターゲット VM のユーザー名およびパスワードを入力します。

- 7 既存のすべてのファイルを上書きするには、[既存のファイルの上書き (Overwrite existing files)] チェックボックスにチェックマークを付けます。

メモ: ストレージサーバーが NetBackup 8.1.2 の場合、リストア時にこのオプションが自動的に使用されます。

選択内容の概略が表示されます。

- 8 [リカバリの開始 (Start recovery)] をクリックしてファイルをリストアします。
[アクティビティ (Activity)] タブにリカバリの状態が表示されます。

VM バックアップイメージからのファイルとフォルダのダウンロード

VM のインスタントアクセスイメージを参照して、ファイルとフォルダをダウンロードできます。

メモ: インスタントアクセス VM の使用については、次の情報を参照してください。

p.45 の「[インスタントアクセス機能を使用する前の考慮事項](#)」を参照してください。

VM バックアップイメージからファイルとフォルダをダウンロードするには

- 1 左側の [VMware] をクリックします。
- 2 VM を特定してクリックします。
- 3 [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。
- 4 インスタントアクセスを使用したリカバリのオプションがあるイメージまたはイメージのコピーで、[リカバリ (Recover)]、[ファイルとフォルダのダウンロード (Download files and folders)] の順にクリックします。

- 5 ファイルを選択し、[ダウンロードリストに追加 (Add to download list)]をクリックします。

フォルダをクリックしてドリルダウンします。階層の上位レベルに移動して戻るには、フォルダのパスを使用します。

`yygvm004-win10 / C / $WINDOWS.~BT / Drivers`

ファイルを検索するにはファイル名を入力します。

ダウンロードリストには、選択したファイルとフォルダについて、各ファイルの場所とサイズが表示されます。

- 6 ダウンロードパッケージの作成が完了したら、[ダウンロード (Download)]をクリックします。

[アクティビティ (Activity)]タブにリカバリの状態が表示されます。

インスタントアクセス機能を使用する前の考慮事項

インスタントアクセス仮想マシン機能について、次の点に注意します。

- この機能は、Web UI を使用して保護計画から作成されたバックアップコピー、または NetBackup 管理コンソールで作成された従来のポリシーでサポートされます。
- この機能は、NetBackup Appliance、NetBackup Virtual Appliance、Flex Appliance、BYO (Build Your Own) サーバーでサポートされています。
- この機能では、メディアサーバー重複排除プール (MSDP) メディアサーバー上の同時マウントポイントが 50 個に制限されます。
- デフォルトでは、vSphere は、ESXi Server あたりに最大で 8 つの NFS マウントを許可します。NetBackup では、作成するインスタントアクセス VM それぞれに、NFS マウントが必要であることに注意してください。NFS マウントを解除するには、使用し終わったインスタントアクセス VM を削除します。

ESXi ホストの NFS の制限に達した場合に別のインスタントアクセス VM を作成しようとすると、その試みは失敗します。ESXi Server あたりの NFS マウントの最大数を増やすには、次の VMware の記事を参照してください。

<https://kb.vmware.com/s/article/2239>

- この機能では、独立したディスクを備えた VM のバックアップをサポートしていません。VMware では、永続的なディスクでも非永続的なディスクでも、VM 内の独立したディスクのスナップショットをサポートしていません。その結果、独立したディスクはバックアップされません。

独立したディスクと NetBackup について詳しくは、次の記事を参照してください。

<https://www.veritas.com/docs/000081966>

- この機能は、バックアップから除外されたディスクを持つ VM をサポートしていません。9.1 管理コンソールで、NetBackup ポリシーの[ディスクを除外 (Exclude Disks)]タブにある[除外したディスクはありません (No disks excluded)]を選択します。または、NetBackup Web UI の保護計画で、[選択した仮想ディスクをバックアップから除外 (Exclude selected virtual disks from backups)]チェックボックスのチェックマークをはずします。
 - raw デバイスマッピングモード (RDM) または永続モードのディスクがある VM は、この機能ではサポートされません。
 - Windows のリストアで、ReFS ファイルシステムはサポートされません。
 - インスタントアクセス仮想マシンを使用した VM 作成に使用される ESXi Server のバージョンは、VM のバックアップイメージを含む ESXi Server のバージョンと同じか、それより新しい必要があります。
 - [ダウンロード (Download)]オプションを使用したファイルまたはフォルダのダウンロードの場合、NetBackup Web UI では、プライマリサーバーがメディアサーバーへの接続に使用するのと同じ名前または IP アドレスを持つメディアサーバーにアクセスする必要があります。
- p.84 の「[インスタントアクセス VM からファイルをダウンロードするときに発生するエラー](#)」を参照してください。
- メディアサーバーのアプライアンスがサードパーティの証明書を使用する場合、この機能を使用する前に、NetBackup プライマリサーバーで特定の構成を作成する必要があります。
 詳しくは、『[NetBackup Appliance セキュリティガイド](#)』で、サードパーティの証明書に関するセクションと、サードパーティの SSL 証明書の実装に関するセクションを参照してください。
 - この機能では、異なるボリューム、パーティション、ディスクにある複数のファイルやフォルダのリストアはサポートされません。
 - 複数のファイルまたはフォルダを Windows VM にリストアする場合は、Windows 管理者アカウントのクレデンシャルを使用します。これらのアカウントのクレデンシャルを使用して、ターゲット Windows VM にログオンする必要があります。
 - 一部の ACL エントリはリストアされたファイルに含まれません。これらのユーザーまたはグループの ACL エントリはリストアできないためです。たとえば、TrustedInstallers、すべてのアプリケーションパッケージが該当します。
 - インスタントアクセス機能は、Windows 10 のコンパクトオペレーティングシステムをサポートしていません。オペレーティングシステムが圧縮されているかどうかを確認するには、VM をバックアップする前に、コマンドプロンプトで compact
 "/compactos:query" を実行します。
 圧縮を無効にするには、VM をバックアップする前に、コマンドプロンプトで "compact /compactos:never" を実行します。これによって、VM のバックアップにインスタントアクセス機能を使用できます。

- ファイルとフォルダをリストアするには、ターゲット VM がスリープまたは休止モードではなく、通常の状態である必要があります。
- **5-minutes-alive-session** のしきい値は、アプライアンスおよび BYO の Web サーバー NGINX で定義されます。ダウンロード用に選択されたファイルとフォルダは、このしきい値内で圧縮されダウンロードされる必要があります。
- インスタントアクセス仮想マシンを作成するには、仮想マシンが作成される VMware データセンターへの読み取りおよび書き込みアクセスが必要です。
- ストレージサーバーとプライマリサーバーが NetBackup の以前のバージョンからアップグレードされた後、確実にインスタントアクセスを有効化するには、次のコマンドを使用して、アップグレードされたプライマリサーバーで NetBackup Web サービスを再起動します。
 - `/usr/opensv/netbackup/bin/nbwmc stop`
 - `/usr/opensv/netbackup/bin/nbwmc start`
- Windows VM からファイルまたはフォルダをダウンロードまたはリストアする必要がある場合は、Windows レジストリハイブの数が 1 万未満であることを確認します。
[レジストリハイブ](#)に関する詳しい情報を参照できます。

インスタントアクセス Build Your Own (BYO)

独自の VM を構築し (Red Hat Enterprise オペレーティングシステムを使用)、VMware インスタントアクセスをサポートできます。次の機能を使用できます。

- インスタントアクセス VM の作成
- VMware vMotion
- ファイルとフォルダのダウンロード
- ファイルとフォルダのリストア

以前の NetBackup リリースで作成された BYO VM でインスタントアクセスを使用するには、NetBackup 8.3 にアップグレードする必要があります。

インスタントアクセス Build Your Own (BYO) の前提条件

前提条件 (新規インストールとアップグレード):

- NetBackup Appliance オペレーティングシステムと同じバージョンの Red Hat Enterprise Linux 7.6 以降を搭載した BYO ストレージサーバー。
- Docker がインストールされている BYO ストレージサーバー。

- **Docker** バージョンは、対応する正式な RHEL バージョンのリリースに存在するものと同じである必要があります。これは、対応する RHEL yum ソース (RHEL extra) からインストールする必要があります。
- **Docker** アプリケーションが環境パスに含まれている。
- **NFS** サービスがインストールされている **BYO** ストレージサーバー。
- **NGINX** バージョンがインストールされている **BYO** ストレージサーバー。
 - **NGINX** バージョンは、対応する正式な RHEL バージョンのリリースに存在するものと同じである必要があります。これは、対応する RHEL yum ソース (epel) からインストールする必要があります。
 - `polycycoreutils` と `polycycoreutils-python` パッケージが同じ RHEL yum ソース (RHEL サーバー) からインストールされていることを確認し、次のコマンドを実行します。
 - `semanage port -a -t http_port_t -p tcp 10087`
 - `setsebool -P httpd_can_network_connect 1`
 - ストレージサーバーの `/mnt` フォルダが、どのマウントポイントによっても直接マウントされていないことを確認します。マウントポイントはそのサブフォルダに対してマウントされる必要があります。
 - 次のコマンドを使用して、**selinux** の `logrotate` 権限を有効にします。

```
semanage permissive -a logrotate_t
```
- **BYO** の場合、**Docker** コンテナは **VMDK** ファイルの参照に使用されます。コンテナに関連するデータは `/var/lib/` に格納され、20 GB 以上の空き容量が必要です。

インスタントアクセス Build Your Own (BYO) のハードウェア構成の必要条件

表 5-1 ハードウェア構成の必要条件

CPU	メモリ	ディスク
■ 2.2 GHz 以上のクロックレート。 ■ 64 ビットのプロセッサ。 ■ 最小 4 コア。8 コアを推奨。64 TB のストレージの場合、Intel x86-64 アーキテクチャでは 8 つのコアを必要とします。 ■ CPU 構成で VT-X オプションを有効にします。	■ 16 GB (8 TB から 32 TB のストレージの場合は、1 TB のストレージ用に 1 GB の RAM)。 ■ 32 TB 以上のストレージの場合は 32 GB の RAM。 ■ ライブマウントごとに追加の 500 MB の RAM。	ディスクのサイズは、バックアップのサイズによって異なります。NetBackup とメディアサーバー重複排除プール (MSDP) のハードウェアの必要条件を参照してください。

よく寄せられる質問

ここでは、Build Your Own (BYO) のインスタントアクセスについてよく寄せられる質問をいくつかご紹介します。

表 5-2 よく寄せられる質問

よく寄せられる質問	回答
Docker をインストールせずにストレージを構成またはアップグレードした後、BYO で (ファイルのダウンロードおよびリストアのため) インスタントアクセスによるファイルの参照を有効にする方法を教えてください。	次に示す順序で操作を実行します。 1 必要な Docker のバージョンをインストールします。 2 インスタントアクセス機能の使用を開始します。 たとえば、ファイルのダウンロード、ファイルのリストアなどを行うことができます。

よく寄せられる質問	回答
Nginx サービスをインストールせずにストレージを構成またはアップグレードした後に、BYO で VMware インスタントアクセス機能を有効にする方法を教えてください。	次に示す順序で操作を実行します。 1 必要な nginx サービスのバージョンをインストールします。 2 新しい BYO nginx 構成エントリ <code>/etc/nginx/conf.d/byo.conf</code> が、元の <code>/etc/nginx/nginx.conf</code> ファイルの HTTP セクションに含まれていることを確認します。 3 コマンド <code>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</code> を実行します。
「MSDP REST API がポート 10087 の HTTPS を介して利用可能であることの確認」で触れている <code>vpfs-config.log</code> ファイルで発生した問題を解決するには、どのようにしたら良いですか。	次に示す順序で操作を実行します。 1 Yum ツールを使用して、<code>polycycoreutils</code> と <code>polycycoreutils-python</code> パッケージをインストールします。 2 Nginx に SELinux が必要な次のルールを追加し、10087 ポートにバインドします。 ■ <code>semanage port -a -t http_port_t -p tcp 10087</code> ■ <code>setsebool -P httpd_can_network_connect 1</code> 3 コマンド <code>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</code> を実行します。

よく寄せられる質問	回答
BYO のインスタントアクセスでは、デフォルトで自己署名証明書が使用され、*.pem 外部証明書のみがサポートされます。 外部 CA (*.pem 証明書) で署名された証明書で置き換えることが必要な場合は、どのようにしたら良いですか。	外部証明書を構成するには、次の手順を実行します。新しい証明書がすでに生成されている場合 (証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります) は、手順 4 に進みます。 1 RSA の公開鍵と秘密鍵のペアを作成します。 2 証明書の署名要求 (CSR) を作成します。 証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります。 3 外部認証局が証明書を作成します。 4 <PDDE ストレージのパス >/spws/var/keys/spws.cert を証明書に置き換え、<PDDE ストレージのパス >/spws/var/keys/spws.key を秘密鍵に置き換えます。 5 次のコマンドを実行して、証明書を再ロードします。 /usr/opensw/pdde/vpfs/bin/vpfs_config.sh --configure_byo
GNOME のインスタントアクセスライブマウント共有で、メディアの自動マウントを無効にする方法を教えてください。 自動マウントが有効になっている場合、ソースフォルダは GNOME のライブマウント共有からマウントされ、小さなディスクが表示されます。このシナリオでは、インスタントアクセス機能が正しく動作しません。 マウントされたディスクコンテンツソースは、ライブマウント共有配下の .../meta_bdev_dir/... フォルダにあり、マウントターゲットは /run/media/... フォルダにあります。	次のガイドラインに従って、GNOME 自動マウントを無効にします。 https://access.redhat.com/solutions/20107

よく寄せられる質問	回答
<pre>/var/log/vpfs/vpfs-config.log</pre> ファイルの次の問題は、どうすれば解決できますか。 <pre>**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/openv/netbackup/bin/rbllibcmd failed (1):</pre>	次に示す順序で操作を実行します。 1 NetBackup プライマリサーバーが起動しており、ファイアウォールが NetBackup プライマリサーバーとストレージサーバー間の接続をブロックしていないことを確認します。 2 ストレージサーバーで次のコマンドを実行して、接続状態を確認します。 <pre>/usr/openv/netbackup/bin/bpclntcmd -pn</pre> 3 NetBackup プライマリサーバーを起動し、NetBackup プライマリサーバーとストレージサーバー間の接続を許可してから、次のコマンドを実行します。 <pre>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</pre>

インスタントロールバック

この章では以下の項目について説明しています。

- [インスタントロールバックの前提条件](#)
- [インスタントロールバック機能を使用する前の考慮事項](#)
- [VM バックアップイメージからのインスタントロールバック](#)

インスタントロールバックの前提条件

インスタントアクセス Build Your Own (BYO) の前提条件は、インスタントロールバック機能にも適用されます。

p.47 の「[インスタントアクセス Build Your Own \(BYO\) の前提条件](#)」を参照してください。

インスタントロールバック機能を使用する前の考慮事項

インスタントロールバック仮想マシン機能について、次の点に注意してください。

- この機能はバックアップコピーでサポートされます。これらのコピーは、保護計画 (Web UI) または従来のポリシー (NetBackup 管理コンソール) で作成されます。
- この機能は、NetBackup Appliance、NetBackup Virtual Appliance および Build Your Own (BYO) サーバーでサポートされています。
- この機能では、独立したディスクを備えた VM のバックアップをサポートしていません。VMware では、永続的なディスクでも非永続的なディスクでも、VM 内の独立したディスクのスナップショットをサポートしていません。その結果、独立したディスクはバックアップされません。

詳しくは、次を参照してください。

<https://www.veritas.com/docs/000081966>

- この機能は、バックアップから除外されたディスクを持つ VM をサポートしていません。
NetBackup 管理コンソールで、ポリシーの[ディスクを除外 (Exclude Disks)]タブにある[除外したディスクはありません (No disks excluded)]を選択します。または、NetBackup Web UI の保護計画で、[選択した仮想ディスクをバックアップから除外 (Exclude selected virtual disks from backups)]チェックボックスのチェックマークをはずします。
- raw デバイスマッピングモード (RDM) のディスクがある VM は、この機能ではサポートされません。
- この機能を使用すると、一度に最大 100 台の VM をロールバック対象として選択できます。100 台を超える VM を選択した場合、[すぐにロールバック (Roll back instantly)]オプションは表示されません。
たとえば、180 台の VM をロールバックする場合は、同じジョブに対して 2 つのロールバック要求を作成する必要があります。1 つは 100 台の VM 用、もう 1 つは 80 台の VM 用です。
- この機能では、1 つのインスタントロールバック VM には 1 つのライブマウントが必要です。各ライブマウントは 1 日間保持できます。したがって、ロールバックをサポートできる VM の数は、利用可能なライブマウントの合計数に依存します。デフォルトでは、ライブマウントの値は 200 に設定されています。
このデフォルト値は、<ストレージパス>/spws/etc/spws.cfg から変更できます。
MaxAllowedLivemounts=200

VM バックアップイメージからのインスタントロールバック

NetBackup 9.1 以降では、バックアップイメージから即座に VM をロールバックできます。インスタントアクセスをサポートするバックアップイメージのみがインスタントロールバックをサポートできます。

複数の VM に対してインスタントロールバックを実行できます。1 つの VM を任意のリカバリポイントに複数回ロールバックすることもできます。

たとえば、3 つのバックアップイメージ B1、B2、B3 がある場合、最初に VM を B1 にロールバックし、次に B3、その次に B2、のようにロールバックできます。

ロールバックが完了すると、選択したリカバリポイント以降のすべてのデータが利用できなくなります。

VM バックアップイメージから即座にロールバックするには

- 1 左側の[VMware]をクリックします。
- 2 バックアップイメージを選択するには、次のいずれかの操作を行います。

- VM をクリックする
- 1 VM を特定してクリックします。
 - 2 [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は、各イメージのバックアップタイムスタンプ付きで各行に表示されます。
 - 3 イメージまたはイメージのコピーで、[リカバリ (Recover)]、[すぐにロールバック (Roll back instantly)] の順にクリックします。

- チェックボックスに
チェックマークを付ける
- 1 ロールバックする VM に対応するチェックボックスにチェックマークを付けて、[すぐにロールバック (Roll back instantly)] をクリックします。

複数の VM を選択してインスタントロールバックを実行できます。
 - 2 次のいずれかのロールバックオプションを選択します。
 - ロールバックするポイント: 最新 (Roll back to: Most recent)
NetBackup は、過去 1 カ月間の最新のインスタントアクセスリカバリポイントを表示します。
 - ロールバックするポイント: 特定の日時前 (Roll back to: Before specific date and time)
日時を選択します。
NetBackup は、選択した日時より前の 1 カ月間で最新のインスタントアクセスリカバリポイントを表示します。
 - 3 [ロールバック (Roll back)] をクリックします。

- [処理 (Actions)] メニューを使用する
- 1 ロールバックする VM に対して [処理 (Actions)]、[すぐにロールバック (Roll back instantly)] の順にクリックします。
 - 2 次のいずれかのロールバックオプションを選択します。
 - ロールバックするポイント: 最新 (Roll back to: Most recent)
NetBackup は、過去 1 カ月間の最新のインスタントアクセスリカバリポイントを表示します。
 - ロールバックするポイント: 特定の日時前 (Roll back to: Before specific date and time)
日時を選択します。
NetBackup は、選択した日時より前の 1 カ月間で最新のインスタントアクセスリカバリポイントを表示します。
 - 3 [ロールバック (Roll back)] をクリックします。

- 3 必要なオプションを選択し、[ロールバック (Roll back)] をクリックします。

[アクティビティモニター (Activity monitor)] タブにロールバックの状態が表示されます。

継続的なデータ保護

この章では以下の項目について説明しています。

- [継続的なデータ保護について](#)
- [前提条件](#)
- [CDP 用の容量ベースのライセンス](#)
- [CDP の構成](#)
- [CDP ゲートウェイの定義](#)
- [サイズ変更の注意事項](#)
- [CDP の並列実行バックアップジョブの制限](#)
- [完全同期の制御](#)
- [CDP ジョブの監視](#)
- [CDP でのアクセラレータの使用](#)
- [CDP で保護されている VM のリカバリ](#)
- [CDP のトラブルシューティング](#)

継続的なデータ保護について

CDP (継続的なデータ保護) は、VMware VM に影響を与えることなく、VM のバックアップの高速コピーをキャプチャするための優れた方法です。CDP を使用すると、バックアップの最新のコピーを迅速に作成し、必要に応じて NetBackup を使用してバックアップを保持およびリストアできます。

CDP の主な機能を次に示します。

- VMware VM の完全な Web UI ベースの保護とリカバリ。

- さまざまな API ベースの保護。
- BYOD (Bring Your Own Device、個人所有デバイスの持ち込み): CDP ゲートウェイとして RedHat Linux ベースの NetBackup メディアサーバーを使用できます。
- ESXi とさまざまなデータストア形式のサポート。最新情報については、ソフトウェア互換性リストを参照してください。
- アクセラレータベースのバックアップ。MSDP や OST のようなアクセラレータが有効なストレージのサポート。
- インスタントアクセスのサポート。MSDP ストレージから VM をブートできます。
- MSDP からのエージェントレスシングルファイルリストア。
- 保護とリストアのワークフロー全体に対する RBAC のサポート。
- 従来ライセンスと容量ベースのライセンス。
- CDP では、Veritas Resiliency Platform と完全に互換性がある Veritas IO フィルタを使用します。

前提条件

CDP を使用するための前提条件

- VMware 用の CDP は、アクセラレータベースのバックアップのみをサポートします。そのため、CDP には MSDP または OST ベースのストレージに基づくアクセラレータ対応のストレージユニットが必要です。
- CDP は、CDP ゲートウェイのステージング領域としてファイルシステムを使用します。サポート対象のファイルシステムについては、ソフトウェア互換性リストを参照してください。
- MSDP に関連付けるメディアサーバーは、NetBackup バージョン 9.1 以上である必要があります。
- 機能を有効にするための容量ベースおよび従来 of ライセンス。
- ESXi Server が CDP ゲートウェイと通信するには、CDP ゲートウェイのポート 33056 が開いている必要があります。
- NetBackup が ESXi ホストで CIM (Common Information Model) サービスを開始、停止、再起動、更新するための権限が、VMware サーバークレデンシャルに必要です。
- RHEL ベースの NetBackup メディアサーバープラットフォームで CDP ゲートウェイを構成できます。
- VAIO コンポーネントを使用し、レプリケーション用の VMware ストレージポリシーを作成します。CDP を使用して保護する VM の各ディスクにストレージポリシーを接続

します。詳しくは、VMware vCenter で vtstap ストレージポリシーを作成する方法に関するベリタスのサポートナレッジベースの記事を参照してください。

VAIO 用の Veritas IO フィルタの要件

CDP の配備で使用するために、VAIO ドライバパッケージのバージョン 4.0.0 をダウンロードして配備できます。最新バージョンとそのダウンロード方法については、ソフトウェア互換性リストを参照してください。

NetBackup で保護を構成する前に、vCenter クラスタに VIB (vSphere Installation Bundle) をインストールする必要があります。ただし、リストア目的で vCenter に VIB を配備する必要はありません。VMware MOB を使用したクラスタへの IO フィルタソリューションの配備に関するベリタスのサポートナレッジベースの記事を参照してください。

ストレージポリシーの要件

CDP を配備する前に、VM ストレージポリシーを作成する必要があります。ストレージポリシーで、コンポーネントに [レプリケーション (Replication)]、プロバイダに「vtstap」を選択する必要があります。このポリシーは、保護する VM の各ディスクに接続する必要があります。そうしないと、バックアップジョブは失敗します。詳しくは、VMware vCenter で vtstap ストレージポリシーを作成する方法に関するベリタスのサポートナレッジベースの記事を参照してください。

メモ: ストレージポリシーを設定解除すると、VM の保護が失われます。

CDP 用の容量ベースのライセンス

ライセンスでは、NetBackup によって保護されているフロントエンドテラバイトの合計数を収集します。CDP バックアップのフロントエンドデータサイズは、VM によって ESX データストアで消費されるストレージサイズとほぼ同じです。

nbdeployutil ユーティリティは、VM のデータ使用状況を報告します。データサイズの報告には、次のルールが適用されます。

- バックアップ時に書き込まれた合計バイト数 (X) と ESX データストアからの VM サイズ (Y) を計算します。報告されるサイズは X と Y のうち小さい方の値です。
- 異なるポリシーで同じ仮想マシンを使用する場合、データサイズが大きい方のポリシーが考慮されます。
- VADP と CDP ポリシーによって同じ VM が保護されている場合、サイズが大きい方のポリシーに 1 回のみ課金されます。

管理者は次の手順を使用して、ライセンスによって報告されるデータサイズを確認できます。

- vCenter の ESX データストアにある VM が占めるサイズを確認します。[データストア (Datastore)]、[ファイル (Files)]、[VM]、[サイズ (size)]列の順に移動すると、データストアで占有されているサイズが表示されます。
- 同じ VM のバックアップ中に書き込まれたバイト数を確認します。
- 上記の 2 つの値の最小値を計算します。

CDP の構成

作業負荷の CDP を構成するには、次のタスクを実行する必要があります。

VMware vCenter での操作

1. Veritas IO フィルタをインストールします。VMware MOB を使用したクラスタへの IO フィルタソリューションの配備に関するベリタスのサポートナレッジベースの記事を参照してください。
2. ESXi にストレージポリシーを接続します。詳しくは、VMware vCenter で vtstap ストレージポリシーを作成する方法に関するベリタスのサポートナレッジベースの記事を参照してください。

NetBackup コンソールでの操作

1. バックアップ先の MSDP または OST ベースのストレージを作成します。『NetBackup Web UI 管理者ガイド』の「ストレージの構成」の章を参照してください。
2. CDP ゲートウェイを作成します。
3. VMware 作業負荷の CDP ベースの保護計画を作成します。『NetBackup Web UI 管理者ガイド』の「保護計画の管理」の章を参照してください。
4. 必要な VM を保護計画で保護します。
5. ジョブを監視します。

CDP ゲートウェイの定義

VM を保護する前に、CDP 配備のゲートウェイを定義する必要があります。NetBackup メディアサーバーまたはプライマリサーバーである VM で、CDP ゲートウェイを定義できます。

CDP ゲートウェイを定義するには

- 1 左側の[作業負荷 (Workloads)]で、[VMware]をクリックします。
- 2 右上の[VMware 設定 (VMware settings)]をクリックし、[継続的なデータ保護ゲートウェイ (Continuous Data Protection Gateway)]をクリックします。

- 3 [追加 (Add)]をクリックします。[ホスト名 (Host name)]と[ストレージパス (Storage path)]を入力します。ストレージパスには、ルート以外の独立したファイルシステムが必要です。MSDP などの他のアプリケーションと、この同じ場所を共有しないでください。
- 4 [追加 (Add)]をクリックして、ゲートウェイを追加します。

サイズ変更の注意事項

このセクションでは、環境内の作業負荷に基づく、CDP ゲートウェイのサイズ変更の要件について説明します。

メモ: CDP ゲートウェイで多数の VM をサポートする予定がある場合、CDP ゲートウェイと、ストレージユニットをホストする MSDP またはメディアサーバーを異なるホストに配備することをお勧めします。

メモ: CDP ゲートウェイと MSDP を同じメディアサーバー上に共存させる場合、CDP サービスは内部で使用するために利用可能なメモリ (RAM) の 20% を消費します。メディアサーバー上で CDP ゲートウェイがスタンドアロンの場合、同じく利用可能なメモリの 50% を消費します。

ゲートウェイのサイズ変更

保護する VM の数に基づいて CDP のサイズを調整する必要があります。ゲートウェイの要件を計算する際に、このセクションで説明する要件を考慮してください。

CDP を使用すると、VM によって実行された IO を継続的にタップできます。NetBackup はデフォルトでは、VM ごとのステージング領域に 10 GB のストレージ領域を使用します。IO タップが開始されると、CDP サービスはこの 10 GB ストレージへのデータの書き込みを開始します。このストレージが制限に達すると、CDP サービス (nbcctd) はバックアップジョブをトリガして、ゲートウェイからバックアップストレージにこのデータを移動します。

VM あたりの割り当て済みストレージを上回る使用に対応するため、NetBackup はデフォルトで、CDP ステージングパスの利用可能な合計領域のうち 25% を予約します。このストレージは、ゲートウェイにサブスクライブされた VM で共有します。nbcct.conf ファイルでこの値を再構成できます。

予約済みストレージを構成するには

- 1 CDP ゲートウェイにログオンします。
- 2 <NBU のインストール場所 >/netbackup/nbcct/ ディレクトリに移動し、テキストエディタで nbcct.conf ファイルを開きます。

3 パラメータ `CCT_VM_QUOTA_RESERVE_PERCENT` の値を入力します。

4 `nbcctd` サービスを再起動します。

ゲートウェイのストレージ要件

NetBackup が **ESXi IO** デーモンからデータを受信すると、そのデータはメモリ内キャッシュに格納されます。推奨される **VM** ごとのデータ量は **160 MB** 以上です。

たとえば、ゲートウェイで **40** 台の **VM** を保護するとします。その場合、 $40 * 160 \text{ MB} = 6400 \text{ MB}$ の **RAM** が必要です。割り当てる **RAM** の量が増えるほど、**CDP** サービスの開始時にメモリ内キャッシュサイズが増加し、最終的にサービスの **IO** パフォーマンスが向上します。

同様に、ステージング用の $40 * 10 \text{ GB} = 400 \text{ GB (75\%)} +$ 予約済み $134 \text{ GB (25\%)}$ として、ステージング領域には約 **540 GB** の領域が必要です。

VM ごとのストレージを増やすと、**NetBackup** がバックアップジョブごとにバックアップできるデータ量がさらに多くなります。**CDP** ゲートウェイの予約済みストレージを増やすと、保護を中断することなく、より多くのデータを受信できます。ステージングパスが完全に占有されている場合でも、**VM** 内のアプリケーションには影響しない点に注意してください。**NetBackup** は、その間にアプリケーションによって生成されたデータを取得し、そのデータを後続のバックアップジョブでバックアップストレージに移動します。

メモ: ステージング領域に **NFS** を使用する場合、必要な最小スループットは **100 MB/秒** です。

最初の 24 時間のエクスペリエンス

CDP 機能を使い始めるときは、システムを監視し、ビジネスのニーズに応じて調整し、保護とパフォーマンスを最大化するためのハードウェア構成を追加することが重要です。最初はデフォルト値を使用して、このセクションで説明されている要件に従って **VM** のサブスクライブを開始できます。次のことを確認する必要があります。

- ステージングストレージの空きのない状態のために **CDP** サービスがトリガした即時バックアップジョブの数。
- **CDP** バックアップエンジンの通知は、**NetBackup Web UI** で確認できます。
- プロビジョニングされた下位ストレージのパフォーマンス。**NetBackup** インストールディスク、**CDP** ステージング領域、**MSDP** ストレージディスクなど。
- ネットワークの使用率と利用可能な帯域幅。
- **ESXi** からのデータの受信時と、バックアップジョブの実行時の **CPU** およびメモリの消費量。

メモ: IO デーモンからの IO の速度が低下する場合は、ネットワーク帯域幅とシステム RAM を確認します。nbcct.conf ファイルの `CCT_POOL_SIZE_QUOTA_PERCENTAGE` パラメータを使用して、メモリ内キャッシュのサイズを増加できます。

CDP の並列実行バックアップジョブの制限

一度に CDP ゲートウェイで実行できる同時 CDP スナップショットジョブの制限を設定できます。たとえば、20 台の VM を保護する場合に制限を 5 に設定すると、5 台の VM のみが同時バックアップを実行でき、15 台の VM がキューに投入されます。この設定は、システムとネットワークリソースの使用を最適化するために必要です。デフォルトでは、リソースの制限値は 0 (制限なし) です。

リソース制限に値を設定するには、次の API を使用します。

POST /config/resource-limits

```
{
  "data": [
    {
      "type": "resource-limits",
      "id": "string",
      "attributes": {
        "resources": [
          {
            "resourceType": "string",
            "resourceName": "string",
            "resourceLimit": 0,
            "additionalData": "string"
          }
        ]
      }
    }
  ]
}
```

ここで、

- `id` は作業負荷を表し、これは `Cdp` です。
- `resourceType` には `Cdp-Backup` を指定する必要があります。
- `resourceName` は、CDP ゲートウェイのホスト名を表します。これは、保護計画で指定されているものと同じにする必要があります。`resourceName` を空の文字列にする

と、resourceLimit 値がグローバル制限として設定され、すべての構成済みの CDP ゲートウェイに適用されます。

- resourceLimit 値には、そのゲートウェイのバックアップジョブの値を設定します。作業負荷の種類 CDP に対するリソース制限のリストを取得するには、次を使用します。

```
GET - /config/resource-limits/cdp
```

特定のゲートウェイの resourceLimit の値を更新するには、同じレコードに対して resourceLimit の変更を指定して POST API を使用します。

指定した詳細なリソース制限を削除するには、次を使用します。

```
DELETE - /config/resource-limits
```

特定のリソースに設定されているリソース制限のみを削除できます。リソース形式と、その形式の特定のリソースの両方を指定します。

完全同期の制御

CDP が有効な保護計画に VM をサブスクライブすると、NetBackup は完全同期を開始して、新しく保護された VM のデータ全体を取得します。新しくサブスクライブした VM に対して増分バックアップ機能を適用するデータが NetBackup に存在しない場合、完全同期が開始されます。完全同期中に、NetBackup は基盤となる VMDK から CDP ステージング場所、さらには NetBackup STU まで、VM のデータ全体をキャプチャします。

通常、CDP が有効な保護計画に新しい VM をサブスクライブすると完全同期がトリガされますが、特定のシナリオでは、完全同期を手動でトリガできます。

- 誤った破損または削除: CDP は、ステージング場所にある VM のバックアップデータを独自の形式のファイルで保持します。VM のこれらのファイルが誤って削除または破損された場合、VM の後続のバックアップジョブはデータ整合性の不一致を原因として失敗します。この場合、強制再スキャンのスケジュールバックアップを開始でき、その後に VM の完全同期が実行されます。
- 手動でトリガされた強制再スキャンのスケジュールに従います。
- CDP サービスは、必要に応じて VM データを受信する完全同期をトリガできます。

完全同期中、データは ESXi から CDP ゲートウェイに転送されます。VM のデータサイズによっては、このデータのボリュームが大幅に大きくなり、ネットワーク、メモリ、処理電力、ストレージなどの多くのリソースを消費する可能性があります。これは、以前にサブスクライブした VM のバックアップ操作にも影響します。

一度に 5 台を超える VM、たとえば 7 台をサブスクライブすると、5 台の VM に対して完全同期が開始され、2 台が待機状態になります。

このため、同時完全同期操作の数を制限して、システムリソースを最適化することをお勧めします。同時に実行できる完全同期のデフォルトの数は 5 です。この場合、5 台の VM

が同時に完全同期を実行できます。完全同期を必要とするその他の VM はキューで待機する必要があります。これにより、システムリソースが最適に管理されます。

完全同期を制御するための推奨事項:

- 5 台以下のバッチで VM をサブスクライブします。
- サブスクライブした VM の完全同期が完了すると、UI にメッセージが表示されます。その後、次のバッチのサブスクライブに進むことができます。

nbcct.conf ファイルでの完全同期の構成

nbcct.conf ファイルで `CCT_MAX_FULL_SYNC_REQS` パラメータの値を指定することで、同時完全同期操作の数を構成できます。例: `CCT_MAX_FULL_SYNC_REQS=7`

CDP ジョブの監視

Web UI でのジョブの監視について詳しくは、p.13 の「[NetBackup ダッシュボード](#)」を参照してください。

CDP は、従来の VMware 用 NetBackup エージェントと同じジョブ階層に従います。保護は、VM とその属性を検出するジョブから開始します。バックアップの準備中という子ジョブがその後に続きます。この子ジョブは、ゲートウェイで利用可能な以前のイメージと現在のデータに基づいて、変更されたブロックを判断します。子ジョブの後に、バックアップジョブが CDP ゲートウェイから宛先ストレージユニットにデータを移動します。

ゲートウェイの各 VM に十分な領域がないと、バックアップイメージが完全にリカバリ可能ではなくなる場合があります。そのようなイメージは部分的にリカバリ不可能なイメージと呼ばれ、Web UI からリストアできません。ただし、後続のバックアップジョブによって、リカバリ可能なバックアップイメージが作成されます。イメージがリカバリ不可能である場合、ESXi から一貫性のあるデータを受信すると、バックアップジョブが自動的にトリガされず。

通知の表示

ほとんどの CDP アクティビティについて、Web UI で通知を参照できます。これらの通知は、ゲートウェイプラットフォームでの IO タッピングの動作状況を確認するために役立ちます。動作が停止した、またはユーザー側からの操作が必要な場合に、通知を参照できます。通知を参照できる重要なシナリオを次に示します。

- データのバックアップ中。バックアップジョブがステージング領域からバックアップストレージにデータを移動しているとき。
- VM の完全同期が開始、一時停止、再開、完了した。
- 部分イメージが生成された。
- ステージング領域のストレージに空き領域が残っていない。
- ステージング領域の場所にメモリ内データを書き込み中にエラーが発生したとき。

次に、通知の一部を示します。

表 7-1 通知の表示

メッセージ	シナリオ	重大度	優先度
ゲートウェイで、IO フィルタから継続的なデータ保護サービスへの VM の接続を一時的に切断しています。割り当てられたステー징領域にほとんど空きがないか、メモリ使用率が最大に達しています。	CDP に割り当てられたステー징領域にほとんど空きがないため、VM が一時的に IO フィルタから切断されます。(Temporarily disconnecting VMs from the IO filter to the Continuous data protection service on the gateway. Either the allocated staging area is almost full, or the memory usage is at maximum. The staging space allocated to CDP is almost full, and the VMs temporarily disconnect from the IO filter.)	重要	高
VM <uuid> で入力/出力エラーが発生しました。 (Input/Output error occurred for the VM: <uuid>)	ストレージから基盤となるディスクが離脱したり、ファイルシステムが読み取り専用モードになったりなどの様々な理由により、CDP サービスはステー징場所で IO を実行できません。	エラー	高
ステー징領域のメモリに空きがなくなったため、継続的なデータ保護サービスを終了します。(Terminating the Continuous data protection service, as the staging area memory is full.)	ステー징領域が 1 GB 未満の場合、CDP がこのエラーを発生させてサービスを終了します。	重要	高
VM <uuid> のデータストレージクォータに空きがありません (ジョブ ID: \${jobid})。データをバックアップストレージに移動しています。(Data storage quota full for the VM: <uuid>, bearing jobid: \${jobid}. Moving data to backup storage.)	VM のデータ転送中に、データの合計が構成済みの VM クォータを超えた場合、バックアップジョブがトリガされ、ステーjingデータがバックアップ先に移動されます。	情報	低

メッセージ	シナリオ	重大度	優先度
VM <uuid> のデータをバックアップストレージに移動できません。VM のストレージオータに空きがありません。 (Cannot move data to backup storage, for the VM: <uuid>. Storage quota for the VM is full.)	ゲートウェイからバックアップ場所へのデータの移動に失敗しました。	エラー	高
VM <uuid> の完全同期を開始しました。(Full sync started for the VM: <uuid>.)	この VM の完全同期プロセスが開始されました。	情報	低
VM <uuid> の完全同期を再開しました。(Full sync resumed for the VM: <uuid>.)	VM の完全同期が、予期しない中断の後で再開されました。	情報	低
VM <uuid> の完全同期が完了しました。(Full sync completed for the VM: <uuid>.)	VM の初回の完全同期が完了しました。	情報	低
VM <uuid> の完全同期を一時的に停止しました。(Full sync suspended for the VM: <uuid>.)	ネットワーク障害など、なんらかの理由で完全同期操作が失敗しました。	情報	低
VM <uuid> に対して生成されたバックアップイメージをリカバリできません。(Backup image generated for the VM: <uuid> is not recoverable.)	VM の同期の進行中に VM のクォータに到達すると、バックアップジョブがトリガされます。バックアップジョブが完了すると、ゲスト VM で生成された中間データを NetBackup が移動中で、イメージをリカバリできない場合があります。	情報	低

ジョブの表示

CDP は、アクティビティモニターを使用して次のジョブ情報を表示します。

- 親バックアップジョブ - VM の情報を検出する検出ジョブ。
- バックアップの準備中 - VM の特定の時点のデータを識別します。
- バックアップ - ステージングパスからバックアップストレージにデータを移動します。

CDP でのアクセラレータの使用

VMware 用の CDP は、アクセラレータベースのバックアップのみをサポートします。そのため、CDP には MSDP または OST ベースのストレージに基づくアクセラレータ対応のストレージユニットが必要です。

強制再スキャン

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。

アクセラレータベースの強制再スキャンを使用すると、CDP ゲートウェイのステージング領域のデータが消去されます。そのため、破損したデータは ESXi Server から同期した新しいデータに置き換えられます。強制再スキャンによってトリガされる最初のバックアップジョブでは、リカバリ可能なイメージに必要なすべてのデータが含まれていない場合があります。データが利用可能になると、後続のバックアップが自動的にトリガされ、イメージのリカバリが可能になります。

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。
- ステージング場所のメモリが一杯になると、UI に通知が表示されます。ステージング場所で十分なメモリを利用できる場合にのみ、強制再スキャンを開始します。

手動で強制再スキャンを実行してバックアップをトリガするには、コマンドプロンプトまたは Linux 端末で次のコマンドを実行します。

```
bpbackup -i -p policyname -s <schedulename>
```

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。

CDP で保護されている VM のリカバリ

NetBackup の VMware 用 CDP で保護される VM のバックアップイメージ形式は、VMware 用 NetBackup エージェントのバックアップイメージ形式と同じです。したがって、すべてのリカバリ操作は VMware 用の NetBackup エージェントと同じです。

以下に、わずかな相違点を示します。

- エージェントレスの単一ファイルリカバリは、MSDP がインスタントアクセス用に構成されている場合にのみサポートされます。
- vCenter プラグインからのリカバリはサポートされません。
- Java UI を介して CDP ベースのバックアップイメージから VM をリストアすることはできません。

Web UI では、部分的で回復不能と表示されるイメージはリカバリできません。このようなファイルは、NetBackup API を使用してリストアできます。ただし、リカバリ後に VM がブートしない場合があります。

CDP のトラブルシューティング

VAIO が CDP ゲートウェイへのデータの送信を停止する

IO フィルタで問題が発生し、NOOP (非動作) モードになる場合に発生します。

考えられる理由:

- IO フィルタでデータストアに問題が発生した。
- IO フィルタで ESXi Server の vmdk からの読み取り中に問題が発生した。

回避方法:

保護対象の VM のすべてのディスクから VTSTAP ポリシーを削除して、再接続します。

エラー: 仮想マシンの 1 つ以上の仮想ディスクからストレージポリシーが設定解除されていません (Error: Storage policy is not detached from one or more virtual disks of virtual machine)

ストレージポリシーが VM のすべての仮想ディスクから接続解除されていない場合に発生します。次のバックアップはエラーコード 156 で失敗します。

回避方法:

CDP が以前に保護した VM のすべてのディスクから、新しい Veritas IO フィルタベースのストレージ (vtstap) ポリシーを削除します。vCenter でこの操作を実行できます。

エラー: Veritas IO フィルタのバージョンの取得または解析に失敗しました (Error: Failed to retrieve or parse the version of Veritas IO filter)

CDP 保護計画に 1 つ以上の VM をサブスクライブしようとする、このエラーが表示される場合があります。ESXi Server の CIM サーバーサービスが応答しない場合に発生します。

回避方法:

ESXi Server で CIM サーバーサービスを再起動し、CDP 保護計画への VM のサブスクリプションを再試行します。ESXi Server の CIM サーバーサービスは、ESXi の [構成 (Configuration)]、[サービス (Services)] セクションにあります。

nbcctd サービスが一貫性のない状態になる。CDP ゲートウェイを構成できない。

考えられる理由:

- 読み取り専用のファイルシステムをマウントし、CDP ゲートウェイ構成でそのパスを指定すると、サービスは構成されますが、ゲートウェイは起動に失敗します。
- 読み取り/書き込みパスを指定してゲートウェイを再び構成しようとしても、サービスは起動に失敗します。

回避方法: この問題が発生した場合は、<NBU インストールパス>/netbackup/nbcct ディレクトリを削除し、操作を再試行する必要があります。

VM 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。

- [VM のリカバリ](#)
- [VMware エージェントレスリストアについて](#)
- [VMware エージェントレスリストアの前提条件と制限事項](#)
- [VMware エージェントレスリストアによるファイルとフォルダのリカバリ](#)
- [制限されたリストアモードについて](#)

VM のリカバリ

バックアップされたときに VM が存在していた元の場所または別の場所に VM をリカバリできます。バックアップイメージのデフォルトのコピーからのリカバリに加え、別のコピーがある場合はそのコピーからもリカバリできます。デフォルトのコピーはプライマリコピーとも呼ばれます。

VM をリカバリするには

- 1 左側の[VMware]をクリックします。
- 2 VM を特定してクリックします。
- 3 [リカバリポイント (Recovery points)] タブをクリックします。左側のカレンダービューで、バックアップが発生した日付を選択します。

利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。

- 4 リカバリするイメージについて、次のいずれかのイメージリカバリオプションを選択します。
 - リカバリ (Recover)

バックアップイメージのデフォルトのコピーからリカバリします。このオプションは、コピーが 1 つだけある場合にのみ表示されます。

- **デフォルトのコピーからリカバリ (Recover from default copy)**
バックアップイメージのデフォルトのコピーからリカバリします。このオプションは、コピーが複数ある場合にのみ表示されます。
- **nn 個のコピー (nn copies)**
バックアップイメージのデフォルトのコピーまたは別のコピーからリカバリします。**NetBackup** では、同じバックアップイメージのコピーを最大 10 個まで保持できます。このオプションを選択すると、利用可能なすべてのコピーが表示されます。それぞれのコピーについて、[ストレージ名 (Storage name)]、[ストレージサーバー (Storage Server)]、[ストレージサーバー形式 (Storage server type)]が表示されます。リカバリするコピーに対して[リカバリ (Recover)]をクリックします。

5 バックアップイメージをリカバリする場所を選択します。

- [元の場所 (Original location)]: バックアップイメージを元の場所にリカバリします。
- [代替の場所 (Alternate location)]: バックアップイメージを代替の場所にリカバリします。
- [インスタントアクセス仮想マシンの作成 (Create instant access virtual machine)]: バックアップイメージを新しいインスタントアクセス仮想マシンにリカバリします。バックアップイメージにインスタントアクセス機能がある場合にのみ、このオプションを利用可能です。p.40 の「[インスタントアクセス VM の作成](#)」を参照してください。
- [ファイルとフォルダのダウンロード (Download files and folders)]: VM バックアップイメージからファイルとフォルダをダウンロードします。バックアップイメージにインスタントアクセス機能がある場合にのみ、このオプションを利用可能です。p.44 の「[VM バックアップイメージからのファイルとフォルダのダウンロード](#)」を参照してください。
- [ファイルとフォルダをリストアする (Restore files and folders)]: VM バックアップイメージからファイルとフォルダをリストアします。バックアップイメージにインスタントアクセス機能がある場合にのみ、このオプションを利用可能です。「p.42 の「[VM バックアップイメージからのファイルとフォルダのリストア](#)」を参照してください。」を参照してください。

6 [リストア先 (Restore to)]の値を確認します。

デフォルト値は VM のバックアップイメージから取得されます。代替の場所にリストアする場合、[新しい表示名 (New display name)]に `_copy` が追加されます。

- バックアップイメージを元の場所にリカバリする場合、デフォルト値を変更できません。

- 代替の場所にリカバリする場合、必要に応じてリストア先の値を変更します。続いて[次へ (Next)]をクリックします。ESXi Server またはクラスタを変更できない場合に詳細を確認できます。
p.87 の「[リカバリ先を変更したときに発生したエラー](#)」を参照してください。

7 [リカバリオプション (Recover option)]の値を確認または変更します。

リカバリオプションについて詳しくは、『[91 for VMware 管理者ガイド](#)』を参照してください。

既存の仮想マシンの上書きを許可する (Allow overwrite of existing virtual machine)	宛先に同じ名前の VM が存在する場合に既存の VM を削除します。そのような VM はリカバリの開始前に削除する必要があります。そうしないと、リカバリは失敗します。 メモ: このオプションを使用するには、[資産の上書き (Overwrite Asset)]権限が必要です。Minions - Amritesh Ranhi tech contact この権限が必要な場合はセキュリティ管理者にお問い合わせください。
---	---

リカバリ後に電源をオンにする (Power on after recovery)	リカバリが完了すると、VM の電源が自動的にオンになります。
--	--------------------------------

リカバリホスト (Recovery host)	リカバリの実行に使用するホストを示します。デフォルトでは、リカバリホストはバックアップを実行するホストです。
-------------------------	--

8 [詳細設定 (Advanced Settings)]の値を確認または変更します。

詳細設定について詳しくは、『[NetBackup for VMware 管理者ガイド](#)』を参照してください。

詳細設定:

新しい BIOS UUID の作成 (Create a new BIOS UUID)	元の BIOS UUID の代わりに、新しい BIOS UUID で VM をリストアします。
--	---

新しいインスタンス UUID の作成 (Create a new instance UUID)	元のインスタンス UUID の代わりに、新しいインスタンス UUID で VM をリストアします。
---	---

デバイスの補助情報を削除 (Remove backing information for devices)	たとえば、このオプションは、VM がバックアップされた時にマウントされた ISO ファイルをリストアせずに VM をリストアします。 このオプションが無効になっていると、DVDドライブ、CD-ROMドライブ、シリアルポート、パラレルポートなどのデバイスの補助情報が利用できなくなった場合にリカバリが失敗する場合があります。
---	--

元のネットワーク構成を削除 (Remove original network configuration)

NIC カードを VM から削除します。ネットワークアクセスでは、リストア済みの VM にはネットワーク構成が必要であることに注意してください。

このオプションは、次の場合に有効にします。

- バックアップの作成後に宛先の仮想マシンのネットワーク接続が変更されている場合。
- 元の仮想マシンがまだ存在し、VM の重複によって競合が発生する場合。

ハードウェアの元のバージョンを保持する (Retain original hardware version)

元のハードウェアバージョン (4 など) で VM をリストアします。ターゲット ESXi Server がデフォルトで異なるハードウェアバージョン (7、8 など) を使用している場合でも、元のバージョンが保持されます。ターゲット ESXi Server が仮想マシンのハードウェアバージョンをサポートしていない場合は、リストアに失敗する可能性があります。

このオプションが無効の場合、リストアされた仮想マシンは ESXi Server によって使われるデフォルトのハードウェアバージョンに変換されます。

リストアされる仮想ディスクのフォーマット:

元のプロビジョニング (Original provisioning)

元のプロビジョニングで VM の仮想ディスクをリストアします。

Lazy Zero をシックプロビジョニング (Thick provisioning lazy zeroed)

シック形式でリストアされた仮想ディスクを構成します。仮想ディスク容量はディスクが作成されるときに割り当て済みです。このオプションは入力されたブロックをリストアしますが、オンデマンドで空いているブロックをゼロで初期化します。

メモ: vm disk が完全に書き込まれると、VMware は Lazy-Zeroed ディスクを [Eager Zeroed をシックプロビジョニング (Thick provisioning Eager Zeroed)] に自動的に変換します。

Eager Zeroed をシックプロビジョニング (Thick provisioning eager zeroed)

シック形式でリストアされた仮想ディスクを構成します。データが入力されたブロックをリストアし、ただちに空のブロックをゼロで初期化します (Eager Zeroed)。このオプションを使用すると仮想ディスクの作成により時間がかかることがあります。ただし、リストアが SAN で起きた場合、Eager Zeroed 機能により vCenter Server とのネットワーク通信が減少することによってリストアが高速化されることがあります。

シンプロビジョニング シン形式でリストアされた仮想ディスクを構成します。データが入力されたブロックはリストアしますが、空いているブロックを初期化したりコミットしたりはしません。シンプロビジョニングは **vmdk** ファイルの動的拡張を介してディスク領域を節約します。**vmdk** ファイルは仮想マシンのデータが必要とする領域より大きくなりません。仮想ディスクのサイズは必要に応じて自動的に増加します。

メモ: **vmdk** が完全書き込まれると、**VMware** はシンディスクを [Eager Zeroed をシックプロビジョニング (Thick provisioning Eager Zeroed)] に自動的に変換します。

トランスポートモード (Transport mode):

バックアップに使用するトランスポートモード
バックアップが実行されたときと同じトランスポートモードを使用します。
使用する (Use transport mode used for backup)

選択したトランスポートモードを次の順序で試行してください。(Try the selected transport modes in the following order)

■ SAN

ファイバーチャネル (SAN) または iSCSI を介した、暗号化されていない転送の場合に指定します。

メモ: このモードは VMware 仮想ボリューム (VVols) を使う仮想マシンではサポートされません。

■ HotADD

仮想マシンで VMware バックアップホストを実行できます。

HotAdd トランスポートモードについて詳しくは、『[NetBackup for VMware 管理者ガイド](#)』を参照してください。

メモ: VVols を使用する仮想マシンの場合、仮想マシンとバックアップホスト (hotadd) の仮想マシンは同じ VVol データストアに存在する必要があります。

このトランスポートモードの手順と、バックアップホストの VMware 仮想マシンへのインストール手順に関しては、VMware のマニュアルを参照してください。

■ LAN

ネットワークを介して仮想ディスクのデータを転送します。

■ NBD

Network Block Device (NBD) ドライバプロトコルを使用する、ローカルネットワークを介した暗号化されていない転送の場合に指定します。この転送モードは、通常、ファイバーチャネルを介した転送よりも低速です。

■ NBDSSL

Network Block Device (NBD) ドライバプロトコルを使用する、ローカルネットワークを介した暗号化転送 (SSL) の場合に指定します。この転送モードは、通常、ファイバーチャネルを介した転送よりも低速です。

9 [リカバリ前チェック (Pre-recovery check)]をクリックします。

NetBackup でクレデンシャルが検証され、パスと接続が適切かどうかを確認されます。さらに、データストアやデータストアクラスタに利用可能な容量があるかどうかなど、その他の要件についても確認されます。リカバリ前チェックについて詳しくは、『[NetBackup for VMware 管理者ガイド](#)』を参照してください。

10 エラーが見つかった場合は解決します。

エラーは無視できます。ただし、その場合はリカバリが失敗する場合があります。

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

ジョブの進捗を監視するには、[リストアアクティビティ (Restore activity)] タブをクリックします。特定のジョブを選択すると、その詳細が表示されます。

リカバリの状態コードについて詳しくは、NetBackup 管理者に問い合わせるか、『[91 状態コードリファレンスガイド](#)』を参照してください。

VMware エージェントレスリストアについて

NetBackup 8.2 以降では、VMware エージェントレスリストアがサポートされています。エージェントレスリストアを使用すると、NetBackup クライアントがインストールされていない仮想マシンに個々のファイルとフォルダをリストアできます。VxUpdate を使用して、NetBackup で仮想マシンにリカバリツールを配備し、ファイルやフォルダをリストアして、必要なクリーンアップを実行できます。ファイルをリカバリするターゲット仮想マシンに NetBackup が接続する必要はありません。すべてのリカバリが VMware vSphere Management API を使用して ESX Server 経由で処理されます。

NetBackup VMware のエージェントレスリストアについて説明するビデオをご覧ください。

VMware のエージェントレスリカバリ

エージェントレスリストア処理の概要

- 1 NetBackup プライマリサーバーで NetBackup Web UI または Agentless Recovery API から入力を受け取ります。この入力には、リストアするファイルとフォルダに加え、ターゲット仮想マシンの VMware 認証クレデンシャルが含まれます。これらのクレデンシャルには管理者またはスーパーユーザーの権限が必要です。
- 2 要求されたデータがプライマリサーバーからリストアホストに送信されます。
- 3 リストアを実行するために必要な VxUpdate リカバリパッケージがリストアホストにあるかどうかを確認されます。必要なパッケージがない場合、リストアホストは VxUpdate を使用してプライマリサーバーからパッケージをダウンロードします。
- 4 リストアホストは、vSphere Management API を使用して仮想マシンにリカバリツールをプッシュします。
- 5 ユーザーが選択したファイルとフォルダを含むデータストリームが一時仮想マシンに関連付けられている vmdk でステージングされます。Veritas がエージェントレスリストア用の一時仮想マシンを作成します。
- 6 NetBackup によって一時仮想マシンに作成された vmdk がターゲット仮想マシンに接続されます。
- 7 リカバリツールが起動され、ファイルとフォルダがリカバリされます。
- 8 NetBackup で必要なクリーンアップが実行されます。処理の一環で作成された一時的なファイルとオブジェクトがすべて削除されます。削除されるオブジェクトには、リカバリツール、一時仮想マシン、ステージング vmdk があります。
- 9 これでジョブは完了です。

VMware エージェントレスリストアの前提条件と制限事項

前提条件:

- 仮想マシンのエージェントレスリカバリを実行するすべてのプラットフォーム用の VxUpdate パッケージを用意する必要があります。
- ターゲット仮想マシンに対する管理者権限またはルート権限があるアカウントが必要です。
- ファイルはターゲット VM にリカバリされます。電源をオンにし、VMware Tools をインストールしておく必要があります。
- ターゲット VM には、準仮想 SCSI コントローラで利用可能な LUN または利用可能な領域を持つ、1 つ以上の準仮想コントローラが必要です。
- ターゲット VM のデフォルトのステージング場所は、Windows の場合は %TEMP% または %TMP%、Linux の場合はルートディレクトリ (/) です。
- ステージング場所がターゲット VM のファイルシステムに存在している必要があります。
- エージェントレスリストアを実行するには、最新のバージョンの VMware Tools をインストールしておく必要があります。

制限事項:

- 組み込みの Windows ゲスト OS 用の管理者以外のアカウントをターゲット VM のクレデンシャルとして使用すると、Windows ターゲット VM へのエージェントレスリストアが失敗することがあります。[管理者承認モードですべての管理者を実行する (Run all administrators in Admin Approval Mode)] が有効になっているため、リストアが失敗します。詳細情報を参照できます。
https://www.veritas.com/content/support/en_US/article.100046138.html
- VMware エージェントレスリストアは、ファイルとフォルダのリストアにのみ使用できません。
- エージェントレスリストアの実行時に NB_ で始まる孤立した VM が残ることがあります。Etrack 3975455 この状況は、ESX Server が vCenter で管理されている場合に、ターゲット VM で ESX Server のクレデンシャルを使用してリストアを実行すると発生することがあります。これは VMware の既知の制限事項です。この問題を解決するには、NetBackup で vCenter を登録し、バックアップやリストアに vCenter のクレデンシャルを使用するようにします。NB_ で始まる孤立した VM は、VMware vSphere Client を使用して vCenter にログインし、手動でインベントリから削除できます。
- TMP または TEMP 環境変数でステージングディレクトリとして指定されているディレクトリを NetBackup で使用できない場合、リストアジョブは失敗します。

- ステージングディレクトリに対する十分な権限が **NetBackup** に割り当てられていない場合やステージングディレクトリに十分な領域がない場合、リストアジョブは失敗します。
- [既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]と[既存のファイルの上書き (Overwrite existing files)]のオプションを選択した場合、同じファイル名のファイルが複数含まれていると正しくリストアされないことがあります。この場合、最後にリストアされたファイルがリストアの完了時に保持されます。
[既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]を選択して[既存のファイルの上書き (Overwrite existing files)]を選択しない場合、リストアは成功し、最初にリストアされたファイルがリストアの完了時に保持されます。この問題を防ぐには、同じ名前の複数のファイルをリストアするときに[既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]を選択しないでください。
- [既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]と[ファイル名に文字列を追加 (Append string to file names)]のオプションはファイルにのみ適用できます。ディレクトリには適用できません。
- 同じ VM に対する複数のリストアジョブはサポートされていません。同じ VM に対して別のリストアジョブを実行する場合は、最初のジョブが完了してから開始する必要があります。
- 同じ VM でバックアップとリストアを同時に実行すると、一方または両方のジョブが予期しない結果になることがあります。ゼロ以外の **NetBackup** の状態コードでバックアップまたはリストアが終了した場合は、それらのジョブが同じ VM で同時に実行されたことが原因である可能性があります。
- **NetBackup** クライアントがターゲット VM にすでに存在する場合、**Veritas** では **VMware** エージェントレスリストアを使用することはお勧めしません。このような場合、**NetBackup** 管理者はエージェントベースのリストアを使用する必要があります。
- **NetBackup** は、ターゲット VM のゲストオペレーティングシステムとして次のプラットフォームをサポートします。
 - Windows 2012、2012R2、2016
 - Red Hat Enterprise Linux (RHEL) 6.8、7
 - SUSE Linux (SLES) 11、12

VMware エージェントレスリストアによるファイルとフォルダのリカバリ

エージェントレスリストアを使用して **VMware** のファイルとフォルダをリストアするには

- 1 ターゲット VM の電源がオンになっていることを確認します。
- 2 Web UI の左側にある[VMware]をクリックします。

- 3 リストアするファイルとフォルダが含まれている VM を特定してクリックします。
- 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、[ファイルとフォルダを復元する (Restore files and folders)] をクリックします。
- 6 [ファイルを選択する (Select files)] で、リカバリするファイルとフォルダを指定し、[次へ (Next)] をクリックします。
- 7 [リカバリターゲット (Recovery target)] で、ファイルとフォルダをリカバリするターゲット VM を指定し、そのターゲット VM の管理者のクレデンシャルを指定します。
- 8 [リカバリオプション (Recovery options)] で、リストアするファイルとフォルダに対するその他のリカバリオプションを指定します。
- 9 [次へ (Next)] をクリックすると、指定したオプションを使用して NetBackup によるリカバリ前チェックが実行されます。
- 10 [確認 (Review)] に、リカバリ前チェックの状態が選択したリカバリオプションとともに表示されます。それらの内容が正しいことを確認したら、リストアを実行します。

制限されたリストアモードについて

制限されたリストアモードオプションは、Windows UAC (ユーザーアカウント制御) のような制限された環境での VMware エージェントレスリストアの 1 つの形式です。ユーザーが選択したファイルは、最初にリカバリホストにステージングされ、その後、仮想マシンにリストアされます。リカバリホストには、ステージング用の十分な容量が必要です。

リカバリホストのデフォルトのステージング場所は

`install_path\VERITAS\NetBackup\var\%tmp%\staging` です。NetBackup は、最初にアクセスされたときに、このディレクトリを適切な権限付きで作成します。ステージングの場所は、リカバリホストの `AGENTLESS_RHOST_STAGING_PATH` レジストリ設定を使用して変更できます。この `REG_SZ` レジストリキーはデフォルトでは存在しません。これは `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config` に作成する必要があります。

ステージングの場所を変更する場合、Veritas では、ステージングディレクトリの作成を NetBackup に任せることをお勧めします。ディレクトリの作成を NetBackup に任せると、権限が正しく設定されます。NetBackup に新しいステージングディレクトリの作成を任せると、すぐ上に親ディレクトリが必要です。リストアで `E:\%recovery%\staging` を使用する場合は、`E:\%recovery\` が存在している必要があります。`E:\%recovery\` ディレクトリが存在しない場合、リストアは失敗します。

自分でディレクトリを作成する場合は、**SYSTEM**、ドメイン管理者、およびローカル管理者アカウントにフルコントロールの権限が付与されている必要があります。さらに、親ディレクトリから継承されたアクセス制御リストは安全でないため、無効にする必要があります。

制限されたリストアモードは代替の場所のリストアをサポートします。**NetBackup Web UI** で代替の場所を設定できます。

制限されたリストアモードの制限事項は次のとおりです。

- 制限されたリストアモードは、現在 **Windows** でのみサポートされています。リカバリホストも **Windows** である必要があります。
- リストアされたファイルのファイル所有権は、**NetBackup** バックアップ操作に使用されたアカウントに設定されます。
- **ACL** のリストアはサポートされていません。
- 制限されたリストアモードは、ソフトリンクのターゲットの名前変更をサポートしていません。
- 制限されたリストアモードでは、ハードリンクが以前に使用されていた新しいファイルが作成されます。
- 通常ではないファイル (スパースファイル、デバイスファイル、特殊ファイル、接合点など) はサポートされません。
- リストアの成功には、サポートされているバージョンの **VMware Tools** が実行されている必要があります。
- ディレクトリのファイルパスの長さは、**260** 文字以下でなければなりません。

パフォーマンスに関する注意事項

このリストア方式に必要なインフラストラクチャを介したファイル転送は、**VMware** エージェントレスリストアより大幅に低速です。パフォーマンス上の懸念により、**Veritas** では、リストアを **100** ファイル未満および **1 GB** 未満のデータに制限することを推奨します。

VMware の操作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。

- [VMware サーバーの追加エラー](#)
- [VMware サーバーを参照するときに発生するエラー](#)
- [新たに検出された VM の状態のエラー](#)
- [インスタントアクセス VM からファイルをダウンロードするときに発生するエラー](#)
- [除外された仮想ディスクのバックアップとリストアのトラブルシューティング](#)
- [複数のデータストアを使用した仮想マシンのリストアが失敗する](#)
- [リカバリ先を変更したときに発生したエラー](#)

VMware サーバーの追加エラー

表 9-1 VMware サーバーの追加エラー

エラーメッセージまたは原因	説明および推奨処置
仮想化サーバーのクレデンシャルの検証に失敗する。	このエラーは、DNAT または同様のセットアップの NetBackup プライマリサーバーが指定された NetBackup ホスト (PROXY_SERVERS) の一部にしかアクセスできない場合に発生します。 クレデンシャルの検証は次の順序で実行されます。 ■ 自動検出された検出ホストが仮想化サーバーへのアクセスに使用されます。 ■ 自動検出された検出ホストで仮想化サーバーに関する情報が見つからない場合は、NetBackup プライマリサーバーが使用されます。 回避方法: 仮想化サーバーのクレデンシャルを追加するときに、仮想化サーバーにアクセスできるプロキシサーバーを検証用バックアップホストとして選択します。 メモ: VMware のクレデンシャルを追加または更新した場合も、VMware サーバーの検出が自動的に開始されます。要求でバックアップホストの情報を指定すると、検出の実行に加えて、クレデンシャルの検証にもその情報が使用されます。検出の場合、バックアップホストとして動作する NetBackup メディアサーバーまたはクライアントでサポートされる最小バージョンは、NetBackup 8.1.2 です。古いバージョンでは、バックアップホストのクレデンシャルは正常に検証されますが、VMware サーバーの検出に失敗します。
Unable to obtain the list of trusted Certificate Authorities.	VMware サーバーのクレデンシャルの追加、更新、または検証の際に、このエラーが発生する可能性があります。NetBackup (プライマリサーバー、メディアサーバー、またはクライアント) と、認証済みの証明書を使用する vCenter、ESX、またはその他の VMware エンティティ間で通信が有効になるように環境が構成されている場合、このエラーが発生します。 回避方法: 証明書がインストールされ、有効であることを確認します。

VMware サーバーを参照するときに発生するエラー

次の表では、[VMware サーバー (VMware servers)] でサーバーをクリックしたときに発生する可能性のある問題について説明します。

表 9-2 VMware サーバーの参照エラー

エラーメッセージまたは原因	説明および推奨処置
VMware サーバーの VM やその他のオブジェクトが検出されていない。	■ サーバーが最近追加された場合は、そのサーバーの VM 検出プロセスがまだ完了していない可能性があります。 推奨処置: 検出プロセスが完了するまで待ちます。 注意: サーバーのクレデンシャルが Web UI や API で追加または更新されると、vCenter または ESXi Server の VM とその他のオブジェクトの検出が開始されます。ただし、UI にはサーバーの VM とその他のオブジェクトがすぐに表示されない場合があります。それらは VMware サーバーの検出プロセスが完了した後に表示されます。検出は VMWARE_AUTODISCOVERY_INTERVAL オプションで設定された間隔でも実行されます (デフォルトの間隔は 8 時間です)。(デフォルトの間隔は 8 時間です)。 VMware サーバーのオブジェクトの自動検出を異なる間隔で実行する方法については、次の情報を参照してください。 p.28 の「VMware 資産の自動検出の間隔の変更」を参照してください。 ■ 追加した VMware サーバーのクレデンシャルで VM やその他のオブジェクトにアクセスできない可能性があります。 推奨処置: 行の右にあるオプションメニューで[編集 (Edit)]を選択します。VMware サーバーのクレデンシャルを確認し、必要に応じて修正します。

新たに検出された VM の状態のエラー

次の表では、[仮想マシン (Virtual machines)]で新たに検出された VM の状態を確認するときに発生する可能性のある問題について説明します。

表 9-3 新たに検出した VM の状態を確認するときに発生するエラー

エラーメッセージまたは原因	説明および推奨処置
VMの保護状態にバックアップ未完了と示されているが、そのVMを含むバックアップジョブは正常に完了している。	NetBackup Web UI で、新たに検出された VM の保護状態は、その VM の次のバックアップが完了するまで、バックアップされたかどうかを示していません。 場合によっては、次のシナリオのように、新しい VM が検出される前にその VM がバックアップされることがあります。 ■ デフォルトでは、8 時間ごとに自動検出が実行されます。 ■ 新しい VM が環境に追加されました。 ■ 検出が完了する前に、バックアップジョブが正常に完了しました。たとえば、新しい VM が既存のポリシーのバックアップの選択条件に含まれており、バックアップジョブがそのポリシーを使用している場合です。 ■ その後、検出が完了しました。ただし、NetBackup Web UI では、VM の保護状態にバックアップ未完了と示されます。 同様の状況が発生した場合、リカバリポイントを参照してリカバリできます。ただし、保護状態に VM のバックアップが完了と表示されるのは、VM の別のバックアップが正常に完了した後です。 NetBackup Web UI で新たに検出された VM の保護状態を確認するには、Veritas は次の正常なバックアップが完了するまで待つことをお勧めします。その後であれば、VM の保護状態が正しく表示されます。

インスタントアクセス VM からファイルをダウンロードするときに発生するエラー

次の表では、インスタントアクセス VM から個別のファイルをダウンロードするときに発生する場合がある問題について説明します。

表 9-4 ファイルのダウンロードのエラー

エラーメッセージまたは原因	説明および推奨処置
Chrome: このサイトにアクセスできません Firefox: サーバーが見つかりませんでした Edge: このページに到達できません	このエラーは、次のいずれかの理由により発生する可能性があります。 ■ NetBackup プライマリサーバーがメディアサーバーへの接続に使用する名前や IP アドレスを使用して、Web UI がこの NetBackup メディアサーバーにアクセスできません。 例: プライマリサーバーが <code>MSserver1.veritas.com</code> を使用してメディアサーバーに接続する場合、Web UI も <code>MSserver1.veritas.com</code> に到達する必要があります。プライマリサーバーが <code>MSserver1</code> などの短縮名をメディアサーバーに使用している場合、Web UI は <code>https://MSserver1/...</code> に到達する必要があります。 推奨処置: プライマリサーバーと Web UI が、メディアサーバーへのアクセスに同じ名前または IP アドレスを使用していることを確認します (<code>hosts</code> ファイルを確認)。 例: プライマリサーバーがメディアサーバーの短縮名を使用している場合は、Web UI を実行している PC またはその他のホストの <code>hosts</code> ファイルに、メディアサーバーの短縮名と IP アドレスを追加します。 Windows 上の <code>hosts</code> ファイルの場所: <code>C:\Windows\System32\drivers\etc\hosts</code> UNIX または Linux 上のホストファイルの場所: <code>/etc/hosts</code> ■ NetBackup メディアサーバーがファイアウォールの背後にあるため、Web UI がそのサーバーにアクセスできません。 推奨処置: NetBackup セキュリティ管理者にお問い合わせください。

除外された仮想ディスクのバックアップとリストアのトラブルシューティング

仮想ディスクを除外するように構成されたバックアップのリストアで問題が発生した場合は、次の表を参照してください。

表 9-5 仮想ディスクの除外に関する問題

問題	説明
ブートディスクをバックアップから除外したにもかかわらず、バックアップされた。	仮想マシンにブートディスクのみが存在し、その他のディスクが存在しません。
	ブートディスクは管理対象ボリューム (Windows LDM または Linux LVM) の一部です。 NetBackup は、ブートディスクが単一ディスクに完全に含まれている場合にのみ、ブートディスクを除外できます。
	仮想マシンのブートディスクは独立したディスクで、その他のディスクが存在しません。
	NetBackup がブートディスクを識別できませんでした。ブートディスクには、ブートパーティションと、システムまたはブートディレクトリを含める必要があります。
リストアされたブートディスクにデータがない。	ブートディスクが独立したディスクです。 NetBackup は、このディスク形式のデータをバックアップできません。
リストアされた仮想マシンのディスクにデータがないか、不完全なデータが格納されている。	データがないか不完全なディスクがバックアップから除外されました。
単一または複数のデータディスクをバックアップから除外したにもかかわらず、バックアップされた。	仮想マシンに 1 つのディスク (C: など) しか含まれていません。この場合、1 台のドライブがバックアップされ、除外されません。
仮想マシンが予期しない状態にリストアされた。	仮想マシンにディスクを追加し、ディスクを除外する設定を変更しましたが、変更を加えた後に仮想マシン全体のバックアップを作成しませんでした。
個別にリストアできないファイルがある。	差分バックアップ間でカスタム属性値からディスクを削除すると、前回のバックアップ以降に変更されたファイルのみを個別にリストアできます。または、仮想ディスクまたは VM 全体をリストアできます。次の完全バックアップの後で、任意のファイルを個別にリストアできます。
	差分バックアップ間で、[除外する特定のディスク (Specific disks to be excluded)]からコントローラを削除すると、前回のバックアップ以降に変更されたファイルのみをリストアできます。次の完全バックアップの後で、すべてのファイルをリストアできます。

複数のデータストアを使用した仮想マシンのリストアが失敗する

表 9-6 複数のデータストアを使用した仮想マシンのリストアに関する問題

問題	説明
データストアに .vmdk ファイル用の十分な領域がないため、リストアが失敗します。	この問題は、仮想マシンが複数のデータストアで構成され、バックアップ時に仮想マシンに残りのスナップショットが存在すると、発生する場合があります。NetBackup は、スナップショットのデータストアにすべての .vmdk ファイルをリストアしようとします。 代わりに、代替の場所に仮想マシンをリストアできます。

リカバリ先を変更したときに発生したエラー

表 9-7 リカバリ先を変更したときに発生したエラー

問題	説明
vCenter Server のリストを表示できない	vCenter Server のリストを参照できない場合、RBAC で [アプリケーションサーバー (Application Servers)] オブジェクトグループプロパティの下にある vCenter Server へのアクセス権がない可能性があります。 推奨処置: NetBackup セキュリティ管理者にお問い合わせください。