

NetBackup™ Web UI VMware 管理者ガイド

リリース 9.0

VERITAS™

NetBackup Web UI VMware 管理者ガイド

最終更新日: 2021-02-01

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で入手できます。

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

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

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

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Veritasがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリース、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	6
	NetBackup Web UI について	6
	用語	8
	NetBackup Web UI へのサインイン	10
	NetBackup Web UI からのサインアウト	11
第 2 章	監視と通知	13
	NetBackup ダッシュボード	13
	ジョブの監視	14
	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	16
	VMware サーバーの追加	16
	VMware サーバーのクレデンシャルの検証と更新	18
	VMware サーバーの参照	18
	VMware サーバーの削除	19
	インテリジェント VM グループの作成	20
	インテリジェント VM グループの削除	24
	VMware アクセスホストの追加	25
	VMware アクセスホストの削除	26
	VMware サーバーの資産の手動での検出	26
	NetBackup サーバーの VMWARE_AUTODISCOVERY_INTERVAL オプション	27
第 4 章	VM の保護	29
	VM またはインテリジェント VM グループの保護	29
	VMware 資産の保護設定の編集	30
	スケジュールと保持	31
	バックアップオプション (Backup options) と詳細オプション (Advanced options)	31
	バックアップからのディスクの除外	32
	スナップショットの再試行オプション (Snapshot retry options)	33
	VM またはインテリジェント VM グループの保護の解除	34

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	34
第 5 章	
インスタントアクセス	36
インスタントアクセス VM の作成	36
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	38
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	40
インスタントアクセス機能を使用する前の考慮事項	41
第 6 章	
VM のリカバリ	44
VM のリカバリ	44
VMware エージェントレスリストアについて	50
VMware エージェントレスリストアの前提条件と制限事項	51
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	52
制限されたリストアモードについて	53
第 7 章	
VMware の操作のトラブルシューティング	55
VMware サーバーの追加エラー	56
VMware サーバーを参照するときに発生するエラー	56
新たに検出された VM の状態のエラー	57
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	58
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	59
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	61
リカバリ先を変更したときに発生したエラー	61

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

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

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

NetBackup Web UI のアクセス制御

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

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

NetBackup ジョブおよびイベントの監視

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

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

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

保護計画には、次の利点があります。

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

セルフサービスリカバリ

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

用語

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

表 1-1 Web ユーザーインターフェースの用語および概念

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

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

用語	定義
保護計画にサブスクライプする	保護計画にサブスクライプ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、サブスクライプを「保護の追加」とも表記します。
保護計画からサブスクライプ解除する	サブスクライプ解除は、保護を解除する処理、または計画から資産や資産グループを削除する処理を指します。
作業負荷 (Workload)	資産のタイプです。たとえば、VMware、RHV、またはクラウドです。

NetBackup Web UI へのサインイン

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

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

ユーザー名とパスワードでサインインする

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

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

- 1 Web ブラウザを開き、次の URL に移動します。

<https://masterserver/webui/login>

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

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

次に例を示します。

ユーザーの種類	使用する形式	例
ローカルユーザー	<i>username</i>	jane_doe
Windows ユーザー	<i>DOMAIN\\$username</i>	WINDOWS\\$jane_doe
UNIX ユーザー	<i>username@domain</i>	john_doe@unix

証明書またはスマートカードでサインインする

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

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

証明書またはスマートカードでサインインするには

- 1 Web ブラウザを開き、次の URL に移動します。

<https://masterserver/webui/login>

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

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

シングルサインオン (SSO) でサインインする

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

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

- 1 Web ブラウザを開き、次の URL に移動します。

<https://masterserver/webui/login>

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

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

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

NetBackup Web UI からのサインアウト

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

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

NetBackup Web UI からサインアウトするには

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

監視と通知

この章では以下の項目について説明しています。

- [NetBackup ダッシュボード](#)
- [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	アクティブジョブやキューに投入済みのジョブの数、試行されたジョブや完了したジョブの状態などのジョブ情報を一覧表示します。
証明書	<p>環境内の NetBackup のホスト ID ベースのセキュリティ証明書または外部証明書に関する情報を表示します。</p> <p>外部証明書では、NetBackup 8.2 以降のホストに関する次の情報が表示されます。</p> <ul style="list-style-type: none"> ■ ホストの合計。ホストの合計数です。ホストはオンラインになっており、NetBackup マスター サーバーと通信できる必要があります。 ■ 不明。外部証明書が登録されていないホストの数です。 ■ 有効。外部証明書が登録されているホストの数です。 ■ 期限切れ。期限切れの外部証明書を持つホストの数です。
トークン	環境内の認証トークンに関する情報を表示します。

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

ジョブの監視

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

ジョブを監視するには

- 1 左側で、[アクティビティモニター (Activity monitor)]>[ジョブ (Jobs)]をクリックします。
- 2 表示するジョブの名前をクリックします。
[概要 (Overview)]タブで、ジョブに関する情報を表示します。
 - [ファイルリスト (File List)]には、バックアップイメージに含まれているファイルが表示されます。
 - [状態 (Status)]セクションには、ジョブに関連する状態と状態コードが表示されます。状態コード番号をクリックすると、この状態コードについての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 サーバーの資産の手動での検出
- NetBackup サーバーの VMWARE_AUTODISCOVERY_INTERVAL オプション

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 [VMware] (左側)、[VMware サーバー (VMware Servers)] タブの順にクリックします。

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ャルを入力します。

- 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 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.27 の「NetBackup サーバーの VMWARE_AUTODISCOVERY_INTERVAL オプション」](#)を参照してください。

- 7 別の VMware サーバーの NetBackup クレデンシャルを入力するには、[+ 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.56 の「VMware サーバーの追加エラー」](#)を参照してください。

[p.56 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.57 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 [VMware] (左側)、[VMware サーバー (VMware Servers)] タブの順にクリックします。
- 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、[クレデンシャル (Credentials)] に [無効 (Invalid)] と表示されます。NetBackupVMware 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 [VMware] (左側)、[VMware サーバー (VMware Servers)] タブの順にクリックします。
- 2 VMware サーバーを特定して選択します。
- 3 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。
- 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 サーバーを参照して、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 左側の[VMware]をクリックします。
- 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 サーバーとスタンドアロンの ESXi サーバー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も確認できます。

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、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 [Vmware] (左側)、[VMware サーバー (VMware Servers)]タブの順にクリックします。
このタブには、アクセス権を持つ vCenter サーバーとスタンドアロンの ESXi サーバー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 行の右にある処理メニューで[削除 (Delete)]を選択します。

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

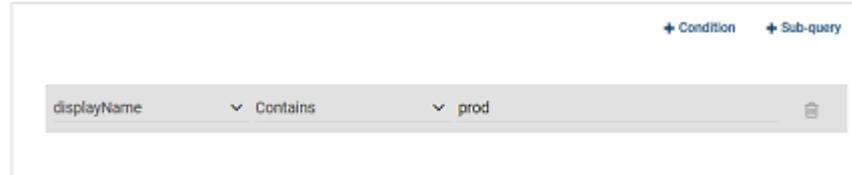
クエリーと呼ばれるフィルタのセットに基づいて、インテリジェント VM グループを作成できます。NetBackup は、クエリーに基づいて自動的に仮想マシンを選択し、それらをグループに追加します。その後、グループに保護を適用できます。インテリジェントグループでは、VM 環境内の変更が自動的に反映されるため、グループ内の VM のリストを手動で修正する必要がないことに注意してください。

インテリジェント VM グループを作成するには

- 1 左側の[VMware]をクリックします。
- 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、デフォルトクエリーを使用して、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、独自のクエリーを作成するため [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オペレータを選択して、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クエリーオプション](#)」。

以下がクエリーの例です。



この例のクエリーは、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。

クエリーの効果を変更するには、[+ 条件 (Condition)]をクリックし、[AND]または [OR]をクリックしたら、キーワード、オペレータ、および条件の値を選択します。次に例を示します。



この例では、[AND]を使用してクエリー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。

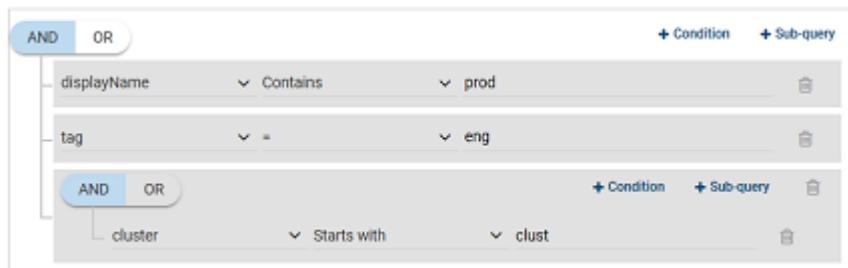
クエリーの範囲を広げるには、[OR]を使用します。



この例では、[OR]が設定されているため、クエリーでグループに次のものが追加されます。

- 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、オペレータ、値を選択します。次に例を示します。



この例では、サブクエリーを使用してクエリー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。

7 クエリーをテストするには、[プレビュー (Preview)]をクリックします。

クエリー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クエリー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時にクエリーが選択する 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。

メモ: [インテリジェント VM グループ (Intelligent VM groups)]でクエリーを使用する場合、クエリー条件に英語以外の文字が含まれていると、NetBackup Web UI に、クエリーに一致する正確な VM のリストが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。

メモ: VMware サーバーの VM の検出が、`VMWARE_AUTODISCOVERY_INTERVAL` オプションに設定された間隔に従って実行されます (デフォルトの間隔は 8 時間です)。クエリー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.27 の「NetBackup サーバーの `VMWARE_AUTODISCOVERY_INTERVAL` オプション」](#) 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.26 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。

- 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、クエリー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、一部のクエリーオプションは、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クエリーオプション」](#)」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クエリーオプション

表 3-1 クエリーキーワード

キーワード	説明
cluster	VM が存在するクラスタ (ESXi Server のグループ) の名前。 保護計画の実行時には大文字と小文字は区別されません。
datacenter	データセンターの名前。 保護計画の実行時には大文字と小文字は区別されません。
datastore	データストアの名前。 保護計画の実行時には大文字と小文字が区別されます。
displayName	VM の表示名。 保護計画の実行時には大文字と小文字が区別されます。
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。 保護計画の実行時には大文字と小文字は区別されません。
tag	VM のタグの名前。 保護計画の実行時には大文字と小文字が区別されます。

キーワード	説明
dnsName	vSphere Client の VM の DNS 名。 保護計画の実行時には大文字と小文字は区別されません。
hostName	IP アドレスの逆引きから導かれる VM 名。 保護計画の実行時には大文字と小文字は区別されません。
instanceUuid	VM のインスタンス UUID。 例: 501b13c3-52de-9a06-cd9a-ecb23aa975d1 保護計画の実行時には大文字と小文字は区別されません。

表 3-2 クエリー演算子

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。

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 左側の[VMware]をクリックします。
- 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ています。
- 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、[サブスクリプション解除 (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 &nbuProductName; 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できる必要があります。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[VMware]をクリックし、[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 これまでに追加されたすべてのアクセスホストがリストに表示されます。
- 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[VMware]をクリックし、[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 これまでに追加されたすべてのアクセスホストがリストに表示されます。
- 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 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 サーバーの 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.27 の「NetBackup サーバーの VMWARE_AUTODISCOVERY_INTERVAL オプション」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 [VMware] (左側)、[VMware サーバー (VMware Servers)] タブの順にクリックします。

このタブには、アクセス権を持つ vCenter サーバーとスタンダードアロンの ESXi サーバー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 行の右にある処理メニューで[検出 (Discover)]を選択します。

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.18 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.34 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.57 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。

NetBackup サーバーの VMWARE_AUTODISCOVERY_INTERVAL オプション

このオプションは、NetBackup が仮想マシンを検出して NetBackup Web UI に表示するするために、vCenter Server をスキャンする頻度を制御します。

NetBackup による自動検出は、最初に前回検出に成功したホストで試行されます。そのホストで自動検出に失敗すると、NetBackup による他のホストへの再試行が、次の順序で行われます。

- NetBackup マスターサーバー
- アクセスホスト、クライアント、プロキシサーバー
- メディアサーバー

表 3-3 VMWARE_AUTODISCOVERY_INTERVAL 情報

使用方法	説明
使用する場所	NetBackup マスターサーバー上。
使用方法	<p>オプションを表示、追加、変更するには、<code>nbgetconfig</code> コマンドと <code>nbsetconfig</code> コマンドを使用します。</p> <p>メモ: これらのコマンドでは、NetBackup マスターサーバーの管理者権限が必要です。サポートが必要な場合は、NetBackup 管理者にお問い合わせください。</p> <p>このオプションは、NetBackup 構成 API でも表示、追加、変更できます。詳しくは、SORT の NetBackup API ドキュメントを参照してください。</p> <p>デフォルトは 8 時間です。最小値は 5 分で、最大値は 1 年です。0 に設定すると、自動検出がすべての VMware サーバーに対して無効になります。</p> <p>次の形式を使用します。</p> <p><code>VMWARE_AUTODISCOVERY_INTERVAL = number of seconds</code></p> <p>次に例を示します。</p> <p><code>VMWARE_AUTODISCOVERY_INTERVAL = 100000</code></p> <p>このエントリは、設定ファイルで一度のみ表示されます。</p> <p>メモ: このオプションを変更した後、NetBackup サービスを停止して再起動します。VM の検出の場合、NetBackup Discovery Framework サービスが実行中である必要があります。</p>
同等の管理コンソールのプロパティ	NetBackup 管理コンソールまたは Web UI に、相当する機能は存在しません。

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。

- [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](#)

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プします。保護計画に資産をサブスクライプするときに、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 左側の[VMware]をクリックします。
- 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.31 の「[スケジュールと保持](#)」を参照してください。
- p.31 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。

- | | |
|--|---|
| <p>VM の設定の編集</p> <p>インテリジェントグループの設定の編集</p> | <ul style="list-style-type: none">■ [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 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.31 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.31 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、いざ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.32 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.33 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。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)	<p>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。</p> <p>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とき、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。</p>
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)	<p>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。</p> <p>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。</p> <p>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。</p>
除外する特定のディスク (Specific disks to be excluded)	<p>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。</p> <p>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。</p>

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ライプを、保護計画から解除できます。資産のサブスクライプが解除されると、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ライプを解除するときに、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ライプされており、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ライプ解除されます。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 左側の[VMware]をクリックします。
- 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 左側の[VMware]をクリックします。
- 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.57 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.29 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 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 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、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.41 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れを許可する(Allow the VM to be deleted before recovery)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。

virtual machine)

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.41 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.41 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 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、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。9.0 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、マスター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できる必要があります。p.58 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 マスター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、次の場所から入手可能な『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。
<https://www.veritas.com/docs/DOC5332>
- 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マスターサーバーが **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マスターサーバーで **NetBackup Web** サービスを再起動します。
 - `/usr/openv/netbackup/bin/nbwmc stop`
 - `/usr/openv/netbackup/bin/nbwmc start`

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応する[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.36 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.40 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。[「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.61 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、『90 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つ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: vmdk 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** が完全に書き込まれると、**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。

を使用する (Use
transport mode used
for backup)

選択したトランSPORT
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SPORT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 を使用的仮想マシンの場合、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SPORT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が確認されま
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、『[90
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いただけます。

[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 マスターサーバーで 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マスター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が確認されます。必要なパッケージがない場合、リストアホストは VxUpdate を使用してマスター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 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:

- 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す。
- 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場合は、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(スペースファイル、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 サーバーの追加工エラー

表 7-1

VMware サーバーの追加工エラー

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。	<p>このエラーは、DNAT または同様のセットアップの NetBackup マスター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。</p> <p>クレデンシャルの検証は次の順序で実行されます。</p> <ul style="list-style-type: none"> ■ 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 マスター サーバーが使用されます。 <p>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。</p> <p>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。</p>
Unable to obtain the list of trusted Certificate Authorities.	<p>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 (マスター 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。</p> <p>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。</p>

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 7-2 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。	<ul style="list-style-type: none"> ■ 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。 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 サーバーの 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.27 の「NetBackup サーバーの VMWARE_AUTODISCOVERY_INTERVAL オプション」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 7-3 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
<p>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。</p>	<p>NetBackup Web UI で、新たに検出された VM の保護状態は、その VM の次回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。</p> <p>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。</p> <ul style="list-style-type: none"> ■ 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。 <p>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。</p> <p>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 は次回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。</p>

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 7-4

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	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。
Firefox: サーバーが見つかりませんでした	<ul style="list-style-type: none"> ■ NetBackup マスター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。 <p>例: マスターサーバーが <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> に到達できる必要があります。マスターサーバーが <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></p> <p>推奨処置: マスターサーバーと 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 (hosts ファイルを確認)。</p> <p>例: マスター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 hosts 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。</p> <p>Windows 上のホストファイルの場所: <code>C:\Windows\System32\drivers\etc\hosts</code></p> <p>UNIX または Linux 上のホストファイルの場所: <code>/etc/hosts</code></p>
Edge: このページに到達できません	<ul style="list-style-type: none"> ■ 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。 <p>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。</p>

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 7-5 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 7-6 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。	<p>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。</p> <p>代わりに、代替の場所に仮想マシンをリストアできます。</p>

リカバリ先を変更したときに発生したエラー

表 7-7 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	<p>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。</p> <p>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。</p>