# NetBackup™ Web UI VMware 管理者ガイド

リリース 10.3

VERITAS™

最終更新日: 2023-12-28

## 法的通知と登録商標



Veritas、Veritas ロゴ、NetBackup は、Veritas Technologies LLC または関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Veritas 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア (「サードパーティ製プログラム」) が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このVeritas製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

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

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

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

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Veritasがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

## テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

| | |
|---|---|
| 世界共通 (日本を除く) | CustomerCare@veritas.com |
| 日本 | CustomerCare_Japan@veritas.com |

## マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、Veritasの Web サイトで入手できます。

https://sort.veritas.com/documents

## マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

http://www.veritas.com/community/

## Veritas Services and Operations Readiness Tools (SORT)

Veritas SORT (Service and Operations Readiness Tools) は、特定の時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供するWeb サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

# 目次

1

# VMware 管理者向けの RBAC とクレデンシャルの構成

この章では以下の項目について説明しています。



## VMware 管理者の RBAC の役割

デフォルトの VMware 管理者の役割によって、ユーザーは VMware 資産のジョブを管理、保護、リカバリできます。この役割を使用すると、管理者は vCenter、ESX Server などのクレデンシャルを管理することもできます。(これらのクレデンシャルは、[作業負荷 (Workloads)]、[VMware]の[VMware サーバー (VMware servers)]タブで管理します。)

さらに、VMware 管理者に追加のアクセス権を付与するために、他のカスタム役割が必要になる場合があります。たとえば、ゲスト VM クレデンシャルに VMware 管理者のアクセス権を付与する役割が必要になる場合があります。これにより、ユーザーは VM のユーザー名とパスワードを使用せずに、ゲスト VM に対してファイルとフォルダのエージェントレスリカバリを実行できます。

p.84 の「ゲスト VM へのエージェントレス単一ファイルリカバリのクレデンシャルへのアクセスの提供」を参照してください。

次の点に注意してください。

- RBAC の役割を作成するには、RBAC 管理者の役割、または役割を作成する権限が必要です。
- クレデンシャルを作成するには、RBAC 管理者の役割、またはクレデンシャルを作成する権限を持つ役割が必要です。デフォルトの VMware 管理者の役割はユーザー

にクレデンシャルを割り当てることはできますが、クレデンシャル管理でクレデンシャルを作成することはできません。

- 役割とクレデンシャルの作成については、NetBackup 管理者にお問い合わせください。

2

# 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

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、ESXi サーバー、VMware Cloud Director サーバーが表示されます。

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。
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。

   VM やその他のオブジェクトは 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。

# VMware サーバーのクレデンシャルの検証と更新

VMware サーバーを追加した後、サーバーのクレデンシャルを検証または更新できます。

**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 つ以上の VMware サーバーを選択し、[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**

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。

5 [保存 (Save)]をクリックします。

# VMware サーバーの参照

vCenter Server、スタンドアロンの ESXi サーバー、VMware Cloud Director サーバーを参照して、VM を見つけて詳細を表示できます。VM の詳細には、保護計画とリカバリポイントが含まれます。

**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、スタンドアロンの ESXi Server、VMware Cloud Director 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、NetBackup から VMware サーバーを削除する手順を示します。

---

**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。

---

**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、スタンドアロンの ESXi サーバー、VMware Cloud Director サーバーの名前と種類が一覧表示されます。[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。
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:** 問い合わせで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。

p.23 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.23 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。

---

**メモ:** インテリジェント VM グループは VMware Cloud Director VM ではサポートされていません。

---

**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。

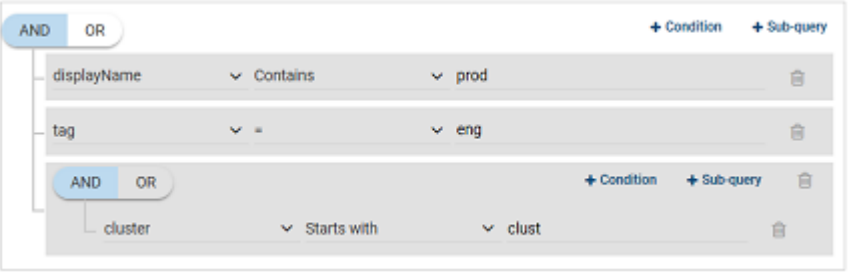
6 条件を追加するには、ドロップダウンを使用してキーワードと演算子を選択し、値を入力します。

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。


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。



**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) 資産を含む資産が戻されます。`tag` などの複数値の属性では、属性値のうち少なくとも 1 つに一致しないと資産は戻されません。
- 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 2-1 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 (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。<br>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。<br>p.19 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 |

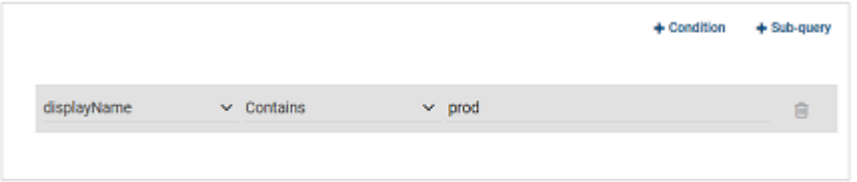
## 問い合わせ演算子

**表 2-2** 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。<br>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。<br>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。<br>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。<br>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 が含められます。

# 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 のメディア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[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します。 | [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。<br>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。<br>リストから、リソースを選択します。<br>適用する[制限 (Limits)]の値を選択します。<br>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 検出について

NetBackup では、VMware サーバーを追加したりクレデンシャルを更新したりすると、VMware サーバーの検出が自動的に開始されます。バックアップホストの情報は、クレデンシャルを検証して検出を実行するために使用されます。

バックアップホストとして機能するには、メディアサーバーまたはクライアントが NetBackup 8.1.2 以降である必要があります。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。検出は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)。

p.23 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.23 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。

# 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、ESXi サーバー、または VMware Cloud Director 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.23 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、スタンドアロンの ESXi サーバー、VMware Cloud Director サーバーの名前と種類が一覧表示されます。[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.11 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.31 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.112 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。

3

# 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

NetBackup Web UI 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。

**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. 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:** 保護計画は VMware Cloud Director VM ではサポートされていません。

**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. 必要に応じて設定を調整します。
   - バックアップの開始時間帯を変更します。
     p.26 の「スケジュール」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 (Advanced)]オプション。
     p.27 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。

   [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。

## スケジュール

次のスケジュール設定が保護計画に含まれています。

資産の保護計画をカスタマイズする場合は、次のスケジュール設定のみを編集できることに注意してください。

- 開始時間帯 (Start window)

**表 3-1** 保護計画のスケジュールオプション

| オプション | 説明 |
|---|---|
| バックアップ形式 (Backup type) | スケジュールで制御するバックアップ形式。 |
| 反復 (Recurrence) (間隔) | バックアップを実行する頻度またはタイミング。 |

| オプション | 説明 |
| --- | --- |
| 保持期間 (Keep for) (保持) | スケジュールによってバックアップされたファイルを保持する期間。 |
| このバックアップをレプリケートする (Replicate this backup) | 別のボリュームにスナップショットをレプリケートします。 |
| 長期保持用にすぐにコピーを複製する (Duplicate a copy immediately to long-term retention) | スケジュールが作成された直後に、長期保持用ストレージに選択されたメディアにコピーが複製されます。 |
| 開始時間帯 (Start window) | このタブで、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 3-2　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。<br>p.28 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 3-3　　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。<br>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.29 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 3-4　　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。<br>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。 |
| 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。<br>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。 |

| 除外オプション | 説明 |
| --- | --- |
| 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。<br>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。<br>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。<br>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 3-5　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。 |
| 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。 |

# VMware 資産の保護設定のカスタマイズ

スケジュールバックアップの時間帯や他のオプションなど、保護計画の特定の設定をカスタマイズできます。

- p.26 の「スケジュール」を参照してください。
- p.27 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 資産の保護設定をカスタマイズするには

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. 次の設定を調整します。
   - バックアップ開始時間帯。
     p.26 の「スケジュール」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.27 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。

# 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ブを、保護計画から解除できます。資産のサブスクライブが解除されると、バックアップは実行されなくなります。

**メモ:** 保護計画から資産のサブスクライブを解除するときに、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ブされており、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ブ解除されます。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.112 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.26 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。

4

# マルウェアスキャン

この章では以下の項目について説明しています。



## 作業負荷の種類ごとの資産

このセクションでは、VMware、ユニバーサル共有、およびクラウド VM の資産でマルウェアをスキャンする手順について説明します。

次の前提条件を満たしていることを確認します。

- バックアップが NetBackup 10.1 以降のストレージサーバーで実行された。
- バックアップイメージが、サポート対象のポリシー形式に限り、インスタントアクセス機能のみを備えた MSDP ストレージに格納されている。
- 前回のバックアップが正常に実行されている。
- マルウェアスキャンを実行する権限がある RBAC の役割を持っている。

**サポート対象の資産でマルウェアをスキャンするには、次の手順を実行します。**

1. 左側の[作業負荷 (Workloads)]で、サポートされている作業負荷を選択します。
2. バックアップが完了したリソース (VMware/Cloud VM、ユニバーサル共有など) を選択します。
3. [処理 (Actions)]、[マルウェアのスキャン (Scan for malware)]を選択します。
4. [マルウェアスキャン (Malware scan)]ページで、次の操作を行います。
   - [開始日時 (Start date/time)]と[終了日時 (End date/time)]を選択して、スキャンの日付範囲を選択します。
   - [スキャナホストプール (Scanner host pool)]を選択します
   - [マルウェアスキャンの現在の状態を選択 (Select current status of malware scan)]リストから、次のいずれかを選択します。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- すべて (All)

**5** ［マルウェアのスキャン (Scan for malware)］をクリックします。

**メモ:** マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

**6** スキャンが開始されると、［マルウェアの検出 (Malware Detection)］にマルウェアスキャンの進行状況が表示され、次のフィールドが表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

  **メモ:** 検証で失敗したバックアップイメージは無視されます。

- 処理中 (In progress)
- 保留中 (Pending)

5

# 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の前提条件

インスタントアクセスを使用している場合は、WORM インスタンスが vCenter Server の次のポートにアクセスできることを確認します。

**表 5-1　　ポートの詳細**

| インスタンス | VMware コンポーネント | ポート番号 |
|---|---|---|
| WORM | vCenter | 443 |

## 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、NetBackup Web UI またはインスタントアクセス API を使用してローカルまたはクラウド LSU (論理ストレージユニット) から作成されたバックアップコピーでサポートされます。

クラウド LSU (論理ストレージユニット) でのインスタントアクセスの制限事項については、『NetBackup 重複排除ガイド』を参照してください。

- この機能は、保護計画またはポリシーから作成されたバックアップコピ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。

  Flex WORM ストレージでのインスタントアクセスには、次のサービスが必要です:

  - NGINX、NFS、SAMBA、WINBIND (Active Directory が必要な場合)、SPWS、VPFS
- この機能では、メディアサーバー重複排除プール (MSDP) メディアサーバーまたは WORM ストレージサーバーからの同時マウントポイントが 50 個に制限されます。Flex Appliance を使用している場合、この機能では、各ノードから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。ポリシーの場合、[ディスクを除外 (Exclude Disks)]タブで[除外するディスクなし (No disks excluded)]を選択します。保護計画の場合、[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できる必要があります。
  p.113 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/openv/netbackup/bin/nbwmc stop
- /usr/openv/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。
- イメージからインスタントアクセス VM が作成されている場合、イメージは削除できません。インスタントアクセス機能では、バックアップイメージのデータが使用されます。イメージが期限切れになると、データが利用不能になり、インスタントアクセス VM でデータ損失が起こる可能性があります。インスタンスアクセス VM が削除された後、イメージを期限切れにできます。
- インスタントアクセス機能では、ハードリンクがサポートされません。イメージにハードリンクファイルが含まれている場合にイメージからユニバーサル共有を作成すると、vpfsd では、これらのハードリンクファイルのサイズが 0 バイトと表示されます。
- インスタントアクセスは、vSphere 8.0 からデータセット機能をサポートします。

# 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、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.35 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. マルウェアに感染したイメージをリカバリするには、[マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。

   **メモ:** このオプションは、必要な権限を持つユーザーに対してのみ有効になります。
5. 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。
6. 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書きを許可する (Allow overwrite of existing virtual machine) | 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 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電源をオン (Power on after provisioning) | 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。 |
   | 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。<br>**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。 |
7. [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。

8 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。

9 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.35 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 マルウェアに感染したイメージをリカバリするには、[マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。

**メモ:** このオプションは、必要な RBAC の役割または関連する RBAC 権限を持つユーザーに対してのみ有効になります。

5 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。

6 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。


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概算サイズが表示されます。

7 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。

8 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。

9 [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.35 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 マルウェアに感染したイメージをリカバリするには、[マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。

**メモ:** このオプションは、必要な権限を持つユーザーに対してのみ有効になります。

5 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。

6 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。


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概算サイズが表示されます。

7 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 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/Podman がインストールされている BYO ストレージサーバー。
  - Docker/Podman 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/Podman 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。
  - `policycoreutils` と `policycoreutils-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/Podman 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 5-2 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。<br>■ 64 ビットのプロセッサ。<br>■ 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。<br>■ 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)。<br>■ 32 TB 以上のストレージの場合は 32 GB の RAM。<br>■ 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 5-3 よく寄せられる質問

| よく寄せられる質問 | 回答 |
| --- | --- |
| Docker/Podman 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。<br>1 必要な Docker/Podman のバージョンをインストールします。<br>2 インスタントアクセス機能の使用を開始します。<br>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。 |
| 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。<br>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。<br>2 新しい BYO nginx 構成エントリ `/etc/nginx/conf.d/byo.conf` が、元の `/etc/nginx/nginx.conf` 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。<br>3 コマンド `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo` 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 vpfs-config.log 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。<br>1 Yum ツールを使用して、`policycoreutils` と `policycoreutils-python` パッケージをインストールします。<br>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。<br>■ `semanage port -a -t http_port_t -p tcp 10087`<br>■ `setsebool -P httpd_can_network_connect 1`<br>3 コマンド `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo` 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。<br><br>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。<br><br>**1** RSA の公開鍵と秘密鍵のペアを作成します。<br><br>**2** 証明書の署名要求 (CSR) を作成します。<br><br>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。<br><br>**3** 外部認証局が証明書を作成します。<br><br>**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。<br><br>**5** 次のコマンドを実行して、証明書を再ロードします。<br><br>`/usr/openv/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。<br><br>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。<br><br>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。<br><br>https://access.redhat.com/solutions/20107 |

| よく寄せられる質問 | 回答 |
| --- | --- |
| /var/log/vpfs/vpfs-config.log ファイルの次の問題は、どうすれば解決できますか。<br><br>**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/openv/netbackup/bin/nblibcurlcmd<br><br>failed (1): | 次に示す順序で操作を実行します。<br><br>**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。<br><br>**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。<br><br>/usr/openv/netbackup/bin/bpclntcmd -pn<br><br>**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。<br><br>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo |

# VM マルウェアスキャン

NetBackup Recovery API を使用して、NetBackup イメージからマルウェアスキャンのライブマウントを作成できます。ライブマウントは、NFS または SMB プロトコルを介してすべての VM ファイルとフォルダを即座にエクスポートします。これにより、NFS または SMB クライアントがエクスポートパスをマウントし、エクスポートされた VM ファイルとフォルダにマルウェアスキャンを実行できます。

この機能では、以下のマルウェアスキャン API が提供されます。

- POST /recovery/workloads/vmware/malware-scan-mounts
- GET /recovery/workloads/vmware/malware-scan-mounts
- GET /recovery/workloads/vmware/malware-scan-mounts/{mountId}
- DELETE /recovery/workloads/vmware/malware-scan-mounts/{mountId}。

詳しくは、SORT で NetBackup 10.0.1 API リファレンスを参照してください。

6

# 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.43 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。

NetBackup FlexScale では、インスタントロールバックに必要なソフトウェアパッケージが NetBackup FlexScale 配備に含まれています。詳しくは、『Veritas NetBackup Flex Scale 管理者ガイド』を参照してください。

インスタントロールバックを使用している場合は、WORM インスタンスが vCenter Server と ESXi サーバーの次のポートにアクセスできることを確認します。

**表 6-1　　ポートの詳細**

| インスタンス | VMware コンポーネント | ポート番号 |
|---|---|---|
| WORM | vCenter | 443 |
| WORM | ESXi ホスト | 902 |

## 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、保護計画または従来のポリシーで作成されます。
- この機能は、NetBackup Appliance、NetBackup Virtual Appliance、Build Your Own (BYO) サーバー、および NetBackup FlexScale 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。ポリシーの場合、[ディスクを除外 (Exclude Disks)]タブで[除外するディスクなし (No disks excluded)]を選択します。保護計画の場合、[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
  NetBackup FlexScale の場合、MSDP クラスタ内の各 MSDP エンジンで、ライブマウントの値がデフォルトで 100 に設定されます。
  このデフォルト値は MSDP エンジンの場所
  `/msdp/data/dp1/pdvol/spws/etc/spws.cfg` から変更できます。

---

**メモ:** インスタントロールバック、VMware インスタントアクセス、MSSQL インスタントアクセス、ユニバーサル共有で構成されるライブマウントの合計数が MaxAllowedLivemounts 値を超えてはなりません。

---

- この機能は、仮想マシンのデータセット機能の追加、削除、更新をサポートしません。インスタントロールバック機能は、データセットをロールバックしません。

# 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。<br>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。<br>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。<br>3. マルウェアに感染したイメージをリカバリするには、[マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。<br>**メモ:** このオプションは、必要な権限を持つユーザーに対してのみ有効になります。<br>4. 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。

  **メモ:** NetBackup は、マルウェアに感染したイメージに関する警告を表示します。
- マルウェアに感染したイメージをリカバリするには、[マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。

**メモ:** このオプションは、必要な権限を持つユーザーに対してのみ有効になります。

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。
   - マルウェアに感染したイメージをリカバリするには、［マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)］を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。
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。

7

# 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。

# CDP の用語

次の表に、継続的なデータ保護 (CDP) で使用される概念と用語を示します。

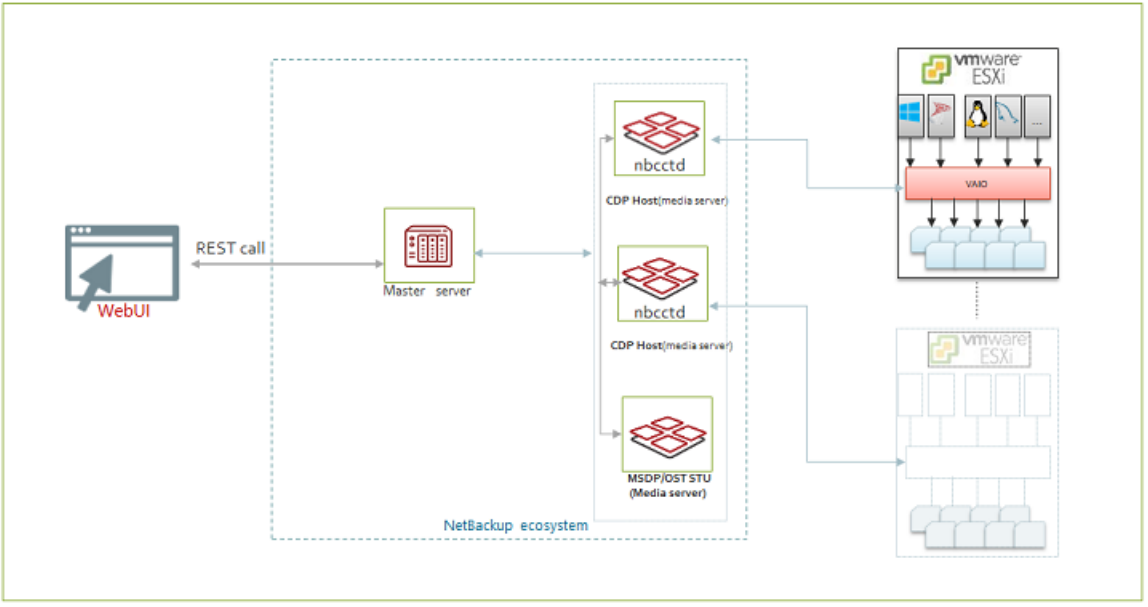
**表 7-1** CDP の用語

| 用語 | 説明 |
|---|---|
| CDP ゲートウェイ | CDP が構成されたメディアサーバーです。 |
| VAIO | I/O フィルタリング用 vSphere API で構成される VMware フレームワークです。このフレームワークを使用すると、CDP は ESXi Server でフィルタを実行し、ゲストオペレーティングシステムから仮想ディスクへの I/O 要求を傍受できます。 |
| 完全同期 | NetBackup が ESXi から VM のデータ全体をフェッチします。 |
| OST | OpenStorage 技術 (Open Storage Technology) は、NetBackup がサポートする STU です。 |
| MSDP | メディアサーバー重複排除ストレージプール (Media Server Deduplication Storage Pool) は、バックアップストレージを最適化するための NetBackup の重複排除技術エンジンです。 |
| ストレージポリシー | 管理者がストレージプロファイルを作成できる VMware vSphere の機能です。これにより、VM を個別にプロビジョニングする必要がなくなり、管理を自動化できます。 |
| VIB | vSphere Installation Bundle。概念レベルでは、VIB は tarball または圧縮アーカイブに類似しています。VIB は単一のアーカイブにパッケージ化されたファイルのコレクションで、容易に配布できます。 |
| nbcctd | CDP ゲートウェイで実行されている CDP サービス (デーモン) です。 |
| ステージング領域 | ESXi から受信した I/O を NetBackup が一時的に格納する CDP ゲートウェイ上のストレージの場所です。 |
| ストレージクォータ | CDP 保護を使用する VM に割り当てられたストレージサイズの制限です。 |
| 予約済みクォータ | CDP ゲートウェイに登録されているすべての VM で共有されるストレージです。 |
| VADP | VMware VADP は、vSphere 仮想マシン (VM) をバックアップおよびリストアする VMware vStorage API です。 |

# CDP アーキテクチャ

CDP ゲートウェイは、NetBackup メディアサーバー上で構成されます。構成が完了したら、NetBackup は CDP ゲートウェイで nbcctd デーモンを起動します。このプロセスが ESX からのすべての I/O を処理して、ゲートウェイのその他の NetBackup コンポーネントがバックアップを作成できるようにします。このデータをバックアップするには、MSDP または OST アクセラレータベースの STU も構成する必要があります。必要に応じて、複数の CDP ゲートウェイと MSDP/OST アクセラレータベースの STU を構成できます。CDP 用の NetBackup REST API は、この機能を活用する Web API インターフェースです。詳しくは、NetBackup REST API Swagger のマニュアルを参照してください。

**図 7-1** CDP アーキテクチャ




# 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。
- 従来の VADP ベースのバックアップと CDP を VMware に使用できます。バックアップイメージは互いに独立しており、増分バックアップまたはリカバリのために別々に処理されます。
- 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 Red Hat 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 を起動できます。
- 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のライセンス。
- 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。VM から Veritas IO フィルタストレージポリシーを切断すると、VM の IO タッピングが停止するため、この VM のデータは CDP ゲートウェイに保存されません。そのため、その結果として生じるバックアップジョブは、CDP ステージング領域のすべてのデータがバックアップストレージに移動された後も空白のままです。このため、VM から vtstap ポリシーを切断したら、NetBackup 保護計画から VM の保護を削除することをお勧めします。

---

# 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 を構成する手順

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。ストレージの構成方法について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。
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 ゲートウェイからの VM の削除

VM で CDP 保護が不要になった場合は、その VM から保護を削除するか、VM を従来のポリシーに切り替えることができます。

**VM から CDP 保護を削除するには**

1. vCenter に移動し、VM のストレージポリシーを `vtstap` から**データストアのデフォルト**に変更します。
2. NetBackup Web UI の左側の[作業負荷 (Workloads)]で[VMware]をクリックすると、VM のリストが保護の詳細を含めて表示されます。
3. 保護を削除する VM の名前をクリックします。その後のページで、[保護の削除 (Remove protection)]をクリックします。

   VM が削除されるときに確認メッセージが表示されます。

VM から `vtstap` ポリシーを削除せずに VM の保護を削除すると、部分的に成功した削除についてのメッセージが UI に表示されます。これらの部分的に削除された VM は、[継続的なデータ保護ゲートウェイ (Continuous Data Protection Gateway)]タブの[サブスクライブ済みの VM の合計数 (Total VMs subscribed)]のカウントには含まれません。

---

**メモ:** 部分的に削除された VM は、CPD によっても従来のポリシーによっても保護されません。また、CDP ゲートウェイに VM を再サブスクライブすることもできません。そのため、VM から `vtstap` ストレージポリシーを分離し、CDP ゲートウェイから VM のサブスクライブを完全に解除することをお勧めします。

---

# 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。

---

**メモ:** CDP ゲートウェイを定義する前に、システム時間とネットワーク時間が同期していることを確認します。

---

**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、root 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 次のページに進み、ゲートウェイのバージョンが 9.1 の場合は、次の表で説明するパラメータ[並列実行ジョブの最大数 (Maximum number of concurrent jobs)]を指定し、[保存 (Save)]をクリックしてゲートウェイを保存します。

ゲートウェイのバージョンが 10.0 の場合は、[詳細 (Advanced)]をクリックして詳細パラメータを指定し、CDP ゲートウェイを構成して微調整します。このパラメータのセットを使用して、ゲートウェイの特定の構成で CDP 保護を使用して何台の VM をサポートできるかを概算することもできます。

| パラメータ | 説明 |
|---|---|
| 並列実行ジョブの最大数 (Maximum number of concurrent jobs) | ゲートウェイで同時に実行できる CDP ジョブの最大数。数値が大きいと、ピーク時のリソース消費が高くなる可能性があります。 |
| 同時初期同期の最大数 (Maximum number of simultaneous initial sync) | CDP 保護の初期フェーズで、完全バックアップを同時に実行できる VM の数。デフォルト値より高い値を指定すると、リソース消費が増加し、既存の保護に影響する可能性があります。 |
| 継続的なデータ保護の予約済みメモリ (Reserved memory for Continuous data protection) | ゲートウェイ用の予約済みメモリ。合計物理メモリの 90% 以下の値を GB 単位で入力します。 |
| VM ごとのデータステージング領域 (Data staging area per VM) | 各 VM のストレージを指定します。 |
| 予約済みのステージング領域 (Reserved staging area) | VM の I/O スパイクを処理する追加のストレージ領域。 |

5 [VM の数を概算 (Estimate the number of VMs)]をクリックし、この指定した構成についてこのゲートウェイが何台の VM をサポートできるかを計算します。

6 [保存 (Save)]をクリックして、ゲートウェイを追加します。

# サイズ調整の注意事項

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調整の要件について説明します。

**メモ:** CDP ゲートウェイを使用して多数の 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。NetBackup バージョン 10.0 以降では、UI でこの値を構成できます。

## ゲートウェイのサイズ調整

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 I/O 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開始して、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。バージョン 10.0 以降でそれを行う方法については、p.59 の「CDP ゲートウェイの定義」を参照してください。。NetBackup 9.1 では、`nbcct.conf` ファイルでこの値を再構成できます。

**NetBackup 9.1 で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. *<stagginglocation>*`/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_SIZE_IN_MB* と *CCT_VM_QUOTA_RESERVE_PERCENT* に必要な値を入力します。
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。したがって、40 x 160 MB = 6400 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 x 10 GB = 400 GB (75%) + 予約済み 134 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 サービスが開始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:** I/O デーモンからの I/O 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。NetBackup 10.0 以降でメモリ内キャッシュのサイズを増やす方法については、p.59 の「CDP ゲートウェイの定義 」を参照してください。。NetBackup 9.1 では、`nbcct.conf` ファイルの *CCT_POOL_SIZE_QUOTA_PERCENTAGE* パラメータを使用して、それを行うことができます。

---

# 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 がキューに残ります。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。

NetBackup バージョン 10.0 以降でそれを行う方法については、p.59 の「CDP ゲートウェイの定義 」を参照してください。。NetBackup 9.1 の場合は、次に示す手順に従います。

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、完全同期を手動で開始できます。

- 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開始できます。

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。

## 完全同期の構成

NetBackup バージョン 10.0 以降で完全同期を構成する方法については、p.59 の「CDP ゲートウェイの定義 」を参照してください。。

NetBackup 9.1 では、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関する多くの情報が利用可能です。

NetBackup ダッシュボード

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ます。

## 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 7-2 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接続を一時的に切断しています。割り当てられたステージング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ジング領域にほとんど空きがないため、CDP サービスが一時的に IO フィルタから切断されます。<br>バックアップジョブが CDP ゲートウェイのステージングデータベースからバックアップストレージにデータを移動できない場合には、これも発生する可能性があります。<br>バックアップジョブの失敗の理由と STU の基礎となるストレージを確認します。 | 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 サービスはステージング場所で IO を実行できません。 | エラー | 高 |
| ステージング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.) | ステージング領域が 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、ステージング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 のストレージクォ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、次回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 が起動しない場合があります。

# CDP の制限事項

CDP の制限事項は、次のとおりです。

- インテリジェントポリシー、今すぐバックアップ、Web UI からすぐにロールバックなどの NetBackup の機能はサポートされません。
- VMware 向けの CDP と Veritas Resiliency Platform は、同じ VM に対して併用できません。ただし、どちらの製品も同じ vCenter クラスタ上の異なる VM を保護できます。
- CDP は、どの VC によっても管理されていないスタンドアロン ESX はサポートしません。ESXi クラスタの一部ではなく、VC によって管理されている ESXi もサポートしません。
- CDP ベースの保護計画にサブスクライブする前と、最初の完全バックアップの際に、VM をオンにする必要があります。
- CDP バックアップポリシーに VM をサブスクライブした後、VM からディスクを削除するか、新しいディスクを追加すると、以降のバックアップが失敗します。このような場合は、CDP の保護から VM のサブスクライブを解除し、再度サブスクライブします。
- VMware の制限により、VMware 用 NetBackup エージェントと CDP を両方同時に使用して VM を保護しようとすると、エラーでバックアップ操作が失敗するか、VDDK のシンボルで操作がクラッシュする場合があります。

# 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 サーバーの 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。次回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と、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: 以下から `nbcct` ディレクトリを削除した後、操作を再試行します。

- NetBackup 9.1 では、`<NBU installation path>/netbackup/nbcct`。
- NetBackup 10.0 以降では、`<staginglocation>/nbcct`。

## CDP ベースの保護計画が次のエラーで失敗する: IO タッピングに登録される仮想マシンの 1 つ以上の仮想ディスクにストレージポリシーが設定されていません。(Storage policy is not attached to one or more virtual disks of virtual machine to be registered for IO tapping.)

考えられる理由:

現在、NetBackup は CDP のストレージポリシーとして vtstap ポリシーのみをサポートします。ハイブリッドストレージポリシー (暗号化 + レプリケーション) を使用して VM をサブスクライブしようとすると、エラーが表示されます。

回避方法: CDP で保護されている VM にハイブリッドストレージポリシー (暗号化 + レプリケーション) を使用しないようにします。

## メディアサーバーの再起動またはマウントパス関連の変更後に CDP サービスが開始されません。

考えられる理由:

構成されたステージング領域が、再ブート後にマウント解除されるか、サポートされていないファイルシステムを持っています。たとえば、サポートされているマウント (`/mnt/stage_area` など) を使用して CDP ゲートウェイを構成し、自動マウントを構成しない場合です。システムの再起動後、このパスは CDP がサポートしない root ファイルシステムを指しているため、CDP サービス (nbcctd) を開始できません。

回避方法: マウント解除またはシステムの再ブートに関連するシステム変更を加えるたびに、ステージング領域または関連するディスクマウントが正しく再マウントされていることを確認します。

## 電源がオフの状態で、I/O タッピングポリシーが VMDK に設定されている場合に VM のサブスクライブを解除すると、ストレージポリシーを削除してからサブスクライブを解除するように警告されます。

考えられる理由:

CDP 保護を削除するときに、保護対象の VM の電源がオフの場合、CDP ゲートウェイは VAIO からストレージポリシーの必要な情報を取得できません。そのため、CDP 保護は VM から削除されますが、I/O タッピングポリシーはその VM の VMDK に設定されたままになり、引き続き I/O がタップされ、パフォーマンスに影響します。

回避方法: 電源の状態がオンかオフかにかかわらず、VM のサブスクライブを解除する前に、必ず VM のストレージポリシーを設定解除します。

## NetBackup 保護計画へのサブスクリプションは失敗しますが、バックアップジョブはステージング領域にデータをダンプし続けます。

説明

同じプライマリサーバーの保護計画を使用して、NetBackup プライマリサーバーを保護すると発生します。

回避方法: 同じプライマリサーバーを使用して作成された保護計画を使用して、NetBackup プライマリサーバーを保護することはお勧めしません。このエラーが発生した場合は、NetBackup プライマリサーバー VM から Veritas ストレージポリシーを切断し、保護計画から VM のサブスクライブを解除します。

## CDP ゲートウェイにアクセスできない場合、CDP 保護計画を削除できない

説明:

ホストにアクセスできない場合にエントリを削除しても、CDP ポリシーは削除されません。

回避方法: CDP 保護計画のサブスクリプションが削除されないのは、CDP ホストのクリーンアップ前に CDP ポリシーを削除しないからです。そのため、アクセスできないゲートウェイのエントリを削除するには、CDP ゲートウェイ削除 API を呼び出した後、ポリシー削除 API を手動で呼び出す必要があります。

次の API を使用して、アクセスできない CDP ゲートウェイをクリーンアップできます。

```
To DELETE CDP Gateway

URL : https://netbackup/config/cdp-gateway/force

HTTP Method : DELETE

Headers:

    Authorisation: Bearer <Token>

    Content-Type:
application/vnd.netbackup+json;version=7.0;charset=UTF-8

To Delete Policy

URL : https://netbackup/config/policies/policy_name

HTTP Method : DELETE

Headers:

    Authorisation: Bearer <Token>
```

上記の 2 つの API が正常に実行された後も、ポリシーと VM のマッピングは Web UI に表示されます。その VM の保護を Web UI から削除しようとすると、エラーメッセージ[サブスクリプション ID が見つかりません (Subscription ID not found)]が表示されます。これは想定される動作です。

## CDP ゲートウェイの更新操作で、ゲートウェイでの CDP サービス (nbcctd) の再起動に失敗する

説明: CDP ゲートウェイの更新操作でサービスの再起動が試行されます。サービスの停止に通常より長い時間がかかる場合は、更新操作で CDP サービス (nbcctd) の再起動に失敗したことを示すエラーが表示されます。

回避方法: この場合は、nbcctd サービスがゲートウェイで実行されているかどうかを確認します。サービスが実行中の場合は、停止するまで待機します。サービスを手動で停止するには、次のコマンドを使用します: `/usr/openv/netbackup/bin/nbcctd -terminate`。サービスが停止したら、コマンド `/usr/openv/netbackup/bin/nbcctd -x` を使用してサービスを起動します。

## ストレージプラットフォーム Web サービス (SPWS) からのバージョンの取得に失敗しました。選択した MSDP ストレージサーバーで、Nginx が実行され、正しく構成されていることを確認してください。(Failed to get version from the Storage Platform Web Service (SPWS). Ensure that Nginx is running and configured correctly on the selected MSDP storage server.)

説明: ユニバーサル共有を使用するために CDP 保護計画を作成するときに、ユニバーサル共有機能がないストレージデバイスを選択すると、このエラーが表示されます。

回避策: ユニバーサル共有機能を備えたストレージデバイスを選択する必要があります。

## ユニバーサル共有を含む CDP ゲートウェイのバージョンがサポートされていません。サポートされるバージョンは 10.2 以降です。(Minimum supported version is 10.2.)

説明: ユニバーサル共有を使用するために CDP 保護計画を作成するときに、NetBackup バージョン 10.2 より前の CDP ゲートウェイサーバーを選択すると、このエラーが表示されます。

回避策: ユニバーサル共有を使用するには、CDP ゲートウェイのバージョンが NetBackup バージョン 10.2 以降である必要があります。

8

# 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

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. マルウェアに感染したイメージをリカバリするには、[マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージが含まれるリカバリポイントでのみ使用できます。

   **メモ:** このオプションは、必要な権限を持つユーザーに対してのみ有効になります。
5. 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して[リカバリ (Recover)]をクリックします。

**6** 実行するリカバリの種類を選択します。

- [仮想マシンのリストア (Restore virtual machine)]: 元の場所か代替の場所にバックアップイメージをリカバリします。
- [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.38 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.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.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リストア」を参照してください。

**7** [リストア先 (Restore to)]タブで、次の操作を行います。

- [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。
- [データストアまたはストレージポリシーを使用する (Use datastore or storage policy)]から適切なオプションを選択します。
  - 元の場所にリカバリするには、[次へ (Next)]をクリックします。

- 代替の場所にリカバリする場合は、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。

詳しくは、p.76 の「ストレージポリシー」を参照してください。

**8** [オプション (Options)]を確認または変更します。

p.77 の「リカバリオプション」を参照してください。

**9** [詳細 (Advanced)]オプションを確認または変更します。

p.77 の「高度なリカバリオプション」を参照してください。

p.78 の「高度なリカバリオプション: リストアされる仮想ディスクのフォーマット」を参照してください。

p.79 の「高度なリカバリオプション: トランスポートモード」を参照してください。

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

NetBackup がクレデンシャルを検証し、パスと接続が適切かどうかを確認します。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します。

**11** 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。

**12** [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。

# ストレージポリシー

仮想マシンのストレージポリシーは、仮想マシンに提供されるストレージ形式を制御します。VM 全体に 1 つのストレージポリシーを適用するか、VM のホームディレクトリや仮想ディスクに異なるストレージポリシーを適用できます。

## 仮想マシン全体への適用

| | |
|---|---|
| ストレージポリシーの選択 (Select storage policy) | 選択した vCenter Server に関連付けられているすべてのストレージポリシーのリストから、仮想マシン全体に適用するストレージポリシーを選択します。 |
| データストアまたはデータストアクラスタ (Datastore or datastore cluster) | 選択したストレージポリシーと互換性があるデータストアを選択します。 |

## 仮想マシンのカスタマイズ

| | |
|---|---|
| 仮想ディスク (Virtual disk) | バックアップ時にキャプチャされた VM のホームディレクトリまたは仮想ディスクと、関連付けられたストレージポリシー情報を一覧表示します。 |
| ストレージポリシー (Storage policy) | 選択した vCenter Server に関連付けられているすべてのストレージポリシーのリストから、VM ホームディレクトリまたは仮想ディスクに適用するストレージポリシーを選択します。 |
| データストア、クラスタ、またはパス (Datastore or cluster or path) | 選択したストレージポリシーと互換性があるデータストアを選択します。 |

# リカバリオプション

| | |
|---|---|
| 既存の仮想マシンの上書きを許可 (Allow overwrite of existing virtual machine) | NetBackup は、宛先に同じ表示名の VM が存在する場合、リカバリを開始する前にその VM を削除します。NetBackup が削除するのは同じ表示名を持つ VM であることに注意してください。これは同じ VM ではなく、同じ表示名を持つ別の VM である可能性があります。 |
| リカバリ後に電源をオン (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。 |

# 高度なリカバリオプション

| | |
|---|---|
| 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。<br>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。

## 高度なリカバリオプション: 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。<br>**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。 |

## 高度なリカバリオプション: トランスポートモード

トランスポートモードは、バックアップに使用する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。

トランスポートモードを選択する場合は、次の点に注意してください。

- SAN 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 モードの場合、VVols を使用する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。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。

# VMware Cloud Director 仮想マシンのリカバリ

VM が VMware Cloud Director からバックアップされている場合、VMware Cloud Director にのみ仮想マシン (VM) をリカバリできます。

**VMware Cloud Director VM をリカバリするには**

1. [作業負荷 (Workloads)]、[VMware]を選択し、リカバリする仮想マシンを選択します。
2. [リカバリポイント (Recovery points)]タブで[リカバリ (Recover)]、[仮想マシンのリストア (Restore virtual machine)]を選択します。
3. [リカバリターゲット (Recovery target)]ページで VM を VMware Cloud Director または vSphere にリストアすることを選択します。
   - vSphere を選択する場合は、次の情報を参照してください。
     p.74 の「VM のリカバリ」を参照してください。。
   - VMware Cloud Director を選択した場合は、この手順を続行します。

4 [リカバリターゲット (Recovery target)]ページで VMware Cloud Director と vSphere のリカバリ先情報を指定します。

- 表示されるデフォルト値は、VM を元の場所にリストアします。
- VMware Cloud Director のリカバリ先情報のいずれかを変更する場合は、vSphere リカバリ先情報を更新する必要があります。
- VMware Cloud Director のデフォルトのリカバリ先情報を受け入れる場合は、vSphere リカバリ先情報を必要に応じて変更できます。

[次へ (Next)]をクリックします。

5 [vApp オプション (vApp options)]画面で vApp 情報を指定します。

- 既存の vApp にリストアするには、vApp のリストを参照するか、存在する vApp の名前を入力します。
- 新しい vApp にリストアするには、新しい vApp の名前を入力します。
- vApp が VMware Cloud Director に存在しない場合、[状態 (Status)]には[新規 (New)]と表示されます。新しい vApp が作成されます。

[次へ (Next)]をクリックします。

6 [リカバリオプション (Recovery options)]ページでリストアのリカバリオプションを指定して[次へ (Next)]をクリックします。

7 [レビュー (Review)]画面は選択内容の概略を示します。リカバリ前チェックでは、選択したオプションのいずれかに問題があるかどうかを判断します。表示されたエラーは上書きできますが、エラーに対処しないとリカバリは失敗する可能性があります。

9

# VMware エージェントレスリストア

この章では以下の項目について説明しています。



## 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 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、root、または sudo 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

VMware エージェントレスリストアには、次の前提条件があります。

- 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、root 権限、または sudo 権限があるクレデンシャルが必要です。
- 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 の最新バージョン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、利用可能な LUN がある準仮想コントローラが少なくとも 1 つ必要です。または、準仮想 SCSI コントローラに利用可能な領域があるようにします。

- Linux ターゲット VM でルート以外のクレデンシャルを使用するには、sudo がインストールされ、ユーザーが次の権限を持つように /etc/sudoers ファイルが構成されている必要があります。

```
username ALL=(ALL) NOPASSWD: /bin/tar SETENV: /usr/openv/tmp/rt/netbackup/bin/nbtar_rt
```

または

```
username ALL=(ALL) NOPASSWD: ALL
```

- 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 tmp ディレクトリ (/tmp) 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。
- ファイルとフォルダのリカバリにインスタントアクセスの使用を許可する場合は、リカバリポイントがインスタントアクセスをサポートしている必要があります。
p.38 の「インスタントアクセス VM の作成」を参照してください。

## 制限事項

VMware エージェントレスリストアには、次の制限事項があります。

- 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。
- NetBackup がステージングディレクトリを使用できない場合、リストアジョブは失敗します。このディレクトリは、TMP または TEMP の環境変数で指定します。
- 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、リストアジョブは失敗します。または、ステージングディレクトリに十分な領域がない場合にも失敗します。

- [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、リストアは成功します。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。0 (ゼロ) 以外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。
- ターゲット VM について NetBackup がサポートするゲストオペレーティングシステムの最新リストについては、次のドキュメントの「Supported guest operating systems for VMware」を参照してください。
  『Support for NetBackup in virtual environments』

# ゲスト VM へのエージェントレス単一ファイルリカバリのクレデンシャルへのアクセスの提供

ゲスト VM に対してエージェントレス単一ファイルリカバリを実行する VMware 管理者が、ゲスト VM のクレデンシャルにアクセスできない場合があります。RBAC の役割を使用して、あるクレデンシャルにユーザーアクセス権を付与できます。ユーザーは、次のいずれかの方法を使用することで、保存されたクレデンシャルを使用してリカバリを実行できるため、VM の実際のユーザー名とパスワードを知る必要はありません。

p.85 の「VMware ゲスト VM のクレデンシャルの追加」を参照してください。

**メモ:** このクレデンシャル形式は VMware サーバー用ではありません。[作業負荷 (Workloads)]、[VMware]の[VMware サーバー (VMware servers)]タブでこれらのクレデンシャルを構成します。

次の方法で、あるクレデンシャルにユーザーアクセス権を付与できます。

- [デフォルトの VMware 管理者 (Default VMware Administrator)]の役割にユーザーを追加します。この RBAC の役割により、ユーザーはすべてのクレデンシャルを表示し、リカバリに任意のクレデンシャルを使用できます。
- 限られた数のクレデンシャルへのアクセス権を持つカスタム役割を作成します。その後、その役割にユーザーを追加します。
  p.86 の「ゲスト VM へのエージェントレス単一ファイルリカバリのカスタム役割の作成 (クレデンシャルを使用)」を参照してください。

## VMware ゲスト VM のクレデンシャルの追加

この種類のクレデンシャルを使用すると、ゲスト VM のクレデンシャルをクレデンシャル管理に保存できます。VMware 管理者アクセスをこのクレデンシャルに付与できます。このユーザーは、保存されたクレデンシャルを使用してゲスト VM にエージェントレスシングルファイルリカバリを実行できます。VM の実際のユーザー名とパスワードを知っている必要はありません。

**メモ:** このクレデンシャル形式は VMware サーバー用ではありません。[作業負荷 (Workloads)]、[VMware]の[VMware サーバー (VMware servers)]タブでこれらのクレデンシャルを構成します。

p.10 の「VMware サーバーの追加」を参照してください。

**VMware ゲスト VM のクレデンシャルを追加するには**

1. 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
2. [指定したクレデンシャル (Named credentials)]タブで[追加 (Add)]をクリックします。
3. 次のプロパティを指定します。
   - クレデンシャル名 (Credential name)
   - タグ (Tag)
   - 説明 (Description)
     例:「このクレデンシャルは VMware ゲスト VM へのリカバリに使用されます。」
4. [次へ (Next)]をクリックします。
5. VMware ゲスト VM を選択します。

6 認証に必要なクレデンシャルの詳細を入力します。

7 [次へ (Next)]をクリックします。

8 クレデンシャルへのアクセス権を付与する役割を追加します。

- [追加 (Add)]をクリックします。
- 次のいずれかの役割を選択します。
  デフォルトの VMware 管理者の役割。この役割には、作成されたすべてのクレデンシャルへのアクセス権があります。
- VMware の単一ファイルリカバリ操作を実行するために必要な権限を持つ別の役割。
  役割には、最低でも表示とクレデンシャルの割り当ての権限が必要です。

9 [次へ (Next)]をクリックし、プロンプトに従ってウィザードを完了します。

## ゲスト VM へのエージェントレス単一ファイルリカバリのカスタム役割の作成 (クレデンシャルを使用)

カスタム役割を使用すると、VM 管理者は、保存されたクレデンシャルを使用してゲスト VM にエージェントレス単一ファイルリカバリを実行できます。このようにすると、ユーザーが VM の実際のユーザー名とパスワードを知っている必要がありません。

ユーザーにデフォルトの VMware 管理者の役割を割り当てない場合は、この役割を使用します。または、すべてのクレデンシャルへのアクセス権をユーザーに付与しない場合にも使用します。

**ゲスト VM へのエージェントレス単一ファイルリカバリのカスタム役割をクレデンシャルを使用して作成するには**

1 ゲスト VM のユーザー名とパスワードを含むクレデンシャルが存在する必要があります。

p.85 の「VMware ゲスト VM のクレデンシャルの追加」を参照してください。

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。

2 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]をクリックします。

3 [デフォルトの VMware 管理者 (Default VMware Administrator)]を選択し、[次へ (Next)]をクリックします。

4 [役割名 (Role name)]と説明を指定します。

たとえば、この役割でユーザーが特定のゲスト VM に対して単一ファイルリカバリを実行できるという説明を含めます。

5 [クレデンシャル (Credentials)]で、[編集 (Edit)]をクリックします。

6 [新規と既存のクレデンシャルに権限を適用します。(Apply permissions to new and existing credentials)]オプションのチェックマークをはずします。

7 この役割に追加するクレデンシャルを選択します。次に[割り当て (Assign)]をクリックします。

この役割を持つユーザーは、選択した各クレデンシャルにアクセスできます。

8 [ユーザー (Users)]で、[編集 (Edit)]をクリックします。次に、この RBAC の役割を付与するユーザーを追加します。

9 役割の構成が完了したら、[役割の追加 (Add role)]をクリックします。

# 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

この種類のリストアには、ゲスト VM のクレデンシャルを指定する必要があります。または、NetBackup のクレデンシャル管理に保存されている VMware ゲスト VM のクレデンシャルへのアクセス権を持っていることが必要です。詳しくは、NetBackup 管理者にお問い合わせください。

**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 ターゲットマシンの電源がオンになっていることを確認します。

2 左側で[作業負荷 (Workloads)]、[VMware]の順にクリックします。

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、[リカバリ (Recover)]、[ファイルとフォルダをリストアする (Restore files and folders)]の順に選択します。

6 [ファイルを追加 (Add files)]ページで[追加 (Add)]をクリックし、リカバリするファイルとフォルダを選択します。[次へ (Next)]をクリックします。

正しいディレクトリ構造が表示されない場合は、[インスタントアクセスに切り替え (Switch to instant access)]をクリックします。リカバリポイントではインスタントアクセスがサポートされている必要があることに注意してください。それでも期待するファイルとフォルダが表示されない場合は、最初からやり直して、別のリカバリポイントを選択します。

p.38 の「インスタントアクセス VM の作成」を参照してください。

インスタントアクセスに切り替えると、選択したすべてのファイルが削除され、すべてのリカバリオプションがリセットされます。インスタントアクセスを使用して、ファイルとフォルダの新しいリカバリが開始されます。エージェントレス単一ファイルリカバリに再度切り替える場合は、リカバリウィザードをキャンセルしてから再開する必要があります。

7 エージェントレスのリカバリ形式を選択し、ファイルとフォルダをリカバリするターゲットマシンを指定します。

8 ターゲットゲスト VM のクレデンシャルを入力します。または、[既存のクレデンシャルの選択 (Select existing credentials)]をクリックして、使用するクレデンシャルを選択します。

9 [次へ (Next)]をクリックします。

10 [リカバリオプション (Recovery options)]ページで、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。[次へ (Next)]をクリックします。

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。

11 [確認 (Review)]ページで、リカバリ前チェックの状態と選択したリカバリオプションを確認します。内容が正しいことを確認したら、[リカバリの開始 (Start recovery)]をクリックします。

# 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¥temp¥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。

10

# 個々のファイルとフォルダのリストア

この章では以下の項目について説明しています。



## 個々のファイルのリストアについて

NetBackup 10.3 以降では、VM バックアップイメージから NetBackup クライアントソフトウェアがインストールされているコンピュータへの個々のファイルとフォルダのリストアがサポートされています。

VMware エージェントレスリストアを使用して個々のファイルとフォルダをリストアするには、p.87 の「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」を参照してください。

インスタントアクセスを使用して個々のファイルとフォルダをリストアするには、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リストア」を参照してください。

## 個々のファイルとフォルダのリストアの前提条件と制限事項

前提条件:

- ターゲットコンピュータに NetBackup クライアントソフトウェアがインストールされている必要があります。

- 個々のファイルおよびフォルダのリカバリは、[VM バックアップからのファイルリカバリを有効にする (Enable file recovery from VM backup)]ポリシーオプションが有効な場合に、完全バックアップと増分バックアップからサポートされます。

制限事項:

- インスタントアクセスでは、NetBackup クライアントへのファイルとフォルダのリストアはサポートされていません。

# 個別のファイルとフォルダのリカバリ

**個別のファイルとフォルダをリカバリするには**

1. 左側で[作業負荷 (Workloads)]、[VMware]の順に選択します。
2. 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。
3. [リカバリポイント (Recovery points)]タブをクリックし、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. リカバリするイメージで、[リカバリ (Recover)]、[ファイルとフォルダをリストアする (Restore files and folders)]の順に選択します。
5. [ファイルを追加 (Add files)]ページで[追加 (Add)]をクリックし、リカバリするファイルとフォルダを選択します。[追加 (Add)]をクリックし、[次へ (Next)]をクリックします。
6. [リカバリターゲット (Recovery target)]ページで、[ターゲットマシン (Target machine)]フィールドをクリックします。[NetBackup クライアント (NetBackup client)]のリカバリ形式を選択し、ファイルとフォルダをリカバリするターゲットコンピュータを選択します。[選択 (Select)]をクリックします。リストアターゲットオプションを選択します。[次へ (Next)]をクリックします。
7. [リカバリオプション (Recovery options)]ページで、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。[次へ (Next)]をクリックします。
8. [確認 (Review)]ページで、リカバリに選択したオプションを確認します。内容が正しいことを確認したら、[リカバリの開始 (Start recovery)]をクリックしてリカバリを開始します。

11

# ハードウェアスナップショットとレプリケーションを使用した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。



## 仮想マシンとハードウェアスナップショットについて

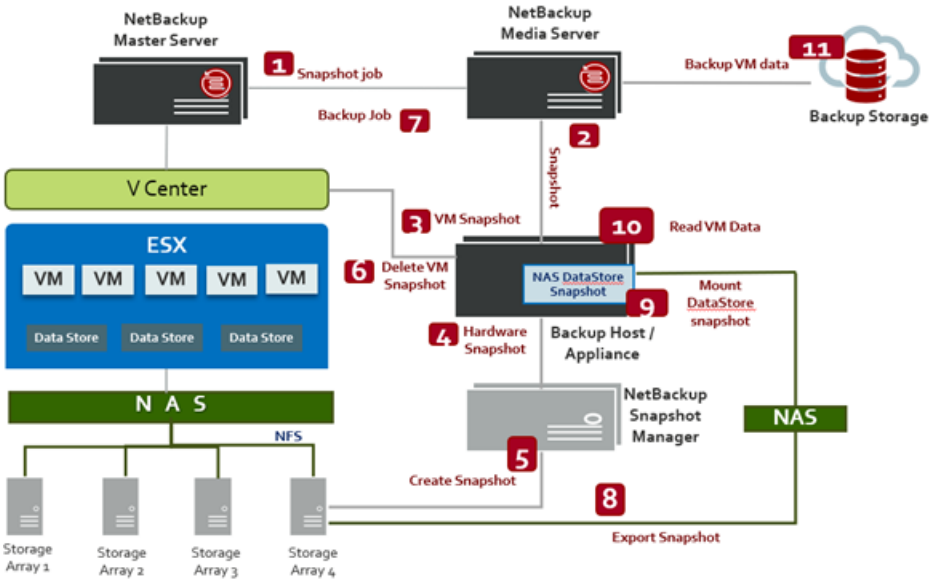
VMware のハードウェアスナップショットベースのソリューションでは、VMware 仮想マシンを保護するために、ストレージアレイスナップショットを使用します。ハードウェアスナッ

プショットを使用する利点は、仮想マシンに影響を与える時間が短縮されることです。VM スナップショットは、ハードウェアスナップショットの期間中のみ保持されます。

このソリューションでは、NetBackup Snapshot Manager を使用して、ハードウェアスナップショットを実行します。NetBackup Snapshot Manager について詳しくは、『NetBackup™ Snapshot Manager for Data Center 管理者ガイド』を参照してください。

# 配備とアーキテクチャ

次の図は、VMware ハードウェアのスナップショットベースのソリューションの配備とアーキテクチャを示しています。




**メモ:** このソリューションでは、NAS ストレージで作成された VMware データストアのみがサポートされます。SAN ストレージで作成される VMware データストアは、サポートされていません。

サポート対象のすべての NAS ストレージアレイについては、『NetBackup ハードウェアおよびクラウドストレージ互換性リスト (HCL)』の「スナップショットソリューション」にある「NetBackup Snapshot Manager」セクションを参照してください。

# サポートされる機能とアプリケーション

VMware のハードウェアスナップショットベースの保護では、仮想マシンのスナップショットとレプリケートした複製を保護するために次の機能を備えています。

- 非常に短い時間での仮想マシンのハードウェアスナップショットを作成します。
- プライマリの場所のスナップショットからと、リモートの場所でのレプリケートされたスナップショットから、仮想マシンをバックアップします。
- プライマリの場所のスナップショットからと、リモートの場所でのレプリケートされたスナップショットから、仮想マシンを Block Level Incremental バックアップ (BLIB) します。
- プライマリの場所のスナップショットからと、リモートの場所でのレプリケートされたスナップショットから、アクセラレータを有効にして仮想マシンをバックアップします。
- 仮想マシンのスナップショットの参照をサポートします。
- スナップショットにある vmdk ファイルから仮想マシンをリストアします。
- スナップショットにある個々の vmdk をリストアします。
- スナップショットの vmdk ファイルから個々のファイルをリストアします。
- ストレージライフサイクルポリシー (SLP) をサポートします。
- ［アプリケーション保護 (Application Protection)］では、VMware ポリシーで次のアプリケーションがサポートされています。
  - Microsoft Exchange データベース
  - Microsoft SQL Server

# ハードウェアスナップショットとレプリケーションの前提条件

ハードウェアスナップショットベースのサポートの前提条件を次の表で説明します。

**表 11-1　　ハードウェアスナップショットサポートの前提条件**

| サポートパラメータ | 説明 |
|---|---|
| システム | ■ サポートされているすべての NetBackup プライマリサーバー、メディアサーバーのプラットフォーム。<br>■ VMware のバックアップホストは、RHEL、SUSE、または Windows である必要があります。<br>■ Snapshot Manager サーバーは、以下のオペレーティングシステムプラットフォームでサポートされています。<br>　■ Ubuntu 16.04 および 18.04 Server LTS<br>　■ Red Hat Enterprise Linux (RHEL) 8.2 および 7.x |
| 構成 | ■ NetBackup バージョン 10.1 プライマリ、メディアサーバー、およびバックアップホスト。<br>■ VMware バックアップホストは、次のいずれかの NetBackup Appliance フォームファクタに対応します。<br>　■ NBA<br>　■ Flex<br>　■ NetBackup FlexScale (NBFS)<br>■ NetBackup Snapshot Manager バージョン 10.1 |
| 権限 | ■ Windows バックアップホストでは、同様のドメインユーザーアカウントを使用して、次の NetBackup サービスを開始する必要があります。<br>　■ NetBackup Client Service<br>　■ NetBackup Legacy Network Service<br>■ ドメインユーザーは、ローカル管理者グループに属している必要があります。 |
| VMware NFS データストア | ESX ホストにマウントされる VMware NFS データストアは、バージョンが NFS 4.1 または NFS 3.0 である必要があります。 |
| 仮想マシンをホストする VMware vCenter と ESX Server | 仮想マシンは、NFS データストアに存在する必要があります。 |

# ハードウェアスナップショットでサポートされる操作

**表 11-2　ハードウェアスナップショットを使用した仮想マシンの操作**

| 操作 | 説明および注意事項 |
|---|---|
| NFS データストアで仮想マシンのアレイベースのスナップショットを作成します。 | 仮想マシンのアレイスナップショットを作成するために、ストレージライフサイクルポリシー (SLP) とバックアップポリシーを構成します。スナップショットはアレイかファイラに保持されるので、NetBackup メディアサーバーストレージユニットにはバックアップされません。<br>注意:<br>■ スナップショットは NFS データストアだけに作成されます。<br>■ 仮想マシンやその個々のファイルはストレージアレイのスナップショットから直接リストアできます。スナップショットは他の場所にレプリケートすることもできます。<br>■ リストアするファイルを速く参照するには、SLP に[スナップショットからのインデックス (Index From Snapshot)]オプションを含めます。このオプションは仮想マシンのメタデータをカタログします。 |
| NFS データストアにあるスナップショット (またはスナップショットレプリカ) から静止した仮想マシンをバックアップします。 | 仮想マシンのスナップショットからバックアップイメージを作るために SLP およびバックアップポリシーを構成します。NetBackup はスナップショットが発生する前に静止していた仮想マシンだけをバックアップします。<br>バックアップイメージは NetBackup ストレージユニットに書き込まれます。イメージはポリシーの保持期間に従って保持されます。<br>**メモ:** ポリシーの[アプリケーションの整合性スナップショット (Application Consistent Snapshot)]オプションは有効にする必要があります ([オプション (Options)] > [Snapshot Client オプション (Snapshot Client Options)]の下)。 |
| NFS データストアにあるスナップショット (またはスナップショットレプリカ) から、または NetBackup ストレージユニットに書き込まれたバックアップイメージから、仮想マシンをリストアします。 | NetBackup Web UI インターフェースを使用して、仮想マシンをリストアします。サポートされるリストア先は元のデータストア (NFS) または代替データストア (NFS または非 NFS) です。 |

| 操作 | 説明および注意事項 |
| --- | --- |
| NFS データストアにあるスナップショット (またはスナップショットレプリカ) から、または NetBackup ストレージユニットに書き込まれたバックアップイメージから、個々のファイルおよび VMDK をリストアします。 | バックアップ、アーカイブ、およびリストアインターフェースを使用して、ファイルをリストアします。<br>注意:<br>■ スナップショットのレプリカからファイルをリストアするには、レプリカがスナップショットと同じ NetBackup ドメインに存在する必要があります。<br>■ 元の仮想マシンにファイルをリストアするには、NetBackup クライアントが元の仮想マシンにインストールされている必要があります。 |
| スナップショットからのインデックス | [スナップショットからのインデックス (Index From Snapshot)] 操作は、仮想マシンのメタデータをカタログします。これにより、リストアするファイルの高速参照が可能になります。<br>この機能を使用するには、SLP の [スナップショットからのインデックス (Index From Snapshot)] オプションを使用します。 |
| スナップショットのライブ参照 | ライブ参照機能を使用すると、ストレージアレイにある VM スナップショットの内容を参照できます。 |

# ハードウェアスナップショットを使用するための VMware ポリシーの構成

次の手順は、NFS データストアにある仮想マシンのハードウェアスナップショットを作成するために、VMware のポリシーを NetBackup Web UI を使用して構成する方法を説明します。

VMware ポリシーの構成について詳しくは、次の項を参照してください。

p.25 の「Web UI での VMware ポリシーの操作」を参照してください。

**表 11-3 構成手順と説明**

| 手順 | 説明 | 参照先 |
| --- | --- | --- |
| 1 | NetBackup で NetBackup Snapshot Manager サーバーを構成します。 | NetBackup Snapshot Manager for Data Center 管理者ガイド |
| 2 | NAS ストレージアレイプラグインを構成します。 | NetBackup Snapshot Manager for Data Center 管理者ガイド |

| 手順 | 説明 | 参照先 |
|---|---|---|
| 3 | VMware バックアップホストを NetBackup 構成に追加します。 | 『NetBackup for VMware 管理者ガイド』で、NetBackup への VMware バックアップホストの追加に関連するトピックを参照してください。 |
| 4 | VMware vCenter Server または ESX Server の NetBackup アクセスクレデンシャルを設定します。 | 『NetBackup Web UI VMware 管理者ガイド』で、VMware 用 NetBackup クレデンシャルの追加に関連するトピックを参照してください。 |
| 5 | スナップショットを使用するための SLP の構成 | 詳しくは、『NetBackup™ Snapshot Manager for Data Center 管理者ガイド』のトピック「スナップショットおよびスナップショットレプリケーションのストレージライフサイクルポリシーの構成」を参照してください。 |
| 6 | SLP で指定された操作を実行するために NetBackup VMware ポリシーを構成します。 | 詳しくは、『NetBackup for VMware 管理者ガイド』を参照してください。 |

次の手順では、NFS データストアにある VM のハードウェアスナップショットを使用するように VMware ポリシーを構成するために必要なポリシーオプションのみが一覧に表示されています。

**メモ:** この機能は、VMware の保護計画ではサポートされていません。この機能を使用するには、NetBackup Web UI を使用して VMware ポリシーを作成する必要があります。

**Web UI で VM ハードウェアスナップショットを使用するポリシーを作成するには**

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. ポリシーの[属性 (Attributes)]タブでオプションを構成します。以下の項目は、ハードウェアスナップショット用の VMware ポリシーを作成する場合に限定されます。
   - ポリシーストレージ (Policy storage): スナップショットベースの保護用に構成されている SLP を選択します。
   - スナップショットバックアップを実行する (Perform snapshot backups): このオプションを有効にすると、スナップショットバックアップに必要な他のオプションが自動的に選択されます。

- [スナップショットバックアップを実行する (Perform snapshot backup)]のオプション: [オプション (Options)]ボタンをクリックすると、[スナップショットオプション (Snapshot Options)]ダイアログボックスと、デフォルトの構成の[パラメータ (Parameters)]が次のように表示されます。
  - スナップショット形式 (Snapshot Type): 適切なスナップショット形式を選択します。デフォルトでは[自動 (Auto)]オプションが選択されており、アレイスナップショットに使用するスナップショット形式を NetBackup が自動的に判断できます。
  - Snapshot Manager: スナップショット操作を実行するためにストレージアレイと通信する NetBackupSnapshot Manager ホストを選択します。

    **メモ:** 構成済みの NetBackup Snapshot Manager ホストのリストを表示するには、ユーザーに表示権限を提供します。MANAGE > SNAPSHOT-MGMT-SERVER > View

  - [最大スナップショット数 (Maximum Snapshots)]: 一度に保持されるスナップショットの最大数を設定します。最大数に達すると、スナップショットのローテーションが実行されます。

    新しいスナップショットが作成されるたびに一番古いスナップショットから順に削除されます。[SLP 保持で管理 (Managed by SLP retention)]は、[固定 (Fixed)]または[コピー後に期限切れにする (Expire after Copy)]の保持が現在 SLP で選択されている場合に自動選択されます。
  - アプリケーションの整合性スナップショット (Application Consistent Snapshot): このオプションはデフォルトでは有効になっています。ほとんどの場合、NetBackupではこのオプションを有効にしておくことを推奨します。

    このオプションが無効になれば、仮想マシンのデータはスナップショットが起きたときに、一貫した状態になっているとは限りません。スナップショットは仮想マシンのすべてのデータをキャプチャしない可能性があります。

    注意:
    - スナップショットからのバックアップイメージを生成することを SLP に許可するには、このオプションを有効にする必要があります。
    - このオプションを無効にした場合は、[VMware]タブに関して次の点に注意してください。
      - [削除されたブロックのエクスクルード (Exclude deleted blocks)]および[スワップおよびページングファイルのエクスクルード (Exclude swap and paging files)]は無効になります。
        - [ブロックレベルの増分バックアップを有効にする (Enable block-level incremental backup)]は無効になります。

- [アプリケーション保護 (Application Protection)]オプションは無効になります。

- アクセラレータを使用 (Use Accelerator): バックアップ操作を高速化するには、このオプションを選択します。

---

**メモ:** バックアップを高速化するには、SLP で[スナップショットからのバックアップ (Backup From Snapshot)]を定義する必要があります。

[スナップショットからのバックアップ (Backup From Snapshot)]操作に使用される MSDP ストレージユニットは、スナップショット (またはスナップショットレプリケーション) で使用される MSDP ストレージユニットと同じである必要があります。

---

**4** [スケジュール (Schedules)]タブをクリックし、バックアップ用の完全スケジュールと増分スケジュールを選択して、[追加 (Add)]をクリックします。

---

**メモ:** 増分スケジュールを追加するには、[ブロックレベルの増分バックアップ (BLIB) (Block-level incremental backup (BLIB))]オプションを有効にする必要があります。

---

**5** [クライアント (Clients)]タブを使用して、仮想マシンの自動選択のための問い合わせを作成します。選択する VM は、NFS データストアにある必要があります。

---

**メモ:** 問い合わせの作成の手順については、『NetBackup for VMware 管理者ガイド』の「バックアップする仮想マシンの自動選択の構成」セクションを参照してください。

---

6 [VMware]タブを使用して、仮想マシンのバックアップのオプションを選択します。

ブロックレベルの増分バックアップを実行するには、[ブロックレベルの増分バックアップ (BLIB) を有効にする (Enable block-level incremental backup (BLIB))]オプションを選択します。

**メモ:** [トランスポートモード (Transport modes)]はサポートされておらず、無効になっています。NetBackup はバックアップホストとストレージアレイの間でデータを移動するのに VMware ファイルトランスポートモードを使用します。

**メモ:** [アプリケーション保護 (Application Protection)]オプションでサポートされているのは、Microsoft Exchange と Microsoft SQL だけです。

7 ポリシーの構成が完了したら、[作成 (Create)]をクリックします。

# NetBackup Snapshot Manager レプリケーションを使用するための VMware ポリシーの構成

NetBackup™ Snapshot Manager for Data Center を使用して、VM のハードウェアスナップショットをレプリケートできます。レプリケートされたスナップショットは、VM の特定の時点のバックアップコピーを作成するために、VMware バックアップホスト上でアクセスされます。次の手順は、NFS データストアにあるハードウェアスナップショットおよび VM のレプリケーションを使用するための VMware のポリシーを、NetBackup Web UI を使用してどのように構成するかを示しています。

VMware ポリシーの構成について詳しくは、p.25 の「Web UI での VMware ポリシーの操作」を参照してください。を参照してください。

**表 11-4** 説明と参照トピックを含む構成手順

| 手順 | 説明 | 参照トピック |
|---|---|---|
| 1 | Snapshot Manager サーバーを NetBackup に登録します。 | 詳しくは、『NetBackup™ Snapshot Manager for Data Center 管理者ガイド』を参照してください。 |
| 2 | NAS ストレージアレイプラグインを構成します。 | 詳しくは、『NetBackup™ Snapshot Manager for Data Center 管理者ガイド』を参照してください。 |
| 3 | VMware アクセスホストを NetBackup 構成に追加します。 | p.20 の「VMware アクセスホストの追加」を参照してください。 |

| 手順 | 説明 | 参照トピック |
|---|---|---|
| 4 | VMware vCenter Server または ESX Server の NetBackup アクセスクレデンシャルを構成します。 | p.10 の「VMware サーバーの追加」を参照してください。<br>p.11 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。 |
| 5 | スナップショットとレプリケーションを使用するために SLP を構成します。 | 詳しくは、『NetBackup™ Snapshot Manager for Data Center 管理者ガイド』の以下の章を参照してください。<br>■ ストレージアレイのレプリケーション<br>■ スナップショットおよびスナップショットレプリケーション用のストレージライフサイクルポリシーの構成<br>■ データセンターでサポートされているストレージアレイ |
| 6 | SLP で指定された操作を実行するために NetBackup VMware ポリシーを構成します。 | p.97 の「ハードウェアスナップショットを使用するための VMware ポリシーの構成」を参照してください。。手順: Web UI で VM ハードウェアスナップショットを使用するポリシーを作成するには |

# VM にハードウェアスナップショットを使用するアクティビティモニターのジョブ

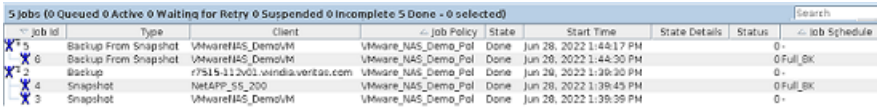
NetBackup アクティビティモニターを使用して、実行中の仮想マシンバックアップを追跡できます。アクティビティモニターに表示されるジョブの数は、ポリシーの[アプリケーションの整合性スナップショット (Application Consistent Snapshot)]オプションによって決まります。

**メモ:** [アプリケーションの整合性スナップショット (Application Consistent Snapshot)]オプションはデフォルトでは有効になっています。ほとんどの場合は、このオプションを有効にしておくことをお勧めします。このオプションが無効になっていると、スナップショットの取得時に仮想マシンのデータが一貫した状態になっていない可能性があります。

表 11-5　アクティビティモニターのジョブフロー

| [アプリケーションの整合性スナップショット (Application Consistent Snapshot)]オプション | アクティビティモニターのジョブフロー |
|---|---|
| 有効 | 最初のジョブで仮想マシンを検出します。このジョブは、[バックアップ (Backup)]とラベル付けされます。<br>次のとおり、バックアップジョブが開始します。<br>■ 各仮想マシンのためのスナップショップジョブ。<br>■ 各データストアのためのスナップショップ (Snapshot) ジョブ。 |
| 無効 | 最初のジョブで仮想マシンを検出します。このジョブは、[バックアップ (Backup)]とラベル付けされます。<br>次のとおり、バックアップジョブが開始します。<br>■ すべての仮想マシンの構成データを収集するスナップショップジョブ。<br>■ 各データストアのためのスナップショップ (Snapshot) ジョブ。 |

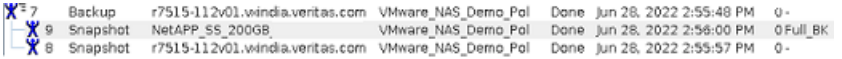
例 1: [アプリケーションの整合性スナップショット (Application Consistent Snapshot)] オプションの仮想マシンジョブは、有効に設定されます。




ジョブは次のように実行されています。

- 仮想マシンの検出のための検出 (親) バックアップジョブは、ID 2 です。
- ジョブ 3 では、仮想マシン VMwareNAS_DemoVM の VMware スナップショットを作成しました。
- ジョブ 4 では、データストア NetAPP_SS_200 のスナップショットを作成しました。
- ジョブ 5 (スナップショットからの親バックアップ) では、スナップショットをエクスポートし、マウントします。
- ジョブ 6 (スナップショットからの子バックアップ) では、バックアップを実行し、バックアップイメージを作成します。

例 2: [アプリケーションの整合性スナップショット (Application Consistent Snapshot)] オプションが無効になっている仮想マシンジョブ。



ジョブは次のように実行されています。

- 仮想マシンの検出のための検出 (親) バックアップジョブは、ID 7 です。
- ジョブ 8 では、選択したすべての仮想マシン (VM1、VM2 など) の構成データを収集しました。
- ジョブ 9 は、仮想マシンデータストアのスナップショットを作成します。

# 注意事項および制限事項

仮想マシンデータストアの VMware NAS ハードウェアスナップショットについては、次の点に注意してください。

- スナップショットからのインデックス、スナップショットからのシングルファイルリストア (SFR)、XFS のスナップショットからのライブ参照、Btrfs ファイルシステムは、現在サポートされていません。
- エージェントレスシングルファイルリストア (ALVR) は、NetBackup Web UI からはサポートされていません。
- GRT と個々の VMDK のリストアは、NetBackup Web UI からはサポートされていません。
- 増分スナップショットコピーから VM 全体をリストアする際、リストアは増分バックアップ中に取得されたスナップショットからのみ実行されます。
  増分バックアップイメージコピーからリストアする場合、リストアは、すべての増分イメージと完全バックアップイメージから実行されます。
- 増分バックアップイメージからリストアするには、すべてのプライマリコピーがスナップショットコピーまたはバックアップイメージコピーである必要があります。
- ハードウェアスナップショットベースのバックアップを使用して Microsoft Exchange を保護する VMware ポリシーでは、Windows のみをバックアップホストとして指定する必要があります。

# VMware ハードウェアスナップショットとレプリケーション操作のトラブルシューティング

## 情報の収集とログの確認について

詳細なログ情報を作成するには、NetBackup プライマリおよびクライアントの bp.conf ファイルに VERBOSE エントリを指定します。または、[プライマリサーバープロパティ (Primary Server Properties)]と[クライアントプロパティ (Client Properties)]の両方の[ログ (Logging)]ダイアログボックスで、グローバルログレベルの値を大きくします。

これらのディレクトリは、最終的に多くのディスク容量を必要とする可能性があります。トラブルシューティングが終了した後にディレクトリを削除し、bp.conf ファイルから VERBOSE オプションを削除します。または、[グローバルログレベル (Global logging level)]の値を小さくします。

## Linux プラットフォームのログディレクトリ

ログディレクトリを作成するには、/usr/openv/netbackup/logs/mklogdir スクリプトを使用します。また、NetBackup がログを書き込めるように、アクセスモード 755 を使用してディレクトリを作成することもできます。

**表 11-6** スナップショット操作用の Linux ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/netbackup/logs/bprd | NetBackup プライマリサーバー |
| /usr/openv/logs/nbjm | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpbrm | NetBackup メディアサーバー |
| /usr/openv/netbackup/logs/bpfis | バックアップホストクライアント |

**表 11-7** バックアップ操作用の Linux ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/netbackup/logs/bprd | NetBackup プライマリサーバー |
| /usr/openv/logs/nbjm | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpdbm | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bptm | NetBackup メディアサーバー |
| /usr/openv/netbackup/logs/bpbrm | NetBackup メディアサーバー |
| /usr/openv/netbackup/logs/bpfis | バックアップホストクライアント |
| /usr/openv/netbackup/logs/bppfi | バックアップホストクライアント |
| /usr/openv/netbackup/logs/bpbkar | バックアップホストクライアント |
| /usr/openv/netbackup/logs/bppfi | バックアップホストクライアント |
| /usr/openv/netbackup/logs/vxms | バックアップホストクライアント |

表 11-8 シングルファイルリストア操作用の Linux ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/netbackup/logs/bprd | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpcd | リストアホストクライアント |
| /usr/openv/netbackup/logs/bpbkar | リストアホストクライアント |
| /usr/openv/netbackup/logs/bpfis | リストアホストクライアント |
| /usr/openv/netbackup/logs/bppfi | リストアホストクライアント |
| /usr/openv/logs/ncfnbhfr | リストアホストクライアント |
| /usr/openv/netbackup/logs/vxms | リストアホストクライアント |
| /usr/openv/netbackup/logs/tar | ファイルのリストア先クライアント。 |

表 11-9 完全 VM リストア操作用の Linux ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/netbackup/logs/bprd | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpbrm | NetBackup メディアサーバー |
| /usr/openv/logs/ncfnbvmcopyback | リストアホストクライアント |
| /usr/openv/netbackup/logs/vxms | リストアホストクライアント |

表 11-10 ライブ参照操作用の Linux ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/netbackup/logs/bprd | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpdbm | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpcd | バックアップホストクライアント |
| /usr/openv/netbackup/logs/bppfi | バックアップホストクライアント |
| /usr/openv/logs/ncfnbbrowse | バックアップホストクライアント |
| /usr/openv/netbackup/logs/vxms | バックアップホストクライアント |

表 11-11 スナップショット操作からのインデックス用の Linux ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/logs/ncflbc | バックアップホストクライアント |
| /usr/openv/netbackup/logs/vxms | バックアップホストクライアント |

## Windows プラットフォームのログフォルダ:

表 11-12 スナップショット操作用の Windows ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| /usr/openv/netbackup/logs/bprd | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpdbm | NetBackup プライマリサーバー |
| /usr/openv/netbackup/logs/bpcd | NetBackup メディアサーバー |
| /usr/openv/netbackup/logs/bppfi | バックアップホストクライアント |

表 11-13 バックアップ操作用の Windows ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| install_path¥NetBackup¥logs¥bprd | NetBackup プライマリサーバー |
| install_path¥NetBackup¥logs¥nbjm | NetBackup プライマリサーバー |
| install_path¥NetBackup¥logs¥bpdbm | NetBackup プライマリサーバー |
| install_path¥NetBackup¥logs¥bptm | NetBackup メディアサーバー |
| install_path¥NetBackup¥logs¥bpbrm | NetBackup メディアサーバー |
| install_path¥NetBackup¥logs¥bpfis | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥bppfi | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥bpbkar | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥bppfi | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥vxms | バックアップホストクライアント |

表 11-14 シングルファイルリストア操作用の Windows ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| install_path¥NetBackup¥logs¥bprd | NetBackup プライマリサーバー |

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| install_path¥NetBackup¥logs¥bpcd | リストアホストクライアント |
| install_path¥NetBackup¥logs¥bpbkar | リストアホストクライアント |
| install_path¥NetBackup¥logs¥bpfis | リストアホストクライアント |
| install_path¥NetBackup¥logs¥bppfi | リストアホストクライアント |
| install_path¥NetBackup¥logs¥ncfnbhfr | リストアホストクライアント |
| install_path¥NetBackup¥logs¥vxms | リストアホストクライアント |
| install_path¥NetBackup¥logs¥tar | ファイルのリストア先クライアント。 |

**表 11-15** 完全 VM リストア操作用の Windows ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| install_path¥NetBackup¥logs¥bprd | NetBackup プライマリサーバー |
| install_path¥NetBackup¥logs¥bpbrm | NetBackup メディアサーバー |
| install_path¥NetBackup¥logs¥ncfnbvmcopyback | リストアホストクライアント |
| install_path¥NetBackup¥logs¥vxms | リストアホストクライアント |

**表 11-16** ライブ参照操作用の Windows ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| install_path¥NetBackup¥logs¥bprd | NetBackup プライマリサーバー |
| install_path¥NetBackup¥logs¥bpdbm | NetBackup プライマリサーバー |
| install_path¥NetBackup¥logs¥bpcd | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥bppfi | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥ncfnbbrowse | バックアップホストクライアント |
| install_path¥NetBackup¥logs¥vxms | バックアップホストクライアント |

**表 11-17** スナップショット操作からのインデックス用の Windows ログディレクトリ

| ログディレクトリのパス | ディレクトリを作成する場所 |
|---|---|
| install_path¥NetBackup¥logs¥ncflbc | バックアップホストクライアント |

| ログディレクトリのパス | ディレクトリを作成する場所 |
| --- | --- |
| install_path¥NetBackup¥logs¥vxms | バックアップホストクライアント |

12

# 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

表 12-1 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。<br>クレデンシャルの検証は次の順序で実行されます。<br>■ 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。<br>■ 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。<br>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。<br>**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。<br>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 12-2 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。<br>推奨処置: 検出プロセスが完了するまで待ちます。<br>**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、ESXi サーバー、または VMware Cloud Director 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)。<br>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。<br>p.23 の「VMware 資産の自動検出の間隔の変更」を参照してください。<br>■ 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。<br>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 12-3 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。<br>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。<br>■ デフォルトでは、8 時間ごとに自動検出が実行されます。<br>■ 新しい VM が環境に追加されました。<br>■ 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。<br>■ 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。<br>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。<br>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。 |

# 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 12-4 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<br>Firefox: サーバーが見つかりませんでした<br>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。<br>■ 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。<br>例: プライマリサーバーが MSserver1.veritas.com を使用してメディアサーバーに接続する場合、Web UI も MSserver1.veritas.com に到達できる必要があります。プライマリサーバーが MSserver1 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 https://MSserver1/... に到達できる必要があります。<br>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 (hosts ファイルを確認)。<br>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 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。<br>Windows 上の hosts ファイルの場所:<br>C:¥Windows¥System32¥drivers¥etc¥hosts<br>UNIX または Linux 上のホストファイルの場所:<br>/etc/hosts<br>■ 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。<br>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 12-5 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 12-6 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。<br><br>代わりに、代替の場所に仮想マシンをリストアできます。 |