# VMwareワークロードを保護する

## NetApp Backup and Recovery

NetApp
June 25, 2026

# 目次

# VMwareワークロードを保護する

## NetApp Backup and Recoveryによる VMware ワークロードの保護の概要

NetApp Backup and RecoveryでVMwareのVMおよびデータストアを保護します。NetApp Backup and Recoveryは、高速でスペース効率に優れた、「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態の、およびVM整合性のあるバックアップとリストアの操作を提供します。サポートされているバックアップターゲットにVMwareワークロードをバックアップし、オンプレミスのVMwareホストにVMwareワークロードをリストアできます。

> このバージョンのNetApp Backup and Recovery はVMware vCenter のみをサポートし、 vVolsまたはvVols上の VM を検出しません。

NetApp Backup and Recoveryを使用して 3-2-1 戦略を実装します。この戦略では、ソース データのコピーを 2 つの異なるストレージ システムに 3 つ、クラウドに 1 つ保存します。3-2-1 アプローチの利点は次のとおりです。

- 複数のデータ コピーにより、内部および外部のサイバー セキュリティの脅威から保護されます。
- 異なるタイプのメディアを使用すると、1 つのタイプに障害が発生した場合でも回復しやすくなります。
- オンサイト コピーから迅速に復元し、オンサイト コピーが侵害された場合はオフサイト コピーを使用できます。

NetApp Backup and Recoveryを使用すると、VMware ワークロードに関連する次のタスクを実行できます。

- "VMware ワークロードを発見"
- "VMware ワークロードの保護グループの作成と管理"
- "VMwareワークロードのバックアップ"
- "VMwareワークロードを復元する"

## NetApp Backup and Recoveryで VMware ワークロードを発見

NetApp Backup and Recoveryサービスを使用するには、まずONTAPシステムで実行されている VMware データストアと VM を検出する必要があります。すでにインストールされている場合は、オプションでSnapCenter Plug-in for VMware vSphereからバックアップ データとポリシーをインポートできます。

必要なコンソール ロール バックアップとリカバリのスーパー管理者。詳細はこちら"バックアップとリカバリの役割と権限"。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します" 。

### VMware ワークロードを検出し、オプションでSnapCenterリソースをインポートする

検出中に、 NetApp Backup and Recovery は組織内の VMware ワークロードを分析し、既存の保護ポリシ

ー、スナップショット、バックアップおよび復元オプションを評価してインポートします。

VMware NFS および VMFS データストアと VM を、オンプレミスのSnapCenter Plug-in for VMware vSphere からNetApp Backup and Recoveryインベントリにインポートできます。

> このバージョンのNetApp Backup and Recovery はVMware vCenter のみをサポートし、 vVols またはvVols上の VM を検出しません。

インポート プロセス中に、 NetApp Backup and Recovery は次のタスクを実行します。

- vCenter サーバーへの安全な SSH アクセスを有効にします。
- vCenter サーバー内のすべてのリソース グループでメンテナンス モードをアクティブ化します。
- vCenter のメタデータを準備し、 NetApp Consoleで管理対象外としてマークします。
- データベース アクセスを構成します。
- VMware vCenter、データストア、および VM を検出します。
- SnapCenter Plug-in for VMware vSphereから既存の保護ポリシー、スナップショット、バックアップおよび復元オプションをインポートします。
- 検出されたリソースをNetApp Backup and Recoveryインベントリ ページに表示されます。

検出は次のように行われます。

- SnapCenter Plug-in for VMware vSphere がすでにインストールされている場合は、 NetApp Backup and Recovery UI を使用してSnapCenterリソースをNetApp Backup and Recoveryにインポートします。

  > SnapCenterプラグインがすでにある場合は、 SnapCenterからインポートする前に前提条件を満たしていることを確認してください。たとえば、 SnapCenterからインポートする前に、まずNetApp Consoleですべてのオンプレミスの SnapCenterクラスター ストレージ用のシステムを作成する必要があります。見る"SnapCenterからリソースをインポートするための前提条件"。

- SnapCenterプラグインがまだインストールされていない場合でも、vCenter を手動で追加して検出を実行することで、システム内のワークロードを検出できます。

**SnapCenter**プラグインがまだインストールされていない場合は、**vCenter**を追加してリソースを検出します。

SnapCenter Plug-in for VMware がまだインストールされていない場合は、vCenter 情報を追加し、 NetApp Backup and Recoveryでワークロードを検出します。各コンソール エージェント内で、ワークロードを検出するシステムを選択します。

手順

1. NetApp Consoleの左側のナビゲーションから、保護 > バックアップとリカバリ を選択します。

   初めて Backup and Recovery にログインし、コンソールにシステムがあるがリソースが検出されていない場合は、[新しいNetApp Backup and Recovery へようこそ] ページが表示され、[リソースの検出] オプションが表示されます。

2. *リソースの検出*を選択します。

3. 次の情報を入力してください。
   a. ワークロード タイプ: **VMware** を選択します。
   b. **vCenter** 設定: 新しい vCenter を追加します。新しい vCenter を追加するには、vCenter FQDN または IP アドレス、ユーザー名、パスワード、ポート、プロトコルを入力します。

      vCenter 情報を入力する場合は、vCenter 設定とホスト登録の両方の情報を入力します。ここで vCenter 情報を追加または入力した場合は、次に詳細設定でプラグイン情報も追加する必要があります。

   c. ホスト登録: VMware では必要ありません。
4. *Discover*を選択します。

   このプロセスには数分かかる場合があります。

5. 詳細設定に進みます。

**SnapCenter**プラグインがすでにインストールされている場合は、**VMware**リソース用の**SnapCenter**プラグインを**NetApp Backup and Recovery**にインポートします。

SnapCenter Plug-in for VMware がすでにインストールされている場合は、次の手順に従ってSnapCenter Plug-in リソースをNetApp Backup and Recoveryにインポートします。コンソールは、vCenter 内の ESXi ホスト、データストア、VM を検出し、プラグインからスケジュールを設定します。すべての情報を再作成する必要はありません。

これは次の方法で実行できます。

- 検出中に、 SnapCenterプラグインからリソースをインポートするオプションを選択します。
- 検出後、インベントリ ページからSnapCenterプラグイン リソースをインポートするオプションを選択します。
- 検出後、[設定] メニューから、 SnapCenterプラグイン リソースをインポートするオプションを選択します。詳細については、"NetApp Backup and Recoveryを構成する" 。これは VMware ではサポートされていません。

このセクションでは、次の 2 つの部分から成るプロセスについて説明します。

1. SnapCenterプラグインからvCenterメタデータをインポートします。インポートされたvCenterリソースは、まだNetApp Backup and Recoveryによって管理されていません。
2. NetApp Backup and Recoveryで選択した vCenter、VM、およびデータストアの管理を開始します。管理を開始すると、 NetApp Backup and Recovery は、インベントリ ページで vCenter を「管理対象」としてラベル付けし、インポートしたリソースをバックアップおよびリカバリできるようになります。 NetApp Backup and Recoveryで管理を開始すると、 SnapCenterプラグインでそれらのリソースを管理できなくなります。

#### **SnapCenter**プラグインから**vCenter**メタデータをインポートする

この最初のステップでは、 SnapCenterプラグインからvCenterメタデータをインポートします。この時点では、リソースはまだNetApp Backup and Recoveryによって管理されていません。

SnapCenterプラグインから vCenter メタデータをインポートした後、 NetApp Backup and Recovery は保護管理を自動的に引き継ぎません。そのためには、 NetApp Backup and Recoveryでインポートされたリソースを管理することを明示的に選択する必要があります。これにより、 NetApp Backup and Recoveryによってそれらのリソースをバックアップする準備が整います。

手順

1. コンソールの左側のナビゲーションから、保護 > *バックアップとリカバリ*を選択します。
2. *在庫*を選択します。
3. NetApp Backup and Recovery のワークロード リソースの検出ページで、* SnapCenterからのインポート*を選択します。
4. [インポート元] フィールドで、* SnapCenter Plug-in for VMware* を選択します。
5. **VMware vCenter** の資格情報 を入力してください:
   a. **vCenter IP/**ホスト名: NetApp Backup and Recoveryにインポートする vCenter の FQDN または IP アドレスを入力します。
   b. **vCenter** ポート番号: vCenter のポート番号を入力します。
   c. **vCenter** ユーザー名 と パスワード: vCenter のユーザー名とパスワードを入力します。
   d. コネクタ: vCenter のコンソール エージェントを選択します。
6. * SnapCenterプラグイン ホストの資格情報* を入力してください:
   a. 既存の資格情報: このオプションを選択すると、すでに追加されている既存の資格情報を使用できます。資格情報の名前を選択します。
   b. 新しい資格情報の追加: 既存のSnapCenterプラグイン ホスト資格情報がない場合は、新しい資格情報を追加できます。資格情報名、認証モード、ユーザー名、およびパスワードを入力します。
7. インポート を選択してエントリを検証し、 SnapCenterプラグインを登録します。

SnapCenterプラグインがすでに登録されている場合は、既存の登録詳細を更新できます。

結果

明示的に管理対象として選択するまで、インベントリ ページには、NetApp Backup and Recoveryで vCenter が管理対象外として表示されます。

#### SnapCenterプラグインからインポートされたリソースを管理する

SnapCenter Plug-in for VMware から vCenter メタデータをインポートした後、 NetApp Backup and Recoveryでリソースを管理します。これらのリソースを管理することを選択すると、 NetApp Backup and Recovery はインポートしたリソースをバックアップおよびリカバリできるようになります。 NetApp Backup and Recoveryで管理を開始すると、 SnapCenterプラグインでそれらのリソースを管理できなくなります。

リソースを管理することを選択すると、リソース、VM、およびポリシーがSnapCenter Plug-in for VMware からインポートされます。リソース グループ、ポリシー、スナップショットはプラグインから移行され、NetApp Backup and Recoveryで管理されるようになります。

手順

1. SnapCenterプラグインから VMware リソースをインポートした後、[バックアップとリカバリ] メニュー

から [インベントリ] を選択します。

2. [インベントリ] ページで、今後NetApp Backup and Recoveryで管理するインポート済みの vCenter を選択します。
3. アクションアイコンを選択します ••• > 詳細を表示 をクリックして、ワークロードの詳細を表示します。
4. インベントリ > ワークロードページから、アクションアイコンを選択します ••• > 管理 をクリックして、vCenter の管理ページを表示します。
5. 「移行を続行しますか？」のボックスをチェックし、「移行」を選択します。

結果

インベントリ ページには、新しく管理された vCenter リソースが表示されます。

#### NetApp Backup and Recoveryダッシュボードに進みます

1. ダッシュボードを表示するには、「バックアップとリカバリ」メニューから「ダッシュボード」を選択します。
2. データ保護の健全性を確認します。新しく検出され、保護され、バックアップされたワークロードに基づいて、危険にさらされているワークロードまたは保護されているワークロードの数が増加します。

   "ダッシュボードに表示される内容を学ぶ"。

# NetApp Backup and Recoveryを使用して VMware ワークロードの保護グループを作成および管理します

一連のワークロードのバックアップおよび復元操作を管理するための保護グループを作成します。保護グループとは、一緒に保護する VM やデータストアなどのリソースの論理的なグループです。

保護グループに関連する次のタスクを実行できます。

- VMをグループに手動で追加するか、VMware vSphereタグを使用して保護グループを作成します。
- 保護の詳細を表示します。
- 今すぐ保護グループをバックアップします。"VMwareワークロードを今すぐバックアップ"を参照してください。
- 保護グループのバックアップ スケジュールを一時停止および再開します。
- 保護グループを削除します。

## タグベースの保護グループ

保護グループに追加するリソースを選択するときは、データストア、仮想マシン、またはvSphereタグで整理できます。

タグベースの保護（vSphereタグを使用）により、NetApp Backup and Recoveryにおける保護グループの管理が簡素化されます。

タグベースの保護にはいくつかの利点があります：

- VMまたはデータストアにvSphereタグをvCenterで追加すると、そのタグを参照するすべてのBackup and Recovery保護グループの次のバックアップに、そのオブジェクトが自動的に含められます。
- VM またはデータストアから vSphere タグを削除すると、そのオブジェクトは、そのタグベースの保護グループの以降のバックアップから自動的に除外されます。
- vCenterでvSphereタグが削除された場合、今後のバックアップではそのタグがスキップされ、警告が報告されます。
- VMが別のデータストアに移行された場合でも、タグベースの保護グループに属するタグが付与されている限り、保護された状態は維持されます。

タグメンバーシップは、バックアップ時に vCenter から解決されます。vCenter でタグに加えた変更（タグの追加 / 削除、タグの削除、VM の追加 / 削除）は、次回のバックアップに自動的に反映されます。

## 保護グループを作成する

バックアップと復元をまとめて行いたいリソースを整理するために、保護グループを作成します。

必要なコンソール ロール バックアップおよびリカバリのスーパー管理者またはバックアップおよびリカバリのバックアップ管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します" 。

開始する前に

- ご使用の環境で、サポートされているバージョンのVMware vSphereが使用されていることを確認してください。
- タグベースの保護グループを作成する場合は、保護する仮想マシンとデータストアがvCenterで1つ以上のvSphereタグにすでに関連付けられていることを確認してください。
- VMwareワークロードの場合、スケジュールされたバックアップ時間は管理ホストのタイムゾーンで解釈されることに注意してください。詳細については、"NetApp Backup and Recovery での VMware バックアップ ポリシーの作成と管理"を参照してください。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します ••• > 詳細を表示。
4. *保護グループ*タブを選択します。
5. *保護グループの作成*を選択します。
6. 保護グループの名前を指定し、保護グループにリソースを追加する方法を選択してください。データストア、仮想マシン、または*タグ*ごとに整理されたリソースを追加できます。

   リソースタイプを混在させること（たとえば、同じ保護グループ内でタグと個々の VM やデータストアを組み合わせること）はサポートされていません。

7. 表示されたリストから、保護グループに含めるリソースを選択します。

   リスト内の利用可能なリソースを絞り込むには、特定のvCenterまたはデータセンターを選択します。選択されたリソースは右側のリストに表示されます。

8. 完了したら、* Next *を選択します。
9. 保護グループが、仮想ディスクが複数のデータストアにまたがる仮想マシンをどのように処理するかを選択します：
   - 常にすべてのスパンニングデータストアを除外します：保護グループには、直接追加されたデータストアと、保護グループに直接追加されたVMのプライマリデータストアのみが含まれます。
   - 常にすべてのスパンニングデータストアを含める：保護グループには、含まれる VM によってスパンニングされるすべてのデータストアが含まれます。
   - 含めるスパンニングデータストアを手動で選択：このオプションを選択した場合、表示されるリストから保護グループに含めるスパンニングデータストアを手動で選択する必要があります。この選択は静的なものです。グループに新しい仮想マシンが追加されるたびに、スパンニングデータストアのリストを更新する必要があります。
10. *次へ*を選択します。
11. 保護グループに適用する保護ポリシーを選択します。

    新しいポリシーを作成するには、*Create new policy*を選択し、画面の指示に従ってください。詳細については、"ポリシーを作成"を参照してください。
12. *次へ*を選択します。
13. 構成を確認します。
14. 保護グループを作成するには、[作成] を選択します。

## 保護グループのバックアップスケジュールを一時停止する

保護グループを一時停止して、スケジュールされたバックアップを一時停止します。

保護グループを一時停止すると、保護ステータスが「メンテナンス中」に変わります。バックアップ スケジュールはいつでも再開できます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します ••• > 詳細を表示。
4. *保護グループ*タブを選択します。
5. アクションアイコンを選択します ••• > 保護グループを一時停止します。
6. 確認メッセージを確認し、「一時停止」を選択します。

## 保護グループのバックアップ スケジュールを再開する

一時停止された保護グループを再開すると、保護グループのスケジュールされたバックアップが再開されます。

保護グループを一時停止すると、保護ステータスは「メンテナンス中」から再開すると「保護済み」に変わります。バックアップ スケジュールはいつでも再開できます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します > 詳細を表示。
4. *保護グループ*タブを選択します。
5. アクションアイコンを選択します > 保護グループを再開します。
6. 確認メッセージを確認し、「再開」を選択します。

結果

システムはスケジュールを検証し、スケジュールが有効な場合は保護ステータスを「保護済み」に変更します。スケジュールが有効でない場合、システムはエラー メッセージを表示し、保護グループは再開しません。

## 保護グループを編集する

保護グループを編集して、名前または設定を変更します。グループ内のリソースが変更された場合は、保護グループを編集する必要がある場合があります。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します > 詳細を表示。
4. *保護グループ*タブを選択します。
5. 編集する保護グループを選択します。
6. アクションアイコンを選択します > 編集。

   保護グループの編集ウィザードは、保護グループの設定手順を案内します。
7. ウィザードの各画面で必要な変更を行ってください。
8. 完了したら、*送信*を選択します。

### 更新された **vCenter** タイムゾーンを既存の保護グループに適用する

スケジュールされたバックアップは、保護グループのスケジュールが作成された際に記録されるvCenter Serverのタイムゾーンを使用します。vCenter Serverのタイムゾーンを変更した場合、既存の保護グループは、スケジュールを更新するまで元のタイムゾーン（通常はUTC）で実行され続けます。

> スケジュールは、保護グループ名を変更した場合、VMを追加または削除した場合、割り当てられたポリシーを変更した場合、またはプリスクリプト/ポストスクリプトを更新した場合にのみ再作成されます。変更を加えず保存しても、スケジュールは更新されません。このスケジュール更新は、保護グループごとに一度だけ実行される処理であり、即座にバックアップを開始するものではありません。

手順

1. vCenter サーバーを更新して、現在のタイムゾーンを取得します。

2. 保護グループを編集し、名前を別の値に変更してから保存してください。

### 保護グループを削除する

保護グループを削除すると、保護グループとグループのすべてのバックアップ スケジュールが削除されます。保護グループが不要になった場合は削除します。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します > 詳細を表示。
4. *保護グループ*タブを選択します。
5. 削除する保護グループを選択します。
6. アクションアイコンを選択します > 削除。
7. 関連するバックアップの削除に関する確認メッセージを確認し、削除を確定します。

# NetApp Backup and Recovery での VMware バックアップ ポリシーの作成と管理

NetApp Backup and Recoveryでは、バックアップの頻度、バックアップの取得時間、および保持するバックアップファイルの数を制御する独自のVMwareバックアップポリシーを作成できます。

これらのオプションと構成セクションの一部は、すべてのワークロードで使用できるわけではありません。

SnapCenterからリソースをインポートする場合、 SnapCenterで使用されるポリシーとNetApp Backup and Recoveryで使用されるポリシーとの間に若干の違いが生じる可能性があります。見る"SnapCenterとNetApp Backup and Recoveryのポリシーの違い"。

ポリシーに関連する次の目標を達成できます。

- ローカルスナップショットポリシーを作成する
- セカンダリストレージへのレプリケーションのポリシーを作成する
- オブジェクトストレージ設定のポリシーを作成する
- 詳細なポリシー設定を構成する
- ポリシーの削除

VMwareワークロードの場合、バックアップスケジュールはUTCやブラウザのローカル時刻ではなく、VMware vCenter Serverのタイムゾーンを使用します。このタイムゾーンは、スケジュールを作成する際に設定されます。ホストのタイムゾーンが変更された場合は、ホストを更新し、新しいタイムゾーンが有効になるようにスケジュールを再作成する必要があります。詳細については、"VMware ワークロードの保護グループの作成と管理"を参照してください。

## ポリシーを表示

1. NetApp Backup and Recoveryメニューから、ポリシー を選択します。
2. ポリシーの詳細を確認してください。例：
   - ワークロード：例：Microsoft SQL Server、ONTAP ボリューム、VMware、KVM、Hyper-V、Oracle Database、または Kubernetes。
   - バックアップの種類: 例としては、完全バックアップやログ バックアップなどがあります。
   - アーキテクチャ: 例としては、ローカル スナップショット、ファンアウト、カスケード、ディスク間、ディスクからオブジェクト ストアなどがあります。
   - 保護されているリソース: そのワークロード上のリソースの合計数のうち、保護されているリソースの数を表示します。
   - ランサムウェア保護: ポリシーに、ローカル スナップショットのスナップショット ロック、セカンダリ ストレージのスナップショット ロック、またはオブジェクト ストレージの DataLock ロックが含まれているかどうかを示します。

## ポリシーを作成します。

ローカル スナップショット、セカンダリ ストレージへのレプリケーション、オブジェクト ストレージへのバックアップを管理するポリシーを作成できます。3-2-1 戦略の一部として、プライマリ ストレージ システム上のインスタンス、データベース、アプリケーション、または VM のスナップショットを作成します。

必要な**NetApp Console**ロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者。詳細はこちら"バックアップとリカバリの役割と権限"。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します" 。

開始する前に

セカンダリ ストレージに複製し、ローカル スナップショットまたはリモートONTAPセカンダリ ストレージでスナップショット ロックを使用する予定の場合は、まずクラスタ レベルでONTAPコンプライアンス クロックを初期化する必要があります。これは、ポリシーでスナップショット ロックを有効にするための要件です。

これを行う方法については、以下を参照してください。 "ONTAPのコンプライアンスクロックを初期化する" 。

スナップショットロック全般については、以下を参照してください。 "ONTAPのスナップショットロック" 。

手順

1. NetApp Backup and Recoveryメニューから、ポリシー を選択します。
2. [ポリシー] ページで、[新しいポリシーの作成] を選択します。

   ポリシーページが表示されます。

3. * 詳細 * セクションに情報を入力します。
   - ワークロードのタイプ：*VMware*を選択します。
   - ポリシー名を入力します。
   - エージェント リストからコンソール エージェントを選択します。

4. * Backup architecture * セクションに情報を入力します。リストからバックアップのデータフローを選択します：

   - **3-2-1** ファンアウト：プライマリストレージ（ディスク）からセカンダリストレージ（ディスク）を経てクラウド（オブジェクトストア）へ。ONTAP to ONTAP や ONTAP to オブジェクトストア構成など、異なるストレージシステム間でデータの複数のコピーを作成します。これは、クラウドハイパースケーラーのオブジェクトストア、またはプライベートオブジェクトストアのいずれかです。最適なデータ保護と災害復旧に最適です。このオプションは Amazon FSx for NetApp ONTAP では利用できません。

     VMware ワークロードの場合、これにより、プライマリ上のデータストアまたは VM 上のローカル スナップショットが構成され、プライマリ ディスク ストレージからセカンダリ ディスク ストレージにレプリケートされるとともに、プライマリからクラウド オブジェクト ストレージにレプリケートされます。

   - **3-2-1** カスケード：プライマリストレージ（ディスク）からセカンダリストレージ（ディスク）へ、およびプライマリストレージ（ディスク）からクラウドストレージ（オブジェクトストア）へ。これは、クラウド ハイパースケーラー オブジェクト ストアまたは StorageGRID などのプライベート オブジェクト ストアです。これにより、複数のシステム間でデータレプリケーションのチェーンが作成され、冗長性と信頼性が確保されます。このオプションは、Amazon FSx for NetApp ONTAP では使用できません。

     VMware ワークロードの場合、これにより、プライマリ ストレージ上のデータストアまたは VM 上のローカル スナップショットと、プライマリ ディスク ストレージからセカンダリ ディスク ストレージ、そしてクラウド オブジェクト ストレージへのカスケードが構成されます。

   - ディスク間：プライマリストレージ（ディスク）からセカンダリストレージ（ディスク）へ。ONTAP to ONTAP データ保護戦略は、2つのONTAPシステム間でデータをレプリケートし、高可用性とディザスタリカバリを確保します。これは通常、SnapMirrorを使用して実現され、同期レプリケーションと非同期レプリケーションの両方をサポートします。この方法により、データは最新の状態に保たれ、複数の場所で利用可能になり、強力なデータ保護が実現します。

     VMware ワークロードの場合、これにより、プライマリ ストレージ システム上のデータストアまたは VMware にローカル スナップショットが構成され、プライマリ ディスク ストレージ システムからセカンダリ ディスク ストレージ システムにデータが複製されます。

   - ディスクからオブジェクトストレージ：プライマリストレージ（ディスク）からクラウド（オブジェクトストア）へ。ONTAP システムからオブジェクトストレージシステムにデータをレプリケートします。これは、クラウド ハイパースケーラー オブジェクト ストアまたは StorageGRID などのプライベート オブジェクト ストアです。この方法は、長期的なデータ保持とアーカイブに最適です。このオプションは、Amazon FSx for NetApp ONTAP では使用できません。

     VMWare ワークロードの場合、これにより、プライマリ上のデータストアまたは VM 上のローカル スナップショットと、プライマリ ディスク ストレージからクラウド オブジェクト ストレージへのレプリケーションが構成されます。

   - ディスク間ファンアウト：プライマリストレージ（ディスク）からセカンダリストレージ（ディスク）へ、およびプライマリストレージ（ディスク）からセカンダリストレージ（ディスク）へ。ディスク間ファンアウトオプションには、複数のセカンダリ設定を構成できます。

     VMware ワークロードの場合、これによりプライマリ ディスク ストレージがセカンダリ ディスク ストレージに構成され、プライマリ ディスク ストレージがセカンダリ ディスク ストレージに複製されます。

- ローカルスナップショット：選択したボリューム上のローカルスナップショット。これにより、ワークロードが実行されている本番環境ボリュームの読み取り専用のポイントインタイムコピーが作成されます。ローカルスナップショットを使用すると、データの損失や破損から復旧できるだけでなく、ディザスタリカバリのためのバックアップを作成することもできます。

  VMware ワークロードの場合、これにより、プライマリ ストレージ システム上のデータストアまたは VM 上のローカル スナップショットが構成されます。

5. * ローカルスナップショット設定 * セクションの情報を入力します：
   - スナップショット スケジュールを選択するには、[スケジュールの追加] オプションを選択します。最大 5 つのスケジュールを設定できます。
   - スナップショットの頻度: 時間ごと、日ごと、週ごと、月ごと、または年ごとの頻度を選択します。年間頻度は Kubernetes ワークロードでは利用できません。
   - スナップショットの保持: 保持するスナップショットの数を入力します。
6. *セカンダリ設定*セクション（セカンダリストレージへのレプリケーション）の情報を入力します：
   - バックアップ: 時間ごと、日ごと、週ごと、月ごと、または年ごとの頻度を選択します。
   - バックアップ対象: バックアップの対象となるセカンダリ ストレージ上のターゲット システムを選択します。
   - 保持: 保持するスナップショットの数を入力します。
   - スナップショットのロックを有効にする: 改ざん防止スナップショットを有効にするかどうかを選択します。
   - スナップショットのロック期間: スナップショットをロックする日数、月数、または年数を入力します。
   - 二次転送:
     - * ONTAP転送スケジュール - インライン* オプションはデフォルトで選択されており、スナップショットがセカンダリ ストレージ システムに直ちに転送されることを示します。バックアップをスケジュールする必要はありません。
     - その他のオプション: 延期転送を選択した場合、転送は即時に行われず、スケジュールを設定できます。
   - 既存の **SnapMirror** および **SyncMirror** セカンダリ関係を使用する：このオプションを有効にすると、既存の SnapMirror または SyncMirror 関係を使用して、指定されたデスティネーション クラスタにスナップショットを転送します。
7. * Object store settings * セクション（オブジェクトストレージへのバックアップ）の情報を入力します。

   表示されるフィールドは、選択したプロバイダーとアーキテクチャによって異なります。

   - プロバイダー：オブジェクトストアのプロバイダーを選択し、適切なフィールドに認証情報を入力します（認証情報フィールドはプロバイダーによって異なります）。
   - バックアップ対象: 登録済みのオブジェクト ストレージ対象を選択します。バックアップ環境内でターゲットにアクセスできることを確認します。
   - **IPspace**: バックアップ操作に使用する IPspace を選択します。これは、複数の IPspace があり、どの IPspace をバックアップに使用するかを制御したい場合に便利です。
   - スケジュール設定: ローカル スナップショットに設定されたスケジュールを選択します。スケジュールはローカル スナップショット スケジュールに従って設定されるため、削除することはできますが、

追加することはできません。

- 保持コピー数: 保持するスナップショットの数を入力します。
- 実行時間: データをオブジェクト ストレージにバックアップするためのONTAP転送スケジュールを選択します。
- オブジェクト ストアからアーカイブ ストレージにバックアップを階層化します: バックアップをアーカイブ ストレージ (AWS Glacier など) に階層化する場合は、階層オプションとアーカイブする日数を選択します。
- 整合性スキャンを有効にする：オブジェクト ストレージで整合性スキャン（Snapshotロック）を有効にするかどうかを選択します。これにより、バックアップが有効かつリストア可能であることが保証されます。整合性スキャンの頻度は、デフォルトでは7日に設定されています。バックアップが変更または削除されないように保護するには、*整合性スキャン*オプションを選択します。スキャンは最新のSnapshotに対してのみ実行されます。最新のSnapshotに対して、整合性スキャンを有効または無効にすることができます。

ポリシーの詳細設定を構成する

ポリシー内で、必要に応じて詳細設定を行うことができます。これらのオプションは、あらゆるバックアップアーキテクチャとストレージ保存先で使用できます。利用可能な詳細オプションは、ページ上部で選択したワークロードによって異なります。そのため、ここで説明するオプションの中には、すべてのワークロードに適用されないものもあります。

手順

1. NetApp Backup and Recoveryメニューから、ポリシー を選択します。
2. [ポリシー] ページで、[新しいポリシーの作成] を選択します。
3. *ポリシー > 詳細*設定セクションで、*詳細アクションの選択*メニューを選択して、詳細設定のリストから選択します。
4. 表示または変更したい設定を有効にして、[承認] を選択します。
5. 次の情報を入力します。
   - **VM**設定：
     - **VM**整合性スナップショットとアプリケーション整合性スナップショットを有効にする：このオプションを有効にすると、VM整合性スナップショットとアプリケーション整合性スナップショットが作成されます。これには、VMware Toolsが仮想マシン上で実行されている必要があります。VMware Toolsが実行されていない場合、スナップショットは「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態になります。このオプションを有効にすると、バックアップ時間が長くなり、より多くのストレージ容量を使用する可能性があることに注意してください。さらに、VMのアクティブなRAMは、整合性のあるスナップショットには含まれません。
   - **SnapMirror**ボリュームと**Snapshot**のフォーマット：次のいずれかのオプションを選択します。
     - スナップショットのコピーにカスタム名形式を使用する：スナップショットの命名規則を選択します。空欄のままにした場合、各スナップショット名の末尾にタイムスタンプが追加されます。
     - **SnapMirror**ボリューム形式の指定：デフォルトのSnapMirrorボリューム名を変更するには、プレフィックス、サフィックス、またはその両方を指定します。デフォルトでは、SnapMirrorボリュームはソースボリュームの名前を継承します。
   - 最大転送速度：帯域幅の使用制限を設定しない場合は、*無制限*を選択してください。転送速度を制限する場合は、*制限付き*を選択し、オブジェクトストレージへのバックアップのアップロードに割り当てるネットワーク帯域幅を1～1,000Mbpsの間で選択します。デフォルトでは、ONTAPはシステム内のボリュームからオブジェクトストレージへバックアップデータを転送するために、無制限の帯域幅を使用できます。バックアップトラフィックがワークロードに影響を与える場合は、転送用のネットワーク帯域幅を削減してください。
   - バックアップ再試行：障害や中断が発生した場合にジョブを再試行するには、*障害発生時にジョブの再試行を有効にする*を選択します。スナップショットおよびバックアップ ジョブの最大再試行回数と再試行間隔を入力してください。再試行回数は10未満である必要があります。

     スナップショット頻度が 1 時間に設定されている場合、再試行回数と合わせた最大遅延は 45 分を超えてはなりません。

   - ランサムウェア スキャン: 各バケットでランサムウェア スキャンを有効にするかどうかを選択します。これには、オブジェクト ストレージに対する DataLock ロックが必要です。スキャンの頻度を日単位で入力します。このオプションは、AWS および Microsoft Azure オブジェクト ストレージに適用されます。このオプションは、クラウド プロバイダーによっては追加料金が発生する場合があることに注意してください。

- 通知：バックアップ操作に関するメール通知を有効にするかどうかを選択してください。通知をトリガーするイベントを選択できます。たとえば、バックアップが成功したとき、失敗したとき、または警告付きで完了したときなどです。

### ポリシーを削除する

不要になったポリシーは削除できます。

ワークロードに関連付けられているポリシーを削除することはできません。

手順

1. コンソールで、[保護] > [バックアップと復元] に移動します。
2. ポリシー オプションを選択します。
3. 削除するポリシーを選択します。
4. *アクション*を選択します ••• アイコンをクリックし、[削除] を選択します。
5. 操作を確認し、[削除] を選択します。

# NetApp Backup and Recoveryで VMware ワークロードをバックアップする

データが確実に保護されるように、オンプレミスのONTAPシステムから VMware VM とデータストアを Amazon Web Services、 Azure NetApp Files、またはStorageGRIDにバックアップします。バックアップは自動的に生成され、パブリック クラウド アカウントまたはプライベート クラウド アカウントのオブジェクト ストアに保存されます。

- ワークロードをスケジュールに基づいてバックアップするには、バックアップおよび復元操作を管理するポリシーを作成します。手順については"保護ポリシーを作成する"を参照してください。
- 保護グループを作成して、リソース セットのバックアップおよび復元操作を管理します。詳細については、"保護グループの作成と管理"を参照してください。
- 今すぐワークロードをバックアップします (今すぐオンデマンド バックアップを作成します)。

### オンデマンドバックアップでワークロードを今すぐバックアップ

オンデマンド バックアップをすぐに作成します。システムに変更を加える予定があり、開始する前にバックアップがあることを確認したい場合は、オンデマンド バックアップを実行することをお勧めします。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します" 。

手順

1. [バックアップとリカバリ] メニューから、[インベントリ] を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。

3. アクションアイコンを選択します ••• > 詳細を表示。
4. * Protection Groups * 、 * Datastores * 、 * Virtual machines * 、または * Tags * のメニュー項目を選択します。
5. バックアップする保護グループ、データストア、仮想マシン、またはタグ付きリソースを選択します。
6. アクションアイコンを選択します ••• > 今すぐバックアップ。

> バックアップに適用されるポリシーは、保護グループ、データストア、仮想マシン、またはタグ付きリソースに割り当てられているポリシーと同じです。

7. スケジュール層を選択します。
8. *今すぐバックアップ*を選択します。

# NetApp Backup and Recoveryを使用したVMwareワークロードのクローニング

NetApp Backup and Recoveryを使用して、プライマリまたはセカンダリのスナップショットからVMware仮想マシンの書き込み可能なクローンを作成します。VMクローンを使用すると、本番データに影響を与えることなく、テスト、統合、トレーニング用の仮想マシンを作成および管理できます。

必要なコンソール ロール バックアップおよびリカバリのスーパー管理者またはバックアップおよびリカバリのバックアップ管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します" 。

開始する前に

スナップショットをクローンする仮想マシンが保護グループに追加され、バックアップされていることを確認してください。

## VMware VMのクローンを作成する

既存のスナップショットからすぐにクローンを作成します。

> VMクローンを作成した後、元のVMとのIPアドレスの競合を防ぐため、クローンした仮想マシンのIPアドレスを更新する必要があります。

手順

1. NetApp Consoleメニューから、保護 > バックアップとリカバリ を選択します。
2. *ワークロード*で、*VMware*タイルを選択します。
3. *Clone*を選択します。
4. *新しいクローンを作成*を選択します。
5. *Select virtual machines*セクションで、保護グループを選択します。保護グループ内のVMが選択リストに表示されます。
6. クローンする仮想マシンをリストから1つ以上選択してください。選択した仮想マシンは、右側の選択済み仮想マシン一覧に表示されます。

7. 完了したら、* Next *を選択します。
8. 「スナップショットを選択」ページの「スナップショット」セクションで、作成日でスナップショットを絞り込むための期間を選択します。
9. クローン作成のベースとして使用する既存のスナップショットをリストから選択し、*次へ*を選択します。

   スナップショットが複数の場所に保存されている場合は、**Select snapshot location** が表示されます。

10. 使用するスナップショットの場所を選択し、*次へ*を選択します。
11. **Destination settings** ページで、以下の操作を行います：
    a. VMクローンを作成する宛先のvCenterサーバーのFQDNまたはIPアドレスを選択してください。
    b. クローンをホストするESXiホストを選択してください。
    c. クローンのネットワーク環境を選択します。
    d. **Virtual machine name** フィールドに、新しくクローンした仮想マシンの接尾辞を入力します。
12. *Clone*を選択します。

## クローンのスプリット

VMware VMのクローンを分割することで、親ボリュームから切り離すことができます。分割されると、クローンは親ボリュームに依存しない独立したボリュームになります。

分割後、クローンされた仮想マシンに関連付けられていたデータストアは、新しい独立したデータストアになります。クローンされた仮想マシン自体は保持されます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. クローンを選択します。
3. アクションアイコンを選択します > 分割クローン。
4. ダイアログの詳細を確認し、*Split*を選択します。
5. 新しい独立した VM が作成されると、* Inventory * ページで確認できます。

## クローンを削除する

VMware VMクローンを削除できます。VMクローンを削除すると、クローンはvCenterから削除され、VMに関連付けられたデータストアはマウント解除され、ストレージシステムから削除されます。

ポリシーによってクローンが保護されている場合、クローンとそのジョブの両方が削除されます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. クローンを選択します。
3. アクションアイコンを選択し、*削除*を選択します。
4. 削除確認ダイアログボックスで、削除の詳細を確認します。

5. *削除*を選択します。
6. クローンを削除すると、インベントリ ページから削除されます。

# VMwareワークロードを復元する

## NetApp Backup and Recoveryで VMware ワークロードを復元する

NetApp Backup and Recoveryを使用して、スナップショット、セカンダリ ストレージに複製されたワークロード バックアップ、またはオブジェクト ストレージに保存されたバックアップから VMware ワークロードを復元します。

これらの場所から復元

異なる開始場所からワークロードを復元できます。

- プライマリロケーション（ローカルスナップショット）からの復元
- セカンダリストレージ上の複製されたリソースから復元する
- オブジェクトストレージバックアップからの復元

これらのポイントに復元する

以下のポイントまでデータを復元できます:

- 元の場所に復元: VM は元の場所、同じ vCenter 展開、ESXi ホスト、およびデータストアに復元されます。VM とそのすべてのデータが上書きされます。
- 別の場所に復元: VM の復元先として、別の vCenter、ESXi ホスト、またはデータストアを選択できます。これは、異なる場所や状態にある同じ VM の異なるコピーを管理するのに役立ちます。

オブジェクトストレージからの復元に関する考慮事項

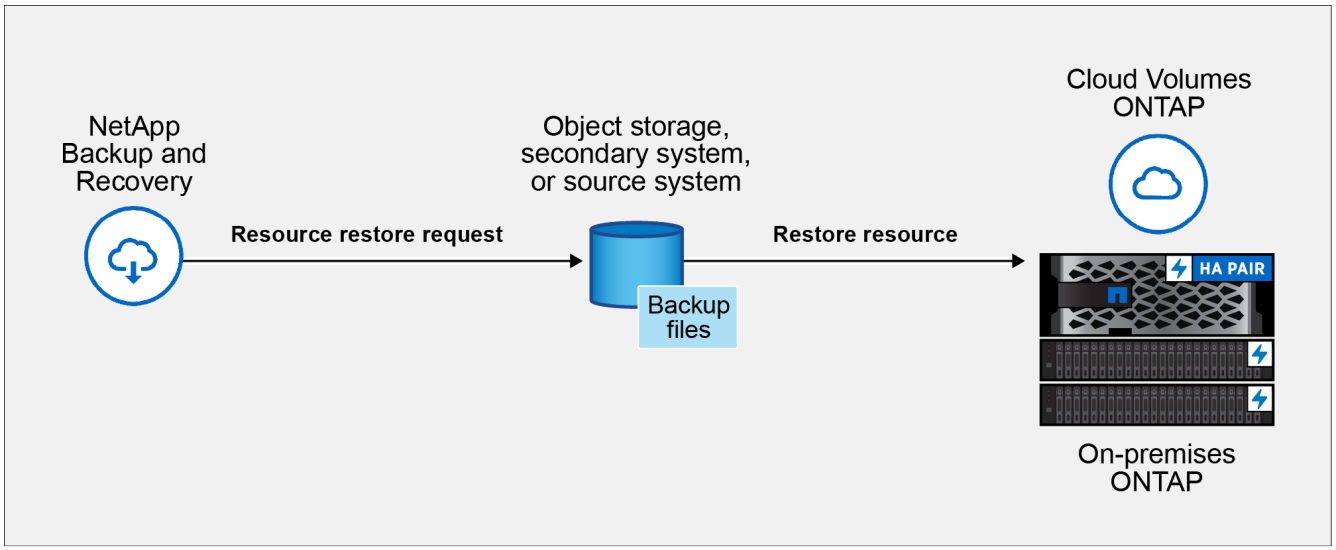
オブジェクトストレージ内のバックアップファイルに対してランサムウェア対策が有効になっている場合、復元前に追加のチェックを実行するように求められます。スキャンを実行することをお勧めします。

バックアップ ファイルにアクセスするには、クラウド プロバイダーに追加料金を支払う必要がある場合があります。

ワークロードの復元の仕組み

ワークロードを復元すると、次のことが起こります。

- ローカル スナップショットまたはリモート バックアップからワークロードを復元する場合、 NetApp Backup and Recovery は、元の場所に復元する場合は元の VM を上書きし、別の場所に復元する場合は新しいリソースを作成します。
- 複製されたワークロードからリストアする場合、ワークロードを元のオンプレミスのONTAPシステムまたは別のオンプレミスのONTAPシステムにリストアできます。




- オブジェクト ストレージからバックアップを復元する場合、データを元のシステムまたはオンプレミスのONTAPシステムに復元できます。

[復元] ページ (検索と復元) では、正確な名前、場所、または最終日付を覚えていなくても、フィルターを使用してスナップショットを検索することでリソースを復元できます。

復元オプション（検索と復元）からワークロード データを復元します。

復元オプションを使用して VMware ワークロードを復元します。スナップショットは、名前またはフィルターを使用して検索できます。

必要な**NetApp Console**ロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ リストア管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します" 。

手順

1. NetApp Backup and Recoveryメニューから、[復元] を選択します。
2. 名前検索フィールドの右側にあるドロップダウン リストから、**VMware** を選択します。
3. 復元するリソースの名前を入力するか、復元するリソースが配置されている vCenter、データセンター、またはデータストアでフィルタリングします。

   検索条件に一致する仮想マシンのリストが表示されます。
4. リストから復元する VM を見つけて、その VM のオプション メニュー ボタンを選択します。
5. 表示されるメニューで、「仮想マシンの復元」を選択します。

   その仮想マシン上に作成されたスナップショット (復元ポイント) のリストが表示されます。デフォルトでは、[時間枠] ドロップダウンで選択した時間枠の最新のスナップショットが表示されます。

   各スナップショットについて、場所 列の点灯したアイコンは、スナップショットが使用可能なストレージの場所 (プライマリ、セカンダリ、またはオブジェクト ストレージ) を示します。
6. 復元するスナップショットのラジオ ボタンを有効にします。
7. *次へ*を選択します。

スナップショットの場所のオプションが表示されます。

8. スナップショットの復元先を選択します。
   - ローカル: ローカルの場所からスナップショットを復元します。
   - セカンダリ: リモート ストレージの場所からスナップショットを復元します。
   - オブジェクト ストア: オブジェクト ストレージからスナップショットを復元します。

     セカンダリ ストレージを選択した場合は、ドロップダウン リストから保存先の場所を選択します。
9. 続行するには、[次へ] を選択します。
10. 復元先と設定を選択します。

目的地の選択

元の場所へのリストア

元の場所に復元する場合、宛先の vCenter、ESXi ホスト、データストア、または VM の名前を変更することはできません。復元操作により元の VM が上書きされます。

1. 元の場所 ペインを選択します。
2. 次のいずれかのオプションを選択します。
   - *復元前オプション*セクション:
     - プレスクリプト: 復元操作を開始する前にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
   - *復元後のオプション*セクション:
     - 仮想マシンを再起動: 復元操作が完了し、復元後のスクリプトが適用された後に仮想マシンを再起動するには、このオプションを有効にします。
     - **Postscript**: 復元が完了した後にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
3. *復元*を選択します。

別の場所へのリストア

別の場所に復元する場合は、宛先の vCenter、ESXi ホスト、データストア、および VM の名前を変更して、別の場所または別の名前で VM の新しいコピーを作成できます。

1. 代替の場所 ペインを選択します。
2. 次の情報を入力してください。
   - *宛先設定*セクション:
     - **vCenter FQDN** または **IP** アドレス: スナップショットを復元する vCenter サーバーを選択します。
     - **ESXi** ホスト: スナップショットを復元するホストを選択します。
     - ネットワーク: スナップショットを復元するネットワークを選択します。
     - データストア: ドロップダウン リストから、スナップショットを復元するデータストアの名前を選択します。
     - 仮想マシン名: スナップショットを復元する仮想マシンの名前を入力します。名前がデータストア内に既に存在する VM と一致する場合、Backup and Recovery は現在のタイムスタンプを追加して名前を一意にします。
   - *保存先ストレージ*セクション（オブジェクトストアから復元する場合のみ表示されます）：
     - デフォルトのストレージ場所を変更する：このオプションを有効にすると、ソースストレージの場所にアクセスできない場合や、ストレージがいっぱいになった場合に、オブジェクトストアのバックアップを別のStorage VMに復元できます。別のクラスタ、Storage VM、またはアグリゲートを選択してください。
   - *復元前オプション*セクション:
     - クイック リストア：このオプションを有効にすると、Backup and Recoveryはオブジェクトストアから VMメタデータ（ファイル、LUN、および名前空間）のみをリストアするように指

示されます。これにより、フル リストアよりも速くボリュームを利用できるようになります。

- プレスクリプト: 復元操作を開始する前にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。

◦ *復元後のオプション*セクション:

- 仮想マシンを再起動: 復元操作が完了し、復元後のスクリプトが適用された後に仮想マシンを再起動するには、このオプションを有効にします。
- **Postscript**: 復元が完了した後にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。

3. *復元*を選択します。

## バックアップから特定の仮想ディスクを復元する

従来の VM のプライマリ バックアップまたはセカンダリ バックアップから、既存の仮想ディスク (VMDK)、または削除あるいは切断された仮想ディスクを復元できます。これにより、特定の VM データまたはアプリケーションのみを復元できるため、特定のデータのみが影響を受ける状況では、VM 全体とそれに関連付けられたすべての仮想ディスクを復元する必要がなくなります。仮想ディスクが復元されると、元の VM に接続され、使用できるようになります。

VM 上の 1 つ以上の仮想マシン ディスク (VMDK) を同じデータストアまたは異なるデータストアに復元できます。

NFS環境でのリストア処理のパフォーマンスを向上させるには、VMwareアプリケーションのvStorage API for Array Integration（VAAI）を有効にします。

開始する前に

- バックアップが存在している必要があります。
- 転送中のVMはリストアできません。

  リストアするVMがvMotionまたはStorage vMotionの状態であってはいけません。

タスク概要

- VMDKがVMから削除されているか切断されている場合、リストア処理によってVMDKがVMに接続されます。
- VMが配置されているFabricPoolのストレージ階層が使用できない場合、リストア処理が失敗することがあります。
- 接続処理とリストア処理では、デフォルトのSCSIコントローラを使用してVMDKが接続されます。ただし、NVMeディスクを使用してVMに接続されたVMDKがバックアップされる際、接続処理とリストア処理では、利用可能な場合はNVMeコントローラが使用されます。

手順

1. NetApp Backup and Recoveryメニューから、[復元] を選択します。
2. 名前検索フィールドの右側にあるドロップダウン リストから、**VMware** を選択します。
3. 復元するリソースの名前を入力するか、復元するリソースが配置されている vCenter、データセンター、またはデータストアでフィルタリングします。

   検索条件に一致する仮想マシンのリストが表示されます。

4. リストから復元する VM を見つけて、その VM のオプション メニュー ボタンを選択します。
5. 表示されるメニューで、「仮想ディスクの復元」を選択します。

   その仮想マシン上に作成されたスナップショット (復元ポイント) のリストが表示されます。デフォルトでは、[時間枠] ドロップダウンで選択した時間枠の最新のスナップショットが表示されます。

   各スナップショットについて、場所 列の点灯したアイコンは、スナップショットが使用可能なストレージの場所 (プライマリ、セカンダリ、またはオブジェクト ストレージ) を示します。

6. 復元するスナップショットのラジオ ボタンを有効にします。
7. *次へ*を選択します。

   スナップショットの場所のオプションが表示されます。

8. スナップショットの復元先を選択します。
   - ローカル: ローカルの場所からスナップショットを復元します。
   - セカンダリ: リモート ストレージの場所からスナップショットを復元します。
   - オブジェクト ストア: オブジェクト ストレージからスナップショットを復元します。

     セカンダリ ストレージを選択した場合は、ドロップダウン リストから保存先の場所を選択します。

9. 続行するには、[次へ] を選択します。
10. 復元先と設定を選択します。

目的地の選択

元の場所へのリストア

元の場所に復元する場合、宛先の vCenter、ESXi ホスト、データストア、または仮想ディスクの名前を変更することはできません。元の仮想ディスクは上書きされます。

1. 元の場所 ペインを選択します。
2. *宛先設定*セクションで、復元する仮想ディスクのチェックボックスをオンにします。
3. 次のいずれかのオプションを選択します。
   - *復元前オプション*セクション:
     - プレスクリプト: 復元操作を開始する前にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
   - *復元後のオプション*セクション:
     - **Postscript**: 復元が完了した後にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
4. *復元*を選択します。

別の場所へのリストア

別の場所に復元する場合は、宛先データストアを変更できます。選択したデータストアに関係なく、復元操作後に仮想ディスクは元の VM に接続されます。

1. 代替の場所 ペインを選択します。
2. *宛先設定*セクションで、復元する仮想ディスクのチェックボックスをオンにします。
3. 選択した仮想ディスクの場合:
   a. 仮想ディスクの別のデータストア復元ターゲットを選択するには、「データストアの選択」を選択します。
   b. *選択*を選択して選択を確認し、選択ウィンドウを閉じます。
4. 次のいずれかのオプションを選択します。
   - *復元前オプション*セクション:
     - プレスクリプト: 復元操作を開始する前にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
   - *復元後のオプション*セクション:
     - **Postscript**: 復元が完了した後にカスタム スクリプトを実行して追加のタスクを自動化するには、このオプションを有効にします。実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
5. *復元*を選択します。

## VMwareのファイルとフォルダをリストアする

ゲストファイルとフォルダを復元する際の要件と制限

# WindowsまたはLinuxゲストOS上で、仮想マシンディスク（VMDK）からファイルやフォルダを復元できます。

## ゲスト リストアのワークフロー

ゲストOSリストア処理には、次の手順が含まれます。

1. 接続

   仮想ディスクをゲストVMまたはプロキシVMに接続し、ゲスト ファイル リストア セッションを開始します。

2. 待機

   参照および復元する前に、接続操作が完了するまで待機してください。アタッチ操作が完了すると、ゲスト ファイルの復元セッションが自動的に作成されます。

3. ファイルまたはフォルダの選択

   仮想ディスクファイルを参照または検索し、復元するファイルまたはフォルダを1つ以上選択します。

4. リストア

   選択したファイルまたはフォルダを指定した場所にリストアします。

## ゲスト ファイルとフォルダをリストアするための前提条件

VMDKからファイルやフォルダをリストアする前に、すべての要件を確認してください。

- VMware Toolsがインストールされ、実行されている必要があります。

  NetApp Backup and Recoveryは、VMwareツールの情報を使用して、VMwareゲストOSへの接続を確立します。

- 復元元のバックアップ スナップショットと VMDK を知っておく必要があります。
- 接続する仮想ディスクは、NetApp Backup and Recoveryバックアップに含まれている必要があります。

  復元するファイルまたはフォルダを含む仮想ディスクは、NetApp Backup and Recoveryを使用して実行された VM バックアップに含まれている必要があります。

- プロキシVMを使用するには、プロキシVMを設定する必要があります。

  仮想ディスクをプロキシVMに接続する場合は、接続およびリストア処理を開始する前にプロキシVMを設定しておく必要があります。

- 英語のアルファベット以外を使った名前のファイルの場合は、単一のファイルとしてではなく、ディレクトリにリストアする必要があります。

  日本語の漢字など、アルファベット以外の名前のファイルをリストアするには、ファイルが配置されているディレクトリをリストアします。

ゲストOSのサポートに関する最新情報については、 "NetApp Interoperability Matrix Tool（IMT）"を参照してください。

**Windows**ゲスト

- Windows ゲスト OS は Windows Server 2008 R2 以降を実行している必要があります。

  サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool（IMT）"。

- ターゲット VM の資格情報には、ユーザー名が「Administrator」の組み込みドメインまたはローカル管理者アカウントが使用されます。復元操作を開始する前に、仮想ディスクを接続する VM の資格情報を構成します。アタッチ操作と復元操作の両方に資格情報が必要です。ワークグループ ユーザーは、組み込みのローカル管理者アカウントを使用できます。

  組み込みの管理者アカウントではなく、VM内の管理者権限を持つアカウントを使用する必要がある場合は、ゲストVMのUACを無効にする必要があります。

**Linux**ゲスト

- 以下のゲストOSディストリビューションがサポートされています：
  - Red Hat Enterprise Linux
  - Ubuntu
  - Debian
- 実行アカウントにはroot権限またはsudo権限が必要です。
- クロスVM復元（異なるLinux VMへの復元）を行う場合、ターゲットVMでSSHが実行されている必要があります。

ゲスト ファイル リストアに関する制限事項

ゲスト OS からファイルまたはフォルダーを復元する前に、機能の制限に注意する必要があります。

- ゲストOS内でダイナミック ディスク タイプをリストアすることはできません。
- 暗号化されたファイルまたはフォルダをリストアした場合、暗号化属性は保持されません。
- ファイルまたはフォルダを暗号化されたフォルダにリストアすることはできません。
- 隠しファイルとフォルダーはファイル参照ページに表示されますが、フィルタリングすることはできません。
- 異なるオペレーティングシステムを搭載したゲスト間では、ファイルやフォルダを復元することはできません（別のVMに復元する場合、デスティネーションのOSタイプはソースのOSタイプと同じである必要があります）。
- NTFSファイルシステムからFATファイルシステムにリストアすることはできません。

  NTFS形式からFAT形式にリストアしようとした場合、FATファイルシステムはWindowsセキュリティ属性をサポートしていないため、NTFSセキュリティ記述子はコピーされません。

- クローニングされたVMDKまたは初期化されていないVMDKからゲスト ファイルをリストアすることはできません。

- ファイルのディレクトリ構造はリストアできません。

  ネストされたディレクトリからファイルを復元する場合、システムはディレクトリ構造ではなくファイルのみを復元します。ディレクトリ ツリー全体を復元するには、最上位のディレクトリをコピーします。

- vVol VMから別のホストにゲスト ファイルをリストアすることはできません。
- 暗号化されたゲスト ファイルはリストアできません。

仮想ディスクからファイルとフォルダを復元する

# 仮想ディスクから個々のファイルまたはフォルダを、元の仮想マシンまたは別の仮想マシンに復元します。これは、仮想マシン全体を復元する必要はなく、特定のファイルやフォルダだけが必要な場合に便利です。

仮想ディスクからファイルとフォルダを復元する

仮想ディスクからファイルやフォルダを元の仮想マシン、または別の仮想マシンに復元します。仮想ディスクを元の仮想マシンに接続したくない場合は、代わりにプロキシ仮想マシンに接続することもできます。

開始する前に

- "ゲストファイルとフォルダを復元する際の要件と制限"の前提条件と制限事項を確認してください。
- プロキシVMを使用してファイルとフォルダを復元するには、ファイルとフォルダの復元プロセスを開始する前に、プロキシVMが既に構成されていることを確認してください。
- ファイルやフォルダを復元する前に、NetApp Backup and Recoveryでソース仮想ディスクと宛先VMの認証情報を作成する必要があります。NetApp Backup and Recoveryでは、ファイルやフォルダを復元する際に、これらの認証情報を使用して仮想ディスクと宛先VMに対して認証を行います。

タスク概要

ファイルまたはフォルダの復元パフォーマンスは、復元対象のファイルまたはフォルダのサイズと、復元対象のファイルまたはフォルダの数という2つの要因に依存します。復元対象のデータセットのサイズが同じ場合、多数の小さなファイルを復元するには、少数の大きなファイルを復元する場合と比べて、予想以上に時間がかかる可能性があります。

リモートの仮想マシンに復元することは可能ですが（これはクロスVM復元と呼ばれます）、復元元と復元先のオペレーティングシステムは同じである必要があります。

1つのVMで一度に実行できる接続処理またはリストア処理は1つだけです。同じVMに対して並行して接続処理またはリストア処理を実行することはできません。

ファイルとフォルダの復元機能を使用すると、システムファイルや隠しファイルを表示および復元したり、暗号化されたファイルを表示したりできます。既存のシステムファイルを上書きしたり、暗号化されたファイルを暗号化されたフォルダに復元したりしないでください。復元操作中、ゲストファイルの隠し属性、システム属性、および暗号化属性は復元されたファイルには保持されません。予約済みパーティションを表示または閲覧すると、エラーが発生する可能性があります。

**VMDK**を元の**VM**に接続して、ファイルとフォルダをリストアします

仮想ディスクからゲストファイルとフォルダを元の（ソース）仮想マシンに復元します。

手順

1. NetApp Backup and Recoveryメニューから、[復元] を選択します。
2. ページ右上のワークロード一覧から*VMware*を選択してください。
3. 仮想マシンの一覧で、復元するファイルが含まれているVMの[アクション]アイコン ••• を選択します。
4. *ファイルとフォルダの復元*を選択します。
5. 復元するスナップショットを選択し、[次へ] を選択します。
6. 復元するスナップショットの場所を選択します。セカンダリ ロケーションを選択する場合は、リストからセカンダリ スナップショットを選択します。
7. *次へ*を選択します。
8. リストから、復元する必要のあるファイルとフォルダーが含まれている仮想ディスクを選択し、**Next** を選択します。
9. *Guest virtual machine details* ページで、以下の操作を行います：

   a. * ゲスト仮想マシンの詳細 * セクションで、* 元の仮想マシン * を選択して、仮想ディスクを元の仮想マシンに接続します。

   b. *ゲスト仮想マシンの認証情報*セクションで、ソース仮想ディスクと宛先VMの認証情報をまだ保存していない場合は、*認証情報の追加*を選択し、WindowsまたはLinuxの認証情報を入力して、*追加*を選択します。

      ⓘ ソースVMと宛先VMは同じOSファミリーで動作している必要がありますが、OSのバージョンは異なっていても構いません。

   c. リストから、使用する仮想マシンのクレデンシャルを選択します。

   d. *次へ*を選択します。

      NetApp Backup and Recoveryは、仮想ディスクを元のVMにアタッチし、隠しファイルを含むすべてのファイルとフォルダを表示します。Windowsゲストの場合、システムで予約済みのパーティションを含め、すべてのパーティションにドライブ文字を割り当てます。

   ファイルブラウザーペインの近くにある虫眼鏡（検索）アイコンを使用して、ファイルやフォルダーを検索できます。パターンマッチングはサポートされていませんが、ファイル名または拡張子の一部に基づいてファイルやフォルダーを検索することは可能です。

10. 復元するファイルまたはフォルダを選択します。

    復元対象として選択したファイルとフォルダは、画面右側のペインに一覧表示されます。

11. *次へ*を選択します。
12. 「復元先パス」セクションで、選択したファイルを復元する宛先VMのパスとファイルシステム上の場所を入力します：

- Windowsゲストの場合は、UNC共有パスを入力してください：
  - IPv4パスの例： `\\10.60.136.65\c$`
  - IPv6パスの例： `\\fd20-8b1e-b255-832e-61.ipv6-literal.net\C\restore`
- Linuxゲストの場合は、ローカルファイルシステムのパス、またはリモートゲストのアドレスとパスを入力してください：
  - ローカルパスの例： `/home/user/documents/file.txt`
  - IPv4パスの例： `10.60.136.65:/home/user/restore/`
  - IPv6パスの例： `fd20-8b1e-b255-832e-61.ipv6-literal.net:/home/user/restore/`

同じ名前のファイルが存在する場合は、上書きするかスキップするかを選択できます。

13. 「Post-restore-options」セクションでは、*Disconnect guest session after the restore completes*設定を有効にすることで、復元完了後にゲストセッションを切断することができます。これにより、仮想ディスクが切り離され、データストアがアンマウントされます。つまり、追加のファイルやフォルダの復元操作を実行する前に、ゲストセッションに再接続する必要があるということです。
14. *復元*を選択します。

    ジョブ監視ページで復元の進行状況を確認できます。

**VMDK**をプロキシ**VM**に接続して、ファイルとフォルダを復元します。

プロキシ VM（元の VM と同じvCenter上の別の VM）を使用して、仮想ディスクを元の VM に接続したくない場合にゲスト ファイルとフォルダーを復元します。

手順

1. NetApp Backup and Recoveryメニューから、[復元] を選択します。
2. ページ右上のワークロード一覧から*VMware*を選択してください。
3. 仮想マシンの一覧で、復元するファイルが含まれているVMの[アクション]アイコン ••• を選択します。
4. *ファイルとフォルダの復元*を選択します。
5. 復元するスナップショットを選択し、[次へ] を選択します。
6. 復元するスナップショットの場所を選択します。セカンダリ ロケーションを選択する場合は、リストからセカンダリ スナップショットを選択します。
7. *次へ*を選択します。
8. リストから、復元する必要のあるファイルとフォルダーが含まれている仮想ディスクを選択し、**Next** を選択します。
9. *Guest virtual machine details* ページで、以下の操作を行います：
   a. *ゲスト仮想マシンの詳細*セクションで：
      i. **Proxy virtual machine** を選択して、仮想ディスクをプロキシ VM に接続します。
      ii. リストから、プロキシ VM が配置されている vCenter、データセンター、およびデータストアを選択します。

iii. プロキシVMとして使用するVMをリストから選択してください。仮想ディスクはこのVMに接続されます。選択したプロキシVMは右側のペインに表示されます。

b. *ゲスト仮想マシンの認証情報*セクションで、ソース仮想ディスクと宛先VMの認証情報をまだ保存していない場合は、*認証情報の追加*を選択し、WindowsまたはLinuxの認証情報を入力して、*追加*を選択します。

ソースVMと宛先VMは同じOSファミリーで動作している必要がありますが、OSのバージョンは異なっていても構いません。

c. リストから、使用する仮想マシンのクレデンシャルを選択します。

d. *次へ*を選択します。

NetApp Backup and Recoveryは、仮想ディスクをプロキシVMに接続し、隠しファイルを含むすべてのファイルとフォルダを表示します。Windowsゲストの場合、システムで予約済みのパーティションを含め、すべてのパーティションにドライブ文字を割り当てます。

ファイルブラウザーペインの近くにある虫眼鏡（検索）アイコンを使用して、ファイルやフォルダーを検索できます。パターンマッチングはサポートされていませんが、ファイル名または拡張子の一部に基づいてファイルやフォルダーを検索することは可能です。

10. 復元するファイルまたはフォルダを選択します。

復元対象として選択したファイルとフォルダは、画面右側のペインに一覧表示されます。

11. *次へ*を選択します。

12. 「復元先パス」セクションで、選択したファイルを復元する宛先VMのパスとファイルシステム上の場所を入力します：

- Windowsゲストの場合は、UNC共有パスを入力してください：
  - IPv4パスの例： `\\10.60.136.65\c$`
  - IPv6パスの例： `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`
- Linuxゲストの場合は、ローカルファイルシステムのパス、またはリモートゲストのアドレスとパスを入力してください：
  - ローカルパスの例： `/home/user/documents/file.txt`
  - IPv4パスの例： `10.60.136.65:/home/user/restore/`
  - IPv6パスの例： `fd20-8b1e-b255-832e—61.ipv6-literal.net:/home/user/restore/`

同じ名前のファイルが存在する場合は、上書きするかスキップするかを選択できます。

13. 「Post-restore-options」セクションでは、*Disconnect guest session after the restore completes*設定を有効にすることで、復元完了後にゲストセッションを切断することができます。これにより、仮想ディスクが切り離され、データストアがアンマウントされます。つまり、追加のファイルやフォルダの復元操作を実行する前に、ゲストセッションに再接続する必要があるということです。

14. *復元*を選択します。

ジョブ監視ページで復元の進行状況を確認できます。

### アクティブな **VMDK** マウントセッションを表示する

ファイルやフォルダを復元する際に、アクティブなゲストセッションを表示します。これは、現在開いているセッションに接続されているVMDKを表示します。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. ページ右上のワークロード一覧から*VMware*を選択してください。
3. *Live disk mount sessions*メニューを選択します。

   開いているVMDKマウントセッションの一覧が表示されます。関連するバックアップ、ソースVM、マウントパス、その他の情報を確認できます。

## ゲストファイルの復元のトラブルシューティング

ゲスト ファイルをリストアしようとすると、次のいずれかの状況が発生することがあります。

### ゲスト ファイル リストア セッションが空白

この問題は、ゲスト ファイルの復元セッションを作成し、そのセッション中にゲスト オペレーティング システムが再起動した場合に発生します。ゲスト OS の VMDK がオフラインのままになる可能性があるため、ゲスト ファイルの復元セッション リストは空白になります。

この問題を修正するには、ゲストOSでVMDKを手動でオンラインに戻します。VMDKがオンラインになると、ゲスト ファイル リストア セッションに正しい内容が表示されます。

### ゲスト ファイル リストアのディスク接続処理が失敗する

この問題は、ゲスト ファイルの復元操作を開始したときに、VMware ツールが実行されていてゲスト OS の資格情報が正しいにもかかわらず、ディスクの接続操作が失敗した場合に発生します。これが発生すると、次のエラーが返されます。

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMware Tools is running properly on the system and that the account used is an Administrator account. Error is SystemError vix error codes = (3016, 0).
```

この問題を修正するには、ゲストOSでVMware Tools Windowsサービスを再起動してから、ゲスト ファイル リストア処理を再試行します。

### ゲスト ファイル リストア セッションを中断してもバックアップが切断されない

この問題は、VM整合性バックアップからゲスト ファイル リストア処理を実行した場合に発生します。ゲスト ファイル リストア セッションがアクティブな間に、同じVMに対して別のVM整合性バックアップが実行されます。ゲスト ファイル リストア セッションが手動または24時間後に自動的に切断されても、セッションのバックアップは切断されません。

この問題を修正するには、アクティブ ゲスト ファイル リストア セッションから接続されていたVMDKを手動で切断します。

## 著作権に関する情報



## 商標に関する情報