Hyper-V ワークロードを保護する

NetApp Backup and Recovery

NetApp
June 25, 2026

目次

Hyper-V ワークロードを保護する

Hyper-V ワークロードの保護の概要

NetApp Backup and Recoveryを使用して Hyper-V VM を保護します。NetApp Backup and Recovery は、スタンドアロン インスタンスと FCI クラスタ インスタンスの両方に対して、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、VM 整合性のあるバックアップおよびリストア操作を提供します。System Center Virtual Machine Manager (SCVMM) によってプロビジョニングされ、CIFS 共有でホストされている Hyper-V 仮想マシンを保護することもできます。

Hyper-V ワークロードを Amazon Web Services S3 またはStorageGRIDにバックアップし、Hyper-V ワークロードをオンプレミスの Hyper-V ホストに復元できます。

NetApp Backup and Recoveryを使用して 3-2-1 保護戦略を実装します。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。
- 複数のメディア タイプにより、1 つのメディア タイプに物理的または論理的な障害が発生した場合でも、フェイルオーバーの実行可能性が確保されます。
- オンサイト コピーを使用すると、データを迅速に復元できます。また、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。

Hyper-V ホストを追加してリソースを検出すると、 NetApp Backup and Recoveryによって、仮想マシンの管理と保護を支援するために、Hyper-V ホストにNetApp Hyper-V プラグインとNetApp SnapCenter Windows FileSystem プラグインがインストールされます。

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

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

NetApp Backup and Recoveryで Hyper-V ワークロードを発見

NetApp Backup and Recovery、 Hyper-V 仮想マシンを保護する前に、それらを検出する必要があります。

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" 。

Hyper-Vホストを追加してリソースを検出する

Hyper-V ホスト情報を追加し、 NetApp Backup and Recovery で仮想マシンを検出できるようにします。各コンソール エージェント内で、リソースを検出するシステムを選択します。

Hyper-V ホストを追加してリソースを検出すると、 NetApp Backup and Recoveryによって、仮想マシンの管理と保護を支援するために、Hyper-V ホストにNetApp Hyper-V プラグインとNetApp SnapCenter Windows FileSystem プラグインがインストールされます。

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。

   NetApp Backup and Recoveryに初めてログインする場合、コンソールにはすでにシステムがあるがリソースがまだ検出されていないと、「新しいNetApp Backup and Recoveryへようこそ」ランディング 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. ワークロードの種類: **Hyper-V** を選択します。
   b. この Hyper-V ホストの資格情報をまだ保存していない場合は、[資格情報の追加] を選択します。
      i. このホストで使用するコンソール エージェントを選択します。
      ii. この資格情報の名前を入力します。
      iii. アカウントのユーザー名とパスワードを入力します。
      iv. *完了*を選択します。
   c. ホスト登録: ホストの FQDN または IP アドレス、資格情報、コンソール エージェント、およびポート番号を入力して、新しい Hyper-V ホストを追加します。FQDN がコンソール エージェントによって解決できない場合は、代わりに IP アドレスを使用します。FCI クラスターの場合は、FCI クラスター管理 IP アドレスを入力します。
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。

結果

NetApp Backup and Recovery がリソースを検出すると、インベントリ ページのワークロード リストに Hyper-V ワークロードが表示されます。

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

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 タイル (Microsoft SQL Server など) を選択します。
3. 「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。
4. 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。

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

一連の仮想マシンのバックアップ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 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。

- 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。見る"Hyper-Vワークロードを今すぐバックアップ"。
- 保護グループを削除します。

保護グループを作成する

保護するワークロードを保護グループにグループ化します。保護グループを作成して、ワークロードをまとめてバックアップおよび復元します。

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

- Hyper-V 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ます。詳細については、"NetApp Backup and RecoveryでのHyper-V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 メニューを選択します。
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ます。
7. 保護グループに含める VM を選択します。
8. *次へ*を選択します。
9. 保護グループに適用する*バックアップ ポリシー*を選択します。
10. *次へ*を選択します。
11. 構成を確認します。
12. 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。

更新されたホスト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たHyper-Vホストのタイムゾーンを使用します。ホスト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. Hyper-V ホストを更新して、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、保護グループとそれに関連付けられている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することができます。

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. 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Hyper-V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Hyper-Vバックアップ ポリシーを作成できます。

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
- ポリシーを編集する
- ポリシーの削除

> Hyper-V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タイムではなく、Hyper-Vホスト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、"Hyper-V 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。
   - ワークロードの種類：*Hyper-V*を選択してください。
   - 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。

- 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。
- 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。
- 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。
- 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。

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。
     - バックアップ後にアーカイブ ログを削除する：ログ バックアップが有効になっている場合、この機能をオプションで有効にして、NetApp Backup and RecoveryがOracleアーカイブ ログを保持する期間を制限できます。保持期間と、NetApp Backup and Recoveryがアーカイブ ログを削除する場所を選択できます。
   - プロバイダー：Kubernetesアプリケーションリソースをホストするストレージプロバイダーを選択し、プロバイダーへの認証に必要な認証情報を入力します。
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：
     - 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、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、仮想マシン上でHyper-V統合サービスとVSSの両方が実行されている必要があります。どちらかのサービスが実行されていない場合、代わりにcrash-consistentバックアップが取得されます。アプリケーション整合性を有効にすると、バックアップ時間とストレージ使用量の両方が増加する可能性があります。さらに、VMのゲストメモリ（RAM）は、アプリケーション整合性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でのDataLockロックが必要です。スキャンの頻度を日数で入力します。このオプションはオブジェクトストレージに適用されます。このオプションでは、クラウド プロバイダによっては追加料金が発生する場合があります。
   - 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。

ポリシーを編集する

バックアップアーキテクチャ、バックアップ頻度、保持ポリシー、およびポリシーに関するその他の設定を編集できます。

ポリシーを編集するときに別の保護レベルを追加することはできますが、保護レベルを削除することはできません。たとえば、ポリシーがローカル スナップショットのみを保護する場合は、セカンダリ ストレージへのレプリケーションやオブジェクト ストレージへのバックアップを追加できます。ローカル スナップショットとレプリケーションがある場合は、オブジェクト ストレージを追加できます。ただし、ローカル スナップショット、レプリケーション、およびオブジェクト ストレージがある場合は、これらのレベルのいずれかを削除することはできません。

オブジェクト ストレージにバックアップするポリシーを編集している場合は、アーカイブを有効にすることができます。

SnapCenterからリソースをインポートした場合、 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にいくつか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"。

必要な**NetApp Console**ロール

バックアップとリカバリのスーパー管理者。 "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 Consoleで、保護 > バックアップとリカバリ に移動します。
2. ポリシー オプションを選択します。
3. 編集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、[編集] を選択します。

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 Hyper-V ワークロードをバックアップする

オンプレミスのONTAPシステムから Amazon Web Services、 Azure NetApp Files、またはStorageGRIDに Hyper-V VM をバックアップして、データが保護されるようにします。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。

- スケジュールに従ってワークロードを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。見る"ポリシーを作成"手順についてはこちらをご覧ください。
- 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。見る"NetApp Backup and Recoveryを使用して Hyper-V ワークロードの保護グループを作成および管理します"詳細についてはこちらをご覧ください。
- 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

システムを変更する前にデータが保護されるように、オンデマンド バックアップを使用します。

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" 。

手順

1. 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、データストア、または*仮想マシン*タブを選択します。
5. バックアップする保護グループまたは仮想マシンを選択します。
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。

   バックアップでは、保護グループまたは仮想マシンに割り当てたのと同じポリシーが使用されます。

7. スケジュール層を選択します。
8. *バックアップ*を選択します。

Hyper-V ワークロードを復元する

NetApp Backup and Recoveryを使用して Hyper-V 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 Hyper-V 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 ストレージのバックアップからリストアする（元の場所にのみ）

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:

- 元の場所に復元します（プライマリストレージ、セカンダリストレージ、オブジェクトストレージから）
- 別の場所に復元する（プライマリ ストレージとセカンダリ ストレージの両方から）

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 ストレージでバックアップ ファイルを選択し、そのバックアップに対してランサムウェア保護がアクティブになっている場合（バックアップ ポリシーで Datalock とランサムウェア保護を有効にした場合）、データのリストア前にバックアップ ファイルに対して追加の整合性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推奨します。

バックアップ ファイルの内容にアクセスするには、クラウド プロバイダーから追加の送信コストが発生します。

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 バックアップ ファイルからワークロードを復元すると、 NetApp Backup and Recovery はバックアップのデータを使用して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復元する場合、ワークロード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」ページからは、リソースの正確な名前、保存場所、最後に正常に動作していた日付を覚えていなくても、リソースを復元できます。フィルターを使用してスナップショットを検索できます。

Hyper-V ワークロードを復元する

「復元」メニューを使用して、Hyper-Vワークロードを復元します。スナップショットは、名前で検索するか、フィルタを使用して検索できます。

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復元管理者ロール。 "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、**Hyper-V** 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 VM 名、VM ホスト、またはストレージ プールでフィルターします。

検索条件に一致するスナップショットのリストが表示されます。

4. 復元したいスナップショットの*復元*ボタンを選択します。

   可能な復元ポイントのリストが表示されます。

5. 使用する復元ポイントを選択します。
6. スナップショットのソースの場所を選択します。
7. 続行するには、[次へ] を選択します。
8. 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

   a. * Original location * ペインを選択します。元の場所に復元すると、* Destination settings * セクションを展開することで保存先設定を表示できますが、変更することはできません。
   b. 復元後のオプション セクションで、次のオプションを検討してください。
      - 仮想マシンを起動: このオプションを有効にすると、復元後に新しい仮想マシンを起動できます。

   別の場所へのリストア

   a. 代替の場所 ペインを選択します。
   b. 宛先設定: セクションで、次の情報を入力します。
      - **Hyper-V FQDN** または **IP** アドレス: 宛先 Hyper-V ホストの完全修飾ドメイン名または IP アドレスを入力します。
      - ネットワーク: スナップショットを復元する宛先ネットワークを選択します。
      - 仮想マシン名: 復元する仮想マシンの名前を入力します。
      - 宛先場所: 復元されたデータを保存する宛先フォルダまたは CIFS 共有を入力します。
   c. 復元前オプション セクションで、次のオプションを検討してください。
      - クイック復元: このオプションを有効にすると、復元された VM をすぐに使用できるようになります。ボリューム全体ではなく、VM の実行に必要なファイルのみがオブジェクト ストアから復元されます。
   d. *復元後のオプション*セクションで、次のオプションを検討してください。
      - 仮想マシンを起動: このオプションを有効にすると、復元後に新しい仮想マシンを起動できます。

9. *復元*を選択します。

Hyper-V VMバックアップからファイルとフォルダをリストアする

プライマリストレージまたはセカンダリストレージ上のHyper-V VMバックアップから、ファイルとフォルダをWindowsゲストVMにリストアします。

ファイルとフォルダを復元する

スナップショットから仮想ディスクをマウントし、そこからファイルとフォルダを元の（ソース）Windows VMに復元します。

開始する前に

ファイルとフォルダーを復元する前に、NetApp Backup and Recovery でソース VM の資格情報を作成する必要があります。この認証情報は、復元プロセス中に仮想マシンとの認証を行うために使用されます。

タスク概要

仮想ディスクをマウントしてファイルとフォルダの復元セッションを開くと、そのセッションは48時間アクティブな状態を維持します。

復元パフォーマンスは、復元するファイルまたはフォルダのサイズと数の両方に依存します。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方が、少数の大きなファイルを復元するよりも一般的に時間がかかります。

ファイルやフォルダを復元する際は、以下の点に注意してください：

- 現時点では、LinuxゲストVMにファイルやフォルダを復元することはできません。
- 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のファイルやフォルダの復元はサポートされていません。
- 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。
- 予約済みパーティションを表示または参照すると、エラーが発生する可能性があります。
- 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。
- システムファイルや隠しファイルを表示・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。

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*Hyper-V*を選択してください。
3. 仮想マシンのリストで、復元するファイルまたはフォルダを含むVMの*復元*アクションを選択します。
4. *ファイルとフォルダ*を選択します。
5. *Restore from snapshots*ページで、次の操作を実行します：
   a. 必要に応じて、作成時間でSnapshotのリストを絞り込む期間を選択します。
   b. 復元するプライマリストレージまたはセカンダリストレージ上のスナップショットを選択し、*次へ*を選択します。
6. 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。
7. *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. オプションとして、*ゲスト仮想マシンの資格情報*セクションで、ソース仮想ディスクと宛先VMの資格情報をまだ保存していない場合は、*資格情報の追加*を選択し、Windows資格情報を入力して、*追加*を選択します。

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に接続し、隠しファイルや隠しフォルダを含むすべてのファイルとフォルダを表示します。システムで予約済みのパーティションを含む、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。

8. _復元するファイルまたはフォルダーを選択してください_ページで、次の操作を行います：

a. 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ーは、*選択したファイルとフォルダー*エリアに表示されます。

b. *次へ*を選択します。

9. *Guest file restore - destination* ページで、以下の操作を行います：

a. 「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とファイルシステムの場所へのUNCパスを入力します：

- 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`

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。

10. 「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。

11. *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。

アクティブなライブディスクマウントセッションを管理する

NetApp Backup and Recovery内から、アクティブなHyper-Vファイルおよびフォルダのリストアセッションを表示、使用、および削除できます。

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*Hyper-V*を選択してください。
3. *Live disk mount sessions*メニューを選択します。

   開いている仮想ディスクのマウント セッションの一覧が表示されます。

4. オプションとして、セッションを使用してファイルとフォルダーをゲストVMに復元するには、セッションの[アクション]メニュー ••• を開き、*ファイルとフォルダーを復元*を選択します。
5. 必要に応じて、セッションを削除するには、セッションの [アクション] メニュー ••• を開き、*削除*を選択します。