KVMワークロードを保護する

NetApp Backup and Recovery

NetApp
June 25, 2026

目次

KVMワークロードを保護する

KVM ワークロードの保護の概要

NetApp Backup and Recoveryを使用して、管理対象の KVM VM とストレージ プールを保護します。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、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。バックアップとリカバリを使用して KVM ホストと VM を保護する前に、Apache CloudStack などの管理プラットフォームで KVM ホストと VM を管理する必要があります。

KVM ワークロードを Amazon Web Services S3、 Azure NetApp Files、またはStorageGRIDにバックアップし、KVM ワークロードをオンプレミスの KVM 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。
- 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を使用して、KVM ワークロードに関連する次のタスクを実行できます。

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

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

NetApp Backup and Recovery、 KVM ホストと仮想マシンを保護する前に検出する必要があります。KVM ホストと VM をバックアップとリカバリに追加する前に、Apache CloudStack などの管理プラットフォームで管理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" 。

管理プラットフォーム、KVMホストを追加し、リソースを検出します

管理プラットフォームと KVM ホスト情報を追加し、 NetApp Backup and Recoveryでワークロードを検出できるようにします。

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*の下で、*KVM*タイルを選択します。

   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。

3. *リソースの検出*を選択します。
4. 次の情報を入力してください。
   a. ワークロード タイプ: **KVM** を選択します。
   b. 管理プラットフォームをバックアップとリカバリとまだ統合していない場合は、[管理プラットフォームの追加] を選択します。
      i. 次の情報を入力してください。
         - 管理プラットフォームの **IP** アドレスまたは **FQDN**: 管理プラットフォームの IP アドレスまたは完全修飾ドメイン名を入力します。
         - **API** キー: API リクエストの認証に使用する API キーを入力します。
         - 秘密キー: API リクエストの認証に使用する秘密キーを入力します。
         - ポート: バックアップとリカバリと管理プラットフォーム間の通信に使用するポートを入力します。
         - エージェント: バックアップとリカバリと管理プラットフォーム間の通信を容易にするために使用するコンソール エージェントを選択します。
      ii. 完了したら、[追加]を選択します。
   c. **KVM** 設定: 次の情報を入力して新しい KVM ホストを追加します。
      - **KVM FQDN** または **IP** アドレス: ホストの FQDN または IP アドレスを入力します。
      - 資格情報: KVM ホストのユーザー名とパスワードを入力します。
      - コンソール エージェント: バックアップおよびリカバリと KVM ホスト間の通信に使用するコンソール エージェントを選択します。
      - ポート番号: バックアップおよびリカバリと KVM ホスト間の通信に使用するポートを入力します。
      - 管理プラットフォーム: KVM ホストが管理されており、管理プラットフォームをバックアップとリカバリに追加している場合は、リストから管理プラットフォームを選択します。
5. *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

KVM ワークロードは、インベントリ ページのワークロード リストに表示されます。

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 KVM ワークロードの保護グループを作成および管理します

KVM リソース セット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 やストレージ プールなどのリソースの論理的なグループです。 KVM 仮想マシンまたはストレージ プールをバックアップするには、保護グループを作成する必要があります。

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"KVMワークロードを今すぐバックアップ"。
- 保護グループを編集します。
- 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 VM とストレージ プールを保護グループにグループ化します。

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. 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ます。
7. ホストを選択すると、そのホスト上で使用可能な VM が一覧表示されます。検出されたすべてのホストの VM を含めるには、ホストリストで **All** を選択します。
8. 保護グループに含める個々の VM を選択するか、* すべて * を選択してリスト内のすべての VM を含めます。

   選択した VM は、**Added virtual machines** 領域に表示されます。リストから個々の VM を削除したり、

リスト全体を空にしたりすることができます。複数の KVM ホストからの VM をリストに追加できます。

9. *次へ*を選択します。
10. 保護グループに適用する保護ポリシーを選択するか、*新しいポリシーの作成*を選択して新しいポリシーを作成します。

    バックアップポリシーの作成の詳細については、以下を参照してください。"ポリシーの作成と管理" 。

11. *次へ*を選択します。
12. 構成を確認します。
13. 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

保護グループを削除して再作成せずに、保護グループの詳細を変更する必要がある場合は、保護グループを編集します。

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. 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。
7. 保護グループの一般的な詳細と VM に必要な変更を加えます。
8. *次へ*を選択します。
9. 必要に応じて、保護グループに関連付けられている保護ポリシーを変更します。
10. *次へ*を選択します。
11. 設定を確認し、「送信」を選択します。

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KVM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、保持するバックアップファイルの数などを制御する独自のKVM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
- ポリシーの編集（VMware ワークロードでは使用できません）
- ポリシーの削除

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：*KVM*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。
   - **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。
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、VM上でKVM QEMUゲストエージェントが実行されている必要があります。ゲストエージェント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ります。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。Kubernetesワークロードポリシーについては、スケジュールと保持設定のみを編集できます。

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KVMワークロードをバックアップ

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 Amazon Web Services、 Azure NetApp Files、またはStorageGRIDに KVM 保護グループをバックアップします。保護グループをバックアップすると、 NetApp Consoleは保護グループに含まれる VM とストレージ プールを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。

保護グループをスケジュールに従っ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制御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 KVM 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。

オンデマンド バックアップで保護グループ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実行できます。これは、システムに変更を加える前にバックアップがあることを確認したい場合に役立ちます。

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. 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. KVM タイルで、[検出と管理] を選択します。
3. *在庫*を選択します。
4. 保護の詳細を表示するには、ワークロードを選択します。
5. アクションアイコンを選択します ••• > 詳細を表示。
6. 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。
7. バックアップする保護グループを選択します。
8. 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、保護グループに割り当てられているポリシーと同じです。

9. スケジュール層を選択します。
10. *バックアップ*を選択します。

NetApp Backup and Recoveryを使用して KVM 仮想マシンを復元する

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保護グループ 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 KVM 仮想マシンを復元します。

これらの場所から復元

異なる開始場所から仮想マシンを復元できます。

- 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:

- 元の場所に復元する
- 別の場所に復元する

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。

仮想マシンの復元の仕組み

仮想マシンを復元すると、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。
- レプリケートされた VM から復元する場合は、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。
- 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。

復元ページから、仮想マシンの正確な名前、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、仮想マシンを復元できます。フィルタを使用してスナップショットを検索できます。

KVM仮想マシンを復元する

「復元」メニューを使用して、KVM仮想マシンを復元します。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 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. NetApp Backup and Recoveryメニューから、[復元] を選択します。
3. 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、**KVM** を選択します。
4. 復元する VM 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 ホストまたはストレージ プールをフィルターします。

   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。

5. 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。

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

b. **Post-restore options** セクションで、 **Restart virtual machine** オプションを有効にすると、リストア処理の完了後に VM が再起動されます。

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. **Cloudstack settings** セクションで、次の情報を入力します。

- * ゾーン * ：リストからデスティネーション CloudStack ゾーンを選択します。
- **Pod**：リストから選択したゾーン内のデスティネーション Pod を選択します。
- クラスター：リストから選択したポッド内のデスティネーション クラスタを選択します。
- **Host**：リストからクラスタ内のデスティネーションホストを選択します。
- * ストレージプール * ：リストからデスティネーションストレージプールを選択します（デスティネーションボリュームはここに配置する必要があります）。
- **Network**: リストアされた VM が接続されるネットワークを選択します。
- **VM**名：復元するVMの名前を入力してください。
- 表示名：Backup and Recoveryでこの仮想マシンに表示される名前を入力します。
- **Storage Pool Path**：VM ボリュームを格納するストレージプールパスを入力します。

c. **Select service offering** リストから、希望するリソース割り当てレベルを定義するサービスオファリングを選択します。

d. **Forced** オプションを有効にすると、VM の NIC MAC アドレスが 1 つ以上すでに存在する場合でも、リストアされた VM をインポートできます。MAC アドレスがすでに存在する場合は、その NIC 用に新しい MAC アドレスが生成されます。

e. *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。

- 仮想マシンの再起動：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が起動します。

10. *復元*を選択します。