NetApp Backup and Recoveryを使用する

NetApp Backup and Recovery

NetApp
February 10, 2026

目次

NetApp Backup and Recoveryを使用する

NetApp Backup and Recoveryダッシュボードで保護の健全性を確認する

ワークロードの健全性を監視することで、ワークロード保護に関する問題を認識し、解決するための手順を実行できるようになります。 NetApp Backup and Recoveryダッシュボードでバックアップと復元のステータスを表示します。システムの概要、保護の概要、ジョブの概要、復元の概要などを確認できます。

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 バックアップ管理者、バックアップおよびリカバリ リストア管理者、バックアップおよびリカバリ クローン管理者、またはバックアップおよびリカバリ ビューアー ロール。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" 。

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。

   次の種類の情報を確認できます。

   - 検出されたホストまたはVMの数
   - 検出されたKubernetesクラスターの数
   - オブジェクトストレージ上のバックアップ対象の数
   - vCenterの数
   - ONTAPのストレージクラスタの数

保護の概要を表示する

保護の概要で次の情報を確認します。

- 保護されているデータベース、VM、データストアと保護されていないデータベース、VM、データストアの合計数。

  保護されたデータベースとは、バックアップ ポリシーが割り当てられたデータベースです。保護されていないデータベースとは、バックアップ ポリシーが割り当てられていないデータベースです。

- 成功したバックアップ、警告のあったバックアップ、失敗したバックアップの数。
- バックアップ サービスによって検出された合計容量と、保護されている容量と保護されていない容量。「**i**」アイコンにマウスを合わせると詳細が表示されます。

求人概要を見る

ジョブの概要で、完了したジョブ、実行中のジョブ、失敗したジョブの合計数を確認します。

手順

1. 各ジョブの配布について、フィルターを変更して、過去 30 日間、過去 7 日間、過去 24 時間、過去 1 年間などの日数に基づいて、失敗、実行中、完了の概要を表示します。
2. ジョブ監視の表示 を選択して、失敗したジョブ、実行中のジョブ、完了したジョブの詳細を表示します。

復元の概要を表示する

復元の概要で次の情報を確認します。

- 実行された復元ジョブの合計数
- 回復した容量の合計
- ローカル、セカンダリ、オブジェクト ストレージで実行された復元ジョブの数。グラフの上にマウスを移動すると詳細が表示されます。

NetApp Backup and Recoveryでバックアップを管理するポリシーを作成および管理します

NetApp Backup and Recoveryでは、バックアップの頻度、バックアップの実行時間、保持されるバックアップ ファイルの数を制御する独自のポリシーを作成します。

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 プレビュー ワークロードでは利用できません）
- 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. これらのポリシーの詳細を確認してください。

- ワークロード：Microsoft SQL Server、ボリューム、VMware、KVM、Hyper-V、Oracle Database 、Kubernetes などがあります。
- 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。
3. 「ポリシー」ページで、次の情報を入力します。
   - *詳細*セクション:
     - ワークロード タイプ: ポリシーを使用するワークロードを選択します。
     - ポリシー名を入力します。

       避けるべき文字のリストについては、ホバーヒントを参照してください。
     - 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。
   - バックアップ アーキテクチャ セクション: 下矢印を選択し、3-2-1 ファンアウト、3-2-1 カスケード、ディスク間など、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）、クラウド（オブジェクト ストア）へ。ONTAP から ONTAP、ONTAP からオブジェクト ストアへの構成など、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 オブジェクト ストアまたはプライベート オブジェクト ストアになります。これらの構成は、最適なデータ保護と災害復旧の実現に役立ちます。

  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: (Kubernetes ワークロードでは使用できません) 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、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 ストアまたはプライベート オブジェクト ストア (StorageGRID)になります。これにより、複数のシステムにわたるデータ複製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。

- ディスクからディスク: (Kubernetes ワークロードでは使用できません) 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)。ONTAPからONTAPへのデータ保護戦略では、2つのONTAPシステム間でデータを複製し、高可用性と災害復旧を保証します。これは通常、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するSnapMirrorを使用して実現されます。この方法により、データが継続的に更新され、複数の場所で利用可能になり、データ損失に対する強力な保護が提供されます。

  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へのストア: 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。これにより、 ONTAPシステムから AWS S3、Azure Blob Storage、StorageGRIDなどのオブジェクト ストレージ システムにデータが複製されます。これは通常、最初のベースライン転送後に変更されたデータ ブロックのみを転送することで永久増分バックアップを提供するSnapMirror Cloud を使用して実現されます。これは、クラウド ハイパースケーラー オブジェクト ストアまたはプライベート オブジェクト ストア (StorageGRID)になります。この方法は長期的なデータ保持とアーカイブに最適で、データ保護のためのコスト効率が高くスケーラブルなソリューションを提供します。

  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。

- ディスク間のファンアウト: (Kubernetes ワークロードでは使用できません) 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) 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)。

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 (Microsoft SQL Server) 上のローカル スナップショット。ローカル スナップショットは、特定の時点でのデータの状態をキャプチャする、データ保護戦略の重要なコンポーネントです。これにより、ワークロードが実行されている実稼働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。スナップショットは、最後のスナップショット以降のファイルの変更のみを記録するため、最小限のストレージスペースしか消費せず、パフォーマンスのオーバーヘッドもごくわずかです。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回復したり、災害復旧用のバックアップを作成したりできます。

  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。

ローカルスナップショットポリシーを作成する

ローカル スナップショットの情報を提供します。

- 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。
- ログ バックアップを有効にする: (Microsoft SQL Server ワークロードと Oracle Database ワークロードにのみ適用されます。)このオプションを有効にすると、ログをバックアップし、ログ バックアップの頻度と保持期間を設定できます。これを行うには、ログ バックアップをあらかじめ構成しておく必要があります。見る"ログディレクトリを構成する"。
  - バックアップ後にアーカイブ ログを削除する: (Oracle データベース ワークロードのみ) ログ バックアップが有効になっている場合は、オプションでこの機能を有効にして、バックアップとリカバリが 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、バックアップとリカバリでアーカイブ ログを削除する場所を選択できます。
- プロバイダー: (Kubernetes ワークロードのみ) 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ます。

セカンダリ設定（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

セカンダリストレージへのレプリケーションに関する情報を提供します。ローカル スナップショット設定のスケジュール情報が、セカンダリ設定に表示されます。これらの設定は Kubernetes ワークロードでは使用できません。

- 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。
- * SnapMirrorとSnapVault SMAS セカンダリ リレーションシップ*: SQL Server ワークロードにSnapMirrorとSnapVault SMAS セカンダリ リレーションシップを使用します。

オブジェクトストレージ設定のポリシーを作成する

オブジェクト ストレージへのバックアップに関する情報を提供します。これらの設定は、Kubernetes ワークロードの「バックアップ設定」と呼ばれます。

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。

AWSオブジェクトストレージのポリシーを作成する

次のフィールドに情報を入力します。

- プロバイダー: **AWS** を選択します。
- **AWS** アカウント: AWS アカウントを選択します。
- バックアップターゲット: 登録済みの S3 オブジェクトストレージターゲットを選択します。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: (Kubernetes ワークロードでは使用できません) オブジェクト ストレージで整合性スキャン (スナップショット 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になり、正常に復元でき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 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。スキャンは最新のスナップショットに対してのみ実行されます。最新のスナップショットで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。

Microsoft Azure オブジェクト ストレージのポリシーを作成する

次のフィールドに情報を入力します。

- プロバイダー: **Azure** を選択します。
- **Azure** サブスクリプション: 検出された Azure サブスクリプションを選択します。
- **Azure** リソース グループ: 検出された Azure リソース グループから選択します。
- 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: (Kubernetes ワークロードでは使用できません) オブジェクト ストレージで整合性スキャン (スナップショット 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になり、正常に復元でき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 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。スキャンは最新のスナップショットに対してのみ実行されます。最新のスナップショットで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。

StorageGRIDオブジェクトストレージのポリシーを作成する

次のフィールドに情報を入力します。

- プロバイダー: * StorageGRID*を選択します。
- * StorageGRID資格情報*: 検出された資格情報からStorageGRID資格情報を選択します。これらの資格情報は、 StorageGRIDオブジェクト ストレージ システムにアクセスするために使用され、[設定] オプションに入力されました。
- バックアップターゲット: 登録済みの S3 オブジェクトストレージターゲットを選択します。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: 各頻度で保持するスナップショットの数を入力します。
- オブジェクト ストレージの転送スケジュール: (Kubernetes ワークロードでは使用できません) ONTAP転送スケジュールを選択して、データをオブジェクト ストレージにバックアップします。
- 整合性スキャンを有効にする: (Kubernetes ワークロードでは使用できません) オブジェクト ストレージで整合性スキャン (スナップショット 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になり、正常に復元でき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 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。スキャンは最新のスナップショットに対してのみ実行されます。最新のスナッ

プショットで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。

- 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: (Kubernetes ワークロードでは使用できません) バックアップをアーカイブ ストレージ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。

ポリシーの詳細設定を構成する

必要に応じて、ポリシーで詳細設定を構成できます。これらの設定は、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など、すべてのバックアップ アーキテクチャで使用できます。これらの設定は Kubernetes ワークロードでは使用できません。利用可能な詳細設定はページの上部で選択したワークロードによって異なるため、ここで説明する詳細設定はすべてのワークロードに適用されない可能性があります。 Kubernetes ワークロードのポリシーを構成する場合、詳細設定は使用できません。

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。
    - コピーのみのバックアップ: (Microsoft SQL Server ワークロードにのみ適用) 別のバックアップ アプリケーションを使用してリソースをバックアップする必要がある場合は、コピーのみのバックアップ (Microsoft SQL Server バックアップの一種) を選択します。
    - 可用性グループの設定: (Microsoft SQL Server ワークロードにのみ適用) 優先バックアップ レプリカを選択するか、特定のレプリカを指定します。この設定は、SQL Server 可用性グループがあり、バックアップに使用するレプリカを制御する場合に役立ちます。
    - 最大転送速度: 帯域幅の使用に制限を設けない場合は、無制限*を選択します。転送速度を制限する場合は、「*制限」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られるネットワーク帯域幅を 1 ～ 1,000 Mbps の範囲で選択します。デフォルトでは、 ONTAP は無制限の帯域幅を使用して、システム内のボリュームからオブジェクト ストレージにバックアップ データを転送できます。バックアップ トラフィックが通常のユーザー ワークロードに影響を与えていることに気付いた場合は、転送中に使用されるネットワーク帯域幅の量を減らすことを検討してください。
    - バックアップの再試行: (VMware ワークロードには適用されません) 障害または中断が発生した場合にジョブを再試行するには、障害時の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時間間隔を入力します。再集計は10未満でなければなりません。この設定は、障害や中断が発生した場合にバックアップ ジョブが再試行されるようにする場合に役立ちます。

      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。

    - **VM** 整合性スナップショットを有効にする: VM 整合性スナップショットを有効にするかどうかを選択します。これにより、新しく作成されたスナップショットが、スナップショット時の仮想マシンの状態と一致することが保証されます。これは、バックアップが正常に復元され、データが一貫した状態であることを確認するのに役立ちます。これは既存のスナップショットには適用されません。
    - 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。

- バックアップ検証: (VMware ワークロードには適用されません) バックアップ検証を有効にするかどうか、また、すぐに実行するか後で行うかを選択します。この機能により、バックアップが有効であり、正常に復元できることが保証されます。バックアップの整合性を確保するには、このオプションを有効にすることをお勧めします。デフォルトでは、セカンダリ ストレージが構成されている場合、バックアップ検証はセカンダリ ストレージから実行されます。セカンダリ ストレージが構成されていない場合、バックアップ検証はプライマリ ストレージから実行されます。

  さらに、次のオプションを構成します。

  - 毎日、毎週、毎月、または*毎年*の検証: バックアップ検証として*後で*を選択した場合は、バックアップ検証の頻度を選択します。これにより、バックアップの整合性が定期的にチェックされ、正常に復元できるようになります。
  - バックアップ ラベル: バックアップのラベルを入力します。このラベルはシステム内のバックアップを識別するために使用され、バックアップの追跡と管理に役立ちます。
  - データベース整合性チェック: (VMware ワークロードには適用されません) データベース整合性チェックを有効にするかどうかを選択します。このオプションにより、バックアップが取られる前にデータベースが一貫した状態であることが保証されます。これは、データの整合性を確保するために重要です。
  - ログ バックアップの検証: (VMware ワークロードには適用されません) ログ バックアップを検証するかどうかを選択します。検証サーバを選択します。ディスクツーディスクまたは 3-2-1 を選択した場合は、検証の保存場所も選択します。このオプションにより、ログ バックアップが有効であり、正常に復元できることが保証されます。これは、データベースの整合性を維持するために重要です。
- ネットワーク: バックアップ操作に使用するネットワーク インターフェイスを選択します。これは、複数のネットワーク インターフェイスがあり、どれ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。
  - **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。
  - プライベート エンドポイント構成: オブジェクト ストレージにプライベート エンドポイントを使用している場合は、バックアップ操作に使用するプライベート エンドポイント構成を選択します。これは、バックアップがプライベート ネットワーク接続を介して安全に転送されることを確認したい場合に便利です。
- 通知: バックアップ操作に関する電子メール通知を有効にするかどうかを選択します。これは、バックアップ操作が開始、完了、または失敗したときに通知を受け取りたい場合に便利です。
- 独立ディスク: (VMware ワークロードにのみ適用) 一時データを含む独立ディスクを持つすべてのデータストアをバックアップに含めるには、これをチェックします。独立ディスクは、VMware スナップショットに含まれない VM ディスクです。
- * SnapMirrorボリュームとスナップショット形式*: 必要に応じて、Microsoft SQL Server ワークロードのバックアップを管理するポリシーに独自のスナップショット名を入力します。フォーマットとカスタムテキストを入力します。セカンダリ ストレージにバックアップすることを選択した場合は、SnapMirrorボリュームのプレフィックスとサフィックスを追加することもできます。

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、その他のポリシー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。

ONTAPボリュームのワークロードを保護する

NetApp Backup and Recoveryを使用してONTAPボリューム データを保護します

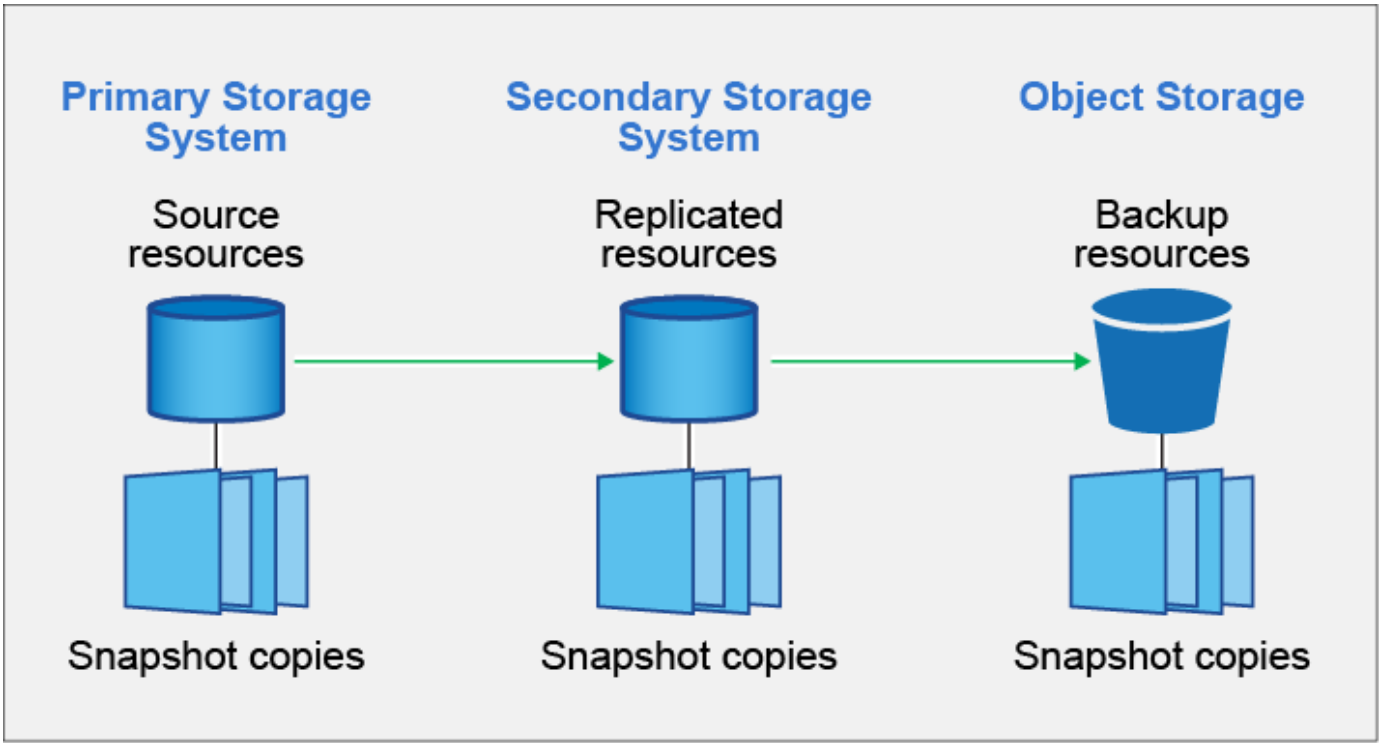
NetApp Backup and Recovery は、 ONTAPボリューム データの保護と長期アーカイブの

ためのバックアップおよび復元機能を提供します。 3-2-1 戦略を実装して、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 つ保存することができます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

アクティブ化後、バックアップとリカバリによって、ブロックレベルの永久増分バックアップが作成され、別のONTAPクラスターとクラウド内のオブジェクト ストレージに保存されます。ソース ボリュームに加えて、次のものも用意します。

- ソースシステム上のボリュームのスナップショット
- 別のストレージシステム上の複製ボリューム
- オブジェクトストレージ内のボリュームのバックアップ



NetApp Backup and Recovery は、 NetApp のSnapMirrorデータ レプリケーション テクノロジを活用して、スナップショットを作成し、それをバックアップの場所に転送することで、すべてのバックアップが完全に同期されるようにします。

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。

必要に応じて、任意のバックアップ コピーから、ボリューム_全体、_フォルダ、または 1 つ以上の_ファイル_を同じシステムまたは別のシステムに復元できます。

機能

レプリケーション機能:

- バックアップと災害復旧をサポートするために、 ONTAPストレージ システム間でデータを複製します。
- 高可用性により DR 環境の信頼性を確保します。
- 2 つのシステム間の事前共有キー (PSK) を介して設定されたネイティブONTAPインフライト暗号化。
- コピーされたデータは、書き込み可能になって使用可能になるまで変更できません。
- 転送に失敗した場合、レプリケーションは自動的に修復されます。
- と比較すると "NetApp Replication"NetApp Backup and Recoveryのレプリケーションには、次の機能が含まれています。
  - 一度に複数のFlexVolボリュームをセカンダリ システムに複製します。
  - UI を使用して、複製されたボリュームをソース システムまたは別のシステムに復元します。

見る"ONTAPボリュームのレプリケーションの制限"ONTAPボリュームのNetApp Backup and Recoveryで使用できないレプリケーション機能のリストについては、こちらをご覧ください。

オブジェクトへのバックアップ機能:

- データ ボリュームの独立したコピーを低コストのオブジェクト ストレージにバックアップします。
- クラスター内のすべてのボリュームに単一のバックアップ ポリシーを適用するか、固有の復旧ポイント目標を持つボリュームに異なるバックアップ ポリシーを割り当てます。
- クラスターで今後作成されるすべてのボリュームに適用されるバックアップ ポリシーを作成します。
- 変更不可能なバックアップ ファイルを作成し、保持期間中はロックされて保護されるようにします。
- バックアップ ファイルをスキャンしてランサムウェア攻撃の可能性を検出し、感染したバックアップを自動的に削除/置き換えます。
- 古いバックアップ ファイルをアーカイブ ストレージに階層化してコストを節約します。
- ボリュームのバックアップを保持しながら不要なソース ボリュームをアーカイブできるように、バックアップ関係を削除します。
- クラウドからクラウドへ、オンプレミス システムからパブリック クラウドまたはプライベート クラウドへバックアップします。
- バックアップ データは、保存時には AES-256 ビット暗号化、実行時には TLS 1.2 HTTPS 接続によって保護されます。
- クラウド プロバイダーのデフォルトの暗号化キーを使用する代わりに、独自の顧客管理キーを使用してデータを暗号化します。
- 単一ボリュームの最大 4,000 件のバックアップをサポートします。

復元機能:

- ローカル スナップショット、複製されたボリューム、またはオブジェクト ストレージ内のバックアップされたボリュームから特定の時点のデータを復元します。
- ボリューム、フォルダー、または個々のファイルをソース システムまたは別のシステムに復元します。
- 別のサブスクリプション/アカウントを使用しているシステム、または別のリージョンにあるシステムにデ

ータを復元します。

- クラウド ストレージからCloud Volumes ONTAPシステムまたはオンプレミス システムへのボリュームのクイック リストア を実行します。ボリュームへのアクセスをできるだけ早く提供する必要がある災害復旧の状況に最適です。
- 元の ACL を維持しながら、ブロック レベルでデータを復元し、指定した場所にデータを直接配置します。
- ファイル カタログを参照して検索し、個々のフォルダーとファイルを簡単に選択して単一ファイルの復元を行うことができます。

バックアップおよび復元操作でサポートされているシステム

NetApp Backup and Recovery は、 ONTAPシステムとパブリックおよびプライベート クラウド プロバイダーをサポートします。

サポートされている地域

NetApp Backup and Recovery は、多くの Amazon Web Services、Microsoft Azure、Google Cloud リージョンでCloud Volumes ONTAPによってサポートされています。

"グローバル地域マップを使用して詳細を確認する"

サポートされているバックアップ先

NetApp Backup and Recoveryと、次のソース システムから次のセカンダリ システムおよびパブリック クラウド プロバイダーとプライベート クラウド プロバイダーのオブジェクト ストレージにONTAPボリュームをバックアップできます。スナップショットはソース システムに存在します。

ソースシステム	セカンダリシステム（レプリケーション）	宛先オブジェクトストア（バックアップ）
AWS のCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	Amazon S3
Azure のCloud Volumes ONTAP	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure ブロブ
Google のCloud Volumes ONTAP	Google オンプレミスONTAPシステムのCloud Volumes ONTAP	Google Cloud Storage
オンプレミスのONTAPシステム	Cloud Volumes ONTAPオンプレミスONTAPシステム	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

サポートされている復元先

セカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップ ファイルから次のシステムにONTAPデータを復元できます。スナップショットはソース システムに存在し、同じシステムにのみ復元できます。

バックアップファイルの場所		宛先システム
オブジェクトストア（バックアップ）	セカンダリシステム（レプリケーション）	

バックアップファイルの場所		宛先システム
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP
Azure ブロブ	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム
Google Cloud Storage	Google オンプレミスONTAPシステムのCloud Volumes ONTAP	Google オンプレミスONTAPシステムのCloud Volumes ONTAP
NetAppStorageGRID	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム
ONTAP S3	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム

「オンプレミスのONTAPシステム」への参照には、 FAS、 AFF、およびONTAP Selectシステムが含まれることに注意してください。

サポートされているボリューム

NetApp Backup and Recovery は、次のタイプのボリュームをサポートしています。

- FlexVol読み取り/書き込みボリューム
- FlexGroupボリューム（ ONTAP 9.12.1以降が必要）
- SnapLock Enterpriseボリューム（ ONTAP 9.11.1 以降が必要）
- オンプレミスボリュームのSnapLock Compliance （ ONTAP 9.14 以降が必要）
- SnapMirrorデータ保護（DP）宛先ボリューム

NetApp Backup and Recovery は、 FlexCacheボリュームのバックアップをサポートしていません。

以下のセクションを参照してください"ONTAPボリュームのバックアップとリストアの制限"追加の要件と制限については、こちらをご覧ください。

料金

ONTAPシステムでNetApp Backup and Recoveryを使用する場合、リソース料金とサービス料金の 2 種類のコストが発生します。これら両方の料金は、サービスのオブジェクト部分へのバックアップに対して発生します。

スナップショットや複製ボリュームの作成には、スナップショットや複製ボリュームを保存するために必要なディスク容量以外は料金はかかりません。

リソース料金

オブジェクト ストレージ容量とクラウドへのバックアップ ファイルの書き込みと読み取りに対して、リソース料金がクラウド プロバイダーに支払われます。

- オブジェクト ストレージへのバックアップの場合、オブジェクト ストレージのコストをクラウド プロバイダーに支払います。

NetApp Backup and Recovery はソース ボリュームのストレージ効率を維持するため、 ONTAP効率化後のデータ (重複排除と圧縮が適用された後の少量のデータ) に対してクラウド プロバイダーのオブジェクト ストレージ コストを支払います。

- 検索と復元を使用してデータを復元する場合、クラウド プロバイダーによって特定のリソースがプロビジョニングされ、検索要求によってスキャンされるデータの量に応じて TiB ごとにコストが発生します。 (これらのリソースは参照と復元には必要ありません。)
  - AWSでは、 "アマゾンアテナ"そして "AWS グルー"リソースは新しい S3 バケットにデプロイされます。
  - Azureでは、 "Azure Synapse ワークスペース"そして "Azure データレイクストレージ"データを保存および分析するためにストレージ アカウントにプロビジョニングされます。
  - Googleでは新しいバケットがデプロイされ、 "Google Cloud BigQuery サービス"アカウント/プロジェクト レベルでプロビジョニングされます。
- アーカイブ オブジェクト ストレージに移動されたバックアップ ファイルからボリューム データを復元する場合は、クラウド プロバイダーから追加の GiB あたりの取得料金とリクエストあたりの料金が発生します。
- ボリューム データの復元プロセス中にバックアップ ファイルをランサムウェアに対してスキャンする予定がある場合 (クラウド バックアップに対して DataLock と Ransomware Resilience を有効にしている場合)、クラウド プロバイダーから追加の送信コストも発生します。

サービス料

サービス料金はNetAppに支払われ、オブジェクト ストレージへのバックアップを 作成 するコストと、それらのバックアップからボリュームまたはファイルを 復元 するコストの両方をカバーします。オブジェクト ストレージにバックアップされるONTAPボリュームのソース論理使用容量 (ONTAP効率前) によって計算された、オブジェクト ストレージで保護するデータに対してのみ料金を支払います。この容量は、フロントエンド テラバイト (FETB) とも呼ばれます。

バックアップ サービスの支払い方法は 3 つあります。最初のオプションは、クラウド プロバイダーにサブスクライブすることです。これにより、月ごとに支払いが可能になります。 2 番目のオプションは、年間契約を結ぶことです。 3 番目のオプションは、 NetAppから直接ライセンスを購入することです。

ライセンス

NetApp Backup and Recovery は、次の消費モデルで利用できます。

- **BYOL**: NetAppから購入したライセンスで、どのクラウド プロバイダーでも使用できます。
- **PAYGO**: クラウド プロバイダーのマーケットプレイスからの時間単位のサブスクリプション。
- 年間: クラウド プロバイダーのマーケットプレイスからの年間契約。

バックアップ ライセンスは、オブジェクト ストレージからのバックアップと復元にのみ必要です。スナップショットおよび複製されたボリュームの作成にはライセンスは必要ありません。

自分のライセンスを持参する

BYOL は期間ベース (1 年、2 年、または 3 年) であり、1 TiB 単位で容量ベースになります。一定期間（たとえば 1 年）および最大容量（たとえば 10 TiB）のサービス使用料をNetApp に支払います。

サービスを有効にするためにNetApp Consoleに入力するシリアル番号を受け取ります。どちらかの制限に達した場合は、ライセンスを更新する必要があります。バックアップ BYOL ライセンスは、 NetApp Console組

織またはアカウントに関連付けられているすべてのソース システムに適用されます。

"BYOLライセンスの管理方法を学ぶ"。

従量課金制サブスクリプション

NetApp Backup and Recovery は、従量課金モデルで消費ベースのライセンスを提供します。クラウド プロバイダーのマーケットプレイスを通じてサブスクライブすると、バックアップされたデータに対して GiB ごとに料金が発生します。前払いはありません。クラウド プロバイダーから毎月の請求書を通じて請求されます。

"従量課金制サブスクリプションの設定方法を学ぶ"。

PAYGO サブスクリプションに最初にサインアップすると、30 日間の無料トライアルが利用できることに注意してください。

年間契約

AWS を使用する場合、1 年、2 年、または 3 年の期間で 2 つの年間契約を利用できます。

- Cloud Volumes ONTAPデータとオンプレミスのONTAPデータをバックアップできる「クラウド バックアップ」プラン。
- Cloud Volumes ONTAPとNetApp Backup and Recovery をバンドルできる「CVO Professional」プラン。これには、このライセンスに対して課金されるCloud Volumes ONTAPボリュームの無制限のバックアップが含まれます (バックアップ容量はライセンスに対してカウントされません)。

Azure を使用する場合、1 年、2 年、または 3 年の期間で 2 つの年間契約を利用できます。

- Cloud Volumes ONTAPデータとオンプレミスのONTAPデータをバックアップできる「クラウド バックアップ」プラン。
- Cloud Volumes ONTAPとNetApp Backup and Recovery をバンドルできる「CVO Professional」プラン。これには、このライセンスに対して課金されるCloud Volumes ONTAPボリュームの無制限のバックアップが含まれます (バックアップ容量はライセンスに対してカウントされません)。

GCP を使用する場合、 NetAppからプライベート オファーをリクエストし、 NetApp Backup and Recovery のアクティベーション中に Google Cloud Marketplace からサブスクライブするときにプランを選択できます。

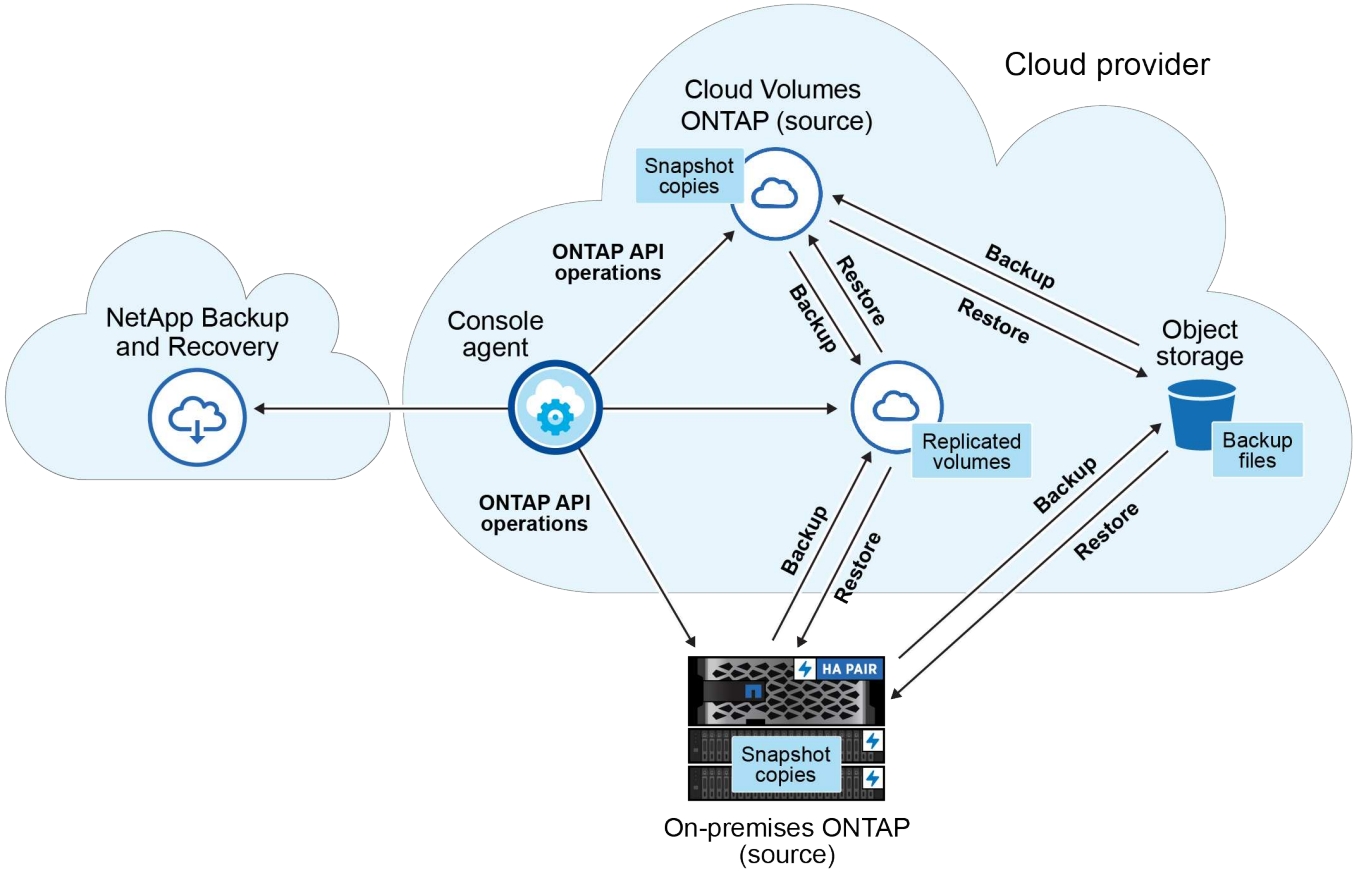
"年間契約の設定方法を学ぶ"。

NetApp Backup and Recoveryの仕組み

Cloud Volumes ONTAPまたはオンプレミスのONTAPシステムでNetApp Backup and Recoveryを有効にすると、サービスによってデータの完全バックアップが実行されます。最初のバックアップ後の追加のバックアップはすべて増分バックアップとなり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワーク トラフィックが最小限に抑えられます。オブジェクトストレージへのバックアップは、 "NetApp SnapMirrorクラウドテクノロジー" 。

クラウド プロバイダー環境から直接クラウド バックアップ ファイルを管理または変更するアクションを実行すると、ファイルが破損し、サポートされていない構成になる可能性があります。

次の図は、各コンポーネント間の関係を示しています。



この図は、ボリュームがCloud Volumes ONTAPシステムに複製されていることを示していますが、ボリュームはオンプレミスのONTAPシステムにも複製できます。

バックアップの保存場所

バックアップは、バックアップの種類に応じて異なる場所に保存されます。

- スナップショット はソース システムのソース ボリュームに存在します。
- _複製されたボリューム_は、セカンダリ ストレージ システム (Cloud Volumes ONTAPまたはオンプレミスのONTAPシステム) に存在します。
- バックアップ コピー は、コンソールがクラウド アカウントに作成するオブジェクト ストアに保存されます。クラスター/システムごとに 1 つのオブジェクト ストアがあり、コンソールではオブジェクト ストアに「netapp-backup-clusteruuid」という名前が付けられます。このオブジェクト ストアを削除しないように注意してください。
  - AWSでは、コンソールで "Amazon S3 ブロックパブリックアクセス機能" S3 バケット上。
  - Azure では、コンソールは、Blob コンテナーのストレージ アカウントを持つ新規または既存のリソース グループを使用します。コンソール "BLOBデータへのパブリックアクセスをブロックします" デフォルトです。
  - GCP では、コンソールは Google Cloud Storage バケットのストレージ アカウントを持つ新規または既存のプロジェクトを使用します。
  - StorageGRIDでは、コンソールは S3 バケットに既存のテナント アカウントを使用します。

- ONTAP S3 では、コンソールは S3 バケットに既存のユーザー アカウントを使用します。

将来的にクラスタの宛先オブジェクトストアを変更する場合は、"システムのNetApp Backup and Recoveryの登録を解除する" 、新しいクラウド プロバイダー情報を使用してNetApp Backup and Recoveryを有効にします。

カスタマイズ可能なバックアップスケジュールと保持設定

システムに対してNetApp Backup and Recovery を有効にすると、最初に選択したすべてのボリュームが、選択したポリシーを使用してバックアップされます。スナップショット、複製されたボリューム、バックアップファイルごとに個別のポリシーを選択できます。異なるリカバリポイント目標 (RPO) を持つ特定のボリュームに異なるバックアップ ポリシーを割り当てる場合は、そのクラスターに追加のポリシーを作成し、 NetApp Backup and Recovery をアクティブ化した後でそれらのポリシーを他のボリュームに割り当てることができます。

すべてのボリュームの毎時、毎日、毎週、毎月、毎年のバックアップの組み合わせを選択できます。オブジェクトへのバックアップでは、3 か月、1 年、7 年間のバックアップと保持を提供するシステム定義のポリシーのいずれかを選択することもできます。 ONTAP System Manager またはONTAP CLI を使用してクラスタ上に作成したバックアップ保護ポリシーも選択肢として表示されます。これには、カスタムSnapMirrorラベルを使用して作成されたポリシーが含まれます。

ボリュームに適用されるスナップショット ポリシーには、レプリケーション ポリシーとオブジェクトへのバックアップ ポリシーで使用しているラベルのいずれかが必要です。一致するラベルが見つからない場合、バックアップ ファイルは作成されません。たとえば、「毎週」複製されたボリュームとバックアップ ファイルを作成する場合は、「毎週」スナップショットを作成するスナップショット ポリシーを使用する必要があります。

カテゴリまたは間隔のバックアップの最大数に達すると、古いバックアップが削除されるため、常に最新のバックアップが保持されます (そのため、古いバックアップがスペースを占有し続けることはありません)。

データ保護ボリュームのバックアップの保持期間は、ソースSnapMirror関係で定義されている期間と同じです。必要に応じて、API を使用してこれを変更できます。

バックアップファイルの保護設定

クラスターでONTAP 9.11.1 以降を使用している場合は、オブジェクト ストレージ内のバックアップを削除やランサムウェア攻撃から保護できます。各バックアップ ポリシーには、特定の期間 (保持期間) にわたってバックアップ ファイルに適用できる *DataLock* および *Ransomware Resilience* のセクションが用意されています。

- *DataLock* は、バックアップ ファイルが変更されたり削除されたりするのを防ぎます。
- ランサムウェア保護 は、バックアップ ファイルの作成時とバックアップ ファイルからのデータの復元時に、バックアップ ファイルをスキャンしてランサムウェア攻撃の証拠を探します。

スケジュールされたランサムウェア保護スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は 7 日間です。スキャンは最新のスナップショットに対してのみ実行されます。コストを削減するために、スケジュールされたスキャンを無効にすることができます。「詳細設定」ページのオプションを使用して、最新のスナップショットでスケジュールされたランサムウェア スキャンを有効または無効にすることができます。有効にすると、デフォルトでスキャンが毎週実行されます。スケジュールを日単位や週単位に変更したり、無効にしたりしてコストを節約できます。

バックアップの保持期間は、バックアップ スケジュールの保持期間に最大 31 日間のバッファを加えた期間と

同じです。たとえば、*5* 個のコピーが保持される 毎週 のバックアップでは、各バックアップ ファイルが 5 週間ロックされます。 *6* 個のコピーが保持される 月次 バックアップでは、各バックアップ ファイルが 6 か月間ロックされます。

現在、バックアップ先が Amazon S3、Azure Blob、またはNetApp StorageGRIDの場合にサポートが利用できます。他のストレージ プロバイダーの宛先は、今後のリリースで追加される予定です。

詳細については、次の情報を参照してください。

- "DataLockとランサムウェア保護の仕組み"。
- "詳細設定ページでランサムウェア保護オプションを更新する方法"。

バックアップをアーカイブ ストレージに階層化している場合、DataLock を有効にすることはできません。

古いバックアップファイルのアーカイブストレージ

特定のクラウド ストレージを使用する場合、一定の日数後に古いバックアップ ファイルをより安価なストレージ クラス/アクセス ティアに移動できます。バックアップ ファイルを標準のクラウド ストレージに書き込まずに、すぐにアーカイブ ストレージに送信することも選択できます。 DataLock を有効にしている場合はアーカイブ ストレージを使用できないことに注意してください。

- AWS では、バックアップは *Standard* ストレージ クラスで開始され、30 日後に *Standard-Infrequent Access* ストレージ クラスに移行します。

  クラスターでONTAP 9.10.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後にNetApp Backup and Recovery UI で古いバックアップを *S3 Glacier* または *S3 Glacier Deep Archive* ストレージに階層化することを選択できます。"AWSアーカイブストレージの詳細"。

- Azure では、バックアップは *Cool* アクセス層に関連付けられています。

  クラスターでONTAP 9.10.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後にNetApp Backup and Recovery UI で古いバックアップを *Azure Archive* ストレージに階層化することを選択できます。"Azure アーカイブ ストレージの詳細"。

- GCP では、バックアップは *Standard* ストレージ クラスに関連付けられています。

  クラスターでONTAP 9.12.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後にNetApp Backup and Recovery UI で古いバックアップをアーカイブ ストレージに階層化することを選択できます。"Google アーカイブ ストレージの詳細"。

- StorageGRIDでは、バックアップは *Standard* ストレージ クラスに関連付けられます。

  オンプレミスのクラスタでONTAP 9.12.1 以上を使用しており、 StorageGRIDシステムで 11.4 以上を使用している場合は、一定の日数後に古いバックアップ ファイルをパブリック クラウド アーカイブ ストレージにアーカイブできます。現在サポートされているのは、AWS S3 Glacier/S3 Glacier Deep Archive または Azure Archive ストレージ層です。"StorageGRIDからのバックアップファイルのアーカイブについて詳しくは"。

古いバックアップ ファイルのアーカイブの詳細については、[link:prev-ontap-policy-object-options.html] を参照してください。

FabricPool階層化ポリシーの考慮事項

バックアップするボリュームがFabricPoolアグリゲート上に存在し、それに割り当てられた階層化ポリシー以外のポリシーがある場合、注意すべき点がいくつかあります。 `none`：

- FabricPool階層化ボリュームの最初のバックアップでは、すべてのローカル データとすべての階層化データ (オブジェクト ストアから) を読み取る必要があります。バックアップ操作では、オブジェクト ストレージに階層化されたコールド データが「再加熱」されることはありません。

  この操作により、クラウド プロバイダーからデータを読み取るためのコストが 1 回だけ増加する可能性があります。

  - 後続のバックアップは増分バックアップであるため、この影響はありません。
  - ボリュームが最初に作成されるときに階層化ポリシーが割り当てられている場合は、この問題は発生しません。
- 割り当てる前にバックアップの影響を考慮してください `all`ボリュームへの階層化ポリシー。データは即座に階層化されるため、 NetApp Backup and Recovery はローカル層ではなくクラウド層からデータを読み取ります。同時バックアップ操作ではクラウド オブジェクト ストアへのネットワーク リンクが共有されるため、ネットワーク リソースが飽和状態になるとパフォーマンスが低下する可能性があります。この場合、このタイプのネットワーク飽和を減らすために、複数のネットワーク インターフェイス (LIF) を事前に構成する必要がある場合があります。

NetApp Backup and Recoveryで保護の旅を計画する

NetApp Backup and Recovery を使用すると、ソース ボリュームのコピーを最大 3 つ作成してデータを保護できます。ボリュームでバックアップと回復を有効にするときに選択できるオプションは多数あるため、準備ができるように選択内容を確認する必要があります。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

以下のオプションについて説明します。

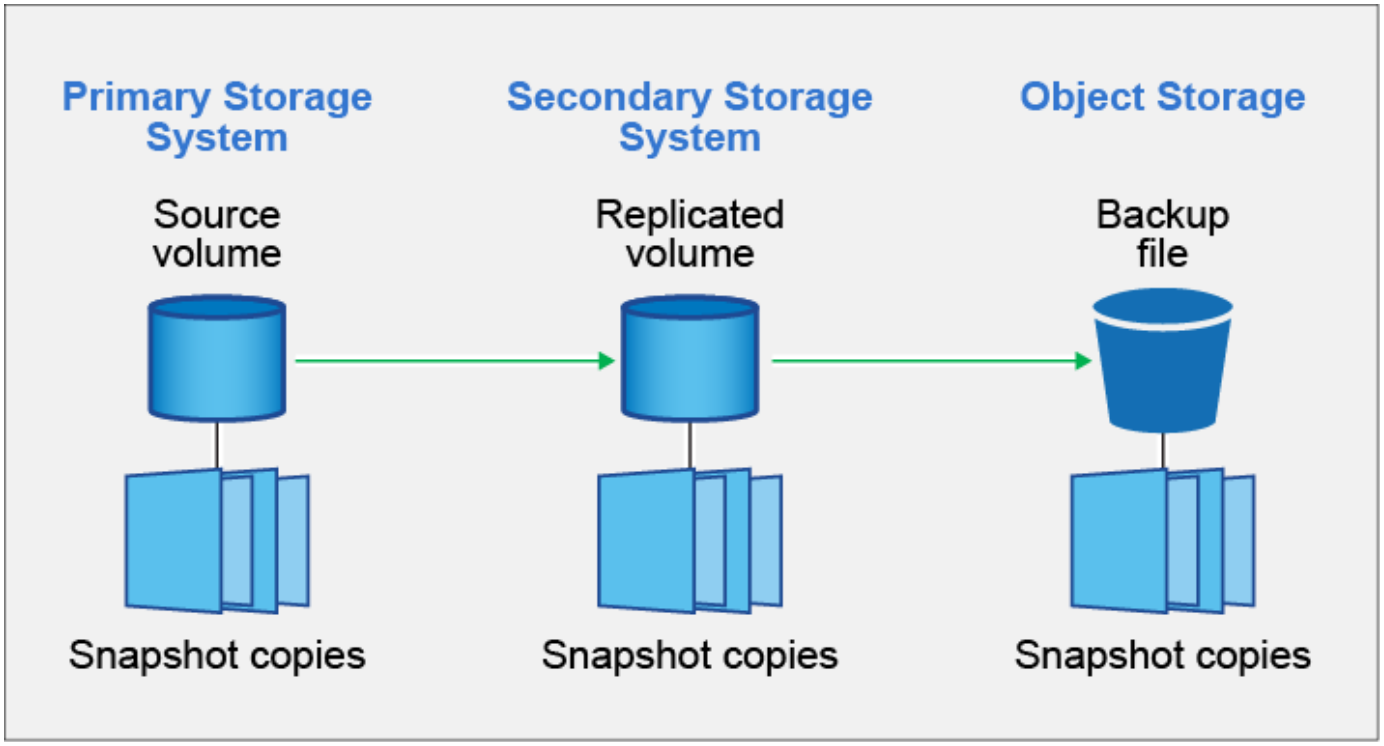
- どのような保護機能を使用しますか: スナップショット、複製ボリューム、クラウドへのバックアップ
- どのバックアップアーキテクチャを使用しますか: ボリュームのカスケードバックアップまたはファンアウトバックアップ
- デフォルトのバックアップポリシーを使用しますか、それともカスタムポリシーを作成する必要がありますか
- サービスにクラウドバケットを作成させたいですか、それとも始める前にオブジェクトストレージコンテナを作成したいですか？
- どのコンソール エージェント展開モードを使用していますか (標準、制限、またはプライベート モード)

どの保護機能を使用するか

使用する機能を選択する前に、各機能の機能と、提供される保護の種類について簡単に説明します。

バックアップ タイプ	説明
Snapshot	ソース ボリューム内のボリュームの読み取り専用の特定時点のイメージをスナップショットとして作成します。スナップショットを使用して、個々のファイルを回復したり、ボリュームの内容全体を復元したりできます。
レプリケーション	別のONTAPストレージ システムにデータのセカンダリ コピーを作成し、セカンダリ データを継続的に更新します。データは最新の状態に保たれ、必要なときにいつでも利用できます。
クラウド バックアップ	保護と長期アーカイブの目的でクラウドにデータのバックアップを作成します。必要に応じて、ボリューム、フォルダー、または個々のファイルをバックアップから同じシステムまたは別のシステムに復元できます。

スナップショットはすべてのバックアップ方法の基礎であり、バックアップおよびリカバリ サービスを使用するために必要です。スナップショットは、ボリュームの読み取り専用の特定時点のイメージです。イメージは、最後のスナップショットが作成されてからファイルに加えられた変更のみを記録するため、最小限のストレージスペースしか消費せず、パフォーマンスのオーバーヘッドもごくわずかです。ボリューム上に作成されたスナップショットは、図に示すように、複製されたボリュームとバックアップ ファイルをソース ボリュームに加えられた変更と同期させるために使用されます。



別のONTAPストレージ システムに複製されたボリュームを作成し、クラウドにファイルをバックアップすることもできます。または、複製されたボリュームまたはバックアップ ファイルのみを作成することもできます。それはあなたの選択です。

要約すると、 ONTAPシステム内のボリュームに対して作成できる有効な保護フローは次のとおりです。

- ソースボリューム → スナップショット → 複製ボリューム → バックアップファイル
- ソースボリューム → スナップショット → バックアップファイル
- ソースボリューム → スナップショット → 複製ボリューム

複製されたボリュームまたはバックアップ ファイルの最初の作成には、ソース データの完全なコピーが含まれます。これは、ベースライン転送 と呼ばれます。後続の転送には、ソース データの差分コピー (スナップショット) のみが含まれます。

さまざまなバックアップ方法の比較

次の表は、3 つのバックアップ方法の一般的な比較を示しています。オブジェクト ストレージ スペースは通常、オンプレミスのディスク ストレージよりも安価ですが、クラウドからデータを頻繁に復元する可能性があると予想される場合は、クラウド プロバイダーからの送信料金によって節約額がいくらか減る可能性があります。クラウド内のバックアップ ファイルからデータを復元する必要がある頻度を特定する必要があります。

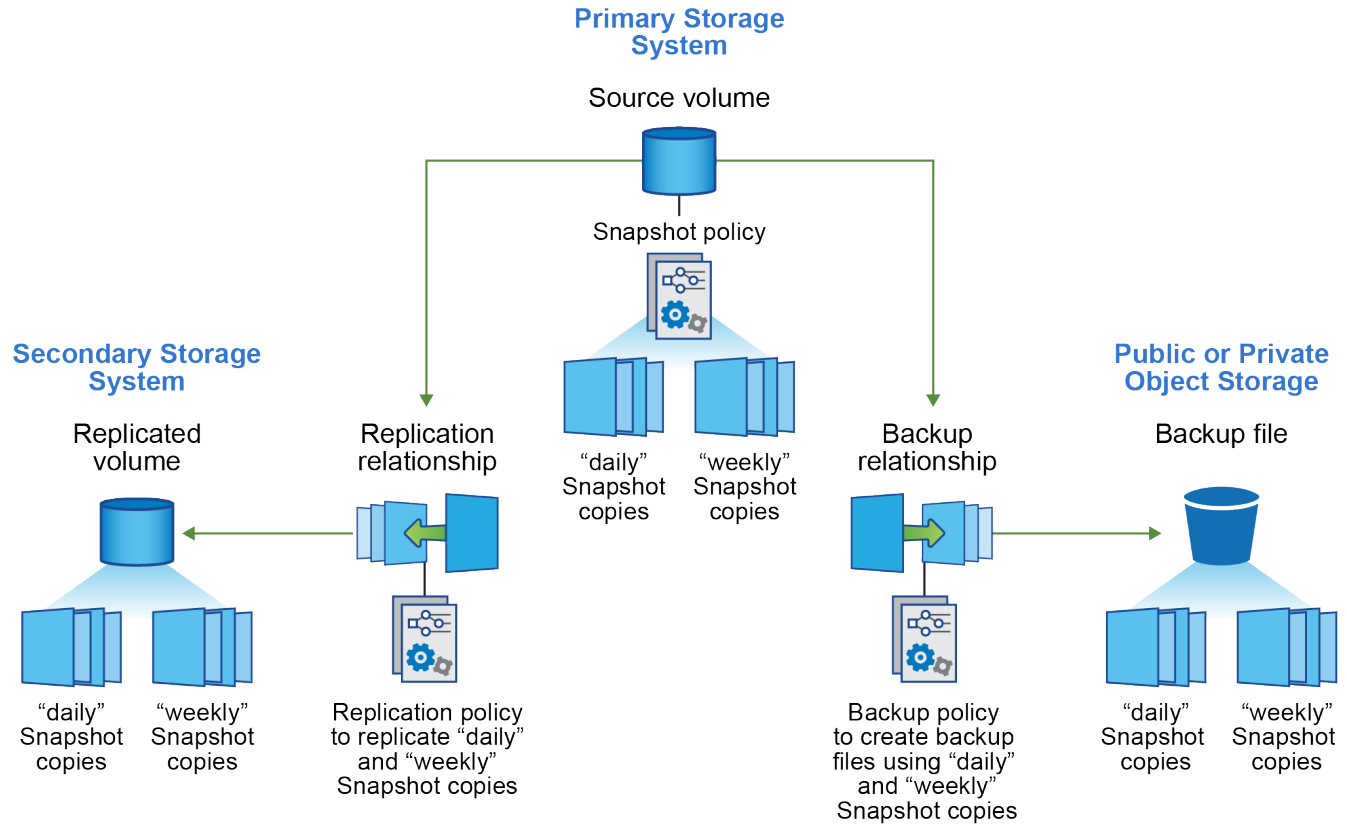
この基準に加えて、クラウド ストレージでは、DataLock および Ransomware Resilience 機能を使用する場合、追加のセキュリティ オプションが提供され、古いバックアップ ファイルにアーカイブ ストレージ クラスを選択することで、さらにコストを節約できます。"DataLockとランサムウェア対策およびアーカイブストレージ設定の詳細"。

バックアップタイプ	バックアップ速度	バックアップコスト	速度を回復する	復元コスト
スナップショット	高	低（ディスク容量）	高	低
複製	中	中（ディスク容量）	中	中規模（ネットワーク）
クラウドバックアップ	低	低（オブジェクト空間）	低	高額（プロバイダー料金）

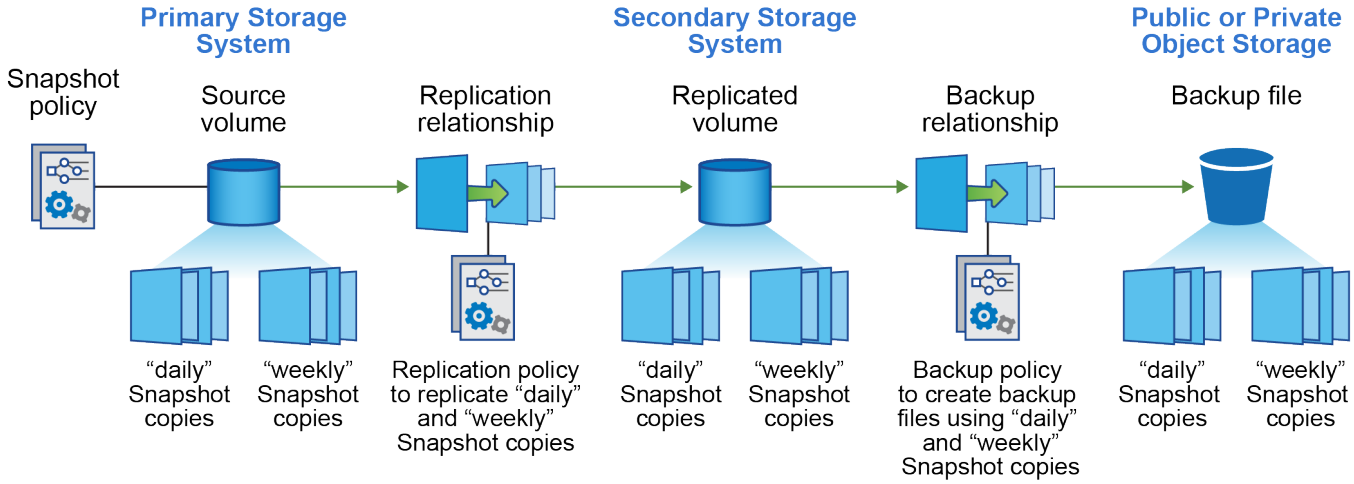
どのバックアップアーキテクチャを使用するか

複製されたボリュームとバックアップ ファイルの両方を作成する場合、ボリュームをバックアップするためにファンアウト アーキテクチャまたはカスケード アーキテクチャを選択できます。

ファンアウト アーキテクチャは、スナップショットを宛先ストレージ システムとクラウド内のバックアップ オブジェクトの両方に独立して転送します。



カスケード アーキテクチャでは、まずスナップショットが宛先ストレージ システムに転送され、次にそのシステムがそのコピーをクラウド内のバックアップ オブジェクトに転送します。



さまざまなアーキテクチャの選択肢の比較

この表は、ファンアウト アーキテクチャとカスケード アーキテクチャの比較を示します。

ファンアウト	カスケード
スナップショットを 2 つの異なるシステムに送信するため、ソース システムのパフォーマンスへの影響はわずかです。	スナップショットを一度だけ送信するため、ソースストレージシステムのパフォーマンスへの影響が少なくなります。

ファンアウト	カスケード
すべてのポリシー、ネットワーク、 ONTAP構成がソースシステム上で実行されるため、セットアップが簡単になります。	一部のネットワークとONTAP構成をセカンダリ システムからも実行する必要があります。

スナップショット、レプリケーション、バックアップのデフォルトポリシーを使用しますか？

NetAppが提供するデフォルトのポリシーを使用してバックアップを作成することも、カスタム ポリシーを作成することもできます。アクティベーション ウィザードを使用してボリュームのバックアップおよびリカバリ サービスを有効にする場合、デフォルトのポリシーと、システム (Cloud Volumes ONTAPまたはオンプレミスのONTAPシステム) にすでに存在するその他のポリシーから選択できます。既存のポリシーとは異なるポリシーを使用する場合は、アクティベーション ウィザードを開始する前または使用中にポリシーを作成できます。

- デフォルトのスナップショット ポリシーでは、時間別、日次、週次スナップショットが作成され、時間別スナップショットが 6 つ、日次スナップショットが 2 つ、週次スナップショットが 2 つ保持されます。
- デフォルトのレプリケーション ポリシーでは、毎日および毎週のスナップショットがレプリケートされ、7 つの毎日のスナップショットと 52 の毎週のスナップショットが保持されます。
- デフォルトのバックアップ ポリシーでは、毎日および毎週のスナップショットが複製され、7 つの毎日のスナップショットと 52 の毎週のスナップショットが保持されます。

レプリケーションまたはバックアップ用のカスタム ポリシーを作成する場合、ポリシー ラベル (「毎日」や「毎週」など) がスナップショット ポリシーに存在するラベルと一致している必要があります。一致していないと、レプリケートされたボリュームとバックアップ ファイルが作成されません。

NetApp Backup and Recovery UI で、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 ポリシーへのバックアップを作成できます。セクションを参照してください"新しいバックアップポリシーの追加"詳細については。

NetApp Backup and Recoveryを使用してカスタム ポリシーを作成するだけでなく、System Manager またはONTAPコマンド ライン インターフェイス (CLI) を使用することもできます。

- "System ManagerまたはONTAP CLIを使用してスナップショットポリシーを作成します"
- "System ManagerまたはONTAP CLIを使用してレプリケーションポリシーを作成します。"

注意: System Manager を使用する場合は、レプリケーション ポリシーのポリシー タイプとして 非同期 を選択し、オブジェクトへのバックアップ ポリシーとして 非同期 と クラウドへのバックアップ を選択します。

ここでは、カスタム ポリシーを作成する場合に役立つ可能性のあるONTAP CLI コマンドのサンプルをいくつか示します。 *admin* vserver（ストレージVM）を `<vserver_name>`これらのコマンドでは。

ポリシーの説明	コマンド
シンプルなスナップショットポリシー	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`

ポリシーの説明	コマンド
クラウドへのシンプルなバックアップ	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
DataLockとランサムウェア対策を備えたクラウドへのバックアップ	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
アーカイブストレージクラスによるクラウドへのバックアップ	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
別のストレージシステムへのシンプルなレプリケーション	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

クラウド関係へのバックアップには、ボールト ポリシーのみを使用できます。

ポリシーはどこに保存されますか**?**

バックアップ ポリシーは、使用する予定のバックアップ アーキテクチャ (ファンアウトまたはカスケード) に応じて異なる場所に存在します。レプリケーションでは 2 つのONTAPストレージ システムがペアになり、オブジェクトへのバックアップではストレージ プロバイダーが宛先として使用されるため、レプリケーション ポリシーとバックアップ ポリシーは同じ方法で設計されていません。

- スナップショット ポリシーは常にプライマリ ストレージ システムに存在します。
- レプリケーション ポリシーは常にセカンダリ ストレージ システムに存在します。
- オブジェクトへのバックアップ ポリシーは、ソース ボリュームが存在するシステム上に作成されます。これは、ファンアウト構成の場合はプライマリ クラスター、カスケード構成の場合はセカンダリ クラスターです。

これらの違いは表に示されています。

アーキテクチャ	スナップショットポリシー	レプリケーションポリシー	バックアップ ポリシー
ファンアウト	プライマリ	セカンダリ	プライマリ
カスケード	プライマリ	セカンダリ	セカンダリ

したがって、カスケード アーキテクチャを使用するときにカスタム ポリシーを作成する予定の場合は、複製

されたボリュームが作成されるセカンダリ システムでオブジェクト ポリシーへのレプリケーションとバックアップを作成する必要があります。ファンアウト アーキテクチャを使用するときにカスタム ポリシーを作成する予定の場合は、複製されたボリュームが作成されるセカンダリ システムにレプリケーション ポリシーを作成し、プライマリ システムにオブジェクト ポリシーへのバックアップを作成する必要があります。

すべてのONTAPシステムに存在するデフォルトのポリシーを使用している場合は、設定は完了です。

独自のオブジェクトストレージコンテナを作成しますか？

システムのオブジェクト ストレージにバックアップ ファイルを作成すると、デフォルトでは、バックアップおよびリカバリ サービスによって、構成したオブジェクト ストレージ アカウントにバックアップ ファイル用のコンテナー (バケットまたはストレージ アカウント) が作成されます。 AWS または GCP バケットの名前は、デフォルトで「netapp-backup-<uuid>」になります。 Azure Blob ストレージ アカウントの名前は「netappbackup<uuid>」です。

特定のプレフィックスを使用したり、特別なプロパティを割り当てたりしたい場合は、オブジェクト プロバイダー アカウントでコンテナーを自分で作成できます。独自のコンテナーを作成する場合は、アクティベーション ウィザードを開始する前にコンテナーを作成する必要があります。 NetApp Backup and Recovery、任意のバケットを使用したり、バケットを共有したりできます。バックアップ アクティベーション ウィザードは、選択したアカウントと資格情報に対してプロビジョニングされたコンテナーを自動的に検出し、使用するコンテナーを選択できるようにします。

バケットは、コンソールから、またはクラウド プロバイダーから作成できます。

- "コンソールから Amazon S3 バケットを作成する"
- "コンソールから Azure Blob ストレージ アカウントを作成する"
- "コンソールから Google Cloud Storage バケットを作成する"

「netapp-backup-xxxxxx」以外のバケットプレフィックスを使用する予定の場合は、コンソールエージェントの IAM ロールの S3 権限を変更する必要があります。

高度なバケット設定

古いバックアップ ファイルをアーカイブ ストレージに移動する場合、または DataLock と Ransomware 保護を有効にしてバックアップ ファイルをロックし、ランサムウェアの可能性をスキャンする場合は、特定の構成設定でコンテナーを作成する必要があります。

- 現時点では、クラスターでONTAP 9.10.1 以降のソフトウェアを使用している場合、独自のバケット上のアーカイブ ストレージは AWS S3 ストレージでサポートされています。デフォルトでは、バックアップは S3 *Standard* ストレージ クラスから開始されます。適切なライフサイクル ルールを使用してバケットを作成してください。
  - 30 日後、バケットの全スコープ内のオブジェクトを S3 *Standard-IA* に移動します。
  - 「smc_push_to_archive: true」タグが付いたオブジェクトを_Glacier Flexible Retrieval_（旧S3 Glacier）に移動します。
- DataLock とランサムウェア保護は、クラスターでONTAP 9.11.1 以降のソフトウェアを使用している場合は AWS ストレージでサポートされ、 ONTAP 9.12.1 以降のソフトウェアを使用している場合は Azure ストレージでサポートされます。
  - AWS の場合、30 日間の保持期間を使用してバケットでオブジェクト ロックを有効にする必要があります。

- Azure の場合、バージョン レベルの不変性をサポートするストレージ クラスを作成する必要があります。

どのコンソールエージェント展開モードを使用していますか

すでにコンソールを使用してストレージを管理している場合は、コンソール エージェントがすでにインストールされています。 NetApp Backup and Recoveryと同じコンソール エージェントを使用する予定であれば、準備は完了です。別のコンソール エージェントを使用する必要がある場合は、バックアップとリカバリの実装を開始する前にそれをインストールする必要があります。

NetApp Consoleは、ビジネス要件とセキュリティ要件を満たす方法でコンソールを使用できるようにする複数の導入モードを提供します。 標準モード では、コンソール SaaS レイヤーを活用して完全な機能を提供しますが、制限モード と プライベート モード は接続制限のある組織で利用できます。

"NetApp Consoleの導入モードの詳細"。

完全なインターネット接続を備えたサイトのサポート

NetApp Backup and Recovery を完全なインターネット接続 (標準モード または *SaaS* モード とも呼ばれます) を備えたサイトで使用する場合、コンソールによって管理されるオンプレミスのONTAPまたはCloud Volumes ONTAPシステムに複製されたボリュームを作成でき、サポートされているいずれかのクラウド プロバイダーのオブジェクト ストレージにバックアップ ファイルを作成できます。"サポートされているバックアップ先の完全なリストを参照してください"。

有効なコンソール エージェントの場所の一覧については、バックアップ ファイルを作成する予定のクラウド プロバイダーの次のいずれかのバックアップ手順を参照してください。コンソール エージェントを Linux マシンに手動でインストールするか、特定のクラウド プロバイダーに展開する必要があるという制限がいくつかあります。

- "Cloud Volumes ONTAPデータを Amazon S3 にバックアップする"
- "Cloud Volumes ONTAPデータを Azure Blob にバックアップする"
- "Cloud Volumes ONTAPデータを Google Cloud にバックアップする"
- "オンプレミスのONTAPデータを Amazon S3 にバックアップする"
- "オンプレミスのONTAPデータを Azure Blob にバックアップする"
- "オンプレミスのONTAPデータを Google Cloud にバックアップする"
- "オンプレミスのONTAPデータをStorageGRIDにバックアップする"
- "オンプレミスのONTAPをONTAP S3 にバックアップする"

インターネット接続が制限されているサイトのサポート

NetApp Backup and Recovery は、インターネット接続が制限されているサイト (制限モード とも呼ばれます) でボリューム データをバックアップするために使用できます。この場合、宛先のクラウド リージョンにコンソール エージェントを展開する必要があります。

- オンプレミスのONTAPシステムまたは AWS 商用リージョンにインストールされたCloud Volumes ONTAPシステムから Amazon S3 にデータをバックアップできます。"Cloud Volumes ONTAPデータを Amazon S3 にバックアップする"。
- オンプレミスのONTAPシステムまたは Azure 商用リージョンにインストールされたCloud Volumes ONTAPシステムから Azure Blob にデータをバックアップできます。"Cloud Volumes ONTAPデータを

Azure Blob にバックアップする"。

インターネットに接続できないサイトのサポート

NetApp Backup and Recovery は、インターネット接続のないサイト (プライベート モード または ダーク サイトとも呼ばれます) でボリューム データをバックアップするために使用できます。この場合、同じサイト内の Linux ホストにコンソール エージェントを展開する必要があります。

BlueXPプライベート モード (レガシーBlueXPインターフェイス) は通常、インターネット接続がなく、AWS Secret Cloud、AWS Top Secret Cloud、Azure IL6 などの安全なクラウド領域があるオンプレミス環境で使用されます。NetApp は、従来のBlueXPインターフェースを使用してこれらの環境を引き続きサポートします。従来のBlueXPインターフェースのプライベートモードのドキュメントについては、 "BlueXPプライベートモードの PDF ドキュメント" 。

- ローカルのオンプレミスONTAPシステムからローカルのNetApp StorageGRIDシステムにデータをバックアップできます。"オンプレミスのONTAPデータをStorageGRIDにバックアップする"。
- ローカルのオンプレミスONTAPシステムから、ローカルのオンプレミスONTAPシステムまたは S3 オブジェクト ストレージ用に構成されたCloud Volumes ONTAPシステムにデータをバックアップできます。"オンプレミスのONTAPデータをONTAP S3 にバックアップする"。

NetApp Backup and Recoveryを使用してONTAPボリュームのバックアップポリシーを管理する

NetApp Backup and Recoveryでは、 NetAppが提供するデフォルトのバックアップ ポリシーを使用してバックアップを作成するか、カスタム ポリシーを作成します。ポリシーは、バックアップの頻度、バックアップの実行時間、保持されるバックアップ ファイルの数を制御します。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

アクティベーション ウィザードを使用してボリュームのバックアップおよびリカバリ サービスを有効にする場合、デフォルトのポリシーと、システム (Cloud Volumes ONTAPまたはオンプレミスのONTAPシステム) にすでに存在するその他のポリシーから選択できます。既存のポリシーとは異なるポリシーを使用する場合は、アクティベーション ウィザードを使用する前または使用中にポリシーを作成できます。

提供されているデフォルトのバックアップポリシーの詳細については、以下を参照してください。"保護の旅を計画する" 。

NetApp Backup and Recovery は、スナップショット、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という 3 種類のONTAPデータのバックアップを提供します。ポリシーは、使用するアーキテクチャとバックアップの種類に応じて異なる場所に存在します。

アーキテクチャ	スナップショットポリシーの保存場所	レプリケーションポリシーの保存場所	オブジェクトポリシーの保存場所へのバックアップ
ファンアウト	プライマリ	セカンダリ	プライマリ
カスケード	プライマリ	セカンダリ	セカンダリ

環境、設定、保護の種類に応じて、次のツールを使用してバックアップ ポリシーを作成します。

- NetApp ConsoleUI
- システムマネージャーUI
- ONTAP CLI

System Manager を使用する場合は、レプリケーション ポリシーのポリシー タイプとして 非同期 を選択し、オブジェクトへのバックアップ ポリシーとして 非同期 と クラウドへのバックアップ を選択します。

システムのポリシーを表示する

1. コンソール UI で、ボリューム > バックアップ設定 を選択します。
2. バックアップ設定ページでシステムを選択し、*アクション*を選択します。 ••• アイコンをクリックし、*ポリシー管理*を選択します。

   ポリシー管理ページが表示されます。スナップショット ポリシーはデフォルトで表示されます。

3. システム内に存在する他のポリシーを表示するには、レプリケーション ポリシー または バックアップ ポリシー のいずれかを選択します。既存のポリシーをバックアップ プランに使用できる場合は、準備は完了です。異なる特性を持つポリシーが必要な場合は、このページから新しいポリシーを作成できます。

ポリシーを作成

オブジェクト ストレージへのスナップショット、レプリケーション、バックアップを管理するポリシーを作成できます。

- [スナップショットを開始する前にスナップショットポリシーを作成する]
- [レプリケーションを開始する前にレプリケーションポリシーを作成する]
- [バックアップを開始する前に、オブジェクトストレージへのバックアップポリシーを作成します。]

スナップショットを開始する前にスナップショットポリシーを作成する

3-2-1 戦略の一部として、プライマリ ストレージ システム上のボリュームのスナップショットを作成します。

ポリシー作成プロセスの一部として、スケジュールと保持を示すスナップショットとSnapMirrorラベルを識別することが含まれます。定義済みのラベルを使用することも、独自のラベルを作成することもできます。

手順

1. コンソール UI で、ボリューム > バックアップ設定 を選択します。
2. バックアップ設定ページでシステムを選択し、*アクション*を選択します。 ••• アイコンをクリックし、*ポリシー管理*を選択します。

   ポリシー管理ページが表示されます。

3. [ポリシー] ページで、[ポリシーの作成] > [スナップショット ポリシーの作成] を選択します。
4. ポリシー名を指定します。

5. スナップショット スケジュールを選択します。最大 5 つのラベルを設定できます。または、スケジュールを作成します。
6. スケジュールを作成する場合:
    a. 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。
    b. スケジュールと保持期間を示すスナップショット ラベルを指定します。
    c. スナップショットをいつ、どのくらいの頻度で取得するかを入力します。
    d. 保持: 保持するスナップショットの数を入力します。
7. *作成*を選択します。

カスケードアーキテクチャを使用したスナップショットポリシーの例

この例では、2 つのクラスターを持つスナップショット ポリシーを作成します。

1. クラスター 1:
    a. ポリシー ページでクラスター 1 を選択します。
    b. レプリケーションおよびオブジェクトへのバックアップ ポリシー セクションは無視します。
    c. スナップショット ポリシーを作成します。
2. クラスター 2:
    a. ポリシー ページでクラスター 2 を選択します。
    b. スナップショット ポリシー セクションは無視します。
    c. オブジェクト ポリシーへのレプリケーションおよびバックアップを構成します。

レプリケーションを開始する前にレプリケーションポリシーを作成する

3-2-1 戦略には、別のストレージ システム上のボリュームの複製が含まれる場合があります。レプリケーション ポリシーは、セカンダリ ストレージ システム上に存在します。

手順

1. [ポリシー] ページで、[ポリシーの作成] > [レプリケーション ポリシーの作成] を選択します。
2. 「ポリシーの詳細」セクションで、ポリシー名を指定します。
3. 各ラベルの保持期間を示すSnapMirrorラベル (最大 5 個) を指定します。
4. 転送スケジュールを指定します。
5. *作成*を選択します。

バックアップを開始する前に、オブジェクトストレージへのバックアップポリシーを作成します。

3-2-1 戦略には、ボリュームをオブジェクト ストレージにバックアップすることが含まれる場合があります。

このストレージ ポリシーは、バックアップ アーキテクチャに応じて異なるストレージ システムの場所に存在します。

- ファンアウト: プライマリストレージシステム
- カスケード: セカンダリストレージシステム

手順

1. ポリシー管理ページで、ポリシーの作成 > *バックアップ ポリシーの作成*を選択します。
2. 「ポリシーの詳細」セクションで、ポリシー名を指定します。
3. 各ラベルの保持期間を示すSnapMirrorラベル (最大 5 個) を指定します。
4. 転送スケジュールやバックアップをアーカイブするタイミングなどの設定を指定します。
5. (オプション) 一定の日数が経過した後に古いバックアップ ファイルを、より安価なストレージ クラスまたはアクセス ティアに移動するには、[アーカイブ] オプションを選択し、データがアーカイブされるまでの経過日数を指定します。バックアップ ファイルをアーカイブ ストレージに直接送信するには、「Archive After Days」に **0** を入力します。

   "アーカイブストレージ設定の詳細"。

6. (オプション) バックアップが変更されたり削除されたりするのを防ぐには、**DataLock** とランサムウェア保護 オプションを選択します。

   クラスターでONTAP 9.11.1 以降を使用している場合は、*DataLock* と *Ransomware protection* を構成することで、バックアップが削除されないように保護することができます。

   "利用可能なDataLock設定の詳細"。

7. *作成*を選択します。

ポリシーを編集する

カスタム スナップショット、レプリケーション、またはバックアップ ポリシーを編集できます。

バックアップ ポリシーを変更すると、そのポリシーを使用しているすべてのボリュームに影響します。

手順

1. ポリシー管理ページでポリシーを選択し、*アクション*を選択します。 ••• アイコンをクリックし、[ポリシーの編集] を選択します。

   プロセスはレプリケーション ポリシーとバックアップ ポリシーで同じです。

2. 「ポリシーの編集」ページで変更を加えます。
3. *保存*を選択します。

ポリシーを削除する

どのボリュームにも関連付けられていないポリシーを削除できます。

ボリュームにポリシーが関連付けられており、そのポリシーを削除する場合は、まずボリュームからポリシーを削除する必要があります。

手順

1. ポリシー管理ページでポリシーを選択し、*アクション*を選択します。 ••• アイコンをクリックし、*スナップショットポリシーの削除*を選択します。
2. *削除*を選択します。

詳細情報の参照

System Manager またはONTAP CLI を使用してポリシーを作成する手順については、以下を参照してください。

"System Managerを使用してスナップショットポリシーを作成する" "ONTAP CLIを使用してスナップショットポリシーを作成する" "System Managerを使用してレプリケーションポリシーを作成する" "ONTAP CLIを使用してレプリケーションポリシーを作成する" "System Manager を使用してオブジェクト ストレージ ポリシーへのバックアップを作成する" "ONTAP CLIを使用してオブジェクトストレージポリシーへのバックアップを作成する"

NetApp Backup and Recoveryのオブジェクトへのバックアップ ポリシー オプション

NetApp Backup and Recovery を使用すると、オンプレミスのONTAPおよびCloud Volumes ONTAPシステム用のさまざまな設定でバックアップ ポリシーを作成できます。

これらのポリシー設定は、オブジェクト ストレージへのバックアップにのみ関連します。これらの設定はいずれもスナップショットまたはレプリケーション ポリシーには影響しません。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

バックアップスケジュールオプション

NetApp Backup and Recovery を使用すると、システム (クラスタ) ごとに固有のスケジュールを持つ複数のバックアップ ポリシーを作成できます。異なる復旧ポイント目標 (RPO) を持つボリュームに、異なるバックアップ ポリシーを割り当てることができます。

各バックアップ ポリシーには、バックアップ ファイルに適用できる「ラベルと保持」のセクションが用意されています。ボリュームに適用されるスナップショット ポリシーは、NetApp Backup and Recoveryによって認識されるポリシーのいずれかである必要があることに注意してください。そうでないと、バックアップ ファイルは作成されません。

スケジュールには、ラベルと保持値の 2 つの部分があります。

- ラベル は、ボリュームからバックアップ ファイルが作成 (または更新) される頻度を定義します。次の種類のラベルから選択できます。
  - 時間別、日別、週別、月別、*年別*の時間枠のいずれか、または組み合わせを選択できます。
  - 3 か月、1 年、または 7 年間のバックアップと保持を提供するシステム定義のポリシーのいずれかを選択できます。
  - ONTAP System Manager またはONTAP CLI を使用してクラスタ上にカスタム バックアップ保護ポリシーを作成した場合は、それらのポリシーのいずれかを選択できます。
- 保持 値は、各ラベル (期間) に保持されるバックアップ ファイルの数を定義します。カテゴリまたは間隔内のバックアップの最大数に達すると、古いバックアップが削除されるため、常に最新のバックアップが保持されます。また、古いバックアップがクラウド内のスペースを占有し続けることがなくなるため、ストレージ コストも節約できます。

たとえば、7 つの 週次 バックアップと 12 つの 月次 バックアップを作成するバックアップ ポリシーを作成す

るとします。

- 毎週、毎月、ボリュームのバックアップファイルが作成されます
- 8週目には、最初の週次バックアップが削除され、8週目の新しい週次バックアップが追加されます（最大7つの週次バックアップが保持されます）
- 13 か月目に、最初の月次バックアップが削除され、13 か月目の新しい月次バックアップが追加されます (最大 12 の月次バックアップが保持されます)

年間バックアップは、オブジェクト ストレージに転送された後、ソース システムから自動的に削除されます。このデフォルトの動作は、システムの「詳細設定」ページで変更できます。

DataLockとランサムウェア保護オプション

NetApp Backup and Recovery は、ボリューム バックアップに対する DataLock およびランサムウェア保護のサポートを提供します。これらの機能を使用すると、バックアップ ファイルをロックしてスキャンし、バックアップ ファイル上のランサムウェアの可能性を検出できます。これは、クラスターのボリューム バックアップをさらに保護したい場合に、バックアップ ポリシーで定義できるオプションの設定です。

これら 2 つの機能はバックアップ ファイルを保護するため、バックアップに対してランサムウェア攻撃が試みられた場合でも、常に有効なバックアップ ファイルがあり、そこからデータを回復することができます。また、バックアップをロックして一定期間保持する必要がある特定の規制要件を満たすのにも役立ちます。DataLock および Ransomware Resilience オプションを有効にすると、 NetApp Backup and Recoveryアクティベーションの一部としてプロビジョニングされるクラウド バケットで、オブジェクトのロックとオブジェクトのバージョン管理が有効になります。

この機能はソース ボリュームを保護するものではなく、ソース ボリュームのバックアップのみを保護します。いくつかの "ONTAPが提供するランサムウェア対策"ソースボリュームを保護します。

- DataLock とランサムウェア保護を使用する予定の場合は、最初のバックアップ ポリシーを作成し、そのクラスターに対してNetApp Backup and Recovery をアクティブ化するときに、これを有効にできます。後で、 NetApp Backup and Recovery の詳細設定を使用して、ランサムウェア スキャンを有効または無効にすることができます。
- ボリューム データを復元するときにコンソールがバックアップ ファイルでランサムウェアをスキャンすると、バックアップ ファイルの内容にアクセスするためにクラウド プロバイダーから追加の送信コストが発生します。

DataLockとは

この機能を使用すると、 SnapMirror経由でクラウドに複製されたクラウド スナップショットをロックできるほか、ランサムウェア攻撃を検出してオブジェクト ストア上のスナップショットの一貫したコピーを回復する機能も有効になります。この機能は、AWS、Azure、Google Cloud Platform、 StorageGRIDでサポートされています。

DataLock は、バックアップ ファイルが一定期間変更または削除されるのを防ぎます。これは、不変ストレージ とも呼ばれます。この機能は、オブジェクト ストレージ プロバイダーの「オブジェクト ロック」テクノロジを使用します。

クラウド プロバイダーは、スナップショットの保持期間に基づいて計算される保持期限 (RUD) を使用します。スナップショットの保持期間は、ラベルとバックアップ ポリシーで定義された保持数に基づいて計算されます。

スナップショットの最小保存期間は 30 日です。これがどのように機能するか、いくつかの例を見てみましょう。

- 保持回数 20 で 毎日 ラベルを選択した場合、スナップショットの保持期間は 20 日となり、デフォルトで最小の 30 日になります。
- 保持回数 4 で **Weekly** ラベルを選択した場合、スナップショットの保持期間は 28 日となり、デフォルトで最小の 30 日になります。
- 保持回数 3 で 月次 ラベルを選択した場合、スナップショットの保持期間は 90 日になります。
- 保持回数 1 で **Yearly** ラベルを選択した場合、スナップショットの保持期間は 365 日になります。

保持期限 **(RUD)** とは何ですか**?** また、それはどのように計算されますか**?**

保持期限 (RUD) は、スナップショットの保持期間に基づいて決定されます。保存期限は、スナップショットの保存期間とバッファーを合計して計算されます。

- バッファは、転送時間のバッファ (3 日) + コスト最適化のバッファ (28 日) で、合計 31 日になります。
- 最小保持期間は 30 日 + 31 日のバッファ = 61 日です。

以下に例をいくつか挙げます。

- 12 回の保持期間を持つ月次バックアップ スケジュールを作成した場合、バックアップは 12 か月間 (プラス 31 日間) ロックされた後、削除され (次のバックアップ ファイルに置き換えられます) ます。
- 毎日 30 回、毎週 7 回、毎月 12 回のバックアップを作成するバックアップ ポリシーを作成する場合、ロックされた保持期間は 3 つあります。
  - 「30日ごと」のバックアップは61日間（30日間＋31日間のバッファ）保持されます。
  - 「7週間ごと」のバックアップは11週間（7週間＋31日）保持され、
  - 「12 か月ごと」のバックアップは 12 か月間 (プラス 31 日間) 保持されます。
- 24 の保持期間を持つ 1 時間ごとのバックアップ スケジュールを作成すると、バックアップが 24 時間ロックされると思われるかもしれません。ただし、これは最小期間の 30 日未満であるため、各バックアップは 61 日間 (30 日 + 31 日のバッファ) ロックされ、保持されます。

> 古いバックアップは、バックアップ ポリシーの保持期間後ではなく、DataLock の保持期間が終了した後に削除されます。

DataLock の保持設定は、バックアップ ポリシーのポリシー保持設定よりも優先されます。バックアップ ファイルがオブジェクト ストアに長期間保存されるため、ストレージ コストに影響する可能性があります。

DataLockとランサムウェア保護を有効にする

ポリシーを作成するときに、DataLock とランサムウェア保護を有効にできます。ポリシーの作成後は、これを有効化、変更、無効化することはできません。

1. ポリシーを作成するときは、**DataLock** および **Ransomware Resilience** セクションを展開します。
2. 次のいずれかを選択します。
   - なし: DataLock 保護とランサムウェア耐性は無効になっています。
   - ロック解除: DataLock 保護とランサムウェア耐性が有効になっています。特定の権限を持つユーザー

は、保持期間中に保護されたバックアップ ファイルを上書きまたは削除できます。

- ロック済み: DataLock 保護とランサムウェア耐性が有効になっています。保持期間中、ユーザーは保護されたバックアップ ファイルを上書きまたは削除することはできません。これにより、完全な規制遵守が実現します。

参照"詳細設定ページでランサムウェア保護オプションを更新する方法"。

ランサムウェア対策とは

ランサムウェア保護は、バックアップ ファイルをスキャンして、ランサムウェア攻撃の証拠を探します。ランサムウェア攻撃の検出は、チェックサムの比較を使用して実行されます。新しいバックアップ ファイルと以前のバックアップ ファイルで潜在的なランサムウェアが特定された場合、その新しいバックアップ ファイルは、ランサムウェア攻撃の兆候が見られない最新のバックアップ ファイルに置き換えられます。(ランサムウェア攻撃を受けたと判断されたファイルは、置き換えられてから 1 日後に削除されます。)

スキャンは次の状況で発生します:

- クラウド バックアップ オブジェクトのスキャンは、クラウド オブジェクト ストレージに転送されるとすぐに開始されます。バックアップ ファイルが最初にクラウド ストレージに書き込まれるときにスキャンが実行されず、次のバックアップ ファイルが書き込まれるときにスキャンが実行されます。
- 復元プロセスのためにバックアップを選択すると、ランサムウェア スキャンを開始できます。
- スキャンはいつでもオンデマンドで実行できます。

回復プロセスはどのように機能しますか**?**

ランサムウェア攻撃が検出されると、サービスは Active Data Console エージェントの Integrity Checker REST API を使用して回復プロセスを開始します。データ オブジェクトの最も古いバージョンが真実のソースであり、回復プロセスの一環として現在のバージョンに作成されます。

これがどのように機能するか見てみましょう:

- ランサムウェア攻撃が発生した場合、サービスはバケット内のオブジェクトを上書きまたは削除しようとします。
- クラウド ストレージはバージョン管理が有効になっているため、バックアップ オブジェクトの新しいバージョンが自動的に作成されます。バージョン管理がオンの状態でオブジェクトを削除すると、そのオブジェクトは削除済みとしてマークされますが、引き続き取得可能です。オブジェクトが上書きされた場合、以前のバージョンが保存され、マークされます。
- ランサムウェア スキャンが開始されると、両方のオブジェクト バージョンのチェックサムが検証され、比較されます。チェックサムが矛盾している場合、潜在的なランサムウェアが検出されています。
- 回復プロセスでは、最後に正常だったコピーに戻す作業が行われます。

サポートされているシステムとオブジェクトストレージプロバイダー

次のパブリックおよびプライベート クラウド プロバイダーのオブジェクト ストレージを使用する場合、次のシステムのONTAPボリュームで DataLock およびランサムウェア保護を有効にできます。

ソースシステム	バックアップファイルの保存先
AWS のCloud Volumes ONTAP	Amazon S3
Azure のCloud Volumes ONTAP	Azure ブロブ

ソースシステム	バックアップファイルの保存先
Google Cloud のCloud Volumes ONTAP	Google Cloud
オンプレミスのONTAPシステム	Amazon S3 Azure Blob Google Cloud NetApp StorageGRID

要件

- AWS の場合:
  - クラスタはONTAP 9.11.1以降を実行している必要があります
  - コンソールエージェントはクラウドまたはオンプレミスに導入できます
  - 次の S3 権限は、コンソール エージェントに権限を提供する IAM ロールの一部である必要があります。これらは、リソース「arn:aws:s3:::netapp-backup-*」の「backupS3Policy」セクションにあります。

AWS S3 の権限

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:オブジェクトのタグ付け
- s3:オブジェクトの削除
- s3:オブジェクトのタグ付けを削除
- s3:GetObjectRetention
- s3:オブジェクトバージョンタグ付けの削除
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:オブジェクトバージョンの削除
- s3:バケットバージョンのリスト
- s3:リストバケット
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketバージョン管理
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:バイパスガバナンス保持
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

"必要な権限をコピーして貼り付けることができるポリシーの完全なJSON形式を表示します。"。

- Azureの場合:
  - クラスタはONTAP 9.12.1以降を実行している必要があります
  - コンソールエージェントはクラウドまたはオンプレミスに導入できます
- Google Cloud の場合:
  - クラスタはONTAP 9.17.1以降を実行している必要があります
  - コンソールエージェントはクラウドまたはオンプレミスに導入できます

- StorageGRIDの場合:
  - クラスタはONTAP 9.11.1以降を実行している必要があります
  - StorageGRIDシステムは11.6.0.3以降を実行している必要があります
  - コンソール エージェントは、オンプレミスで展開する必要があります (インターネット アクセスの有無にかかわらずサイトにインストールできます)
  - 次の S3 権限は、コンソール エージェントに権限を提供する IAM ロールの一部である必要があります。

    StorageGRID S3 権限

    - s3:GetObjectVersionTagging
    - s3:GetBucketObjectLockConfiguration
    - s3:GetObjectVersionAcl
    - s3:オブジェクトのタグ付け
    - s3:オブジェクトの削除
    - s3:オブジェクトのタグ付けを削除
    - s3:GetObjectRetention
    - s3:オブジェクトバージョンタグ付けの削除
    - s3:PutObject
    - s3:GetObject
    - s3:PutBucketObjectLockConfiguration
    - s3:GetLifecycleConfiguration
    - s3:GetBucketTagging
    - s3:オブジェクトバージョンの削除
    - s3:バケットバージョンのリスト
    - s3:リストバケット
    - s3:PutBucketTagging
    - s3:GetObjectTagging
    - s3:PutBucketバージョン管理
    - s3:PutObjectVersionTagging
    - s3:GetBucketVersioning
    - s3:GetBucketAcl
    - s3:PutObjectRetention
    - s3:GetBucketLocation
    - s3:GetObjectVersion

制限事項

- バックアップ ポリシーでアーカイブ ストレージを構成している場合、DataLock およびランサムウェア保護機能は使用できません。
- NetApp Backup and Recoveryをアクティブ化するときに選択した DataLock オプションは、そのクラスターのすべてのバックアップ ポリシーに使用する必要があります。
- 単一のクラスターで複数の DataLock モードを使用することはできません。
- DataLock を有効にすると、すべてのボリュームのバックアップがロックされます。 1 つのクラスターにロックされたボリューム バックアップとロックされていないボリューム バックアップを混在させることはできません。
- DataLock およびランサムウェア保護は、DataLock およびランサムウェア保護が有効になっているバックアップ ポリシーを使用した新しいボリューム バックアップに適用されます。後で「詳細設定」オプションを使用してこれらの機能を有効または無効にすることができます。
- FlexGroupボリュームは、 ONTAP 9.13.1 以降を使用している場合にのみ、DataLock およびランサムウェア保護を使用できます。

DataLockのコストを軽減するヒント

DataLock 機能をアクティブにしたまま、ランサムウェア スキャン機能を有効または無効にすることができます。追加料金を回避するには、スケジュールされたランサムウェア スキャンを無効にすることができます。これにより、セキュリティ設定をカスタマイズし、クラウド プロバイダーからのコストの発生を回避できます。

スケジュールされたランサムウェア スキャンが無効になっている場合でも、必要に応じてオンデマンド スキャンを実行できます。

さまざまなレベルの保護を選択できます。

- ランサムウェア スキャンなしの **DataLock**: ガバナンス モードまたはコンプライアンス モードのいずれかの宛先ストレージ内のバックアップ データを保護します。
  - ガバナンス モード: 管理者が保護されたデータを上書きまたは削除する柔軟性を提供します。
  - コンプライアンス モード: 保持期間が終了するまで完全に消去不可能な状態を保ちます。これにより、規制の厳しい環境における最も厳しいデータ セキュリティ要件を満たすことができます。データはライフサイクル中に上書きまたは変更できないため、バックアップ コピーに対して最強レベルの保護が提供されます。

    代わりに、Microsoft Azure ではロックおよびロック解除モードが使用されます。

- ランサムウェア スキャン機能を備えた **DataLock**: データのセキュリティをさらに強化します。この機能は、バックアップ コピーを変更しようとする試みを検出するのに役立ちます。何らかの試みが行われた場合、データの新しいバージョンが慎重に作成されます。スキャン頻度は 1、2、3、4、5、6、または 7 日に変更できます。スキャンを 7 日ごとに設定すると、コストが大幅に削減されます。

DataLockのコストを軽減するためのヒントについては、以下を参照してください。https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475[]

さらに、DataLockに関連する費用の見積もりは、 "NetApp Backup and Recoveryの総所有コスト (TCO) 計算ツール" 。

アーカイブ保存オプション

AWS、Azure、または Google クラウド ストレージを使用する場合、一定の日数が経過すると、古いバックアップ ファイルをより安価なアーカイブ ストレージ クラスまたはアクセス層に移動できます。バックアップ ファイルを標準のクラウド ストレージに書き込まずに、すぐにアーカイブ ストレージに送信することも選択できます。バックアップ ファイルをアーカイブ ストレージに直接送信するには、「Archive After Days」に **0** と入力するだけです。これは、クラウド バックアップのデータにアクセスする必要がほとんどないユーザーや、テープ ソリューションへのバックアップを置き換えるユーザーにとって特に役立ちます。

アーカイブ層のデータは必要なときにすぐにアクセスできず、取得コストが高くなります。そのため、バックアップ ファイルをアーカイブするかどうかを決定する前に、バックアップ ファイルからデータを復元する必要がある頻度を考慮する必要があります。

- すべてのデータ ブロックをアーカイブ クラウド ストレージに送信するために「0」を選択した場合でも、メタデータ ブロックは常に標準のクラウド ストレージに書き込まれます。
- DataLock を有効にしている場合は、アーカイブ ストレージは使用できません。
- **0** 日 (すぐにアーカイブ) を選択した後は、アーカイブ ポリシーを変更することはできません。

各バックアップ ポリシーには、バックアップ ファイルに適用できる「アーカイブ ポリシー」のセクションが用意されています。

- AWS では、バックアップは *Standard* ストレージ クラスで開始され、30 日後に *Standard-Infrequent Access* ストレージ クラスに移行します。

  クラスターでONTAP 9.10.1 以降を使用している場合は、古いバックアップを *S3 Glacier* または *S3 Glacier Deep Archive* ストレージに階層化できます。"AWSアーカイブストレージの詳細"。

  - NetApp Backup and Recoveryをアクティブ化するときに最初のバックアップ ポリシーでアーカイブ層を選択しなかった場合、将来のポリシーでは *S3 Glacier* が唯一のアーカイブ オプションになります。
  - 最初のバックアップ ポリシーで *S3 Glacier* を選択した場合は、そのクラスターの将来のバックアップ ポリシーを *S3 Glacier Deep Archive* 層に変更できます。
  - 最初のバックアップ ポリシーで *S3 Glacier Deep Archive* を選択した場合、その層はそのクラスターの将来のバックアップ ポリシーで使用できる唯一のアーカイブ層になります。
- Azure では、バックアップは *Cool* アクセス層に関連付けられています。

  クラスターでONTAP 9.10.1 以降を使用している場合は、古いバックアップを *Azure Archive* ストレージに階層化できます。"Azure アーカイブ ストレージの詳細"。
- GCP では、バックアップは *Standard* ストレージ クラスに関連付けられています。

  オンプレミスのクラスターでONTAP 9.12.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後にNetApp Backup and Recovery UI で古いバックアップをアーカイブ ストレージに階層化することを選択できます。"Google アーカイブ ストレージの詳細"。
- StorageGRIDでは、バックアップは *Standard* ストレージ クラスに関連付けられます。

  オンプレミスのクラスタでONTAP 9.12.1 以上を使用しており、 StorageGRIDシステムで 11.4 以上を使用している場合は、古いバックアップ ファイルをパブリック クラウド アーカイブ ストレージにアーカイブできます。

- AWS の場合、AWS *S3 Glacier* または *S3 Glacier Deep Archive* ストレージにバックアップを階層化できます。"AWSアーカイブストレージの詳細"。
- Azure の場合、古いバックアップを *Azure Archive* ストレージに階層化できます。"Azure アーカイブストレージの詳細"。

NetApp Backup and Recoveryの詳細設定でオブジェクト ストレージへのバックアップオプションを管理する

[詳細設定] ページを使用して、各ONTAPシステムに対してNetApp Backup and Recoveryをアクティブ化するときに設定した、クラスタ レベルのオブジェクトへのバックアップ ストレージ設定を変更できます。「デフォルト」のバックアップ設定として適用されているいくつかの設定を変更することもできます。これには、オブジェクト ストレージへのバックアップの転送速度の変更、履歴スナップショットをバックアップ ファイルとしてエクスポートするかどうか、システムのランサムウェア スキャンの有効化または無効化などが含まれます。

これらの設定は、オブジェクト ストレージへのバックアップでのみ使用できます。これらの設定はいずれもスナップショットまたはレプリケーションの設定には影響しません。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

詳細設定ページで次のオプションを変更できます。

- ONTAPシステムにオブジェクトストレージへのアクセス権限を与えるストレージキーを変更する
- オブジェクトストレージに接続されているONTAP IPspaceを変更する
- 最大転送速度オプションを使用して、オブジェクト ストレージにバックアップをアップロードするために割り当てられたネットワーク帯域幅を変更する
- 履歴スナップショットをバックアップ ファイルとしてエクスポートし、将来のボリュームの初期ベースライン バックアップ ファイルに含めるかどうかを変更する
- 「年次」スナップショットをソースシステムから削除するかどうかを変更する
- スケジュールされたスキャンを含む、システムのランサムウェアスキャンを有効または無効にする

クラスターレベルのバックアップ設定を表示する

各システムのクラスターレベルのシステム設定とプロバイダー設定を表示できます。

手順

1. コンソール 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. *ボリューム*タブから*バックアップ設定*を選択します。
3. _バックアップ設定ページ_から、 ••• システムについては、「詳細設定の構成 > システム設定」を選択してシステム設定を表示し、「詳細設定の構成 > プロバイダー設定」を選択してプロバイダー設定を表示します。

   表示されるページには、そのシステムの現在の設定が表示されます。プロバイダー設定を表示する場合、

表示されるプロバイダー設定は、ページの上部で選択したバケットに関連します。

ソース クラスタ上のONTAPのバージョンと、バックアップが存在するクラウド プロバイダの宛先によっては、一部のオプションが使用できないことに注意してください。

オブジェクトストレージにバックアップをアップロードするために利用できるネットワーク帯域幅を変更する

システムに対してNetApp Backup and Recoveryを有効にすると、デフォルトでは、 ONTAP は無制限の帯域幅を使用して、システム内のボリュームからオブジェクト ストレージにバックアップ データを転送できます。バックアップ トラフィックが通常のユーザー ワークロードに影響を与えていることに気付いた場合は、[詳細設定] ページの [最大転送速度] オプションを使用して、転送中に使用されるネットワーク帯域幅の量を調整できます。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、 ••• システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. [詳細設定] ページで、[最大転送速度] セクションを展開します。
4. 最大転送速度として 1 ～ 1,000 Mbps の間の値を選択します。
5. *制限*ラジオ ボタンを選択し、使用できる最大帯域幅を入力するか、*無制限*を選択して制限がないことを示します。
6. *適用*を選択します。

この設定は、システム内のボリュームに対して構成されている可能性のある他のレプリケーション関係に割り当てられる帯域幅には影響しません。

履歴スナップショットをバックアップファイルとしてエクスポートするかどうかを変更する

このシステムで使用しているバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致するボリュームのローカル スナップショットがある場合は、それらの履歴スナップショットをバックアップ ファイルとしてオブジェクト ストレージにエクスポートできます。これにより、古いスナップショットをベースライン バックアップ コピーに移動して、クラウド内のバックアップを初期化できるようになります。

このオプションは、新しい読み取り/書き込みボリュームの新しいバックアップ ファイルにのみ適用され、データ保護 (DP) ボリュームではサポートされないことに注意してください。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、 ••• システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. [詳細設定] ページで、[既存のスナップショットのコピーをエクスポート] セクションを展開します。
4. 既存のスナップショットをエクスポートするかどうかを選択します。
5. *適用*を選択します。

「年次」スナップショットをソースシステムから削除するかどうかを変更する

いずれかのボリュームのバックアップ ポリシーに「年間」バックアップ ラベルを選択すると、作成されるス

ナップショットが非常に大きくなります。デフォルトでは、これらの年次スナップショットは、オブジェクトストレージに転送された後、ソース システムから自動的に削除されます。このデフォルトの動作は、年間スナップショットの削除セクションから変更できます。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、 ••• システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. [詳細設定] ページで、[年次スナップショットの削除] セクションを展開します。
4. ソース システムに年次スナップショットを保持するには、[無効] を選択します。
5. *適用*を選択します。

ランサムウェアスキャンを有効または無効にする

ランサムウェア保護スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は 7 日間です。スキャンは最新のスナップショットに対してのみ実行されます。

DataLockとランサムウェア耐性オプションの詳細については、以下を参照してください。"DataLockとランサムウェア耐性オプション" 。

スケジュールを日単位や週単位に変更したり、無効にしたりしてコストを節約できます。

ランサムウェアスキャンを有効にすると、クラウドプロバイダーに応じて追加料金が発生します。

スケジュールされたランサムウェア スキャンが無効になっている場合でも、オンデマンド スキャンを実行することはでき、復元操作中にスキャンが実行されます。

参照"ポリシーの管理"ランサムウェア検出を実装するポリシーの管理の詳細については、こちらをご覧ください。

システムのランサムウェアスキャンを有効または無効にする

クラスターのランサムウェア スキャンを有効または無効にすることができます。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、 ••• システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. 表示されたページで、ランサムウェア スキャン セクションを展開します。
4. *ランサムウェアスキャン*を有効または無効にします。
5. *スケジュールされたランサムウェアスキャン*を選択します。
6. 必要に応じて、毎週のデフォルトスキャンを日ごとまたは週ごとに変更します。
7. スキャンを実行する頻度を日数または週数で設定します。
8. *適用*を選択します。

プロバイダーのランサムウェアスキャンを有効または無効にする

プロバイダー設定ページを使用して、プロバイダー レベルでランサムウェア スキャンを有効または無効にすることができます。このページの設定は、ページの上部で選択したバケットに関連しています。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、 ••• システムの場合は、[詳細設定の構成] > [プロバイダー設定] を選択します。
3. 表示されたページの上部で、設定を変更する必要があるバケットを選択します。
4. *ランサムウェアスキャン*セクションを展開します。
5. *ランサムウェアスキャン*を有効または無効にします。
6. *スケジュールされたランサムウェアスキャン*を選択します。
7. 必要に応じて、毎週のデフォルトスキャンを日ごとまたは週ごとに変更します。
8. スキャンを実行する頻度を日数または週数で設定します。
9. *適用*を選択します。

NetApp Backup and Recoveryを使用してCloud Volumes ONTAPデータを Amazon S3 にバックアップする

Cloud Volumes ONTAPシステムから Amazon S3 へのボリューム データのバックアップを開始するには、NetApp Backup and Recoveryでいくつかの手順を完了します。

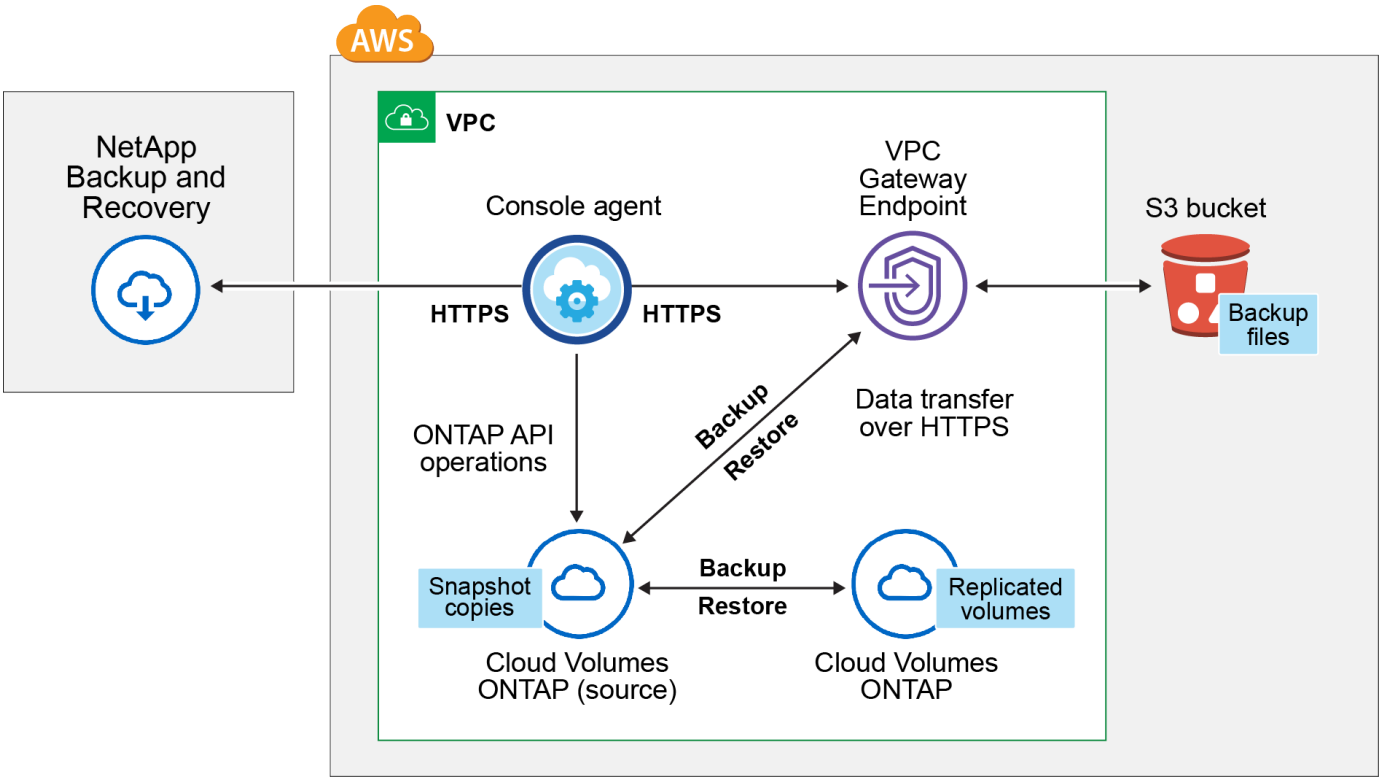
NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

構成のサポートを確認する

ボリュームを S3 にバックアップする前に、次の要件を読んで、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとそれらの間で準備する必要がある接続を示しています。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。



VPC ゲートウェイ エンドポイントがすでに VPC 内に存在している必要があります。 "ゲートウェイエンドポイントの詳細" 。

サポートされる**ONTAP**バージョン

最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。

データ暗号化に顧客管理キーを使用するために必要な情報

アクティベーションウィザードでは、デフォルトの Amazon S3 暗号化キーを使用する代わりに、データ暗号化用に独自のカスタマー管理キーを選択できます。この場合、暗号化管理キーがすでに設定されている必要があります。 "独自のキーの使用方法を確認する" 。

ライセンス要件を確認する

NetApp Backup and Recovery PAYGO ライセンスの場合、 Cloud Volumes ONTAPとNetApp Backup and Recoveryの導入を可能にするコンソールサブスクリプションが AWS Marketplace で利用できます。必要がある "このNetApp Consoleサブスクリプションを購読する"NetApp Backup and Recoveryを有効にする前に。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。

Cloud Volumes ONTAPデータとオンプレミスONTAPデータの両方をバックアップできる年間契約の場合は、"AWSマーケットプレイスページ"その後 "サブスクリプションをAWS認証情報に関連付ける"。

Cloud Volumes ONTAPとNetApp Backup and Recoveryをバンドルできる年間契約の場合は、 Cloud Volumes ONTAPシステムを作成するときに年間契約を設定する必要があります。このオプションでは、オンプレミスのデータをバックアップすることはできません。

NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要です。"BYOLライセンスの管理方法を学ぶ"。コンソールエージェントとCloud Volumes ONTAPシステムをダーク サイトに展開する場合は、BYOL ライセンスを使用する必要があります。

また、バックアップを保存するストレージスペース用の AWS アカウントも必要です。

コンソールエージェントを準備する

コンソールエージェントは、完全なインターネットアクセスまたは制限されたインターネットアクセス (「標準」または「制限」モード) を備えた AWS リージョンにインストールする必要があります。 "詳細については、 NetApp Consoleの展開モードを参照してください。" 。

- "コンソールエージェントについて学ぶ"
- "AWS にコンソールエージェントを標準モード（フルインターネットアクセス）でデプロイする"
- "制限モード（送信アクセスが制限される）でコンソール エージェントをインストールする"

コンソールエージェントへの権限を確認または追加する

コンソールに権限を与えるIAMロールには、最新のS3権限が含まれている必要があります。 "コンソールポリシー" 。ポリシーにこれらの権限がすべて含まれていない場合は、 "AWSドキュメント: IAMポリシーの編集" 。

ポリシーからの具体的な権限は次のとおりです。

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",
```

```
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
}
```

AWS中国リージョンでバックアップを作成する場合、IAMポリシーのすべての_Resource_セクションのAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります。例：`arn:aws-cn:s3:::netapp-backup-*` 。

必要な**AWS Cloud Volumes ONTAP**権限

Cloud Volumes ONTAPシステムがONTAP 9.12.1以降のソフトウェアを実行している場合、そのシステムに権限を提供するIAMロールには、最新のNetApp Backup and Recovery専用の新しいS3権限セットが含まれている必要があります。 "Cloud Volumes ONTAPポリシー" 。

コンソール バージョン 3.9.23 以降を使用してCloud Volumes ONTAPシステムを作成した場合、これらの権限はすでに IAM ロールの一部になっているはずです。それ以外の場合は、不足している権限を追加する必要があります。

サポートされている**AWS**リージョン

NetApp Backup and Recovery は、AWS GovCloud リージョンを含むすべての AWS リージョンでサポートされています。

別の **AWS** アカウントでバックアップを作成するために必要な設定

デフォルトでは、バックアップはCloud Volumes ONTAPシステムに使用されているアカウントと同じアカウントを使用して作成されます。バックアップに別の AWS アカウントを使用する場合は、次の手順を実行する必要があります。

- 権限「s3:PutBucketPolicy」と「s3:PutBucketOwnershipControls」が、コンソールエージェントに権限を提供する IAM ロールの一部であることを確認します。
- コンソールで宛先 AWS アカウントの認証情報を追加します。 "やり方を見る" 。
- 2 番目のアカウントのユーザー資格情報に次の権限を追加します。

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

"独自のバケットの作成について詳しくは"。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。
- 異なるサブネットにある 2 つのCloud Volumes ONTAPシステム間でデータを複製するには、サブネットを一緒にルーティングする必要があります (これがデフォルト設定です)。

Cloud Volumes ONTAPで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recoveryを有効にするのは簡単です。既存のCloud Volumes ONTAPシステムがあるか、新しいシステムがあるかによって、手順が若干異なります。

新しいシステムで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recovery は、システム ウィザードでデフォルトで有効になっています。このオプションは必ず有効にしておいてください。

見る "AWS でCloud Volumes ONTAP を起動"Cloud Volumes ONTAPシステムを作成するための要件と詳細については、こちらをご覧ください。

手順

1. コンソールの システム ページで、システムの追加 を選択し、クラウド プロバイダーを選択して、新規追加 を選択します。 * Cloud Volumes ONTAPの作成*を選択します。
2. クラウド プロバイダーとして **Amazon Web Services** を選択し、単一ノードまたは HA システムを選択します。
3. 「詳細と資格情報」ページに入力します。
4. [サービス] ページで、サービスを有効のままにして、[続行] を選択します。
5. ウィザードのページを完了してシステムを展開します。

結果

システムでNetApp Backup and Recovery が有効になっています。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、 NetApp Backup and Recoveryを起動し、"保護したいボリュームごとにバックアップを有効化します" 。

既存のシステムで**NetApp Backup and Recovery**を有効にする

コンソールからいつでも既存のシステムでNetApp Backup and Recoveryを有効にできます。

手順

1. コンソールの システム ページでクラスターを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 を選択します。

   バックアップの Amazon S3 保存先が システム ページにクラスターとして存在する場合は、クラスターを Amazon S3 システムにドラッグしてセットアップ ウィザードを開始できます。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。

   - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

     バックアップの AWS 保存先がコンソールの [システム] ページにシステムとして存在する場合は、ONTAPクラスターを AWS オブジェクト ストレージにドラッグできます。

   - バックアップとリカバリ バーで ボリューム を選択します。ボリュームタブから*アクション*を選択します ••• アイコン オプションをクリックし、単一ボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていないボリューム) に対して **3-2-1** 保護のアクティブ化 を選択します。

   ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。

   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。

- 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー

> 選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。既存のバケットを選択するか、新しいバケットを構成する場合、クラスターごとに最大 6 つのバケットにボリュームをバックアップできます。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてセカンダリ ストレージ システムからオブジェクト ストレージへ流れます。
   - ファンアウト: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてプライマリ ストレージ システムからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。

   > スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

   ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

   a. ポリシーの名前を入力します。

b. 通常は異なる頻度のスケジュールを最大 5 つ選択します。

c. *作成*を選択します。

4. レプリケーション: 次のオプションを設定します。

   - レプリケーション ターゲット: 宛先システムとストレージ VM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。

     カスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     i. ポリシーの名前を入力します。

     ii. 通常は異なる頻度のスケジュールを最大 5 つ選択します。

     iii. *作成*を選択します。

5. バックアップ: 次のオプションを設定します。

   - プロバイダー: **Amazon Web Services** を選択します。
   - プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

     バックアップを保存するために使用する AWS アカウントを入力します。これは、Cloud Volumes ONTAPシステムが存在するアカウントとは異なるアカウントにすることができます。

     バックアップに別の AWS アカウントを使用する場合は、コンソールでバックアップ先の AWS アカウントの認証情報を追加し、コンソールに権限を付与する IAM ロールに「s3:PutBucketPolicy」および「s3:PutBucketOwnershipControls」権限を追加する必要があります。

     バックアップを保存するリージョンを選択します。これは、Cloud Volumes ONTAPシステムが存在するリージョンとは異なるリージョンにすることができます。

     新しいバケットを作成するか、既存のバケットを選択します。

   - 暗号化: 新しいバケットを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの AWS 暗号化キーを使用するか、AWS アカウントから独自のカスタマー管理キーを選択するかを選択します。("独自の暗号化キーの使用方法を確認する")。

     独自のカスタマー管理キーを使用する場合は、キー コンテナーとキー情報を入力します。

     既存のバケットを選択した場合は、暗号化情報がすでに利用可能であるため、ここで入力する必要はありません。

   - ネットワーク: このプロバイダーのネットワーク オプションを構成します。
   - バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択するか、新しいポリシーを作成します。

バックアップをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

i. ポリシーの名前を入力します。

ii. 通常は異なる頻度のスケジュールを最大 5 つ選択します。

iii. オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。 DataLockとランサムウェア耐性の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシー設定" 。

iv. *作成*を選択します。

- 既存のスナップショットをエクスポート: このシステム内のボリュームに、このシステムに対して選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) と一致するローカル スナップショットがある場合、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの保護が最も完全になります。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、ローカル スナップショット、レプリケーション、およびバックアップの不一致なラベルを自動的に修正する チェックボックスをオンにします。これにより、スナップショット、レプリケーション、およびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。

ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行

する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用して、 Cloud Volumes ONTAPデータを Azure Blob ストレージにバックアップします。

Cloud Volumes ONTAPシステムから Azure Blob ストレージへのボリューム データのバックアップを開始するには、NetApp Backup and Recoveryでいくつかの手順を実行します。

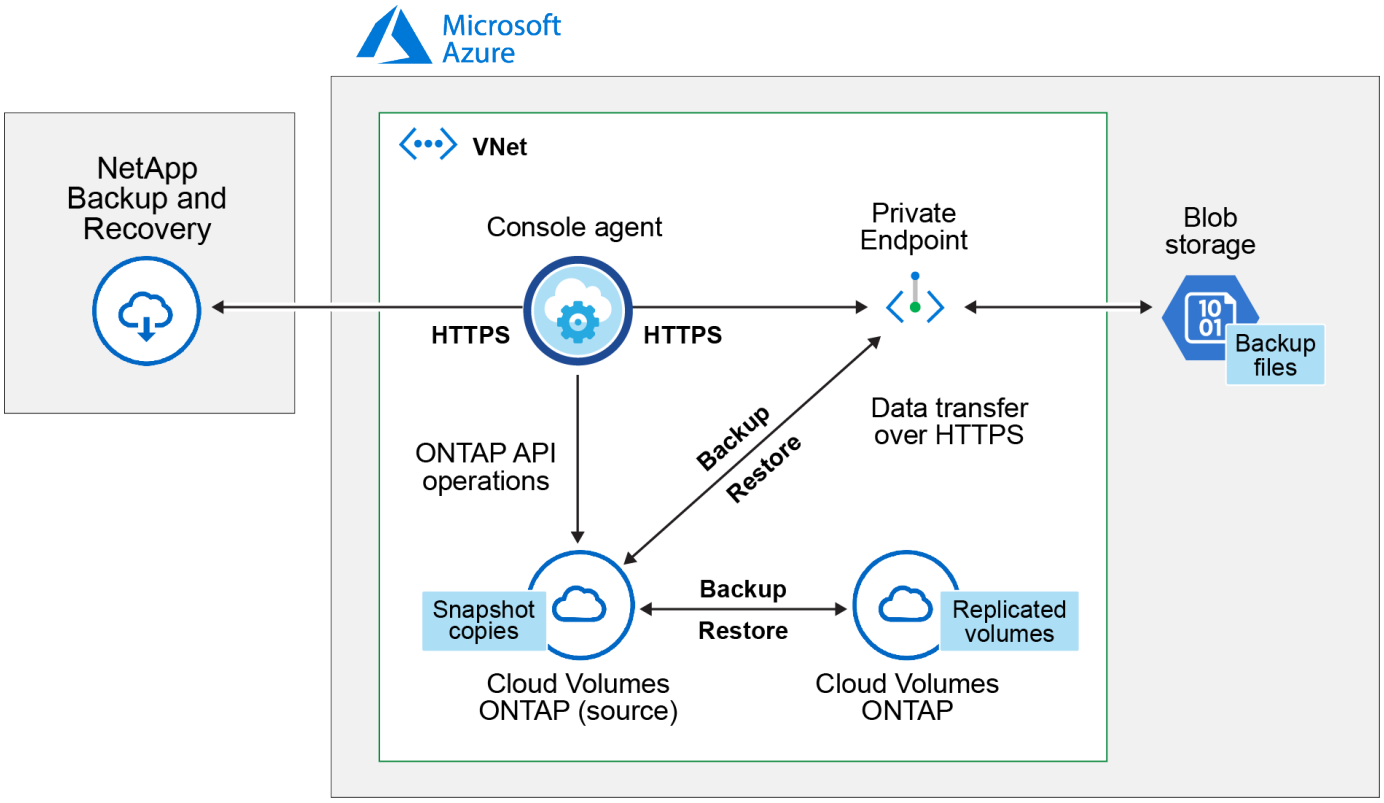
NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

構成のサポートを確認する

ボリュームを Azure Blob ストレージにバックアップする前に、次の要件を読んで、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとそれらの間で準備する必要がある接続を示しています。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。



サポートされる**ONTAP**バージョン

最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。

サポートされている**Azure**リージョン

NetApp Backup and Recovery は、Azure Government リージョンを含むすべての Azure リージョンでサポートされています。

デフォルトでは、 NetApp Backup and Recovery はコストの最適化のためにローカル冗長性 (LRS) を使用して BLOB コンテナーをプロビジョニングします。異なるゾーン間でデータが確実に複製されるようにしたい場合は、NetApp Backup and Recovery をアクティブ化した後、この設定をゾーン冗長 (ZRS) に変更できます。 Microsoftの指示を参照してください "ストレージアカウントの複製方法を変更する"。

別の **Azure** サブスクリプションにバックアップを作成するために必要な設定

デフォルトでは、バックアップはCloud Volumes ONTAPシステムに使用されているものと同じサブスクリプションを使用して作成されます。

ライセンス要件を確認する

NetApp Backup and Recovery PAYGO ライセンスの場合、 NetApp Backup and Recoveryを有効にする前に、Azure Marketplace 経由のサブスクリプションが必要です。 NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。 "システムウィザードの詳細と資格情報ページからサブスクライブできます" 。

NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要です。"BYOLライセンスの管理方法を学ぶ"。コンソール エージェントとCloud Volumes ONTAPシステムをダーク サイト (「プライベート モード」) に展開する場合は、BYOL ライセンスを使用する必要があります。

また、バックアップを保存するストレージ スペース用の Microsoft Azure サブスクリプションが必要です。

コンソールエージェントを準備する

コンソール エージェントは、完全なインターネット アクセスまたは制限されたインターネット アクセス (「標準」または「制限」モード) を備えた Azure リージョンにインストールできます。 "詳細については、NetApp Consoleの展開モードを参照してください。" 。

- "コンソールエージェントについて学ぶ"
- "Azure にコンソール エージェントを標準モード (完全なインターネット アクセス) でデプロイする"
- "制限モード（送信アクセスが制限される）でコンソール エージェントをインストールする"

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の検索と復元機能を使用するには、Azure Synapse ワークスペースと Data Lake ストレージ アカウントにアクセスできるように、コンソール エージェントのロールに特定のアクセス許可が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従ってください。

開始する前に

- Azure Synapse Analytics リソース プロバイダー (「Microsoft.Synapse」と呼ばれます) をサブスクリプションに登録する必要があります。 "このリソースプロバイダーをサブスクリプションに登録する方法をご覧ください" 。リソース プロバイダーを登録するには、サブスクリプションの 所有者 または 投稿者 である必要があります。

- コンソール エージェントと Azure Synapse SQL サービス間の通信には、ポート 1433 が開いている必要があります。

手順

1. コンソール エージェント仮想マシンに割り当てられたロールを識別します。
    a. Azure ポータルで、仮想マシン サービスを開きます。
    b. コンソール エージェント仮想マシンを選択します。
    c. [設定] で、[**ID**] を選択します。
    d. *Azure ロールの割り当て*を選択します。
    e. コンソール エージェント仮想マシンに割り当てられたカスタム ロールをメモします。
2. カスタム ロールを更新します。
    a. Azure ポータルで、Azure サブスクリプションを開きます。
    b. *アクセス制御 (IAM) > ロール*を選択します。
    c. カスタム ロールの省略記号 (**...**) を選択し、[編集] を選択します。
    d. **JSON** を選択し、次の権限を追加します。

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"ポリシーの完全なJSON形式を表示する"

e. *確認+更新*を選択し、*更新*を選択します。

データ暗号化に顧客管理キーを使用するために必要な情報

アクティベーション ウィザードでは、既定の Microsoft 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータの暗号化に使用できます。この場合、Azure サブスクリプション、Key Vault 名、およびキーが必要になります。 "独自のキーの使用方法を確認する" 。

NetApp Backup and Recoveryは、*Azure*アクセスポリシー、*Azure*ロールベースアクセス制御（Azure RBAC）権限モデル、および_マネージドハードウェアセキュリティモデル_（HSM）をサポートしています（ "Azure Key Vault Managed HSM とは何ですか?" ）。

Azure Blob ストレージ アカウントを作成する

デフォルトでは、サービスによってストレージ アカウントが作成されます。独自のストレージ アカウントを使用する場合は、バックアップ アクティブ化ウィザードを開始する前にストレージ アカウントを作成し、ウィザードでそれらのストレージ アカウントを選択できます。

"独自のストレージアカウントの作成について詳しくは、こちらをご覧ください。"。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。
- 異なるサブネットにある 2 つのCloud Volumes ONTAPシステム間でデータを複製するには、サブネットを一緒にルーティングする必要があります (これがデフォルト設定です)。

Cloud Volumes ONTAPで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recoveryを有効にするのは簡単です。既存のCloud Volumes ONTAPシステムがあるか、新しいシステムがあるかによって、手順が若干異なります。

新しいシステムで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recovery は、システム ウィザードでデフォルトで有効になっています。このオプションは必ず有効にしておいてください。

見る "Azure でCloud Volumes ONTAP を起動する"Cloud Volumes ONTAPシステムを作成するための要件と詳細については、こちらをご覧ください。

リソース グループの名前を選択する場合は、 Cloud Volumes ONTAPをデプロイするときにNetApp Backup and Recovery を無効にします。

手順

1. コンソールの システム ページで、システムの追加 を選択し、クラウド プロバイダーを選択して、新規追加 を選択します。 * Cloud Volumes ONTAPの作成*を選択します。
2. クラウド プロバイダーとして **Microsoft Azure** を選択し、単一ノードまたは HA システムを選択します。
3. [Azure 資格情報の定義] ページで、資格情報の名前、クライアント ID、クライアント シークレット、ディレクトリ ID を入力し、[続行] を選択します。
4. [詳細と資格情報] ページに入力し、Azure Marketplace サブスクリプションが設定されていることを確認して、[続行] を選択します。
5. [サービス] ページで、サービスを有効のままにして、[続行] を選択します。
6. ウィザードのページを完了してシステムを展開します。

結果

システムでNetApp Backup and Recovery が有効になっています。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、 NetApp Backup and Recoveryを起動し、"保護したいボリュームごとにバックアップを有効化します" 。

既存のシステムで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recoveryをいつでもシステムから直接有効にできます。

手順

1. コンソールの システム ページでシステムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効 を選択します。

   バックアップの Azure Blob 保存先がコンソールの システム ページにシステムとして存在する場合は、クラスターを Azure Blob システムにドラッグしてセットアップ ウィザードを開始できます。

2. ウィザードのページを完了して、 NetApp Backup and Recoveryを展開します。
3. バックアップを開始する場合は、ONTAPボリューム上のバックアップをアクティブ化する 。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ ア

クティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
   - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

     バックアップの Azure 保存先が **Systems** ページにシステムとして存在する場合は、 ONTAPクラスターを Azure Blob オブジェクト ストレージにドラッグできます。
   - バックアップとリカバリ バーで ボリューム を選択します。ボリュームタブから*アクション*を選択しますアイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

   ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーのうち 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます。 (FlexGroupボリュームは一度に 1 つだけ選択できます。)既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。

- 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてが必要な場合
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー

> 選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてセカンダリ ストレージ システムからオブジェクト ストレージへ流れます。
   - ファンアウト: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてプライマリ ストレージ システムからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいスナップショット ポリシーを作成します。

   > スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

   ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
   - ポリシーの名前を入力します。
   - 通常は異なる頻度のスケジュールを最大 5 つ選択します。

- *作成*を選択します。

4. レプリケーション: 次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。

     レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: **Microsoft Azure** を選択します。
   - プロバイダー設定: プロバイダーの詳細を入力します。

     バックアップを保存するリージョンを入力します。これは、Cloud Volumes ONTAPシステムが存在するリージョンとは異なるリージョンにすることができます。

     新しいストレージ アカウントを作成するか、既存のストレージ アカウントを選択します。

     バックアップを保存するために使用する Azure サブスクリプションを入力します。これは、Cloud Volumes ONTAPシステムが存在するサブスクリプションとは異なるサブスクリプションにすることができます。

     Blob コンテナーを管理する独自のリソース グループを作成するか、リソース グループの種類とグループを選択します。

     バックアップ ファイルが変更されたり削除されたりするのを防ぐには、30 日間の保持期間を使用して不変ストレージが有効になっているストレージ アカウントが作成されていることを確認してください。

     さらにコストを最適化するために古いバックアップ ファイルを Azure Archive Storage に階層化する場合は、ストレージ アカウントに適切なライフサイクル ルールがあることを確認してください。

   - 暗号化キー: 新しい Azure ストレージ アカウントを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、既定の Azure 暗号化キーを使用するか、Azure アカウントから独自のカスタマー管理キーを選択するかを選択します。

     独自のカスタマー管理キーを使用する場合は、キー コンテナーとキー情報を入力します。 "独自のキーの使い方を学ぶ" 。

既存の Microsoft ストレージ アカウントを選択した場合は、暗号化情報が既に用意されているため、ここで入力する必要はありません。

- ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。プライベート エンドポイントはデフォルトで無効になっています。
  i. バックアップするボリュームが存在するONTAPクラスタ内の IPspace。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。
  ii. 必要に応じて、以前に構成した Azure プライベート エンドポイントを使用するかどうかを選択します。 "Azure プライベート エンドポイントの使用について学習します" 。
- バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択します。

バックアップをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。 DataLockとランサムウェア耐性の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシー設定" 。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ボリュームと同期されます。

入力したリソース グループに BLOB ストレージ コンテナーが作成され、そこにバックアップ ファイルが保存されます。

デフォルトでは、 NetApp Backup and Recovery はコストの最適化のためにローカル冗長性 (LRS) を使用して BLOB コンテナーをプロビジョニングします。異なるゾーン間でデータが複製されるようにしたい場合は、この設定をゾーン冗長性 (ZRS) に変更できます。 Microsoftの指示を参照してください "ストレージアカウントの複製方法を変更する"。

ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

次の手順

- あなたはできる"バックアップファイルとバックアップポリシーを管理する"。これには、バックアップの開始と停止、バックアップの削除、バックアップ スケジュールの追加と変更などが含まれます。
- あなたはできる"クラスタレベルのバックアップ設定を管理する"。これには、 ONTAPがクラウド ストレージにアクセスするために使用するストレージ キーの変更、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使用できるネットワーク帯域幅の変更、将来のボリュームの自動バックアップ設定の変更などが含まれます。
- また、"バックアップ ファイルからボリューム、フォルダ、または個々のファイルを復元する" AWS のCloud Volumes ONTAPシステム、またはオンプレミスのONTAPシステムに接続します。

NetApp Backup and Recoveryを使用してCloud Volumes ONTAPデータを Google Cloud Storage にバックアップする

Cloud Volumes ONTAPシステムから Google Cloud Storage へのボリューム データのバックアップを開始するには、NetApp Backup and Recoveryでいくつかの手順を完了します。

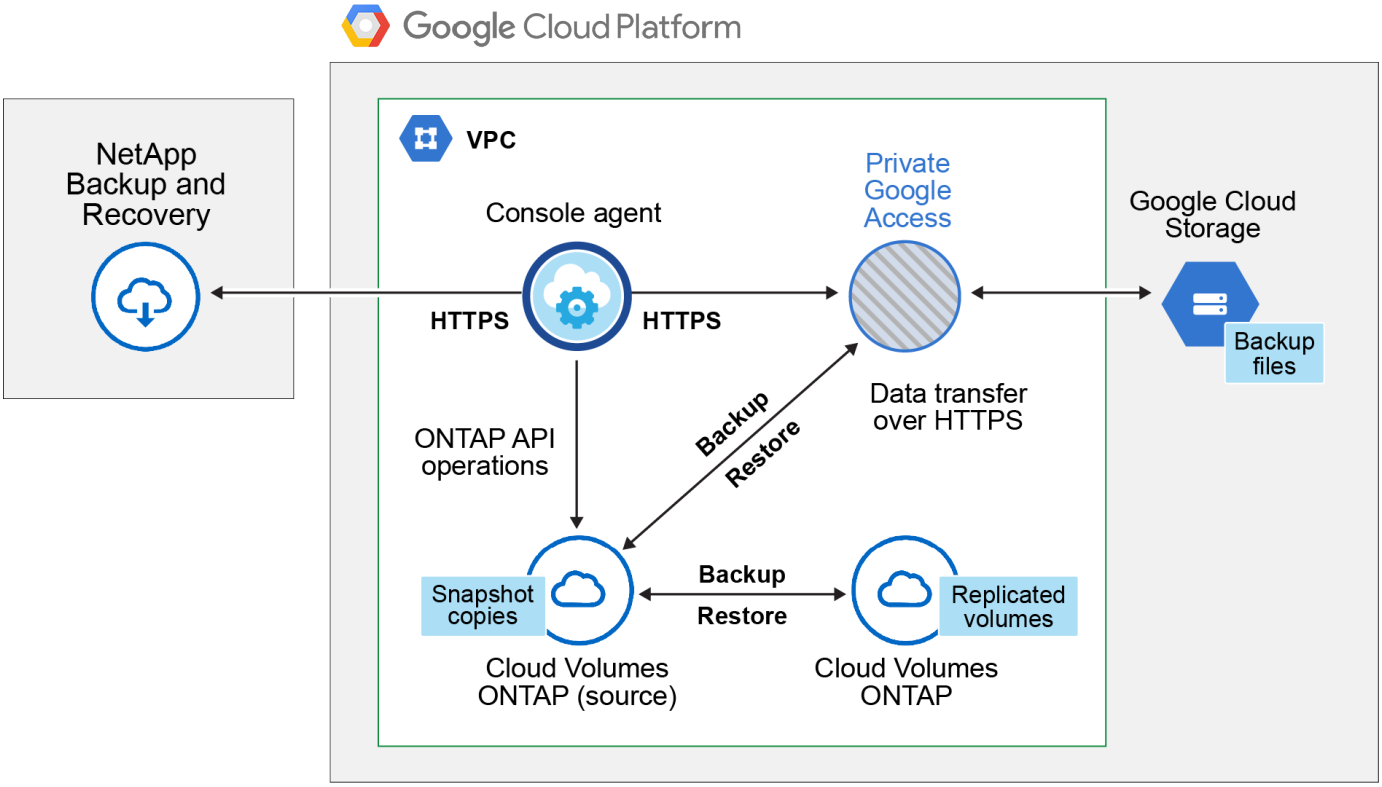
NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

構成のサポートを確認する

Google Cloud Storage へのボリュームのバックアップを開始する前に、次の要件を読んで、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとそれらの間で準備する必要がある接続を示しています。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。



サポートされる**ONTAP**バージョン

最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。

サポートされている**GCP**リージョン

NetApp Backup and Recoveryは、すべての GCP リージョンでサポートされています。

GCP サービス アカウント

Google Cloud プロジェクトにカスタムロールを持つサービス アカウントが必要です。 "サービスアカウントの作成方法を学ぶ" 。

NetApp Backup and Recovery がGoogle Cloud Storage バケットにアクセスできるようにするサービス アカウントには、ストレージ管理者のロールは不要になりました。

ライセンス要件を確認する

NetApp Backup and Recovery PAYGO ライセンスの場合、 Cloud Volumes ONTAPとNetApp Backup and Recoveryの導入を可能にするコンソール サブスクリプションが Google Marketplace で利用できます。必要がある "このコンソールサブスクリプションを購読する"NetApp Backup and Recoveryを有効にする前に。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。 "システムウィザードの詳細と資格情報ページからサブスクライブできます" 。

NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要です。"BYOLライセンスの管理方法を学ぶ"。

また、バックアップを保存するストレージスペース用の Google サブスクリプションが必要です。

コンソールエージェントを準備する

コンソール エージェントは、インターネットにアクセスできる Google リージョンにインストールする必要があります。

- "コンソールエージェントについて学ぶ"
- "Google Cloud にコンソール エージェントをデプロイする"

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の「検索と復元」機能を使用するには、Google Cloud BigQuery サービスにアクセスできるように、コンソール エージェントのロールに特定の権限が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従ってください。

手順

1. の中で "Google Cloud コンソール"、*役割*ページに移動します。
2. ページ上部のドロップダウン リストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタム ロールを選択します。
4. ロールの権限を更新するには、「ロールの編集」を選択します。
5. 次の新しい権限をロールに追加するには、「権限の追加」を選択します。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 編集したロールを保存するには、[更新] を選択します。

顧客管理暗号鍵（**CMEK**）の使用に必要な情報

デフォルトの Google 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータ暗号化に使用できます。クロスリージョン キーとクロスプロジェクト キーの両方がサポートされているため、CMEK キーのプロジェクトとは異なるバケットのプロジェクトを選択できます。独自の顧客管理キーを使用する予定の場合:

- アクティベーション ウィザードでこの情報を追加するには、キー リングとキー名が必要です。 "顧客管理暗号化キーの詳細" 。
- コンソール エージェントのロールに次の必要な権限が含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトで Google の「Cloud Key Management Service (KMS)」API が有効になっていることを確認する必要があります。参照 "Google Cloud ドキュメント: API の有効化"詳細については。

CMEKの考慮事項:

- HSM (ハードウェア バックアップ) キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成された Cloud KMS キーとインポートされた Cloud KMS キーの両方がサポートされます。
- 地域キーのみがサポートされ、グローバル キーはサポートされません。
- 現在、「対称暗号化/復号化」目的のみがサポートされています。
- ストレージ アカウントに関連付けられたサービス エージェントには、NetApp Backup and Recoveryによって「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM ロールが割り当てられます。

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

"独自のバケットの作成について詳しくは"。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。
- 異なるサブネットにある 2 つのCloud Volumes ONTAPシステム間でデータを複製するには、サブネットを一緒にルーティングする必要があります (これがデフォルト設定です)。

Cloud Volumes ONTAPで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recoveryを有効にする手順は、既存のCloud Volumes ONTAPシステムがあるか、新しいシステムがあるかによって若干異なります。

新しいシステムで**NetApp Backup and Recovery**を有効にする

システム ウィザードを完了して新しいCloud Volumes ONTAPシステムを作成すると、 NetApp Backup and Recovery を有効にできます。

サービス アカウントがすでに構成されている必要があります。 Cloud Volumes ONTAPシステムを作成するときにサービス アカウントを選択しない場合は、システムをオフにして、GCP コンソールからCloud Volumes ONTAPにサービス アカウントを追加する必要があります。

見る "GCP でCloud Volumes ONTAP を起動"Cloud Volumes ONTAPシステムを作成するための要件と詳細については、こちらをご覧ください。

手順

1. コンソールの システム ページで、システムの追加 を選択し、クラウド プロバイダーを選択して、新規追加 を選択します。 * Cloud Volumes ONTAPの作成*を選択します。
2. 場所を選択: **Google Cloud Platform** を選択します。
3. タイプを選択: * Cloud Volumes ONTAP* (シングルノードまたは高可用性) を選択します。
4. 詳細と資格情報: 次の情報を入力します。
    a. 使用するプロジェクトがデフォルトのプロジェクト (コンソール エージェントが存在するプロジェクト) と異なる場合は、[プロジェクトの編集] をクリックして新しいプロジェクトを選択します。
    b. クラスタ名を指定します。
    c. サービス アカウント スイッチを有効にし、事前定義されたストレージ管理者ロールを持つサービス アカウントを選択します。これは、バックアップと階層化を有効にするために必要です。
    d. 資格情報を指定します。

        GCP Marketplace サブスクリプションが設定されていることを確認します。
5. サービス: NetApp Backup and Recovery を有効のままにして、[続行] をクリックします。
6. ウィザードのページを完了して、説明に従ってシステムを展開します。 "GCP でCloud Volumes ONTAP を起動" 。

結果

システムでNetApp Backup and Recovery が有効になっています。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、 NetApp Backup and Recoveryを起動し、"保護したいボリュームごとにバックアップを有効化します" 。

既存のシステムで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recovery は、いつでもシステムから直接有効にすることができます。

手順

1. コンソールの システム ページでシステムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効 を選択します。

   バックアップの Google Cloud Storage 保存先がコンソールの [システム] ページにシステムとして存在する場合は、クラスタを Google Cloud Storage システムにドラッグしてセットアップ ウィザードを開始できます。

Google Cloud Storage をバックアップ先として準備する

Google Cloud Storage をバックアップ ターゲットとして準備するには、次の手順を実行します。

- 権限を設定します。
- (オプション) 独自のバケットを作成します。 (必要に応じて、サービスによってバケットが作成されます。)
- （オプション）データ暗号化用の顧客管理キーを設定する

権限を設定する

カスタム ロールを使用して特定の権限を持つサービス アカウントにストレージ アクセス キーを提供する必要があります。サービス アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用される Cloud Storage バケットを認証してアクセスできるようになります。Google Cloud Storage が誰がリクエストを行っているかを認識するために、キーが必要になります。

手順

1. の中で "Google Cloud コンソール"、*役割*ページに移動します。
2. "新しいロールの作成"以下の権限を持ちます:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloudコンソールでは、 "サービスアカウントページに移動します" 。

4. Cloud プロジェクトを選択します。
5. サービス アカウントの作成 を選択し、必要な情報を入力します。
   a. サービス アカウントの詳細: 名前と説明を入力します。
   b. このサービス アカウントにプロジェクトへのアクセスを許可する: 先ほど作成したカスタム ロールを選択します。
   c. *完了*を選択します。
6. へ移動 "GCP ストレージ設定"サービス アカウントのアクセス キーを作成します。
   a. プロジェクトを選択し、*相互運用性*を選択します。まだ行っていない場合は、[相互運用性アクセスを有効にする] を選択します。
   b. サービス アカウントのアクセス キー の下で、サービス アカウントのキーの作成 を選択し、作成したサービス アカウントを選択して、キーの作成 をクリックします。

      後でバックアップ サービスを構成するときに、 NetApp Backup and Recoveryにキーを入力する必要があります。

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。または、独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

"独自のバケットの作成について詳しくは"。

データ暗号化用の顧客管理暗号鍵（**CMEK**）を設定する

デフォルトの Google 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータ暗号化に使用できます。クロスリージョン キーとクロスプロジェクト キーの両方がサポートされているため、CMEK キーのプロジェクトとは異なるバケットのプロジェクトを選択できます。

独自の顧客管理キーを使用する予定の場合:

- アクティベーション ウィザードでこの情報を追加するには、キー リングとキー名が必要です。 "顧客管理暗号化キーの詳細" 。
- コンソール エージェントのロールに次の必要な権限が含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトで Google の「Cloud Key Management Service (KMS)」API が有効になっていることを確認

する必要があります。参照 "Google Cloud ドキュメント: API の有効化"詳細については。

CMEKの考慮事項:

- HSM (ハードウェア バックアップ) キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成された Cloud KMS キーとインポートされた Cloud KMS キーの両方がサポートされます。
- 地域キーのみがサポートされ、グローバル キーはサポートされません。
- 現在、「対称暗号化/復号化」目的のみがサポートされています。
- ストレージ アカウントに関連付けられたサービス エージェントには、NetApp Backup and Recoveryによって「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM ロールが割り当てられます。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。

   - コンソールの システム ページ* からシステムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 **>** バックアップ ボリューム を選択します。

     バックアップの GCP 保存先がコンソールの システム ページにシステムとして存在する場合は、ONTAPクラスターを GCP オブジェクト ストレージにドラッグできます。

   - バックアップとリカバリ バーで ボリューム を選択します。ボリュームタブから*アクション*を選択します ••• アイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

   ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにすでにスナップショットまたはレプリケーション ポリシーが適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされることに注意してください。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
   - 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー

選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実

行する場合は、ローカル スナップショットを作成する必要があります。

- レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
- バックアップ: ボリュームをオブジェクト ストレージにバックアップします。

2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてセカンダリ ストレージ システムからオブジェクト ストレージへ流れます。
   - ファンアウト: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてプライマリ ストレージ システムからオブジェクト ストレージへ流れます。

   これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいスナップショット ポリシーを作成します。

   バックアップをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

   ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
   - ポリシーの名前を入力します。
   - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
   - オブジェクトへのバックアップ ポリシーの場合は、Datalock と Ransomware Resilience を構成します。データロックとランサムウェア耐性の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシー設定" 。
   - *作成*を選択します。
4. レプリケーション: 次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。

     レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - *作成*を選択します。
5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: **Google Cloud** を選択します。

- プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

  新しいバケットを作成するか、既存のバケットを選択します。

- 暗号化キー: 新しい Google バケットを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの Google Cloud 暗号化キーを使用するか、Google アカウントから独自の顧客管理キーを選択するかを選択します。

  独自のカスタマー管理キーを使用する場合は、キー コンテナーとキー情報を入力します。

  既存の Google Cloud バケットを選択した場合は、暗号化情報がすでに利用可能であるため、今すぐ入力する必要はありません。

- バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択するか、新しいポリシーを作成します。

  バックアップをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

  ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

  - ポリシーの名前を入力します。
  - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
  - *作成*を選択します。

- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ システム ボリュームと同期されます。

入力した Google アクセスキーとシークレットキーで示されるサービス アカウントに Google Cloud Storage バケットが作成され、そこにバックアップ ファイルが保存されます。

デフォルトでは、バックアップは *Standard* ストレージ クラスに関連付けられます。低コストの *Nearline* 、*Coldline*、または *Archive* ストレージ クラスを使用できます。ただし、ストレージ クラスは、 NetApp Backup and Recovery UI ではなく、Google を通じて構成します。 Googleトピックを見る "バケットのデフォルトのストレージ クラスを変更する"詳細については。

ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

次の手順

- あなたはできる"バックアップファイルとバックアップポリシーを管理する"。これには、バックアップの開始と停止、バックアップの削除、バックアップ スケジュールの追加と変更などが含まれます。
- あなたはできる"クラスタレベルのバックアップ設定を管理する"。これには、 ONTAPがクラウド ストレージにアクセスするために使用するストレージ キーの変更、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使用できるネットワーク帯域幅の変更、将来のボリュームの自動バックアップ設定の変更などが含まれます。
- また、"バックアップ ファイルからボリューム、フォルダ、または個々のファイルを復元する" AWS のCloud Volumes ONTAPシステム、またはオンプレミスのONTAPシステムに接続します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを Amazon S3 にバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのONTAPシステムからセカンダリ ストレージ システムと Amazon S3 クラウド ストレージへのボリューム データのバックアップを開始します。

「オンプレミスのONTAPシステム」には、 FAS、 AFF、およびONTAP Selectシステムが含まれます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

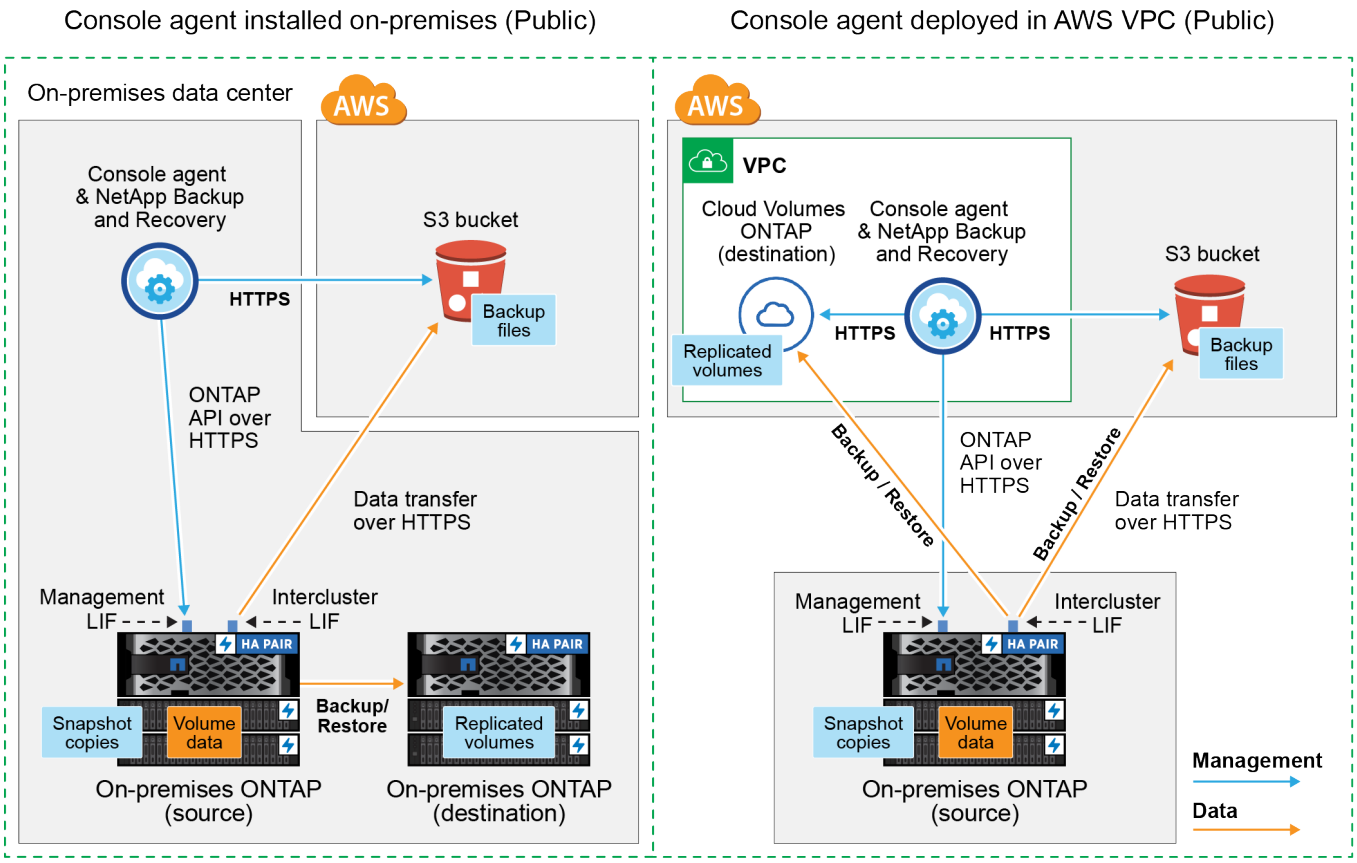
接続方法を特定する

オンプレミスのONTAPシステムから AWS S3 へのバックアップを構成するときに使用する 2 つの接続方法のうちどちらを選択します。

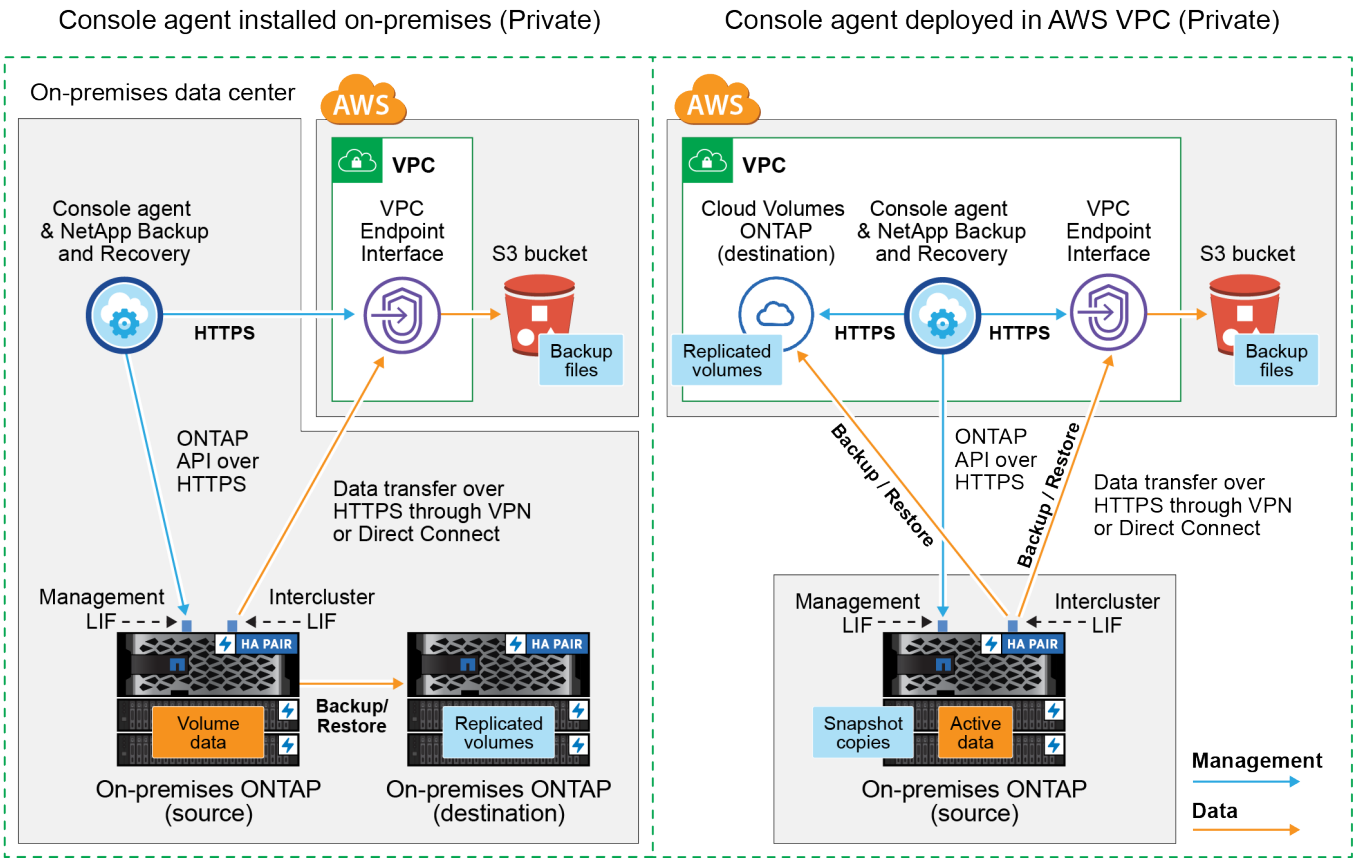
- パブリック接続 - パブリック S3 エンドポイントを使用して、 ONTAPシステムを AWS S3 に直接接続します。
- プライベート接続 - VPN または AWS Direct Connect を使用し、プライベート IP アドレスを使用する VPC エンドポイント インターフェイスを介してトラフィックをルーティングします。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。

次の図は、*パブリック接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソールエージェント、または AWS VPC にデプロイしたコンソールエージェントを使用できます。



次の図は、*プライベート接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソールエージェント、または AWS VPC にデプロイしたコンソールエージェントを使用できます。



コンソールエージェントを準備する

コンソール エージェントは、 NetApp Console機能のメイン ソフトウェアです。 ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

AWS VPC またはオンプレミスにコンソールエージェントがすでにデプロイされている場合は、準備は完了です。

そうでない場合は、 ONTAPデータを AWS S3 ストレージにバックアップするために、これらの場所のいずれかにコンソールエージェントを作成する必要があります。別のクラウド プロバイダーにデプロイされたコンソール エージェントは使用できません。

- "コンソールエージェントについて学ぶ"
- "AWSにコンソールエージェントをインストールする"
- "オンプレミスにコンソールエージェントをインストールする"
- "AWS GovCloud リージョンにコンソールエージェントをインストールする"

  NetApp Backup and Recovery は、コンソール エージェントがオンプレミスでインストールされている場合ではなく、クラウドに展開されている場合に、GovCloud リージョンでサポートされます。さらに、AWS Marketplace からコンソールエージェントをデプロイする必要があります。 NetApp Console SaaS Web サイトからコンソール エージェントを政府地域に展開することはできません。

次のネットワーク要件が満たされていることを確認してください。

- コンソール エージェントがインストールされているネットワークで次の接続が有効になっていることを確認します。
  - ポート443経由のNetApp Backup and RecoveryおよびS3オブジェクトストレージへのHTTPS接続("エンドポイントのリストを見る")
  - ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
  - AWS および AWS GovCloud のデプロイメントには、追加の受信および送信セキュリティ グループ ルールが必要です。見る "AWS のコンソールエージェントのルール"詳細については。
- ONTAPクラスターから VPC への Direct Connect または VPN 接続があり、コンソール エージェントと S3 間の通信を AWS 内部ネットワーク (プライベート接続) 内に維持したい場合は、S3 への VPC エンドポイント インターフェイスを有効にする必要があります。VPC エンドポイント インターフェースを使用してシステムをプライベート接続用に設定する。

ライセンス要件を確認する

AWS とNetApp Consoleの両方のライセンス要件を確認する必要があります。

- クラスターでNetApp Backup and Recoveryを有効にする前に、AWS の従量課金制 (PAYGO) NetApp Console Marketplace オファリングに登録するか、 NetAppからNetApp Backup and Recovery BYOL ライセンスを購入して有効にする必要があります。これらのライセンスはあなたのアカウント用であり、複数のシステムで使用できます。
  - NetApp Backup and Recovery PAYGOライセンスの場合は、 "AWS Marketplace からのNetApp Consoleの提供" 。 NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。
  - NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの有効期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要になります。
- バックアップが保存されるオブジェクト ストレージ スペース用の AWS サブスクリプションが必要です。

サポート対象地域

AWS GovCloud リージョンを含むすべてのリージョンで、オンプレミスシステムから Amazon S3 へのバックアップを作成できます。サービスを設定するときに、バックアップを保存するリージョンを指定します。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAP システムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、 NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["クラスターの検出方法を学ぶ"^]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

  注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

  方法を学ぶ "クラスターライセンスを管理する"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "クラスター時間を設定する"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

  "SnapMirror関係に互換性のあるONTAPバージョンを表示する"。

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャの場合は、プライマリ システムで次の設定を構成します。
- カスケード バックアップ アーキテクチャの場合は、セカンダリ システムで次の設定を構成します。

次のONTAPクラスタ ネットワーク要件が必要です。

- クラスタでは、コンソール エージェントからクラスタ管理 LIF への受信 HTTPS 接続が必要です。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。これらのクラスタ間 LIF はオブジェクト ストアにアクセスできる必要があります。

  クラスターは、バックアップおよび復元操作のために、クラスター間 LIF から Amazon S3 ストレージへのポート 443 経由の送信 HTTPS 接続を開始します。ONTAP はオブジェクト ストレージとの間でデータの読み取りと書き込みを行います。オブジェクト ストレージは開始することはなく、応答するだけです。

- クラスタ間 LIF は、 ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。 "IPspacesについて詳しくはこちら" 。

  NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。これらの LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

  「デフォルト」とは異なる IPspace を使用している場合は、オブジェクト ストレージにアクセスするた

めに静的ルートを作成する必要がある場合があります。

IPspace 内のすべてのクラスタ間 LIF はオブジェクト ストアにアクセスできる必要があります。現在の IPspace に対してこれを構成できない場合は、すべてのクラスタ間 LIF がオブジェクト ストアにアクセスできる専用の IPspace を作成する必要があります。

- ボリュームが配置されているストレージ VM に対して DNS サーバーが設定されている必要があります。方法を見る "SVMのDNSサービスを構成する"。
- 必要に応じてファイアウォール ルールを更新し、 ONTAPからオブジェクト ストレージへのポート 443 経由のNetApp Backup and Recovery接続と、ストレージ VM から DNS サーバーへのポート 53 (TCP/UDP) 経由の名前解決トラフィックを許可します。
- S3 接続に AWS のプライベート VPC インターフェイス エンドポイントを使用している場合は、HTTPS/443 を使用するために、S3 エンドポイント証明書をONTAPクラスターにロードする必要があります。VPC エンドポイント インターフェースを使用してシステムをプライベート接続用に設定する。
- ONTAPクラスターに S3 バケットにアクセスする権限があることを確認します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

Amazon S3をバックアップターゲットとして準備する

Amazon S3 をバックアップターゲットとして準備するには、次の手順を実行します。

- S3 権限を設定します。
- (オプション) 独自の S3 バケットを作成します。 (必要に応じて、サービスによってバケットが作成されます。)
- (オプション) データ暗号化用にカスタマー管理の AWS キーを設定します。
- (オプション) VPC エンドポイント インターフェイスを使用して、システムをプライベート接続用に設定します。

S3の権限を設定する

次の 2 セットの権限を構成する必要があります。

- コンソール エージェントが S3 バケットを作成および管理するための権限。
- オンプレミスのONTAPクラスターが S3 バケットのデータの読み取りと書き込みを行えるようにするための権限。

手順

1. コンソール エージェントに必要な権限があることを確認します。詳細については、 "NetApp Consoleポリシー権限" 。

   AWS中国リージョンでバックアップを作成する場合、IAMポリシーのすべての_Resource_セクションのAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります。例： `arn:aws-cn:s3:::netapp-backup-*` 。

2. サービスをアクティブ化すると、バックアップ ウィザードによってアクセス キーとシークレット キーの入力が求められます。これらの認証情報はONTAPクラスターに渡され、 ONTAP はS3 バケットにデータをバックアップおよび復元できるようになります。そのためには、次の権限を持つ IAM ユーザーを作成する必要があります。

   参照 "AWS ドキュメント: IAM ユーザーに権限を委任するロールの作成"。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。または、独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

"独自のバケットの作成について詳しくは"。

独自のバケットを作成する場合は、「netapp-backup」というバケット名を使用する必要があります。カスタム名を使用する必要がある場合は、 `ontapcloud-instance-policy-netapp-backup`既存のCVOのIAMRoleを作成し、次のJSONブロックをS3権限に追加します。 `Statement`配列。含める必要がある `"Resource": "arn:aws:s3:::*"`バケットに関連付ける必要のあるすべての必要な権限を割り当てます。

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

データ暗号化用の顧客管理 **AWS** キーを設定する

デフォルトの Amazon S3 暗号化キーを使用してオンプレミスのクラスターと S3 バケット間で渡されるデータを暗号化する場合は、デフォルトのインストールでそのタイプの暗号化が使用されるため、すべて準備完了です。

代わりに、デフォルトのキーではなく、独自の顧客管理キーを使用してデータを暗号化する場合は、 NetApp Backup and Recoveryウィザードを開始する前に、暗号化管理キーを事前に設定しておく必要があります。

"Cloud Volumes ONTAPで独自のAmazon暗号化キーを使用する方法を参照してください。"。

"NetApp Backup and Recoveryで独自のAmazon暗号化キーを使用する方法を参照してください。"。

VPC エンドポイント インターフェースを使用してシステムをプライベート接続用に設定する

標準のパブリック インターネット接続を使用する場合は、すべての権限がコンソール エージェントによって設定されるため、他に何もする必要はありません。

オンプレミスのデータセンターから VPC へのインターネット経由のより安全な接続を確立したい場合は、バックアップアクティベーションウィザードで AWS PrivateLink 接続を選択するオプションがあります。プライベート IP アドレスを使用する VPC エンドポイント インターフェイスを介してオンプレミス システムに接続するために VPN または AWS Direct Connect を使用する予定の場合は、これが必要です。

手順

1. Amazon VPC コンソールまたはコマンドラインを使用して、インターフェイスエンドポイント設定を作成します。 "Amazon S3 の AWS PrivateLink の使用に関する詳細については、こちらをご覧ください。" 。
2. コンソール エージェントに関連付けられているセキュリティ グループ構成を変更します。ポリシーを「カスタム」（「フルアクセス」から）に変更し、バックアップポリシーからS3権限を追加する先に示したとおりです。

   プライベート エンドポイントへの通信にポート 80 (HTTP) を使用している場合は、設定は完了です。これで、クラスター上でNetApp Backup and Recoveryを有効にできるようになりました。

   プライベート エンドポイントへの通信にポート 443 (HTTPS) を使用している場合は、次の 4 つの手順に示すように、VPC S3 エンドポイントから証明書をコピーし、 ONTAPクラスターに追加する必要があります。

3. AWS コンソールからエンドポイントの DNS 名を取得します。
4. VPC S3 エンドポイントから証明書を取得します。これを実行するには "コンソールエージェントをホストするVMにログインする"次のコマンドを実行します。エンドポイントの DNS 名を入力するときは、先頭に「*」を置き換えて「bucket」を追加します。

   ```
   openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
   ```

5. このコマンドの出力から、S3 証明書のデータ (BEGIN / END CERTIFICATE タグを含む、その間のすべてのデータ) をコピーします。

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. ONTAPクラスタ CLI にログインし、次のコマンドを使用してコピーした証明書を適用します (独自のストレージ VM 名に置き換えます)。

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
Please enter Certificate: Press <Enter> when done
```

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。

   - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

     バックアップの Amazon S3 保存先がコンソールの システム ページにシステムとして存在する場合は、 ONTAPクラスターを Amazon S3 オブジェクトストレージにドラッグできます。

   - バックアップとリカバリバーで*ボリューム*を選択します。ボリュームタブから*アクション*を選択します ••• アイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

   ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択

された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
   - 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてが必要な場合
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー

選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリからセカンダリ、オブジェクト ストレージへ、そしてセカンダリからオブジェクト ストレージへと流れます。
   - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、ポリシーを作成します。

   スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。
4. ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
   - ポリシーの名前を入力します。
   - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。 DataLockとランサムウェア耐性の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシー設定" 。
   - *作成*を選択します。
5. レプリケーション: 次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、ポリシーを作成します。

     レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
     - ポリシーの名前を入力します。

- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

6. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: **Amazon Web Services** を選択します。
   - プロバイダー設定: プロバイダーの詳細と、バックアップを保存する AWS リージョンを入力します。

     アクセス キーとシークレット キーは、 ONTAPクラスターに S3 バケットへのアクセス権を付与するために作成した IAM ユーザー用です。
   - バケット: 既存の S3 バケットを選択するか、新しいバケットを作成します。参照 "S3バケットを追加する"。
   - 暗号化キー: 新しい S3 バケットを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの Amazon S3 暗号化キーを使用するか、AWS アカウントから独自のカスタマー管理キーを選択するかを選択します。

     既存のバケットを選択した場合は、暗号化情報がすでに利用可能であるため、ここで入力する必要はありません。
   - ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。プライベート エンドポイントはデフォルトで無効になっています。
     i. バックアップするボリュームが存在するONTAPクラスタ内の IPspace。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。
     ii. 必要に応じて、以前に設定した AWS PrivateLink を使用するかどうかを選択します。 "Amazon S3 の AWS PrivateLink の使用に関する詳細をご覧ください" 。
   - バックアップ ポリシー: 既存のバックアップ ポリシーを選択するか、ポリシーを作成します。

     バックアップをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - *作成*を選択します。
   - 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの保護が最も完全になります。
7. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスの ONTAPデータを Azure Blob ストレージにバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのONTAPシステムからセカンダリ ストレージ システムおよび Azure Blob ストレージへのボリューム データのバックアップを開始します。

「オンプレミスのONTAPシステム」には、 FAS、 AFF、およびONTAP Selectシステムが含まれます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

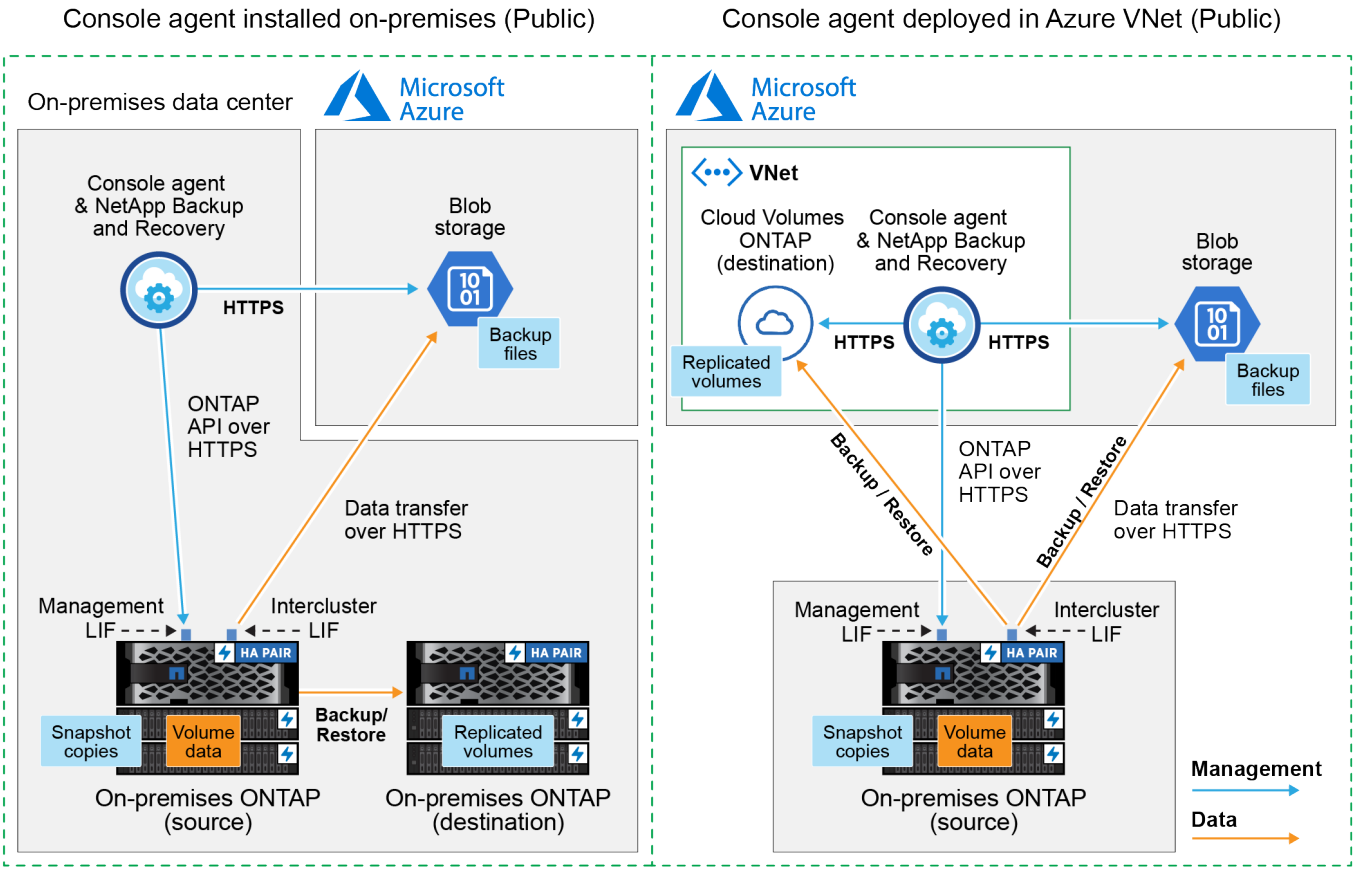
接続方法を特定する

オンプレミスのONTAPシステムから Azure Blob へのバックアップを構成するときに使用する 2 つの接続方法のうちどちらを選択します。

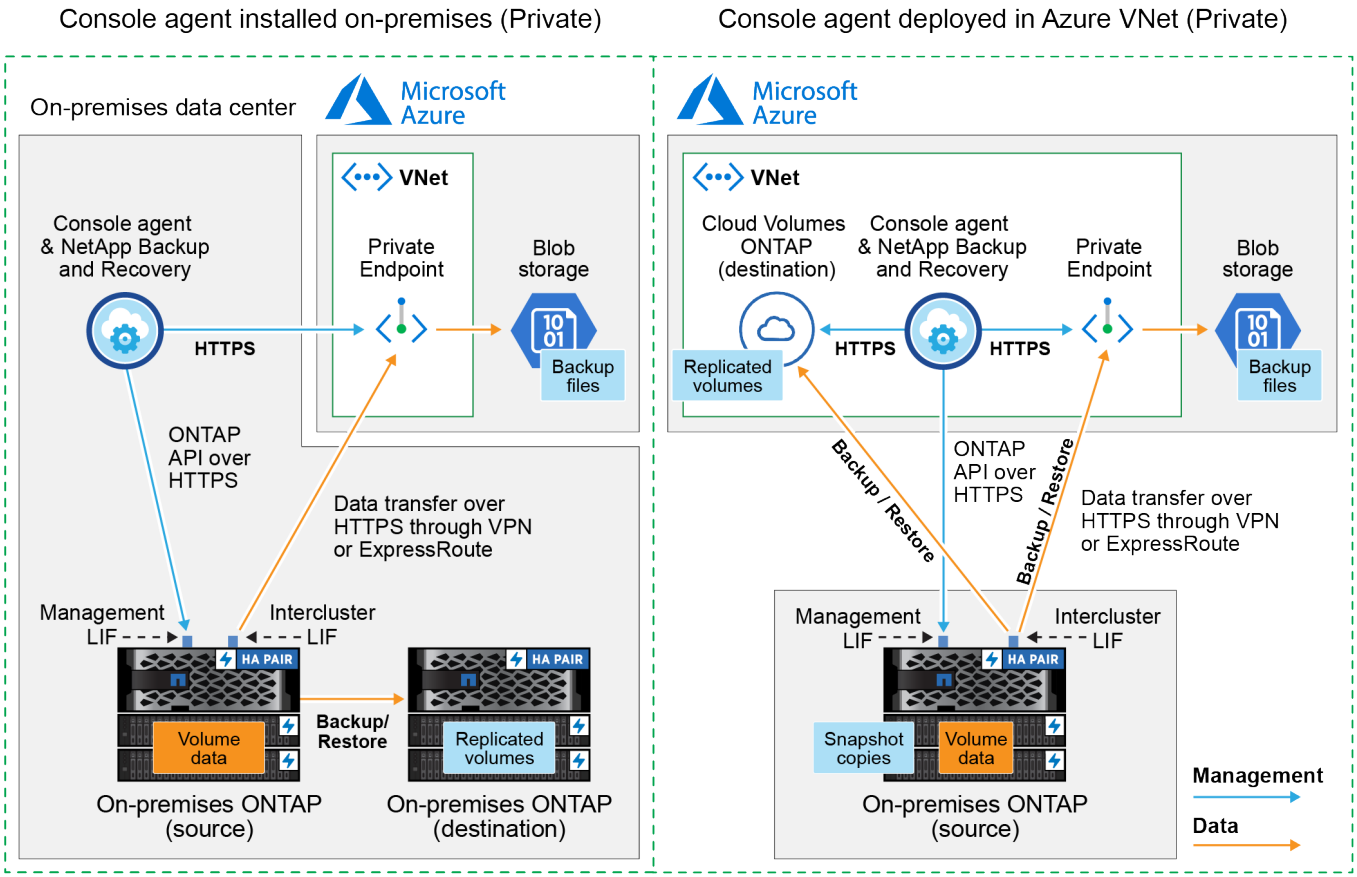
- パブリック接続 - パブリック Azure エンドポイントを使用して、 ONTAPシステムを Azure Blob ストレージに直接接続します。
- プライベート接続 - VPN または ExpressRoute を使用し、プライベート IP アドレスを使用する VNet プライベート エンドポイント経由でトラフィックをルーティングします。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。

次の図は、*パブリック接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソール エージェント、または Azure VNet にデプロイしたコンソール エージェントを使用できます。



次の図は、*プライベート接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソール エージェント、または Azure VNet にデプロイしたコンソール エージェントを使用できます。



コンソールエージェントを準備する

コンソール エージェントは、 NetApp Console機能のメイン ソフトウェアです。 ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

Azure VNet またはオンプレミスにコンソール エージェントが既にデプロイされている場合は、準備は完了です。

そうでない場合は、いずれかの場所にコンソール エージェントを作成し、 ONTAPデータを Azure Blob ストレージにバックアップする必要があります。別のクラウド プロバイダーにデプロイされたコンソール エージェントは使用できません。

- "コンソールエージェントについて学ぶ"
- "Azureにコンソールエージェントをインストールする"
- "オンプレミスにコンソールエージェントをインストールする"
- "Azure Government リージョンにコンソール エージェントをインストールする"

  NetApp Backup and Recovery は、コンソール エージェントがオンプレミスでインストールされている場合ではなく、クラウドに展開されている場合に、Azure Government リージョンでサポートされます。さらに、Azure Marketplace からコンソール エージェントを展開する必要があります。コンソール SaaS Web サイトからコンソール エージェントを政府地域に展開することはできません。

コンソールエージェントのネットワークを準備する

コンソール エージェントに必要なネットワーク接続があることを確認します。

手順

1. コンソール エージェントがインストールされているネットワークで次の接続が有効になっていることを確認します。
   - NetApp Backup and RecoveryおよびBlobオブジェクトストレージへのポート443経由のHTTPS接続("エンドポイントのリストを見る")
   - ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
   - NetApp Backup and Recoveryの検索と復元機能が動作するには、コンソール エージェントと Azure Synapse SQL サービス間の通信用にポート 1433 が開いている必要があります。
   - Azure および Azure Government の展開には、追加の受信セキュリティ グループ ルールが必要です。見る "Azure のコンソール エージェントのルール"詳細については。
2. Azure ストレージへの VNet プライベート エンドポイントを有効にします。これは、 ONTAPクラスターから VNet への ExpressRoute または VPN 接続があり、コンソール エージェントと Blob ストレージ間の通信を仮想プライベート ネットワーク (プライベート接続) 内に維持する場合に必要です。

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の検索と復元機能を使用するには、Azure Synapse ワークスペースと Data Lake ストレージ アカウントにアクセスできるように、コンソール エージェントのロールに特定のアクセス許可が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従ってください。

開始する前に

Azure Synapse Analytics リソース プロバイダー (「Microsoft.Synapse」と呼ばれます) をサブスクリプションに登録する必要があります。 "このリソースプロバイダーをサブスクリプションに登録する方法をご覧ください" 。リソース プロバイダーを登録するには、サブスクリプションの 所有者 または 投稿者 である必要があります。

手順

1. コンソール エージェント仮想マシンに割り当てられたロールを識別します。
   a. Azure ポータルで、仮想マシン サービスを開きます。
   b. コンソール エージェント仮想マシンを選択します。
   c. *設定*の下で*ID*を選択します。
   d. *Azure ロールの割り当て*を選択します。
   e. コンソール エージェント仮想マシンに割り当てられたカスタム ロールをメモします。
2. カスタム ロールを更新します。
   a. Azure ポータルで、Azure サブスクリプションを開きます。
   b. *アクセス制御 (IAM) > ロール*を選択します。
   c. カスタム ロールの省略記号 (...) を選択し、[編集] を選択します。
   d. **JSON** を選択し、次の権限を追加します。

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"ポリシーの完全なJSON形式を表示する"

e. *確認+更新*を選択し、*更新*を選択します。

ライセンス要件を確認する

Azure とコンソールの両方のライセンス要件を確認する必要があります。

- クラスターに対してNetApp Backup and Recoveryをアクティブ化する前に、Azure の従量課金制 (PAYGO) コンソール マーケットプレイス オファリングをサブスクライブするか、 NetAppからNetApp Backup and Recovery BYOL ライセンスを購入してアクティブ化する必要があります。これらのライセンスはあなたのアカウント用であり、複数のシステムで使用できます。
  - NetApp Backup and Recovery PAYGOライセンスの場合は、 "Azure Marketplace からのNetApp Consoleの提供" 。 NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。
  - NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの有効期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要になります。"BYOLライセンスの管理方法を学ぶ"。
- バックアップが保存されるオブジェクト ストレージ スペース用の Azure サブスクリプションが必要です。

サポート対象地域

Azure Government リージョンを含むすべてのリージョンで、オンプレミス システムから Azure Blob へのバックアップを作成できます。サービスを設定するときに、バックアップを保存するリージョンを指定します。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAP システムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、 NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["クラスターの検出方法を学ぶ"^]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ "クラスターライセンスを管理する"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "クラスター時間を設定する"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

  "SnapMirror関係に互換性のあるONTAPバージョンを表示する"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャの場合は、プライマリ システムで次の設定を構成します。
- カスケード バックアップ アーキテクチャの場合は、セカンダリ システムで次の設定を構成します。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよび復元操作のために、クラスタ間 LIF から Azure Blob ストレージへのポート 443 経由の HTTPS 接続を開始します。

  ONTAP はオブジェクト ストレージとの間でデータの読み取りと書き込みを行います。オブジェクト ストレージは開始することはなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。コンソール エージェントは Azure VNet に配置できます。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。 LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。 "IPspacesについて詳しくはこちら" 。

  NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。各 LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

- ノードおよびクラスタ間 LIF はオブジェクト ストアにアクセスできます。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る "SVMのDNSサービスを構成する"。
- デフォルトとは異なる IPspace を使用している場合は、オブジェクト ストレージにアクセスするために静的ルートを作成する必要がある場合があります。
- 必要に応じてファイアウォール ルールを更新し、 ONTAPからオブジェクト ストレージへのポート 443 経由のNetApp Backup and Recoveryサービス接続と、ストレージ VM から DNS サーバーへのポート 53 (TCP/UDP) 経由の名前解決トラフィックを許可します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

Azure Blob をバックアップ先として準備する

1. アクティベーション ウィザードでは、既定の Microsoft 管理の暗号化キーを使用する代わりに、独自のカスタム管理キーを使用してデータを暗号化することができます。この場合、Azure サブスクリプション、Key Vault 名、およびキーが必要になります。 "独自のキーの使い方を学ぶ" 。

   バックアップとリカバリでは、アクセス許可モデルとして *Azure* アクセス ポリシー がサポートされていることに注意してください。 *Azure* ロールベースのアクセス制御 (Azure RBAC) アクセス許可モデルは現在サポートされていません。

2. オンプレミスのデータセンターから VNet へのパブリック インターネット経由のより安全な接続を確立したい場合は、アクティベーション ウィザードで Azure プライベート エンドポイントを構成するオプションがあります。この場合、この接続の VNet とサブネットを知っておく必要があります。 "プライベート エンドポイントの使用に関する詳細を参照してください" 。

Azure Blob ストレージ アカウントを作成する

デフォルトでは、サービスによってストレージ アカウントが作成されます。独自のストレージ アカウントを使用する場合は、バックアップ アクティブ化ウィザードを開始する前にストレージ アカウントを作成し、ウィザードでそれらのストレージ アカウントを選択できます。

"独自のストレージアカウントの作成について詳しくは、こちらをご覧ください。"。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ ア

クティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
   - コンソールの システム ページで、システムを選択し、右側のパネルのバックアップとリカバリ サービスの横にある 有効化 > バックアップ ボリューム を選択します。

     コンソールの [システム] ページにバックアップの Azure 保存先が存在する場合は、 ONTAPクラスターを Azure Blob オブジェクト ストレージにドラッグできます。
   - バックアップとリカバリバーで*ボリューム*を選択します。ボリュームタブから*アクション*を選択します ••• アイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

   ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにすでにスナップショットまたはレプリケーション ポリシーが適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされることに注意してください。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。

- 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー

選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリからセカンダリへ、そしてセカンダリからオブジェクト ストレージへ流れます。
   - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。

スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。

- *作成*を選択します。

4. レプリケーション: 次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいポリシーを作成します。

     レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: **Microsoft Azure** を選択します。
   - プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

     新しいストレージ アカウントを作成するか、既存のストレージ アカウントを選択します。

     Blob コンテナーを管理する独自のリソース グループを作成するか、リソース グループの種類とグループを選択します。

     バックアップ ファイルが変更されたり削除されたりするのを防ぐには、30 日間の保持期間を使用して不変ストレージが有効になっているストレージ アカウントが作成されていることを確認してください。

     さらにコストを最適化するために古いバックアップ ファイルを Azure Archive Storage に階層化する場合は、ストレージ アカウントに適切なライフサイクル ルールがあることを確認してください。

   - 暗号化キー: 新しい Azure ストレージ アカウントを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、既定の Azure 暗号化キーを使用するか、Azure アカウントから独自のカスタマー管理キーを選択するかを選択します。

     独自のカスタマー管理キーを使用する場合は、キー コンテナーとキー情報を入力します。

     既存の Microsoft ストレージ アカウントを選択した場合は、暗号化情報が既に用意されているため、ここで入力する必要はありません。

   - ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。プライベート エンドポイントはデフォルトで無効になっています。

     i. バックアップするボリュームが存在するONTAPクラスタ内の IPspace。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。

ii. 必要に応じて、以前に構成した Azure プライベート エンドポイントを使用するかどうかを選択します。 "Azure プライベート エンドポイントの使用について学習します" 。

- バックアップ ポリシー: 既存のオブジェクト ストレージ ポリシーへのバックアップを選択するか、新しいポリシーを作成します。

> バックアップをアクティブ化する前にカスタムポリシーを作成するには、"ポリシーを作成します。" 。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。 DataLockとランサムウェア耐性の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシー設定" 。
- *作成*を選択します。

- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ボリュームと同期されます。

入力したリソース グループに BLOB ストレージ アカウントが作成され、そこにバックアップ ファイルが保存されます。ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを Google Cloud Storage にバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのプライマリONTAPシステムからセカンダリ ストレージ システムと Google Cloud Storage へのボリューム データのバックアップを開始します。

「オンプレミスのONTAPシステム」には、 FAS、 AFF、およびONTAP Selectシステムが含まれます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

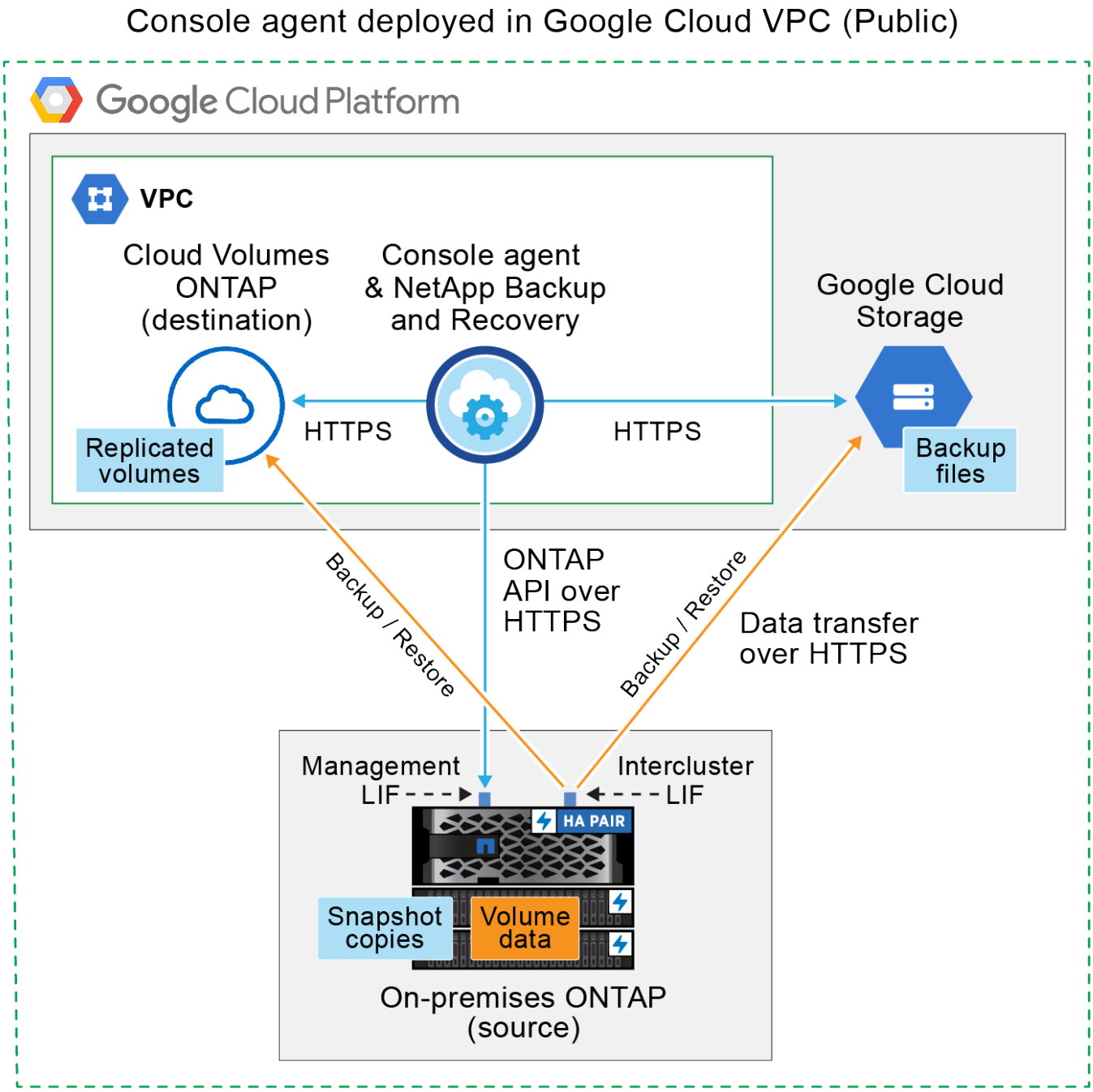
接続方法を特定する

オンプレミスのONTAPシステムから Google Cloud Storage へのバックアップを構成するときに使用する 2 つの接続方法のうちどちらを選択します。

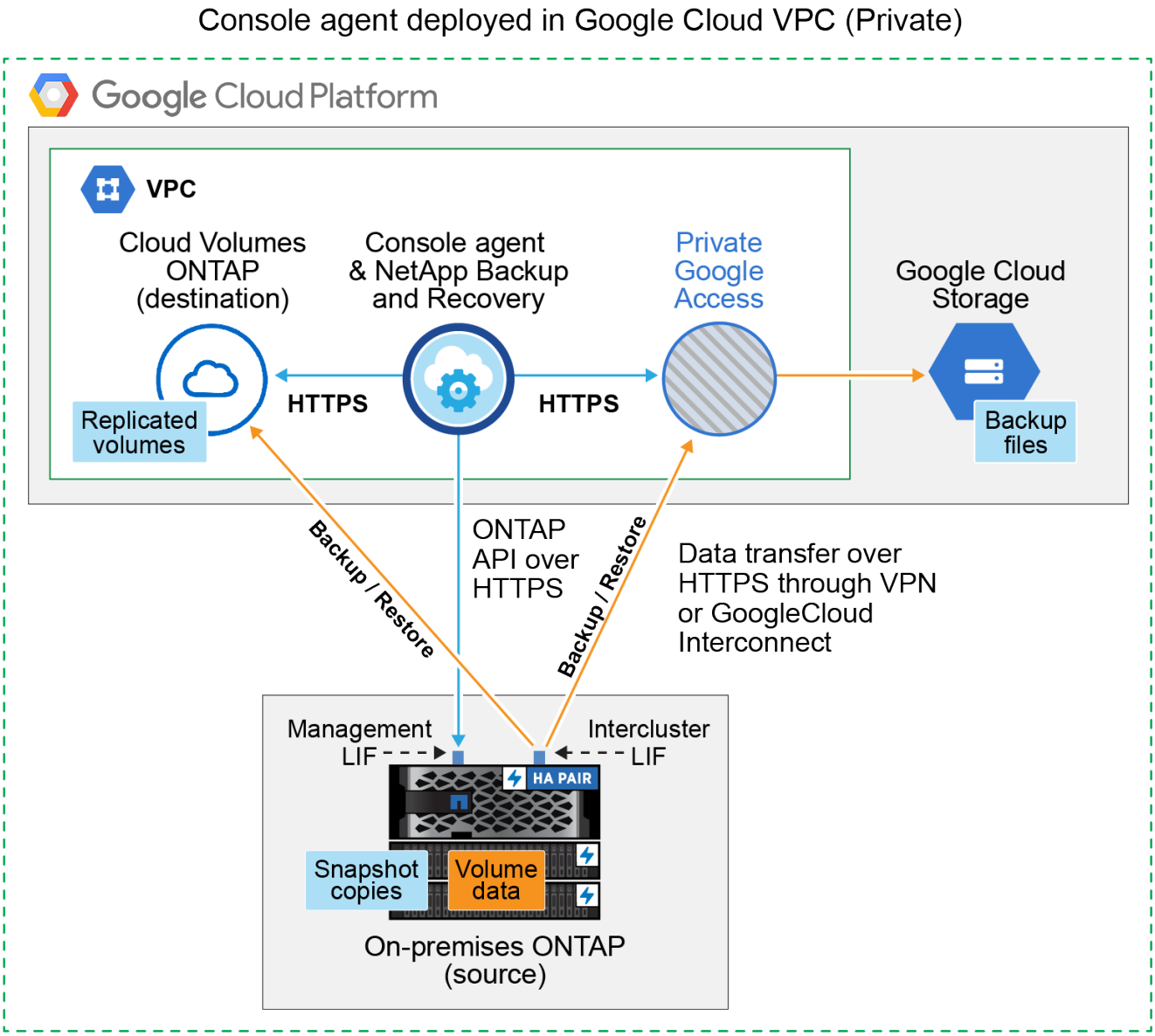
- パブリック接続 - パブリック Google エンドポイントを使用して、 ONTAPシステムを Google Cloud Storage に直接接続します。
- プライベート接続 - VPN または Google Cloud Interconnect を使用して、プライベート IP アドレスを使用するプライベート Google アクセス インターフェース経由でトラフィックをルーティングします。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。

次の図は、*パブリック接続*方式と、コンポーネント間で準備する必要がある接続を示しています。コンソール エージェントは、Google Cloud Platform VPC にデプロイする必要があります。



次の図は、*プライベート接続*方式と、コンポーネント間で準備する必要がある接続を示しています。コンソール エージェントは、Google Cloud Platform VPC にデプロイする必要があります。



コンソールエージェントを準備する

コンソール エージェントは、コンソール機能のメイン ソフトウェアです。 ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

Google Cloud Platform VPC にコンソール エージェントがすでにデプロイされている場合は、準備は完了です。

そうでない場合は、その場所にコンソール エージェントを作成して、 ONTAPデータを Google Cloud Storage にバックアップする必要があります。別のクラウド プロバイダーまたはオンプレミスにデプロイされたコンソール エージェントは使用できません。

- "コンソールエージェントについて学ぶ"
- "GCP にコンソール エージェントをインストールする"

コンソールエージェントのネットワークを準備する

コンソール エージェントに必要なネットワーク接続があることを確認します。

手順

1. コンソール エージェントがインストールされているネットワークで次の接続が有効になっていることを確認します。
   - NetApp Backup and RecoveryとGoogle Cloudストレージへのポート443経由のHTTPS接続("エンドポイントのリストを見る")
   - ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
2. コンソール エージェントをデプロイする予定のサブネットで、プライベート Google アクセス (またはプライベート サービス接続) を有効にします。 "プライベートGoogleアクセス"または "プライベートサービスコネクト"ONTAPクラスタから VPC への直接接続があり、コンソール エージェントと Google Cloud Storage 間の通信を仮想プライベート ネットワーク（プライベート接続）内に維持する必要がある場合に必要です。

   これらのプライベート アクセス オプションを設定するには、Google の指示に従ってください。 DNSサーバーが次のように設定されていることを確認してください。 `www.googleapis.com`そして `storage.googleapis.com`正しい内部 (プライベート) IP アドレスに設定します。

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の「検索と復元」機能を使用するには、Google Cloud BigQuery サービスにアクセスできるように、コンソール エージェントのロールに特定の権限が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従ってください。

手順

1. の中で "Google Cloud コンソール"、*役割*ページに移動します。
2. ページ上部のドロップダウン リストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタム ロールを選択します。
4. ロールの権限を更新するには、「ロールの編集」を選択します。
5. 次の新しい権限をロールに追加するには、「権限の追加」を選択します。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 編集したロールを保存するには、[更新] を選択します。

ライセンス要件を確認する

- クラスタでNetApp Backup and Recoveryを有効にするには、Google の従量課金制（PAYGO）コンソール マーケットプレイス サービスに登録するか、 NetAppからNetApp Backup and Recovery BYOL ライセンスを購入して有効にする必要があります。これらのライセンスはあなたのアカウント用であり、複数のシステムで使用できます。
  - NetApp Backup and Recovery PAYGOライセンスの場合は、 "Google Marketplace のNetApp Consoleの提供" 。 NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。
  - NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの有効期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要になります。"BYOLライセンスの管理方法を学ぶ"。
- バックアップを保存するオブジェクト ストレージ スペース用の Google サブスクリプションが必要です。

サポート対象地域

すべてのリージョンでオンプレミス システムから Google Cloud Storage へのバックアップを作成できます。サービスを設定するときに、バックアップを保存するリージョンを指定します。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、 NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["クラスターの検出方法を学ぶ"^]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

  注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ "クラスターライセンスを管理する"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "クラスター時間を設定する"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

  "SnapMirror関係に互換性のあるONTAPバージョンを表示する"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャの場合は、プライマリ システムで次の設定を構成します。
- カスケード バックアップ アーキテクチャの場合は、セカンダリ システムで次の設定を構成します。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよび復元操作のために、クラスタ間 LIF から Google Cloud Storage へのポート 443 経由の HTTPS 接続を開始します。

  ONTAP はオブジェクト ストレージとの間でデータの読み取りと書き込みを行います。オブジェクト ストレージは開始することはなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。コンソール エージェントは、Google Cloud Platform VPC に配置できます。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。 LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。 "IPspacesについて詳しくはこちら" 。

  NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。各 LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

- ノードのクラスタ間 LIF はオブジェクト ストアにアクセスできます。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る "SVMのDNSサービスを構成する"。

  プライベートGoogleアクセスまたはプライベートサービス接続を使用している場合は、DNSサーバーが次のように設定されていることを確認してください。 `storage.googleapis.com`正しい内部 (プライベート) IP アドレスに設定します。

- デフォルトとは異なる IPspace を使用している場合は、オブジェクト ストレージにアクセスするために静的ルートを作成する必要があることに注意してください。
- 必要に応じてファイアウォール ルールを更新し、 ONTAPからオブジェクト ストレージへのポート 443 経由のNetApp Backup and Recovery接続と、ストレージ VM から DNS サーバーへのポート 53 (TCP/UDP) 経由の名前解決トラフィックを許可します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソ

ース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

Google Cloud Storage をバックアップ先として準備する

Google Cloud Storage をバックアップ ターゲットとして準備するには、次の手順を実行します。

- 権限を設定します。
- (オプション) 独自のバケットを作成します。 (必要に応じて、サービスによってバケットが作成されます。)
- （オプション）データ暗号化用の顧客管理キーを設定する

権限を設定する

カスタム ロールを使用して特定の権限を持つサービス アカウントにストレージ アクセス キーを提供する必要があります。サービス アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用される Cloud Storage バケットを認証してアクセスできるようになります。Google Cloud Storage が誰がリクエストを行っているかを認識するために、キーが必要になります。

手順

1. の中で "Google Cloud コンソール"、*役割*ページに移動します。
2. "新しいロールの作成"以下の権限を持ちます:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloudコンソールでは、 "サービスアカウントページに移動します" 。
4. Cloud プロジェクトを選択します。
5. サービス アカウントの作成 を選択し、必要な情報を入力します。
   a. サービス アカウントの詳細: 名前と説明を入力します。
   b. このサービス アカウントにプロジェクトへのアクセスを許可する: 先ほど作成したカスタム ロールを選択します。
   c. *完了*を選択します。
6. へ移動 "GCP ストレージ設定"サービス アカウントのアクセス キーを作成します。
   a. プロジェクトを選択し、*相互運用性*を選択します。まだ行っていない場合は、[相互運用性アクセスを有効にする] を選択します。
   b. サービス アカウントのアクセス キー の下で、サービス アカウントのキーの作成 を選択し、作成したサービス アカウントを選択して、キーの作成 をクリックします。

      後でバックアップ サービスを構成するときに、 NetApp Backup and Recoveryにキーを入力する必要があります。

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。または、独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

"独自のバケットの作成について詳しくは"。

データ暗号化用の顧客管理暗号鍵（**CMEK**）を設定する

デフォルトの Google 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータ暗号化に使用できます。クロスリージョン キーとクロスプロジェクト キーの両方がサポートされているため、CMEK キーのプロジェクトとは異なるバケットのプロジェクトを選択できます。

独自の顧客管理キーを使用する予定の場合:

- アクティベーション ウィザードでこの情報を追加するには、キー リングとキー名が必要です。 "顧客管理暗号化キーの詳細" 。
- コンソール エージェントのロールに次の必要な権限が含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトで Google の「Cloud Key Management Service (KMS)」API が有効になっていることを確認する必要があります。参照 "Google Cloud ドキュメント: API の有効化"詳細については。

CMEKの考慮事項:

- HSM (ハードウェア バックアップ) キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成された Cloud KMS キーとインポートされた Cloud KMS キーの両方がサポートされます。
- 地域キーのみがサポートされ、グローバル キーはサポートされません。
- 現在、「対称暗号化/復号化」目的のみがサポートされています。
- ストレージ アカウントに関連付けられたサービス エージェントには、NetApp Backup and Recoveryによって「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM ロールが割り当てられます。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
    - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

コンソールの [システム] ページにバックアップの Google Cloud Storage 保存先が存在する場合は、ONTAPクラスターを Google Cloud オブジェクト ストレージにドラッグできます。

- バックアップとリカバリバーで*ボリューム*を選択します。ボリュームタブから*アクション*を選択します ••• アイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
   - 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてが必要な場合

- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー

> 選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリからセカンダリへ、そしてセカンダリからオブジェクト ストレージへ流れます。
   - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。

   > カスタムポリシーを作成するには、"ポリシーを作成します。" 。

   ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
   - ポリシーの名前を入力します。
   - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
   - *作成*を選択します。
4. レプリケーション: 次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいポリシーを作成します。

     > カスタムポリシーを作成するには、"ポリシーを作成します。" 。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: **Google Cloud** を選択します。
   - プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

     新しいバケットを作成するか、すでに作成したバケットを選択します。

     さらにコストを最適化するために古いバックアップ ファイルを Google Cloud Archive ストレージに階層化する場合は、バケットに適切なライフサイクル ルールがあることを確認してください。

     Google Cloud アクセスキーとシークレットキーを入力します。

   - 暗号化キー: 新しい Google Cloud ストレージ アカウントを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの Google Cloud 暗号化キーを使用するか、Google Cloud アカウントから独自の顧客管理キーを選択するかを選択します。

     既存の Google Cloud ストレージ アカウントを選択した場合は、暗号化情報がすでに用意されているため、ここで入力する必要はありません。

     独自の顧客管理キーを使用する場合は、キーリングとキー名を入力します。 "顧客管理暗号化キーの詳細" 。

   - ネットワーク: IPspace を選択します。

     バックアップするボリュームが存在するONTAPクラスタ内の IPspace。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です。

   - バックアップ ポリシー: 既存のオブジェクト ストレージ ポリシーへのバックアップを選択するか、新しいポリシーを作成します。

     カスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - *作成*を選択します。

   - 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイル

としてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、ソース ボリュームと同期されます。

入力した Google アクセスキーとシークレットキーで示されるサービス アカウントに Google Cloud Storage バケットが自動的に作成され、そこにバックアップ ファイルが保存されます。ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータをONTAP S3にバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのプライマリONTAPシステムからボリューム データのバックアップを開始します。バックアップは、セカンダリONTAPストレージ システム (複製されたボリューム)、S3 サーバーとして設定されたONTAPシステム上のバケット (バックアップ ファイル)、またはその両方に送信できます。

プライマリオンプレミスONTAPシステムには、 FAS、 AFF、またはONTAP Selectシステムを使用できま

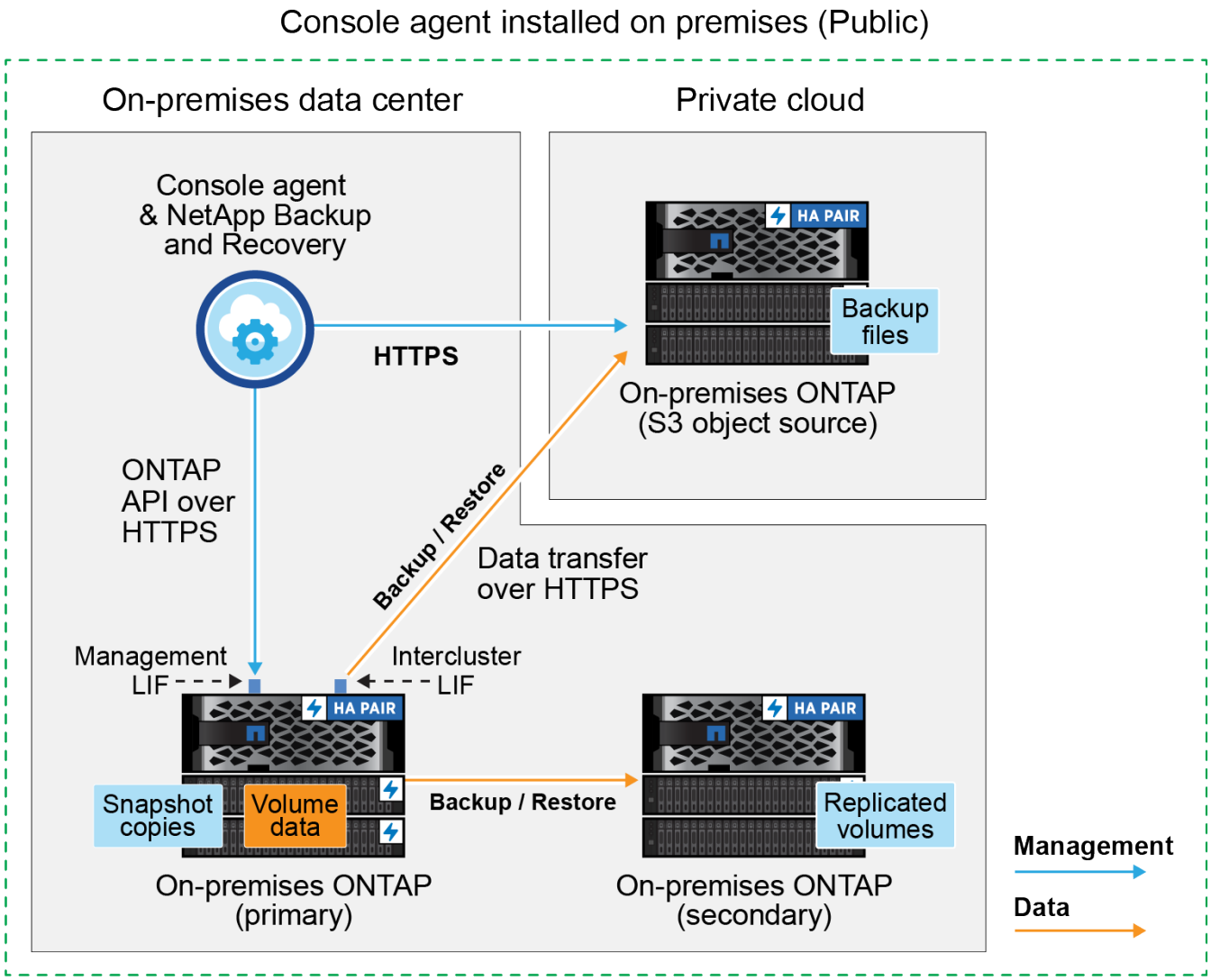
す。セカンダリONTAPシステムは、オンプレミスのONTAPまたはCloud Volumes ONTAPシステムになります。オブジェクト ストレージは、オンプレミスのONTAPシステム、または Simple Storage Service (S3) オブジェクト ストレージ サーバーを有効にしたCloud Volumes ONTAPシステム上に配置できます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

接続方法を特定する

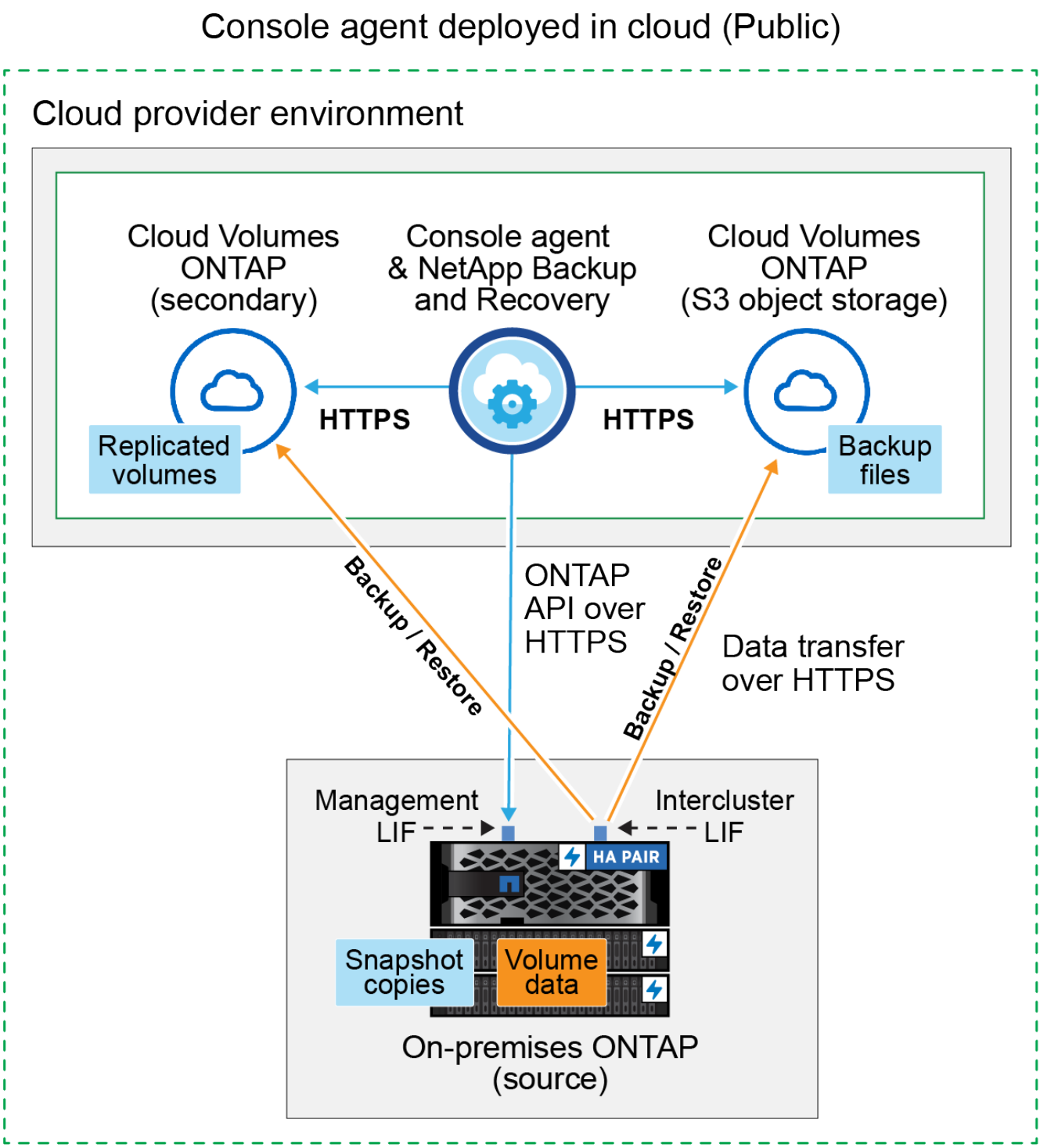
ONTAPシステム上の S3 バケットにバックアップを作成できる構成は多数あります。以下に 2 つのシナリオを示します。

次の図は、プライマリオンプレミスONTAPシステムを S3 用に設定されたオンプレミスONTAPシステムにバックアップする場合の各コンポーネントと、それらの間で準備する必要がある接続を示しています。また、ボリュームをレプリケートするために、同じオンプレミスの場所にあるセカンダリONTAPシステムへの接続も示します。



コンソール エージェントとプライマリ オンプレミスONTAPシステムがインターネット アクセスのないオンプレミスの場所にインストールされている場合 (「プライベート」モードの展開)、 ONTAP S3 システムは同じオンプレミス データセンターに配置する必要があります。

次の画像は、プライマリオンプレミスONTAPシステムを S3 用に構成されたCloud Volumes ONTAPシステムにバックアップする場合の各コンポーネントと、それらの間で準備する必要がある接続を示しています。また、ボリュームを複製するために、同じクラウド プロバイダー環境内のセカンダリCloud Volumes ONTAPシステムへの接続も示します。



このシナリオでは、コンソール エージェントは、Cloud Volumes ONTAPシステムが展開されているのと同じクラウド プロバイダー環境に展開する必要があります。

コンソールエージェントを準備する

コンソール エージェントは、コンソール機能のメイン ソフトウェアです。 ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

ONTAP S3 にデータをバックアップする場合、オンプレミスまたはクラウドでコンソール エージェントが使用可能である必要があります。新しいコンソール エージェントをインストールするか、現在選択されているコンソール エージェントがこれらの場所のいずれかに存在することを確認する必要があります。オンプレミスのコンソール エージェントは、インターネット アクセスの有無にかかわらずサイトにインストールできます。

- "コンソールエージェントについて学ぶ"
- "クラウド環境にコンソールエージェントをインストールする"
- "インターネットにアクセスできる Linux ホストにコンソール エージェントをインストールする"
- "インターネットにアクセスできない Linux ホストにコンソール エージェントをインストールする"
- "コンソールエージェント間の切り替え"

コンソールエージェントのネットワーク要件を準備する

コンソール エージェントがインストールされているネットワークで次の接続が有効になっていることを確認します。

- ポート443経由のONTAP S3サーバへのHTTPS接続
- ソースONTAPクラスタ管理 LIF へのポート 443 経由の HTTPS 接続
- NetApp Backup and Recoveryへのポート 443 経由のアウトバウンド インターネット接続 (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)

プライベートモード（ダークサイト）の考慮事項

NetApp Backup and Recovery機能は、コンソール エージェントに組み込まれています。プライベート モードでインストールされている場合、新しい機能にアクセスするには、コンソール エージェント ソフトウェアを定期的に更新する必要があります。チェックしてください"NetApp Backup and Recoveryの新機能"NetApp Backup and Recovery の各リリースの新機能を確認してください。新しい機能を使用する場合は、次の手順に従ってください。 "コンソールエージェントソフトウェアをアップグレードする" 。

標準の SaaS 環境でNetApp Backup and Recoveryを使用すると、 NetApp Backup and Recovery の構成データがクラウドにバックアップされます。インターネットにアクセスできないサイトでNetApp Backup and Recoveryを使用する場合、 NetApp Backup and Recovery の構成データは、バックアップが保存されているONTAP S3 バケットにバックアップされます。

ライセンス要件を確認する

クラスターに対してNetApp Backup and Recoveryをアクティブ化する前に、 NetAppからNetApp Backup and Recovery BYOL ライセンスを購入してアクティブ化する必要があります。このライセンスはオブジェクト ストレージへのバックアップと復元用です。スナップショットや複製されたボリュームを作成するのにライセンスは必要ありません。このライセンスはアカウント用であり、複数のシステムで使用できます。

ライセンスの有効期間と容量にわたってサービスを使用するには、 NetAppからのシリアル番号が必要になり

ます。"BYOLライセンスの管理方法を学ぶ"。

ONTAP S3 にファイルをバックアップする場合、PAYGO ライセンスはサポートされません。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、 NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["クラスターの検出方法を学ぶ"^]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

  注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

  方法を学ぶ "クラスターライセンスを管理する"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "クラスター時間を設定する"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

  "SnapMirror関係に互換性のあるONTAPバージョンを表示する"。

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件が満たされていることを確認する必要があります。

- ファンアウト バックアップ アーキテクチャを使用する場合は、プライマリ ストレージ システムで設定を構成する必要があります。
- カスケード バックアップ アーキテクチャを使用する場合は、セカンダリ ストレージ システムで設定を構成する必要があります。

"バックアップアーキテクチャの種類について詳しく学ぶ"。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよびリストア操作のために、クラスタ間 LIF からONTAP S3 サーバへのユーザ指定ポートを介して HTTPS 接続を開始します。ポートはバックアップのセットアップ中に構成可能です。

  ONTAP はオブジェクト ストレージとの間でデータの読み取りと書き込みを行います。オブジェクト ストレージは開始することはなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。 LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。"IPspacesについて詳しくはこちら" 。

  NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。各 LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

- ノードのクラスタ間 LIF はオブジェクト ストアにアクセスできます (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る"SVMのDNSサービスを構成する"。
- デフォルトとは異なる IPspace を使用している場合は、オブジェクト ストレージにアクセスするために静的ルートを作成する必要がある場合があります。
- 必要に応じてファイアウォール ルールを更新し、指定したポート (通常はポート 443) を介してONTAPからオブジェクト ストレージへのNetApp Backup and Recoveryサービス接続と、ポート 53 (TCP/UDP) を介してストレージ VM から DNS サーバーへの名前解決トラフィックを許可します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

  Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を

確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

ONTAP S3をバックアップターゲットとして準備する

オブジェクト ストレージ バックアップに使用する予定のONTAPクラスタで、Simple Storage Service (S3) オブジェクト ストレージ サーバを有効にする必要があります。参照 "ONTAP S3 ドキュメント"詳細については。

注意: このクラスターをコンソールの システム ページに追加することはできますが、S3 オブジェクト ストレージ サーバーとして識別されず、ソース システムをこの S3 システムにドラッグ アンド ドロップしてバックアップのアクティブ化を開始することはできません。

このONTAPシステムは次の要件を満たしている必要があります。

サポートされる**ONTAP**バージョン

オンプレミスのONTAPシステムにはONTAP 9.8 以降が必要です。 Cloud Volumes ONTAPシステムにはONTAP 9.9.1 以降が必要です。

S3 認証情報

ONTAP S3 ストレージへのアクセスを制御するには、S3 ユーザーを作成する必要があります。 "詳細については、 ONTAP S3 のドキュメントを参照してください。" 。

ONTAP S3 へのバックアップを設定すると、バックアップ ウィザードによって、ユーザー アカウントの S3 アクセス キーとシークレット キーの入力が求められます。ユーザー アカウントにより、 NetApp Backup and Recovery は、バックアップの保存に使用されるONTAP S3 バケットを認証してアクセスできるようになります。キーは、 ONTAP S3 が誰がリクエストを行っているかを認識するために必要です。

これらのアクセス キーは、次の権限を持つユーザーに関連付ける必要があります。

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket",
"s3:GetBucketLocation"
```

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- バックアップしたいボリュームを選択します
- バックアップ戦略とポリシーを定義する
- 選択内容を確認する

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
   - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。
   - バックアップとリカバリバーで*ボリューム*を選択します。 [ボリューム] タブで、アクション **(...)** オプションを選択し、単一のボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない) に対して バックアップのアクティブ化 を選択します。

   ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにすでにスナップショットまたはレプリケーション ポリシーが適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされることに注意してください。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。

- 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
- 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを構成する必要があります。

- 保護オプション: ローカルスナップショット、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など、バックアップオプションの1つまたはすべてを実装するかどうか
- アーキテクチャ: ファンアウトまたはカスケードバックアップアーキテクチャを使用するかどうか
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー
- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: ローカル スナップショットを作成します。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: S3 用に設定されたONTAPシステム上のバケットにボリュームをバックアップします。
2. アーキテクチャ: レプリケーションとバックアップの両方を選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: バックアップ データはプライマリ システムからセカンダリ システムへ流れ、次にセカンダリ システムからオブジェクト ストレージへ流れます。
   - ファンアウト: バックアップ データはプライマリ システムからセカンダリ システムへ、そしてプライマリ システムからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。

   スナップショットをアクティブ化する前にカスタムポリシーを作成する場合は、System ManagerまたはONTAP CLIを使用できます。 `snapmirror policy create`指示。参照。

   バックアップとリカバリを使用してカスタムポリシーを作成するには、"ポリシーを作成します。" 。

   ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
   - ポリシーの名前を入力します。

- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

4. レプリケーション: レプリケーション を選択した場合は、次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、宛先アグリゲート (FlexGroupボリュームの場合はアグリゲート) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいポリシーを作成します。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: * ONTAP S3* を選択します。
   - プロバイダー設定: S3 サーバーの FQDN の詳細、ポート、ユーザーのアクセス キーとシークレット キーを入力します。

     アクセス キーとシークレット キーは、作成したユーザーがONTAPクラスターに S3 バケットへのアクセス権を付与するためのものです。

   - ネットワーク: バックアップするボリュームが存在するソースONTAPクラスタ内の IPspace を選択します。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。

     正しい IPspace を選択すると、 NetApp Backup and Recovery がONTAPからONTAP S3 オブジェクト ストレージへの接続を確立できるようになります。

   - バックアップ ポリシー: 既存のバックアップ ポリシーを選択するか、新しいバックアップ ポリシーを作成します。

     System Manager またはONTAP CLI を使用してポリシーを作成できます。 ONTAP CLI を使用してカスタムポリシーを作成するには `snapmirror policy create`コマンドについては、 。

     バックアップとリカバリを使用してカスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。 DataLockとランサムウェア耐性の詳細については、以下を参照してください。"オブ

ジェクトへのバックアップポリシー設定" 。

- *作成*を選択します。

◦ 既存のスナップショットをバックアップ ファイルとしてオブジェクト ストレージにエクスポートする: このシステム内のボリュームに、選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致するローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。ポリシーが一致しない場合、バックアップは作成されません。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、ソース データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。

ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータをStorageGRIDにバックアップします。

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのプライマリONTAPシステムからセカンダリ ストレージ システムおよびNetApp StorageGRIDシステムのオブジェクト ストレージへのボリューム データのバックアップを開始します。

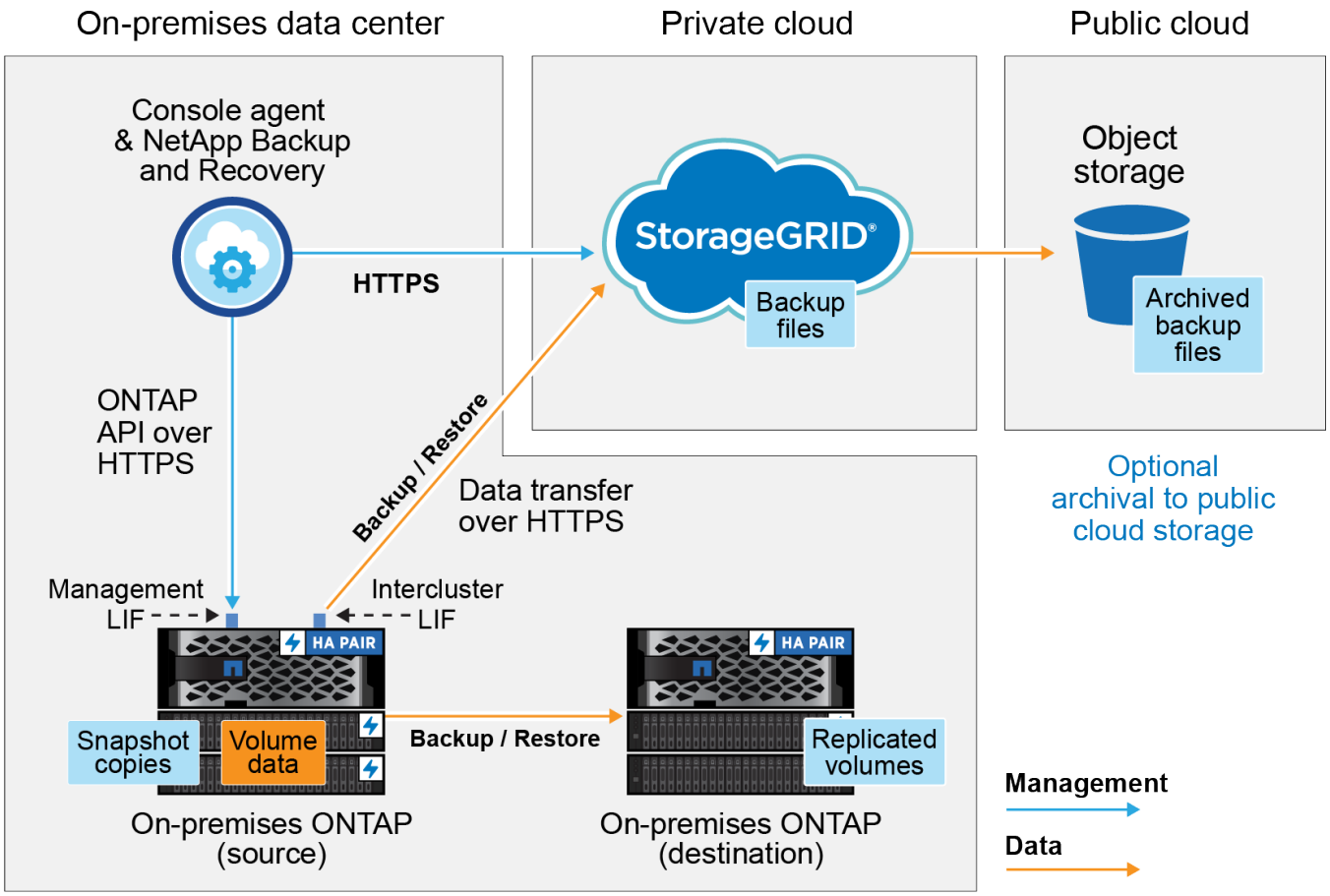
「オンプレミスのONTAPシステム」には、 FAS、 AFF、およびONTAP Selectシステムが含まれます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

接続方法を特定する

次の図は、オンプレミスのONTAPシステムをStorageGRIDにバックアップする場合の各コンポーネントと、それらの間で準備する必要がある接続を示しています。

オプションで、同じオンプレミスの場所にあるセカンダリONTAPシステムに接続してボリュームを複製することもできます。



コンソール エージェントとオンプレミスのONTAPシステムがインターネットにアクセスできないオンプレミスの場所 (「ダーク サイト」) にインストールされている場合、 StorageGRIDシステムは同じオンプレミス デ

ータセンターに配置する必要があります。ダーク サイト構成では、古いバックアップ ファイルのパブリック クラウドへのアーカイブはサポートされていません。

コンソールエージェントを準備する

コンソール エージェントは、コンソール機能のメイン ソフトウェアです。 ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

StorageGRIDにデータをバックアップする場合、オンプレミスでコンソール エージェントが使用可能である必要があります。新しいコンソール エージェントをインストールするか、現在選択されているコンソール エージェントがオンプレミスに存在することを確認する必要があります。コンソール エージェントは、インターネットにアクセスできるサイトにも、アクセスできないサイトにもインストールできます。

- "コンソールエージェントについて学ぶ"
- "インターネットにアクセスできる Linux ホストにコンソール エージェントをインストールする"
- "インターネットにアクセスできない Linux ホストにコンソール エージェントをインストールする"
- "コンソールエージェント間の切り替え"

コンソールエージェントのネットワーク要件を準備する

コンソール エージェントがインストールされているネットワークで次の接続が有効になっていることを確認します。

- ポート443経由のStorageGRIDゲートウェイノードへのHTTPS接続
- ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
- NetApp Backup and Recoveryへのポート 443 経由のアウトバウンド インターネット接続 (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)

プライベートモード（ダークサイト）の考慮事項

- NetApp Backup and Recovery機能は、コンソール エージェントに組み込まれています。プライベート モードでインストールされている場合、新しい機能にアクセスするには、コンソール エージェント ソフトウェアを定期的に更新する必要があります。チェックしてください"NetApp Backup and Recoveryの新機能"NetApp Backup and Recovery の各リリースの新機能を確認してください。新しい機能を使用する場合は、次の手順に従ってください。 "コンソールエージェントソフトウェアをアップグレードする" 。

  オブジェクト ストレージへのバックアップの作成に加えて、スナップショットと複製されたボリュームのスケジュール設定と作成の機能を備えたNetApp Backup and Recoveryの新しいバージョンでは、コンソール エージェントのバージョン 3.9.31 以上を使用する必要があります。したがって、すべてのバックアップを管理するには、この最新リリースを入手することをお勧めします。

- SaaS 環境でNetApp Backup and Recovery を使用すると、 NetApp Backup and Recovery の構成データがクラウドにバックアップされます。インターネットにアクセスできないサイトでNetApp Backup and Recoveryを使用する場合、 NetApp Backup and Recovery構成データは、バックアップが保存されているStorageGRIDバケットにバックアップされます。

ライセンス要件を確認する

クラスターに対してNetApp Backup and Recoveryをアクティブ化する前に、 NetAppからNetApp Backup and Recovery BYOL ライセンスを購入してアクティブ化する必要があります。このライセンスはアカウント用であり、複数のシステムで使用できます。

ライセンスの有効期間と容量にわたってサービスを使用するには、 NetAppからのシリアル番号が必要になります。"BYOLライセンスの管理方法を学ぶ"。

StorageGRIDにファイルをバックアップする場合、PAYGO ライセンスはサポートされません。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、 NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["クラスターの検出方法を学ぶ"^]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、 ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

  注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

  方法を学ぶ "クラスターライセンスを管理する"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "クラスター時間を設定する"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

  "SnapMirror関係に互換性のあるONTAPバージョンを表示する"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャを使用する場合は、プライマリ ストレージ システムで次の設定を構成する必要があります。
- カスケード バックアップ アーキテクチャを使用する場合は、セカンダリ ストレージ システムで次の設定を構成する必要があります。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよびリストア操作のために、クラスタ間 LIF からStorageGRIDゲートウェイ ノードへのユーザ指定ポートを介して HTTPS 接続を開始します。ポートはバックアップのセットアップ中に構成可能です。

  ONTAP はオブジェクト ストレージとの間でデータの読み取りと書き込みを行います。オブジェクト ストレージは開始することはなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。コンソール エージェントは社内に常駐する必要があります。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。 LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。 "IPspacesについて詳しくはこちら" 。

  NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。各 LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

- ノードのクラスタ間 LIF はオブジェクト ストアにアクセスできます (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る "SVMのDNSサービスを構成する"。
- デフォルトとは異なる IPspace を使用している場合は、オブジェクト ストレージにアクセスするために静的ルートを作成する必要がある場合があります。
- 必要に応じてファイアウォール ルールを更新し、指定したポート (通常はポート 443) を介してONTAPからオブジェクト ストレージへのNetApp Backup and Recoveryサービス接続と、ポート 53 (TCP/UDP) を介してストレージ VM から DNS サーバーへの名前解決トラフィックを許可します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 "ONTAPドキュメントでクラスタピアリングの前提条件を確認する" 。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

StorageGRIDをバックアップターゲットとして準備する

StorageGRID は次の要件を満たしている必要があります。参照 "StorageGRIDドキュメント"詳細についてはこちらをご覧ください。

StorageGRIDのDataLockおよびランサムウェア耐性要件の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシーオプション" 。

サポートされている**StorageGRID**バージョン

StorageGRID 10.3 以降がサポートされています。

バックアップに DataLock & Ransomware Resilience を使用するには、 StorageGRIDシステムでバージョン 11.6.0.3 以上を実行している必要があります。

古いバックアップをクラウド アーカイブ ストレージに階層化するには、 StorageGRIDシステムでバージョン 11.3 以降を実行している必要があります。さらに、 StorageGRIDシステムがコンソールの システム ページで検出される必要があります。

アーカイブ ストレージを使用するには、管理ノードの IP アクセスが必要です。

ゲートウェイ IP アクセスは常に必要です。

S3 認証情報

StorageGRIDストレージへのアクセスを制御するには、S3 テナント アカウントを作成する必要があります。 "詳細についてはStorageGRIDのドキュメントを参照してください。" 。

StorageGRIDへのバックアップを設定すると、バックアップ ウィザードによってテナント アカウントの S3 アクセス キーとシークレット キーの入力が求められます。テナント アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用されるStorageGRIDバケットを認証してアクセスできるようになります。キーは、 StorageGRID が誰がリクエストを行っているかを認識するために必要です。

これらのアクセス キーは、次の権限を持つユーザーに関連付ける必要があります。

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

オブジェクトのバージョン管理

オブジェクト ストア バケットでStorageGRIDオブジェクトのバージョン管理を手動で有効にしないでください。

古いバックアップファイルをパブリッククラウドストレージにアーカイブする準備をする

古いバックアップ ファイルをアーカイブ ストレージに階層化することで、必要のないバックアップに安価なストレージ クラスを使用することになり、コストを節約できます。 StorageGRID は、アーカイブ ストレージを提供しないオンプレミス (プライベート クラウド) ソリューションですが、古いバックアップ ファイルをパブリック クラウド アーカイブ ストレージに移動できます。この方法で使用すると、クラウド ストレージに階層化されたデータ、またはクラウド ストレージから復元されたデータは、 StorageGRIDとクラウド ストレージの間で転送されます。このデータ転送にはコンソールは関与しません。

現在のサポートでは、AWS *S3 Glacier*/*S3 Glacier Deep Archive* または *Azure Archive* ストレージにバックアップをアーカイブできます。

- ONTAP の要件*
- クラスタではONTAP 9.12.1 以上を使用する必要があります。
- StorageGRID の要件*
- StorageGRIDは 11.4 以上を使用する必要があります。
- StorageGRIDは "コンソールで発見され利用可能"。

Amazon S3 の要件

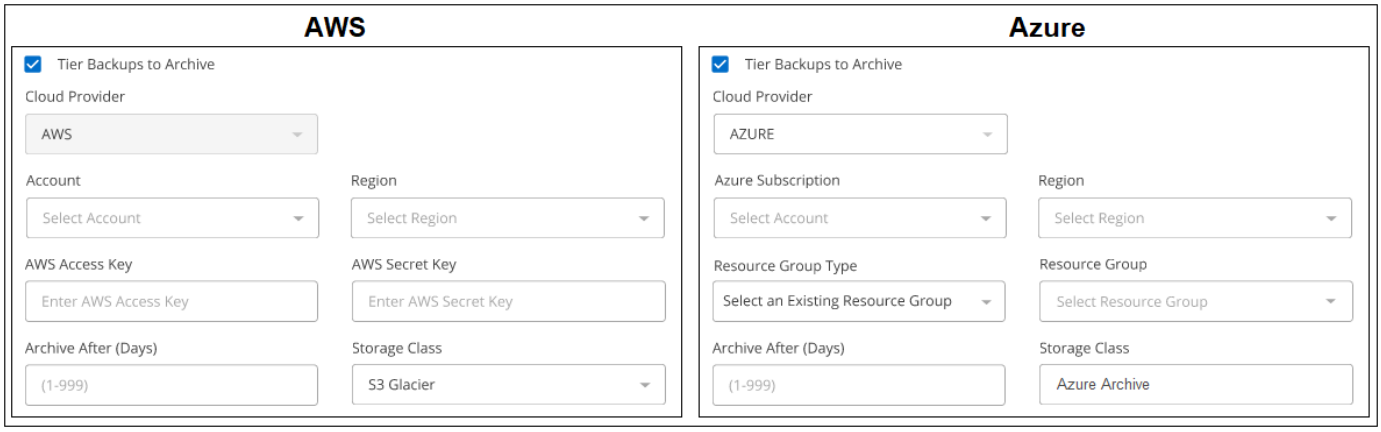
- アーカイブされたバックアップが保存されるストレージスペース用の Amazon S3 アカウントにサインアップする必要があります。
- バックアップを AWS S3 Glacier または S3 Glacier Deep Archive ストレージに階層化することを選択できます。"AWS アーカイブ層の詳細"。
- StorageGRIDはバケットへのフルコントロールアクセス権を持っている必要があります(`s3:*`); ただし、これが不可能な場合は、バケットポリシーでStorageGRIDに次の S3 権限を付与する必要があります。
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Azure Blob の要件

- アーカイブされたバックアップが保存されるストレージ スペースの Azure サブスクリプションにサインアップする必要があります。
- アクティベーション ウィザードを使用すると、既存のリソース グループを使用して、バックアップを保

存する BLOB コンテナーを管理したり、新しいリソース グループを作成したりできます。

クラスターのバックアップ ポリシーのアーカイブ設定を定義するときは、クラウド プロバイダーの資格情報を入力し、使用するストレージ クラスを選択します。 NetApp Backup and Recovery は、クラスターのバックアップをアクティブ化するとクラウド バケットを作成します。 AWS および Azure アーカイブ ストレージに必要な情報を以下に示します。



選択したアーカイブ ポリシー設定により、 StorageGRIDに情報ライフサイクル管理 (ILM) ポリシーが生成され、設定が「ルール」として追加されます。

- 既存のアクティブな ILM ポリシーがある場合は、データをアーカイブ層に移動するための新しいルールが ILM ポリシーに追加されます。
- 既存の ILM ポリシーが「提案」状態にある場合、新しい ILM ポリシーの作成とアクティブ化はできません。 "StorageGRID ILMポリシーとルールの詳細" 。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [バックアップしたいボリュームを選択します]
- [バックアップ戦略を定義する]
- [選択内容を確認する]

また、APIコマンドを表示するレビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
   - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

     コンソールの [システム] ページにバックアップの保存先がシステムとして存在する場合は、 ONTAP クラスターをオブジェクト ストレージにドラッグできます。

- バックアップとリカバリーで*ボリューム*を選択します。 [ボリューム] タブで、アクション **(...)** オプションを選択し、単一のボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていないもの) に対して バックアップのアクティブ化 を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
   - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ*を選択してください。
   - コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[コンソールエージェントを準備する]。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る"システム内の追加ボリュームのバックアップを有効にする"(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。

- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、 SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
   - 個々のボリュームをバックアップするには、各ボリュームのボックスをオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、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など、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー

- レプリケーションターゲットとポリシー

> 選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
   - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
   - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
   - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップの両方を選択した場合は、次のいずれかの情報フローを選択します。
   - カスケード: 情報はプライマリからセカンダリへ流れ、次にセカンダリからオブジェクト ストレージへ流れます。
   - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

     これらのアーキテクチャの詳細については、"保護の旅を計画する" 。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。

   > カスタムポリシーを作成するには、"ポリシーを作成します。" 。

   ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
   - ポリシーの名前を入力します。
   - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
   - *作成*を選択します。
4. レプリケーション: 次のオプションを設定します。
   - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
   - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。

     > カスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー: * StorageGRID*を選択します。
   - プロバイダー設定: プロバイダー ゲートウェイ ノードの FQDN の詳細、ポート、アクセス キー、およびシークレット キーを入力します。

     アクセス キーとシークレット キーは、 ONTAPクラスターにバケットへのアクセス権を付与するために作成した IAM ユーザー用です。

   - ネットワーク: バックアップするボリュームが存在するONTAPクラスター内の IPspace を選択します。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。

     適切な IPspace を選択すると、 NetApp Backup and Recovery がONTAPからStorageGRIDオブジェクト ストレージへの接続を確立できるようになります。

   - バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択するか、新しいポリシーを作成します。

     カスタムポリシーを作成するには、"ポリシーを作成します。" 。

     ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

     - ポリシーの名前を入力します。
     - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
     - オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。 DataLockとランサムウェア耐性の詳細については、以下を参照してください。"オブジェクトへのバックアップポリシー設定" 。

       クラスターでONTAP 9.11.1 以降を使用している場合は、*DataLock* と *Ransomware Resilience* を構成することで、バックアップを削除やランサムウェア攻撃から保護することができます。*DataLock* はバックアップ ファイルが変更されたり削除されたりするのを防ぎ、*Ransomware Resilience* はバックアップ ファイルをスキャンして、バックアップ ファイル内のランサムウェア攻撃の証拠を探します。

     - *作成*を選択します。

     クラスターがONTAP 9.12.1 以上を使用しており、 StorageGRIDシステムがバージョン 11.4 以上を使用している場合は、一定の日数後に古いバックアップをパブリック クラウド アーカイブ層に階層化することを選択できます。現在サポートされているのは、AWS S3 Glacier/S3 Glacier Deep Archive または Azure Archive ストレージ層です。この機能を使用するためにシステムを構成する方法をご覧ください。

   - パブリック クラウドへの階層化バックアップ: バックアップを階層化するクラウド プロバイダーを選択し、プロバイダーの詳細を入力します。

     新しいStorageGRIDクラスターを選択または作成します。コンソールが検出できるStorageGRIDクラ

スタの作成の詳細については、 "StorageGRIDドキュメント" 。

- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの保護が最も完全になります。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、ソース データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。

ボリューム バックアップ ダッシュボードが表示され、バックアップの状態を監視できます。

バックアップと復元ジョブのステータスを監視することもできます。"ジョブ監視ページ" 。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and RecoveryでSnapMirrorを使用してボリュームを Cloud Resync に移行する

NetApp Backup and RecoveryのSnapMirror to Cloud Resync 機能は、 NetApp環境でのボリューム移行中のデータ保護と継続性を効率化します。SnapMirror Logical Replication

(LRSE) を使用してボリュームをオンプレミスのNetApp展開から別の展開へ、またはCloud Volumes ONTAPなどのクラウドベースのソリューションに移行した場合、SnapMirror to Cloud Resync により、既存のクラウド バックアップがそのままの状態で動作し続けることが保証されます。

この機能により、再ベースライン プロセスが不要になり、移行後もバックアップを続行できるようになります。この機能は、FlexVol と FlexGroup の両方をサポートし、ワークロード移行シナリオで役立ち、 ONTAP バージョン 9.16.1 以降で利用できます。

> この機能は、2025 年 5 月にリリースされたNetApp Backup and Recoveryバージョン 4.0.3 以降で利用できます。

SnapMirror to Cloud Resync は、環境間でバックアップの継続性を維持し、ハイブリッドおよびマルチクラウド設定でのデータ管理を容易にします。

> NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

開始する前に

次の前提条件が満たされていることを確認してください。

- 宛先ONTAPクラスタでは、 ONTAPバージョン 9.16.1 以降が実行されている必要があります。
- 古いソースONTAPクラスターは、NetApp Backup and Recoveryを使用して保護する必要があります。
- SnapMirror to Cloud Resync 機能は、2025 年 5 月にリリースされたNetApp Backup and Recoveryバージョン 4.0.3 以降で利用できます。
- オブジェクト ストレージ内の最新のバックアップが、古いソース、新しいソース、およびオブジェクト ストア全体の共通スナップショットであることを確認します。オブジェクト ストアにバックアップされた最新のスナップショットよりも古い共通スナップショットを使用しないでください。
- 再同期操作を開始する前に、古いONTAPクラスタで使用されていたスナップショット ポリシーとSnapMirrorポリシーの両方を、新しいONTAPクラスタに作成する必要があります。再同期プロセスでポリシーを使用する場合は、そのポリシーも作成する必要があります。再同期操作ではポリシーは作成されません。
- 移行ボリュームのSnapMirror関係に適用されるSnapMirrorポリシーに、クラウド関係で使用されるものと同じラベルが含まれていることを確認します。問題を回避するには、ボリュームとすべてのスナップショットの正確なミラーを管理するポリシーを使用します。

> SVM-Migrate、SVM-DR、またはヘッドスワップ方式を使用した移行後のSnapMirrorから Cloud Resync への転送は現在サポートされていません。

NetApp Backup and RecoverySnapMirrorからクラウド再同期への仕組み

技術的な更新を完了したり、ボリュームを 1 つのONTAPクラスターから別のクラスターに移行したりする場合には、バックアップが中断されることなく継続して機能することが重要です。 NetApp Backup and Recovery SnapMirror to Cloud Resync は、ボリュームの移行後もクラウド バックアップの一貫性が維持されるようにすることで、この問題を解決します。

次に例を示します。

Vol1a というオンプレミスのボリュームがあるとします。このボリュームには、S1、S2、S3 の 3 つのスナップショットがあります。これらのスナップショットは復元ポイントです。 Vol1 はSnapMirror to Cloud (SM-C) を使用してクラウドにバックアップされていますが、オブジェクト ストアには S1 と S2 のみが存在します。

ここで、Vol1 を別のONTAPクラスタに移行します。これを行うには、Vol1b という新しいクラウド ボリュームへのSnapMirror論理レプリケーション (LRSE) 関係を作成します。これにより、3 つのスナップショット (S1、S2、S3) すべてが Vol1a から Vol1b に転送されます。

移行が完了すると、次の設定になります。

- 元の SM-C 関係 (Vol1a → オブジェクト ストア) は削除されます。
- LRSE関係（Vol1a → Vol1b）も削除されます。
- Vol1b がアクティブ ボリュームになりました。

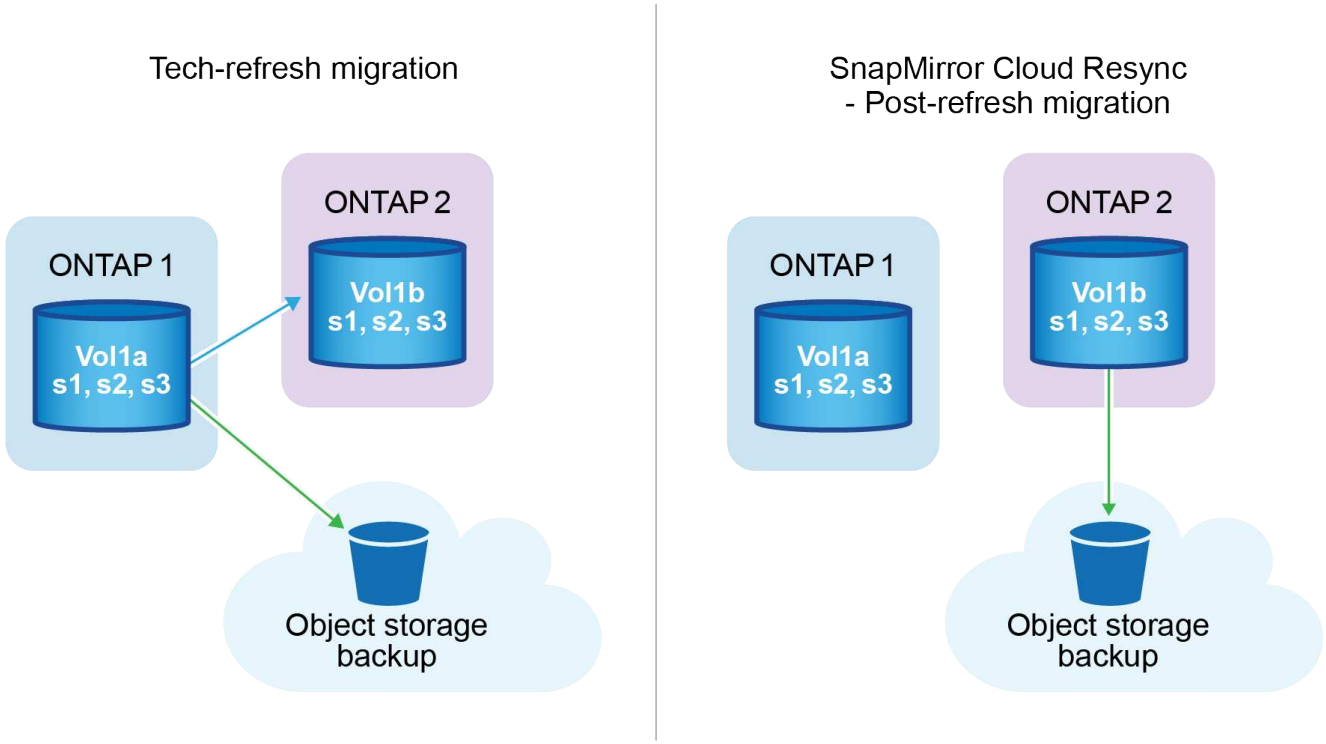
この時点で、Vol1b を同じクラウド エンドポイントにバックアップし続ける必要があります。ただし、最初から完全なバックアップを開始する代わりに (時間とリソースがかかります)、 SnapMirrorを使用して Cloud Resync を実行します。

再同期の仕組みは次のとおりです。

- システムは、Vol1a とオブジェクト ストア間の共通スナップショットをチェックします。この場合、両方とも S2 を持ちます。
- この共有スナップショットにより、システムは S2 と S3 間の増分変更のみを転送する必要があります。

つまり、ボリューム全体ではなく、S2 以降に追加された新しいデータのみがオブジェクト ストアに送信されます。

このプロセスにより、重複したバックアップが防止され、帯域幅が節約され、移行後もバックアップが継続されます。



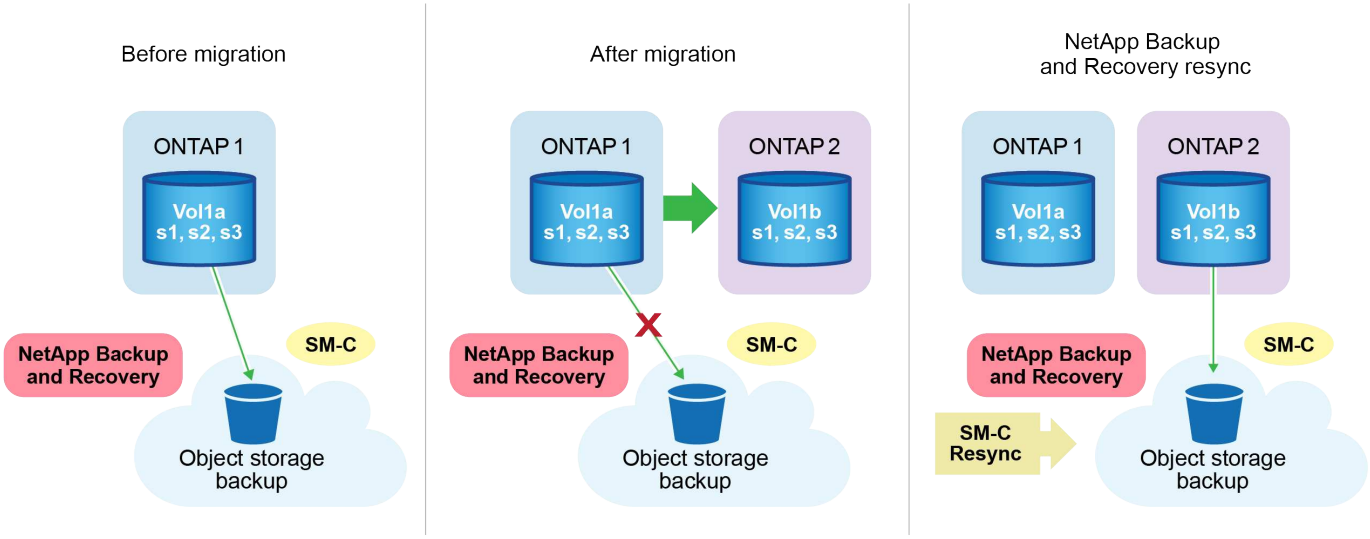
手順に関する注意事項

- 移行と技術更新は、NetApp Backup and Recoveryを使用して実行されません。これらは、専門のサービス チームまたは資格のあるストレージ管理者が実行する必要があります。
- NetApp移行チームは、ボリュームの移動を容易にするために、ソース ONTAP クラスターと宛先ONTAP クラスターの間にSnapMirror関係を作成します。
- 技術更新中の移行がSnapMirrorベースの移行に基づいていることを確認します。

SnapMirrorを使用してボリュームを**Cloud Resync**に移行する方法

SnapMirrorを使用してボリュームを Cloud Resync に移行するには、次の主要な手順が必要です。各手順については以下で詳しく説明します。

- 移行前のチェックリストに従う: 移行を開始する前に、 NetApp Tech Refresh チームは、データの損失を回避し、スムーズな移行プロセスを確実に実行するために、次の前提条件が満たされていることを確認します。
- 移行後のチェックリストに従う: 移行後、 NetApp Tech Refresh チームは、保護を確立し、再同期の準備を整えるために次の手順が完了していることを確認します。
- * SnapMirrorからクラウドへの再同期を実行する*: 移行後、 NetApp Tech Refresh チームはSnapMirrorからクラウドへの再同期操作を実行し、新しく移行されたボリュームからクラウド バックアップを再開します。



移行前のチェックリストに従う

移行前に、 NetApp Tech Refresh チームはこれらの前提条件をチェックして、データの損失を防ぎ、スムーズなプロセスを確保します。

1. 移行するすべてのボリュームがNetApp Backup and Recoveryを使用して保護されていることを確認します。
2. ボリュームインスタンスの UUID を記録します。移行を開始する前に、すべてのボリュームのインスタンス UUID を書き留めておきます。これらの識別子は、後のマッピングおよび再同期操作にとって重要です。
3. SnapMirror関係を削除する前に、各ボリュームの最終スナップショットを取得して最新の状態を保存します。
4. SnapMirrorポリシーを文書化します。各ボリュームの関係に現在添付されているSnapMirrorポリシーを記録します。これは、後でSnapMirrorからクラウドへの再同期プロセス中に必要になります。
5. オブジェクト ストアとのSnapMirror Cloud 関係を削除します。
6. 新しいONTAPクラスタとの標準のSnapMirror関係を作成し、ボリュームを新しいターゲットONTAPクラスタに移行します。

移行後のチェックリストに従う

移行後、 NetApp Tech Refresh チームは、保護を確立し、再同期の準備を整えるために次の手順が完了していることを確認します。

1. 移行先のONTAPクラスタ内のすべての移行されたボリュームの新しいボリューム インスタンス UUID を記録します。
2. 古いONTAPクラスタで使用可能だったすべての必要なSnapMirrorポリシーが、新しいONTAPクラスタで正しく設定されていることを確認します。
3. コンソールの システム ページで、新しいONTAPクラスタをシステムとして追加します。

ボリューム ID ではなく、ボリューム インスタンス UUID を使用する必要があります。ボリューム インスタンス UUID は移行全体で一貫性が保たれる一意の識別子ですが、ボリューム ID は移行後に変更される可能性があります。

移行後、 NetApp Tech Refresh チームはSnapMirror to Cloud Resync 操作を実行し、新しく移行されたボリュームからクラウド バックアップを再開します。

1. コンソールの システム ページで、新しいONTAPクラスタをシステムとして追加します。
2. NetApp Backup and Recoveryボリューム ページを参照して、古いソース システムの詳細が利用可能であることを確認します。
3. NetApp Backup and Recoveryボリューム ページから、バックアップ設定 を選択します。
   - バックアップ設定ページで、[すべて表示] を選択します。
   - 新しいソースの右側にある [アクション…] メニューから、バックアップの再同期 を選択します。
4. 「システムの再同期」ページで、次の操作を行います。
   a. 新しいソース システム: ボリュームが移行された新しいONTAPクラスターを入力します。
   b. 既存のターゲット オブジェクト ストア: 古いソース システムからのバックアップが含まれているターゲット オブジェクト ストアを選択します。
5. 再同期の詳細 Excel シートをダウンロードするには、[CSV テンプレートのダウンロード] を選択します。このシートを使用して、移行するボリュームの詳細を入力します。 CSV ファイルに次の詳細を入力します。
   - ソースクラスターの古いボリュームインスタンスUUID
   - 宛先クラスターからの新しいボリュームインスタンスUUID
   - 新しい関係に適用されるSnapMirrorポリシー。
6. ボリューム マッピングの詳細のアップロード の下の アップロード を選択して、完了した CSV シートをNetApp Backup and Recovery UI にアップロードします。

   ボリューム ID ではなく、ボリューム インスタンス UUID を使用する必要があります。ボリューム インスタンス UUID は移行全体で一貫性が保たれる一意の識別子ですが、ボリューム ID は移行後に変更される可能性があります。

7. 再同期操作に必要なプロバイダーとネットワーク構成情報を入力します。
8. 検証プロセスを開始するには、[送信] を選択します。

   NetApp Backup and Recovery は、再同期対象として選択された各ボリュームが最新のスナップショットであり、少なくとも 1 つの共通スナップショットがあることを検証します。これにより、ボリュームがSnapMirrorから Cloud Resync 操作の準備が整っていることが保証されます。

9. 新しいソース ボリューム名や各ボリュームの再同期ステータスなどの検証結果を確認します。
10. ボリュームの適格性を確認します。システムはボリュームが再同期の対象となるかどうかを確認します。ボリュームが不適格な場合は、最新のスナップショットではないか、共通のスナップショットが見つからなかったことを意味します。

    ボリュームがSnapMirrorから Cloud Resync への操作の対象であり続けるようにするには、移行前のフェーズでSnapMirror関係を削除する前に、各ボリュームの最終スナップショットを作成します。これにより、データの最新の状態が保持されます。

11. 再同期操作を開始するには、「再同期」を選択します。システムは最新の共通スナップショットを使用し

て増分変更のみを転送し、バックアップの継続性を保証します。

12. ジョブ モニター ページで再同期プロセスを監視します。

ダークサイトでの**NetApp Backup and Recovery**構成データの復元

インターネットにアクセスできないサイトでNetApp Backup and Recoveryを使用する場合 (プライベート モード と呼ばれます)、 NetApp Backup and Recovery の構成データは、バックアップが保存されているStorageGRIDまたはONTAP S3 バケットにバックアップされます。コンソール エージェント ホスト システムに問題がある場合は、新しいコンソール エージェントを展開して、重要なNetApp Backup and Recoveryデータを復元できます。

この手順はONTAPボリューム データにのみ適用されます。

クラウド プロバイダーまたはインターネットに接続された独自のホストにコンソール エージェントを導入した SaaS 環境でNetApp Backup and Recoveryを使用すると、システムによってクラウド内のすべての重要な構成データがバックアップされ、保護されます。コンソール エージェントに問題がある場合は、新しいコンソール エージェントを作成し、システムを追加します。バックアップの詳細は自動的に復元されます。

バックアップされるデータには 2 種類あります。

- NetApp Backup and Recoveryデータベース - すべてのボリューム、バックアップ ファイル、バックアップ ポリシー、および構成情報のリストが含まれています。
- インデックス カタログ ファイル - 検索と復元機能に使用される詳細なインデックスが含まれており、復元するボリューム データを探すときに、検索を非常に迅速かつ効率的に行うことができます。

このデータは 1 日に 1 回深夜にバックアップされ、各ファイルの最大 7 つのコピーが保持されます。コンソール エージェントが複数のオンプレミスのONTAPシステムを管理している場合、 NetApp Backup and Recoveryファイルは、最初にアクティブ化されたシステムのバケットに保存されます。

NetApp Backup and Recoveryデータベースまたはインデックス カタログ ファイルにはボリューム データは含まれません。

NetApp Backup and Recoveryデータを新しいコンソール エージェントに復元します

オンプレミスのコンソール エージェントが動作を停止した場合は、新しいコンソール エージェントをインストールし、 NetApp Backup and Recoveryデータを新しいコンソール エージェントに復元する必要があります。

NetApp Backup and Recoveryシステムを動作状態に戻すには、次のタスクを実行する必要があります。

- 新しいコンソールエージェントをインストールする
- NetApp Backup and Recoveryデータベースを復元する
- インデックスカタログファイルを復元する
- オンプレミスのONTAPシステムとStorageGRIDシステムをすべてNetApp ConsoleUIに再検出します。

システムが動作していることを確認したら、新しいバックアップ ファイルを作成します。

要件

バックアップ ファイルが保存されているStorageGRIDまたはONTAP S3 バケットから最新のデータベースとインデックスのバックアップにアクセスする必要があります。

- NetApp Backup and RecoveryMySQL データベース ファイル

  このファイルはバケット内の次の場所にあります `netapp-backup-<GUID>/mysql_backup/` と名付けられています `CBS_DB_Backup_<day>_<month>_<year>.sql`。

- インデックスカタログのバックアップ zip ファイル

  このファイルはバケット内の次の場所にあります `netapp-backup-<GUID>/catalog_backup/` と名付けられています `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`。

新しいオンプレミス **Linux** ホストに新しいコンソール エージェントをインストールする

新しいコンソール エージェントをインストールするときは、元のエージェントと同じソフトウェア バージョンをダウンロードします。 NetApp Backup and Recoveryデータベースを変更すると、新しいソフトウェア バージョンが古いデータベース バックアップで動作しなくなる可能性があります。あなたはできる "バックアップデータベースを復元した後、コンソールエージェントソフトウェアを最新バージョンにアップグレードします。"。

1. "新しいオンプレミス Linux ホストにコンソール エージェントをインストールする"
2. 先ほど作成した管理者ユーザーの資格情報を使用してコンソールにログインします。

NetApp Backup and Recoveryデータベースを復元する

1. バックアップ場所から新しいコンソール エージェント ホストに MySQL バックアップをコピーします。以下では、サンプルファイル名「CBS_DB_Backup_23_05_2023.sql」を使用します。
2. Docker コンテナまたは Podman コンテナのどちらを使用しているかに応じて、次のいずれかのコマンドを使用して、バックアップを MySQL Docker コンテナにコピーします。

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Docker コンテナまたは Podman コンテナのどちらを使用しているかに応じて、次のいずれかのコマンドを使用して MySQL コンテナ シェルに入ります。

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. コンテナ シェルで、「env」をデプロイします。

5. MySQL DB パスワードが必要になるので、キー「MYSQL_ROOT_PASSWORD」の値をコピーします。
6. 次のコマンドを使用して、 NetApp Backup and Recovery MySQL DB を復元します。

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. 次の SQL コマンドを使用して、 NetApp Backup and Recovery MySQL DB が正しく復元されたことを確認します。

```
mysql -u root -p cloud_backup
```

8. パスワードを入力してください。

```
mysql> show tables;
mysql> select * from volume;
```

9. 表示されるボリュームが元の環境に存在していたボリュームと同じであることを確認します。

インデックスカタログファイルを復元する

1. インデックス付きカタログのバックアップ zip ファイル (サンプル ファイル名は「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」を使用します) を、バックアップ場所から「/opt/application/netapp/cbs」フォルダー内の新しいコンソール エージェント ホストにコピーします。
2. 次のコマンドを使用して、「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」ファイルを解凍します。

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. **ls** コマンドを実行して、フォルダー「catalogdb1」が作成され、その下にサブフォルダー「changes」と「snapshots」が作成されていることを確認します。

ONTAPクラスタと**StorageGRID**システムを発見

1. "オンプレミスのONTAPシステムをすべて見る"以前の環境で利用可能でした。これには、S3 サーバーとして使用したONTAPシステムが含まれます。
2. "StorageGRIDシステムを発見"。

StorageGRID環境の詳細を設定する

元のコンソールエージェントセットアップで設定されたとおりに、 ONTAPシステムに関連付けられたStorageGRIDシステムの詳細を追加します。 "NetApp ConsoleAPI" 。

次の情報は、 NetApp Console3.9.xx 以降のプライベート モード インストールに適用されます。古いバージョンの場合は、次の手順に従います。 "DarkSite クラウドバックアップ: MySQL とインデックスカタログのバックアップと復元" 。

StorageGRIDにデータをバックアップするシステムごとにこれらの手順を実行する必要があります。

1. 次の oauth/token API を使用して認証トークンを抽出します。

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

IP アドレス、ユーザー名、パスワードはカスタム値ですが、アカウント名はカスタム値ではありません。アカウント名は常に「account-DARKSITE1」になります。また、ユーザー名には電子メール形式の名前を使用する必要があります。

この API は次のような応答を返します。認証トークンは以下のように取得できます。

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. tenancy/external/resource API を使用して、システム ID と X-Agent-Id を抽出します。

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

この API は次のような応答を返します。「resourceIdentifier」の下の値は *WorkingEnvironment Id* を示し、「agentId」の下の値は *x-agent-id* を示します。

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. システムに関連付けられているStorageGRIDシステムの詳細を使用して、 NetApp Backup and Recovery データベースを更新します。以下に示すように、 StorageGRIDの完全修飾ドメイン名と、アクセス キーおよびストレージ キーを必ず入力してください。

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

NetApp Backup and Recovery設定を確認する

1. 各ONTAPシステムを選択し、右側のパネルのバックアップおよびリカバリ サービスの横にある [バックアップの表示] をクリックします。

   ボリュームに対して作成されたすべてのバックアップが表示されます。

2. 復元ダッシュボードの「検索と復元」セクションで、「インデックス設定」をクリックします。

   以前にインデックスカタログが有効になっていたシステムが有効なままであることを確認します。

3. 「検索と復元」ページから、いくつかのカタログ検索を実行して、インデックス付きカタログの復元が正常に完了したことを確認します。

NetApp Backup and Recoveryを使用して**ONTAP**システムのバックアップを管理します

NetApp Backup and Recoveryを使用すると、バックアップ スケジュールの変更、ボリューム バックアップの有効化/無効化、バックアップの一時停止、バックアップの削除、バックアップの強制削除などを行って、 Cloud Volumes ONTAPおよびオンプレミスのONTAPシステムのバックアップを管理できます。これには、スナップショット、複製されたボリューム、オブジェクト ストレージ内のバックアップ ファイルなど、すべての種類のバックアップが含まれます。NetApp Backup and Recovery の登録を解除することもできます。

ストレージ システム上またはクラウド プロバイダー環境からバックアップ ファイルを直接管理または変更しないでください。これによりファイルが破損し、サポートされない構成になる可能性があります。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

システム内のボリュームのバックアップステータスを表示します

ボリューム バックアップ ダッシュボードで、現在バックアップ中のすべてのボリュームのリストを表示できます。これには、スナップショット、複製されたボリューム、オブジェクト ストレージ内のバックアップ ファイルなど、すべての種類のバックアップが含まれます。現在バックアップされていないシステム内のボリュームを表示することもできます。

手順

1. コンソール 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. ボリューム メニューを選択して、 Cloud Volumes ONTAPおよびオンプレミスのONTAPシステムのバックアップされたボリュームのリストを表示します。
3. 特定のシステム内の特定のボリュームを探している場合は、システムとボリューム別にリストを絞り込むことができます。検索フィルターを使用したり、ボリューム スタイル (FlexVolまたはFlexGroup)、ボリューム タイプなどに基づいて列を並べ替えたりすることもできます。

   追加の列（集計、セキュリティ スタイル（Windows または UNIX）、スナップショット ポリシー、レプリケーション ポリシー、バックアップ ポリシー）を表示するには、プラス記号を選択します。

4. 「既存の保護」列で保護オプションのステータスを確認します。3 つのアイコンは、「ローカル スナップショット」、「複製されたボリューム」、「オブジェクト ストレージ内のバックアップ」を表します。

   各アイコンは、そのバックアップ タイプがアクティブになっているときは点灯し、バックアップ タイプが非アクティブになっているときは灰色になります。各アイコンの上にカーソルを置くと、使用されているバックアップ ポリシーや、各バックアップ タイプに関するその他の関連情報が表示されます。

システム内の追加ボリュームでバックアップを有効にする

NetApp Backup and Recovery を最初に有効にしたときに、システム内の一部のボリュームでのみバックアップをアクティブ化した場合は、後で追加のボリュームでバックアップをアクティブ化できます。

手順

1. ボリューム*タブから、バックアップをアクティブ化するボリュームを特定し、アクションメニューを選択します。 ••• 行の末尾にある **[*3-2-1 保護を有効にする]** を選択します。
2. [バックアップ戦略の定義] ページで、バックアップ アーキテクチャを選択し、ローカル スナップショット、レプリケートされたボリューム、およびバックアップ ファイルのポリシーとその他の詳細を定義します。このシステムでアクティブ化した初期ボリュームからのバックアップ オプションの詳細を参照してください。次に「次へ」を選択します。
3. このボリュームのバックアップ設定を確認し、「バックアップのアクティブ化」を選択します。

既存のボリュームに割り当てられたバックアップ設定を変更する

ポリシーが割り当てられている既存のボリュームに割り当てられたバックアップ ポリシーを変更できます。ローカル スナップショット、複製されたボリューム、およびバックアップ ファイルのポリシーを変更できます。ボリュームに適用する新しいスナップショット、レプリケーション、またはバックアップ ポリシーがすでに存在している必要があります。

単一ボリュームのバックアップ設定を編集する

手順

1. ボリューム*メニューから、ポリシー設定を変更するボリュームを見つけ、アクションメニューを選択します。 ••• 行の末尾にある **[*バックアップ戦略の編集]** を選択します。
2. [バックアップ戦略の編集] ページで、ローカル スナップショット、複製されたボリューム、およびバックアップ ファイルの既存のバックアップ ポリシーを変更し、[次へ] を選択します。

   このクラスターのNetApp Backup and Recovery をアクティブ化するときに、初期バックアップ ポリシーでクラウド バックアップに対して *DataLock* と *Ransomware Resilience* を有効にした場合は、DataLock で構成された他のポリシーのみが表示されます。また、 NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、DataLock が設定されていない他のクラウド バックアップ ポリシーのみが表示されます。

3. このボリュームのバックアップ設定を確認し、「バックアップのアクティブ化」を選択します。

複数のボリュームのバックアップ設定を編集する

複数のボリュームで同じバックアップ設定を使用する場合は、複数のボリュームで同時にバックアップ設定をアクティブ化または編集できます。バックアップ設定がないボリューム、スナップショット設定のみがあるボリューム、クラウドへのバックアップ設定のみがあるボリュームなどを選択し、さまざまなバックアップ設定を持つこれらすべてのボリュームに対して一括変更を行うことができます。

複数のボリュームを操作する場合、すべてのボリュームに次の共通の特性が必要です。

- 同じシステム
- 同じスタイル（FlexVolまたはFlexGroupボリューム）
- 同じタイプ（読み取り/書き込みまたはデータ保護ボリューム）

バックアップに 5 つ以上のボリュームが有効になっている場合、 NetApp Backup and Recovery は一度に 5 つのボリュームのみを初期化します。これらが完了すると、すべてのボリュームが初期化されるまで 5 つのグループごとに続行されます。

手順

1. ボリューム タブから、ボリュームが存在するシステムでフィルタリングします。
2. バックアップ設定を管理するボリュームをすべて選択します。
3. 設定するバックアップ アクションの種類に応じて、[一括アクション] メニューのボタンをクリックします。

バックアップアクション...	このボタンを選択してください...
スナップショットバックアップ設定を管理する	ローカルスナップショットの管理
レプリケーションバックアップ設定を管理する	レプリケーションの管理

バックアップアクション...	このボタンを選択してください...
クラウドへのバックアップ設定を管理する	バックアップの管理
複数の種類のバックアップ設定を管理します。このオプションを使用すると、バックアップ アーキテクチャも変更できます。	バックアップとリカバリの管理

4. 表示されるバックアップ ページで、ローカル スナップショット、複製されたボリューム、またはバックアップ ファイルの既存のバックアップ ポリシーを変更し、[保存] を選択します。

   このクラスターのNetApp Backup and Recovery をアクティブ化するときに、初期バックアップ ポリシーでクラウド バックアップに対して *DataLock* と *Ransomware Resilience* を有効にした場合は、DataLock で構成された他のポリシーのみが表示されます。また、 NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、DataLock が設定されていない他のクラウド バックアップ ポリシーのみが表示されます。

いつでも手動でボリュームバックアップを作成

いつでもオンデマンド バックアップを作成して、ボリュームの現在の状態をキャプチャできます。これは、ボリュームに非常に重要な変更が加えられ、そのデータを保護するために次回のスケジュールされたバックアップまで待ちたくない場合に役立ちます。この機能を使用すると、現在バックアップされていないボリュームのバックアップを作成し、その現在の状態をキャプチャすることもできます。

ボリュームのオブジェクト ストアにアドホック スナップショットまたはバックアップを作成できます。アドホック複製ボリュームを作成することはできません。

バックアップ名にはタイムスタンプが含まれるため、オンデマンド バックアップを他のスケジュールされたバックアップと区別できます。

このクラスターのNetApp Backup and Recovery をアクティブ化するときに *DataLock* と *Ransomware Resilience* を有効にした場合、オンデマンド バックアップも DataLock で構成され、保持期間は 30 日間になります。アドホック バックアップではランサムウェア スキャンはサポートされていません。"DataLockとランサムウェア対策について詳しくはこちら"。

アドホック バックアップを作成すると、ソース ボリュームにスナップショットが作成されます。このスナップショットは通常のスナップショット スケジュールの一部ではないため、オフにはなりません。バックアップが完了したら、ソース ボリュームからこのスナップショットを手動で削除することをお勧めします。これにより、このスナップショットに関連するブロックが解放されます。スナップショットの名前は `cbs-snapshot-adhoc-`。 "ONTAP CLIを使用してスナップショットを削除する方法をご覧ください" 。

> オンデマンド ボリューム バックアップは、データ保護ボリュームではサポートされていません。

手順

1. ボリューム*タブから、•••ボリュームを選択し、[*バックアップ] > [アドホック バックアップの作成*] を選択します。

バックアップが作成されるまで、そのボリュームのバックアップ ステータス列には「進行中」と表示されます。

各ボリュームのバックアップのリストを表示する

各ボリュームに存在するすべてのバックアップ ファイルのリストを表示できます。このページには、ソースボリューム、宛先の場所、最後に実行されたバックアップ、現在のバックアップ ポリシー、バックアップ ファイルのサイズなどのバックアップの詳細が表示されます。

手順

1. *ボリューム*タブから、…ソースボリュームの[ボリュームの詳細を表示]を選択します。

   ボリュームの詳細とスナップショットのリストが表示されます。

2. スナップショット、レプリケーション、または*バックアップ*を選択すると、各バックアップ タイプのすべてのバックアップ ファイルのリストが表示されます。

オブジェクトストレージ内のボリュームバックアップでランサムウェアスキャンを実行する

NetApp Backup and Recovery は、オブジェクト ファイルへのバックアップが作成される際、およびバックアップ ファイルからデータが復元される際に、バックアップ ファイルをスキャンしてランサムウェア攻撃の証拠を探します。また、いつでもオンデマンド スキャンを実行して、オブジェクト ストレージ内の特定のバックアップ ファイルの使用可能かどうかを確認することもできます。これは、特定のボリュームでランサムウェアの問題が発生し、そのボリュームのバックアップが影響を受けていないことを確認したい場合に役立ちます。

この機能は、ボリューム バックアップがONTAP 9.11.1 以降のシステムから作成され、オブジェクトへのバックアップ ポリシーで *DataLock* および *Ransomware Resilience* が有効になっている場合にのみ使用できます。

手順

1. *ボリューム*タブから、…ソースボリュームの[ボリュームの詳細を表示]を選択します。

   ボリュームの詳細が表示されます。

2. バックアップ を選択すると、オブジェクト ストレージ内のバックアップ ファイルのリストが表示されます。
3. 選択…ランサムウェアをスキャンするボリューム バックアップ ファイルを選択し、[ランサムウェアのスキャン] をクリックします。

   ランサムウェア耐性列には、スキャンが進行中であることが示されます。

ソースボリュームとのレプリケーション関係を管理する

2 つのシステム間のデータ レプリケーションを設定したら、データ レプリケーションの関係を管理できます。

手順

1. *ボリューム*タブから、…ソースボリュームに対して*レプリケーション*オプションを選択します。利用可能なオプションをすべて確認できます。
2. 実行するレプリケーション アクションを選択します。

   次の表では、利用可能なアクションについて説明します。

アクション	説明
ビューのレプリケーション	ボリューム関係の詳細（転送情報、最終転送情報、ボリュームの詳細、関係に割り当てられた保護ポリシーに関する情報）を表示します。
更新レプリケーション	増分転送を開始し、宛先ボリュームを更新してソース ボリュームと同期させます。
レプリケーションを一時停止	スナップショットの増分転送を一時停止して、宛先ボリュームを更新します。増分更新を再開したい場合は、後で再開できます。
レプリケーションを中断する	ソース ボリュームと宛先ボリュームの関係を解除し、宛先ボリュームをデータ アクセス用にアクティブ化して、読み取り/書き込み可能にします。このオプションは通常、データの破損、誤った削除、オフライン状態などのイベントによりソース ボリュームがデータを提供できない場合に使用されます。https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["ONTAPドキュメントで、データアクセス用に宛先ボリュームを設定し、ソースボリュームを再アクティブ化する方法について学習します。"^]
レプリケーションを中止する	このボリュームの宛先システムへのバックアップを無効にし、ボリュームを復元する機能も無効にします。既存のバックアップは削除されません。これによって、ソース ボリュームと宛先ボリューム間のデータ保護関係は削除されません。
逆再同期	ソース ボリュームと宛先ボリュームの役割を逆にします。元のソース ボリュームの内容は、宛先ボリュームの内容によって上書きされます。これは、オフラインになったソース ボリュームを再アクティブ化する場合に役立ちます。最後のデータ複製からソース ボリュームが無効になった時点までの間に元のソース ボリュームに書き込まれたデータは保持されません。
関係の削除	ソース ボリュームと宛先ボリューム間のデータ保護関係を削除します。これにより、ボリューム間でデータのレプリケーションは行われなくなります。このアクションでは、データ アクセス用に宛先ボリュームがアクティブ化されません。つまり、読み取り/書き込み可能になりません。システム間に他のデータ保護関係がない場合、このアクションにより、クラスタ ピア関係とストレージ VM (SVM) ピア関係も削除されます。

結果

アクションを選択すると、コンソールは関係を更新します。

既存のクラウドへのバックアップ ポリシーを編集する

システム内のボリュームに現在適用されているバックアップ ポリシーの属性を変更できます。バックアップ ポリシーを変更すると、そのポリシーを使用している既存のすべてのボリュームに影響します。

- このクラスターのNetApp Backup and Recovery をアクティブ化するときに、初期ポリシーで *DataLock* と *Ransomware Resilience* を有効にした場合、編集するポリシーはすべて同じ DataLock 設定 (ガバナンスまたはコンプライアンス) で構成する必要があります。また、 NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、現在 DataLock を有効にすることはできません。
- AWS でバックアップを作成するときに、 NetApp Backup and Recoveryをアクティブ化するときに最初のバックアップポリシーで *S3 Glacier* または *S3 Glacier Deep Archive* を選択した場合、バックアップポリシーを編集するときに使用できるアーカイブ層はその層のみになります。また、最初のバックアップ ポリシーでアーカイブ層を選択しなかった場合は、ポリシーを編集するときに、*S3 Glacier* が唯一のアーカイブ オプションになります。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定_ページで、•••ポリシー設定を変更するシステムを選択し、[ポリシーの管理] を選択します。
3. [ポリシーの管理] ページで、そのシステムで変更するバックアップ ポリシーの [編集] を選択します。
4. [ポリシーの編集] ページで下矢印を選択して [ラベルと保持] セクションを展開し、スケジュールやバックアップの保持を変更して [保存] を選択します。

   クラスタでONTAP 9.10.1 以降を実行している場合は、一定の日数後にアーカイブ ストレージへのバックアップの階層化を有効または無効にするオプションもあります。

   "AWS アーカイブストレージの使用について詳しくはこちら"。"Azure アーカイブ ストレージの使用について詳しく見る"。"Google アーカイブ ストレージの使用について詳しくは、こちらをご覧ください。"。（ ONTAP 9.12.1 が必要です。）

   アーカイブへのバックアップの階層化を停止した場合、アーカイブ ストレージに階層化されたバックアップ ファイルはすべてその階層に残り、標準階層に自動的に戻されないことに注意してください。新しいボリューム バックアップのみが標準層に保存されます。

新しいクラウドへのバックアップポリシーを追加する

システムに対してNetApp Backup and Recovery を有効にすると、最初に選択したすべてのボリュームが、定義したデフォルトのバックアップ ポリシーを使用してバックアップされます。異なる復旧ポイント目標 (RPO) を持つ特定のボリュームに異なるバックアップ ポリシーを割り当てる場合は、そのクラスターに追加のポリシーを作成し、それらのポリシーを他のボリュームに割り当てることができます。

システム内の特定のボリュームに新しいバックアップ ポリシーを適用する場合は、まずそのバックアップ ポリシーをシステムに追加する必要があります。そうするとそのシステム内のボリュームにポリシーを適用する。

- このクラスターのNetApp Backup and Recovery をアクティブ化するときに初期ポリシーで *DataLock and Ransomware Resilience* を有効にした場合、作成する追加ポリシーは同じ DataLock 設定 (ガバナンスまたはコンプライアンス) で構成する必要があります。また、NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、DataLock を使用する新しいポリシーを作成することはできません。
- AWS でバックアップを作成するときに、 NetApp Backup and Recoveryをアクティブ化するときに最初のバックアップポリシーで *S3 Glacier* または *S3 Glacier Deep Archive* を選択した場合、その層がそのクラスターの将来のバックアップポリシーで使用できる唯一のアーカイブ層になります。また、最初のバックアップ ポリシーでアーカイブ層を選択しなかった場合は、将来のポリシーでは *S3 Glacier* が唯一のアーカイブ オプションになります。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定_ページで、•••新しいポリシーを追加するシステムの [ポリシーの管理] を選択します。
3. [ポリシーの管理] ページで、[新しいポリシーの追加] を選択します。
4. [新しいポリシーの追加] ページで下矢印を選択して [ラベルと保持] セクションを展開し、スケジュールとバックアップの保持期間を定義して [保存] を選択します。

クラスタでONTAP 9.10.1 以降を実行している場合は、一定の日数後にアーカイブ ストレージへのバックアップの階層化を有効または無効にするオプションもあります。

"AWS アーカイブストレージの使用について詳しくはこちら"。"Azure アーカイブ ストレージの使用について詳しく見る"。"Google アーカイブ ストレージの使用について詳しくは、こちらをご覧ください。"。（ ONTAP 9.12.1 が必要です。）

バックアップの削除

NetApp Backup and Recovery を使用すると、単一のバックアップ ファイルを削除したり、ボリュームのすべてのバックアップを削除したり、システム内のすべてのボリュームのすべてのバックアップを削除したりできます。バックアップが不要になった場合、またはソース ボリュームを削除してすべてのバックアップを削除する場合は、すべてのバックアップを削除する必要がある場合があります。

DataLock とランサムウェア保護を使用してロックしたバックアップ ファイルは削除できません。ロックされたバックアップ ファイルを 1 つ以上選択した場合、UI から「削除」オプションは使用できません。

> バックアップがあるシステムまたはクラスターを削除する予定の場合は、システムを削除する前にバックアップを削除する必要があります。 NetApp Backup and Recoveryでは、システムを削除してもバックアップは自動的に削除されません。また、システムの削除後にバックアップを削除するための UI は現在サポートされていません。残りのバックアップについては、オブジェクト ストレージ コストが引き続き請求されます。

システムのすべてのバックアップファイルを削除する

システムのオブジェクト ストレージ上のすべてのバックアップを削除しても、このシステム内のボリュームの将来のバックアップは無効になりません。システム内のすべてのボリュームのバックアップの作成を停止したい場合は、バックアップを非アクティブ化できます。ここで説明されているように 。

このアクションはスナップショットや複製されたボリュームには影響しないことに注意してください。これらの種類のバックアップ ファイルは削除されません。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. 選択…すべてのバックアップを削除するシステムを選択し、[すべてのバックアップを削除] を選択します。
3. 確認ダイアログボックスで、システムの名前を入力します。
4. *詳細設定*を選択します。
5. バックアップの強制削除: すべてのバックアップを強制的に削除するかどうかを指定します。

   極端なケースでは、 NetApp Backup and Recovery がバックアップにアクセスできないようにする必要がある場合もあります。これは、たとえば、サービスがバックアップ バケットにアクセスできなくなった場合や、バックアップが DataLock で保護されているが不要になった場合に発生する可能性があります。以前は、これらを自分で削除することはできず、 NetAppサポートに連絡する必要がありました。このリリースでは、バックアップを強制的に削除するオプション (ボリューム レベルとシステム レベル) を使用できるようになりました。

このオプションは慎重に使用し、極端なクリーンアップが必要な場合にのみ使用してください。オブジェクト ストレージでバックアップが削除されていない場合でも、 NetApp Backup and Recovery はこれらのバックアップにアクセスできなくなります。クラウド プロバイダーにアクセスして、バックアップを手動で削除する必要があります。

6. *削除*を選択します。

ボリュームのすべてのバックアップファイルを削除する

ボリュームのすべてのバックアップを削除すると、そのボリュームの今後のバックアップも無効になります。

手順

1. *ボリューム*タブから、…ソースボリュームの[詳細とバックアップリスト]を選択します。

   すべてのバックアップ ファイルのリストが表示されます。

2. アクション > *すべてのバックアップを削除*を選択します。
3. ボリューム名を入力します。
4. *詳細設定*を選択します。
5. バックアップの強制削除: すべてのバックアップを強制的に削除するかどうかを指定します。

   極端なケースでは、 NetApp Backup and Recovery がバックアップにアクセスできないようにする必要がある場合もあります。これは、たとえば、サービスがバックアップ バケットにアクセスできなくなった場合や、バックアップが DataLock で保護されているが不要になった場合に発生する可能性があります。以前は、これらを自分で削除することはできず、 NetAppサポートに連絡する必要がありました。このリリースでは、バックアップを強制的に削除するオプション (ボリューム レベルとシステム レベル) を使用できるようになりました。

   このオプションは慎重に使用し、極端なクリーンアップが必要な場合にのみ使用してください。オブジェクト ストレージでバックアップが削除されていない場合でも、 NetApp Backup and Recovery はこれらのバックアップにアクセスできなくなります。クラウド プロバイダーにアクセスして、バックアップを手動で削除する必要があります。

6. *削除*を選択します。

ボリュームの単一のバックアップファイルを削除する

不要になったバックアップ ファイルを 1 つ削除できます。これには、ボリューム スナップショットの単一のバックアップまたはオブジェクト ストレージ内のバックアップの単一のバックアップの削除が含まれます。

複製されたボリューム (データ保護ボリューム) は削除できません。

手順

1. *ボリューム*タブから、…ソースボリュームの[ボリュームの詳細を表示]を選択します。

   ボリュームの詳細が表示され、スナップショット、レプリケーション、または*バックアップ*を選択して、ボリュームのすべてのバックアップ ファイルのリストを表示できます。デフォルトでは、利用可能なスナップショットが表示されます。

2. 削除するバックアップ ファイルの種類を確認するには、[スナップショット] または [バックアップ] を選択します。
3. 選択•••削除するボリューム バックアップ ファイルを選択し、[削除] を選択します。
4. 確認ダイアログボックスで、[削除] を選択します。

ボリュームバックアップ関係を削除する

ボリュームのバックアップ関係を削除すると、新しいバックアップ ファイルの作成を停止し、ソース ボリュームを削除しながら、既存のバックアップ ファイルはすべて保持する場合に、アーカイブ メカニズムが提供されます。これにより、ソース ストレージ システムのスペースをクリアしながら、必要に応じて将来バックアップ ファイルからボリュームを復元できるようになります。

必ずしもソースボリュームを削除する必要はありません。ボリュームのバックアップ関係を削除し、ソースボリュームを保持することができます。この場合、後でボリューム上のバックアップを「アクティブ化」することができます。この場合、元のベースライン バックアップ コピーが引き続き使用されます。新しいベースライン バックアップ コピーは作成されず、クラウドにエクスポートされません。バックアップ関係を再アクティブ化すると、ボリュームにはデフォルトのバックアップ ポリシーが割り当てられることに注意してください。

この機能は、システムでONTAP 9.12.1 以降を実行している場合にのみ使用できます。

NetApp Backup and Recoveryユーザー インターフェイスからソース ボリュームを削除することはできません。ただし、コンソールの*システム*ページでボリュームの詳細ページを開いて、 "そこからボリュームを削除します" 。

> 関係が削除されると、個々のボリュームのバックアップ ファイルを削除することはできません。ただし、ボリュームのすべてのバックアップを削除することは可能です。

手順

1. ボリューム*タブから、•••ソースボリュームの*バックアップ > *関係の削除*を選択します。

システムの**NetApp Backup and Recovery**を非アクティブ化する

システムに対してNetApp Backup and Recoveryを非アクティブ化すると、システム上の各ボリュームのバックアップが無効になり、ボリュームを復元する機能も無効になります。既存のバックアップは削除されません。これにより、このシステムからバックアップ サービスの登録が解除されるわけではありません。基本的には、すべてのバックアップおよび復元アクティビティを一定期間一時停止できるようになります。

バックアップに使用する容量については、クラウドプロバイダーからオブジェクトストレージの料金が引き続き請求されます。バックアップを削除する 。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、•••バックアップを無効にするシステムで、[バックアップの無効化] を選択します。
3. 確認ダイアログボックスで、「非アクティブ化」を選択します。

バックアップが無効になっている間、そのシステムに対して バックアップをアクティブ化 ボタンが表示されます。そのシステムのバックアップ機能を再度有効にする場合は、このボタンを選択できます。

システムの**NetApp Backup and Recovery**の登録を解除する

バックアップ機能を使用する必要がなくなり、そのシステムでのバックアップに対する課金を停止したい場合は、システムのNetApp Backup and Recovery の登録を解除できます。通常、この機能は、システムを削除する予定があり、バックアップ サービスをキャンセルする場合に使用されます。

クラスターのバックアップが保存される宛先オブジェクト ストアを変更する場合にも、この機能を使用できます。システムからNetApp Backup and Recoveryを登録解除した後、新しいクラウド プロバイダー情報を使用してそのクラスターに対してNetApp Backup and Recovery を有効にすることができます。

NetApp Backup and Recoveryを登録解除する前に、次の手順をこの順序で実行する必要があります。

- システムのNetApp Backup and Recoveryを無効にします
- そのシステムのすべてのバックアップを削除します

これら 2 つのアクションが完了するまで、登録解除オプションは使用できません。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定ページ_から、•••バックアップ サービスを登録解除するシステムで、[登録解除] を選択します。
3. 確認ダイアログボックスで、[登録解除] を選択します。

ONTAPバックアップからの復元

NetApp Backup and Recoveryを使用してバックアップファイルから**ONTAP**データを復元する

ONTAPボリューム データのバックアップは、スナップショットとして、複製されたボリューム上、またはオブジェクト ストレージに保存されます。特定の時点でこれらのいずれかの場所からデータを復元できます。 NetApp Backup and Recovery を使用すると、必要に応じてボリューム全体、フォルダ、または個々のファイルを復元できます。

NetApp Backup and Recoveryのワークロードを切り替えるには、"さまざまなNetApp Backup and Recoveryワークロードに切り替える" 。

- ボリューム (新しいボリュームとして) を元のシステム、同じクラウド アカウントを使用している別のシステム、またはオンプレミスのONTAPシステムに復元できます。
- フォルダー を元のシステムのボリューム、同じクラウド アカウントを使用している別のシステムのボリューム、またはオンプレミスのONTAPシステム上のボリュームに復元できます。
- ファイル を元のシステムのボリューム、同じクラウド アカウントを使用している別のシステムのボリューム、またはオンプレミスのONTAPシステム上のボリュームに復元できます。

実稼働システムにデータを復元するには、有効なNetApp Backup and Recoveryライセンスが必要です。

要約すると、ボリューム データをONTAPシステムに復元するために使用できる有効なフローは次のとおりです。

- バックアップファイル → 復元されたボリューム
- 複製されたボリューム → 復元されたボリューム
- スナップショット → 復元されたボリューム

復元操作が完了しない場合は、ジョブ モニターに「失敗」と表示されるまで待ってから、復元操作を再試行してください。

ONTAPデータのリストアに関する制限については、"ONTAPボリュームのバックアップとリストアの制限" 。

復元ダッシュボード

復元ダッシュボードを使用して、ボリューム、フォルダー、およびファイルの復元操作を実行します。復元ダッシュボードにアクセスするには、コンソール メニューから [バックアップと復元] を選択し、[復元] タブを選択します。選択することもできます > サービス パネルのバックアップと復元サービスから 復元ダッシュボードを表示 します。

NetApp Backup and Recovery は少なくとも 1 つのシステムに対してすでにアクティブ化されており、初期バックアップ ファイルが存在している必要があります。

復元ダッシュボードでは、バックアップ ファイルからデータを復元する方法として、「参照と復元」と「検索と復元」の 2 つの方法が提供されています。

参照と復元と検索と復元の比較

一般的に言えば、参照と復元 は、過去 1 週間または 1 か月間の特定のボリューム、フォルダー、またはファイルを復元する必要がある場合に適しています。この場合、ファイルの名前と場所、およびファイルが最後に正常な状態であった日付が分かっています。通常、ボリューム、フォルダー、またはファイルを復元する必要があるが、正確な名前や、それらが存在するボリューム、またはそれらが最後に正常な状態であった日付を覚えていない場合は、検索と復元 の方が適しています。

この表は、2 つの方法の機能の比較を示しています。

閲覧と復元	検索と復元
フォルダー形式の構造を参照して、単一のバックアップ ファイル内のボリューム、フォルダー、またはファイルを見つけます。	部分的または完全なボリューム名、部分的または完全なフォルダー/ファイル名、サイズの範囲、追加の検索フィルターを使用して、すべてのバックアップ ファイル 間でボリューム、フォルダー、またはファイルを検索します。
ファイルが削除または名前変更され、ユーザーが元のファイル名を知らない場合、ファイルの回復は処理されません。	新しく作成/削除/名前変更されたディレクトリと新しく作成/削除/名前変更されたファイルを処理します
クイック復元がサポートされています。	クイック復元はサポートされていません。

この表には、バックアップ ファイルが存在する場所に基づいて、有効な復元操作の一覧が示されています。

バックアップタイプ	閲覧と復元			検索と復元		
	ボリュームを復元	ファイルを復元	フォルダを復元	ボリュームを復元	ファイルを復元	フォルダを復元
Snapshot	はい	いいえ	いいえ	はい	はい	はい
複製ボリューム	はい	いいえ	いいえ	はい	はい	はい
バックアップファイル	はい	はい	はい	はい	はい	はい

いずれかの復元方法を使用する前に、リソース要件を満たすように環境を構成します。詳細については、次のセクションを参照してください。

使用する復元操作の種類に応じた要件と復元手順を参照してください。

- "参照と復元を使用してボリュームを復元する"
- "参照と復元を使用してフォルダとファイルを復元する"
- "検索と復元を使用してボリューム、フォルダ、ファイルを復元する"

検索と復元を使用して**ONTAP**バックアップから復元する

検索と復元を使用して、 ONTAPバックアップ ファイルからボリューム、フォルダー、またはファイルを回復できます。検索と復元を使用すると、正確なシステム名、ボリューム名、ファイル名を必要とせずに、すべてのバックアップ (ローカル スナップショット、複製されたボリューム、オブジェクト ストレージを含む) を検索できます。

通常、ローカル スナップショットまたは複製されたボリュームからの復元は、オブジェクト ストレージからの復元よりも高速でコストも低くなります。

ボリューム全体を復元する場合、 NetApp Backup and Recovery はバックアップ データを使用して新しいボリュームを作成します。元のシステム、同じクラウド アカウント内の別のシステム、またはオンプレミスのONTAPシステムに復元できます。フォルダーとファイルは、元の場所、同じシステム内の別のボリューム、同じクラウド アカウント内の別のシステム、またはオンプレミス システムに復元できます。

復元機能はONTAP のバージョンによって異なります。

- フォルダ**:** ONTAP 9.13.0 以降を使用すると、すべてのファイルとサブフォルダを含むフォルダを復元できます。それ以前のバージョンでは、フォルダ内のファイルのみを復元できます。
- アーカイブ ストレージ**:** アーカイブ ストレージ (ONTAP 9.10.1 以降で利用可能) からの復元は遅くなり、追加コストが発生する可能性があります。
- 宛先クラスタの要件**:**
  - ボリュームリストア: ONTAP 9.10.1 以上
  - ファイル復元: ONTAP 9.11.1 以上
  - Google Archive およびStorageGRID: ONTAP 9.12.1 以上
  - フォルダの復元: ONTAP 9.13.1 以上

"AWSアーカイブストレージからの復元の詳細"。"Azure アーカイブ ストレージからの復元の詳細"。"Google アーカイブ ストレージからの復元の詳細"。

- オブジェクト ストレージ内のバックアップ ファイルに DataLock および Ransomware 保護が設定されている場合、 ONTAPバージョンが 9.13.1 以上の場合にのみフォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、バックアップ ファイルからボリューム全体を復元し、必要なフォルダーとファイルにアクセスできます。
- オブジェクト ストレージ内のバックアップ ファイルがアーカイブ ストレージに存在する場合、 ONTAPバージョンが 9.13.1 以上の場合にのみ、フォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、アーカイブされていない新しいバックアップ ファイルからフォルダを復元するか、アーカイブされたバックアップからボリューム全体を復元して、必要なフォルダとファイルにアクセスすることができます。
- Azure アーカイブ ストレージからStorageGRIDシステムにデータを復元する場合、「高」復元優先度はサポートされません。
- 現在、 ONTAP S3 オブジェクト ストレージ内のボリュームからのフォルダーの復元はサポートされていません。

開始する前に、復元するボリュームまたはファイルの名前または場所をある程度把握しておく必要があります。

検索と復元がサポートされているシステムとオブジェクト ストレージ プロバイダー

セカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップ ファイルから、次のシステムにONTAPデータを復元できます。スナップショットはソース システム上に存在し、同じシステムにのみ復元できます。

注意: ボリュームとファイルはどのタイプのバックアップ ファイルからでも復元できますが、現時点では、フォルダーを復元できるのはオブジェクト ストレージ内のバックアップ ファイルからのみです。

バックアップファイルの場所		宛先システム
オブジェクトストア（バックアップ）	セカンダリシステム（レプリケーション）	
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP
Azure ブロブ	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム
Google Cloud Storage	Google オンプレミスONTAPシステムのCloud Volumes ONTAP	Google オンプレミスONTAPシステムのCloud Volumes ONTAP
NetAppStorageGRID	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム
ONTAP S3	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム

検索と復元の場合、コンソール エージェントは次の場所にインストールできます。

- Amazon S3の場合、コンソールエージェントはAWSまたはオンプレミスに導入できます。

- Azure Blobの場合、コンソールエージェントはAzureまたはオンプレミスに展開できます。
- Google Cloud Storage の場合、コンソール エージェントを Google Cloud Platform VPC にデプロイする必要があります。
- StorageGRIDの場合、コンソールエージェントは、インターネットアクセスの有無にかかわらず、お客様の敷地内に導入する必要があります。
- ONTAP S3の場合、コンソールエージェントは、オンプレミス（インターネットアクセスの有無にかかわらず）またはクラウドプロバイダー環境に導入できます。

「オンプレミスのONTAPシステム」への参照には、 FAS、 AFF、およびONTAP Selectシステムが含まれることに注意してください。

検索と復元の前提条件

検索と復元を有効にする前に、環境が次の要件を満たしていることを確認してください。

- クラスタの要件：
  - ONTAPバージョンは 9.8 以上である必要があります。
  - ボリュームが存在するストレージ VM (SVM) には、データ LIF が設定されている必要があります。
  - ボリューム上で NFS を有効にする必要があります (NFS ボリュームと SMB/CIFS ボリュームの両方がサポートされています)。
  - SnapDiff RPC サーバを SVM 上でアクティブ化する必要があります。システムでインデックス作成を有効にすると、コンソールはこれを自動的に実行します。(SnapDiff は、スナップショット間のファイルとディレクトリの違いをすばやく識別するテクノロジーです。)
- NetApp、検索と復元の回復力を高めるために、コンソール エージェントに別のボリュームをマウントすることを推奨しています。手順については、ボリュームをマウントしてカタログのインデックスを再作成する 。

レガシー検索と復元の前提条件（インデックスカタログ **v1** を使用）

従来のインデックスを使用する場合の検索と復元の要件は次のとおりです。

- AWS 要件:
  - コンソールに権限を付与するユーザー ロールに、特定の Amazon Athena、AWS Glue、および AWS S3 権限を追加する必要があります。"すべての権限が正しく設定されていることを確認してください"。

    以前に設定したコンソール エージェントでNetApp Backup and Recoveryをすでに使用していた場合は、コンソール ユーザー ロールに Athena および Glue 権限を追加する必要があることに注意してください。これらは検索と復元に必要です。

- Azure の要件:
  - Azure Synapse Analytics リソース プロバイダー (「Microsoft.Synapse」と呼ばれます) をサブスクリプションに登録する必要があります。 "このリソースプロバイダーをサブスクリプションに登録する方法をご覧ください" 。リソース プロバイダーを登録するには、サブスクリプションの所有者 または 投稿者 である必要があります。
  - コンソールに権限を付与するユーザー ロールに、特定の Azure Synapse ワークスペースおよび Data Lake Storage アカウントの権限を追加する必要があります。"すべての権限が正しく設定されていることを確認してください"。

    以前に構成したコンソール エージェントでNetApp Backup and Recovery を既に使用していた場合は、Azure Synapse ワークスペースと Data Lake ストレージ アカウントのアクセス許可をコンソール ユーザー ロールに追加する必要があることに注意してください。これらは検索と復元に必要です。

  - コンソール エージェントは、インターネットへの HTTP 通信用にプロキシ サーバーなしで構成する必要があります。コンソール エージェントに HTTP プロキシ サーバーを構成している場合は、検索と復元機能は使用できません。
- Google Cloud の要件:
  - NetApp Consoleに権限を付与するユーザー ロールに、特定の Google BigQuery 権限を追加する必要があります。"すべての権限が正しく設定されていることを確認してください"。

    以前に構成したコンソール エージェントでNetApp Backup and Recovery をすでに使用していた場合は、コンソール ユーザー ロールに BigQuery 権限を追加する必要があります。これらは検索と復元に必要です。

- StorageGRIDおよびONTAP S3 の要件:

  構成に応じて、検索と復元を実装する方法は 2 つあります。

  - アカウントにクラウド プロバイダーの資格情報がない場合、インデックス カタログ情報はコンソール エージェントに保存されます。

    インデックス カタログ v2 の詳細については、インデックス カタログを有効にする方法に関する以下のセクションを参照してください。

  - プライベート (ダーク) サイトでコンソール エージェントを使用している場合、インデックス カタログ情報はコンソール エージェントに保存されます (コンソール エージェント バージョン 3.9.25 以上が必要です)。
  - もしあなたが "AWS認証情報"または "Azure 資格情報"アカウントにインデックスカタログがある場合は、クラウドに展開されたコンソールエージェントと同様に、インデックスカタログはクラ

ウドプロバイダーに保存されます。 (両方の認証情報がある場合、デフォルトで AWS が選択されます。)

オンプレミスのコンソール エージェントを使用している場合でも、コンソール エージェントの権限とクラウド プロバイダー リソースの両方について、クラウド プロバイダーの要件を満たす必要があります。この実装を使用する場合は、上記の AWS および Azure の要件を参照してください。

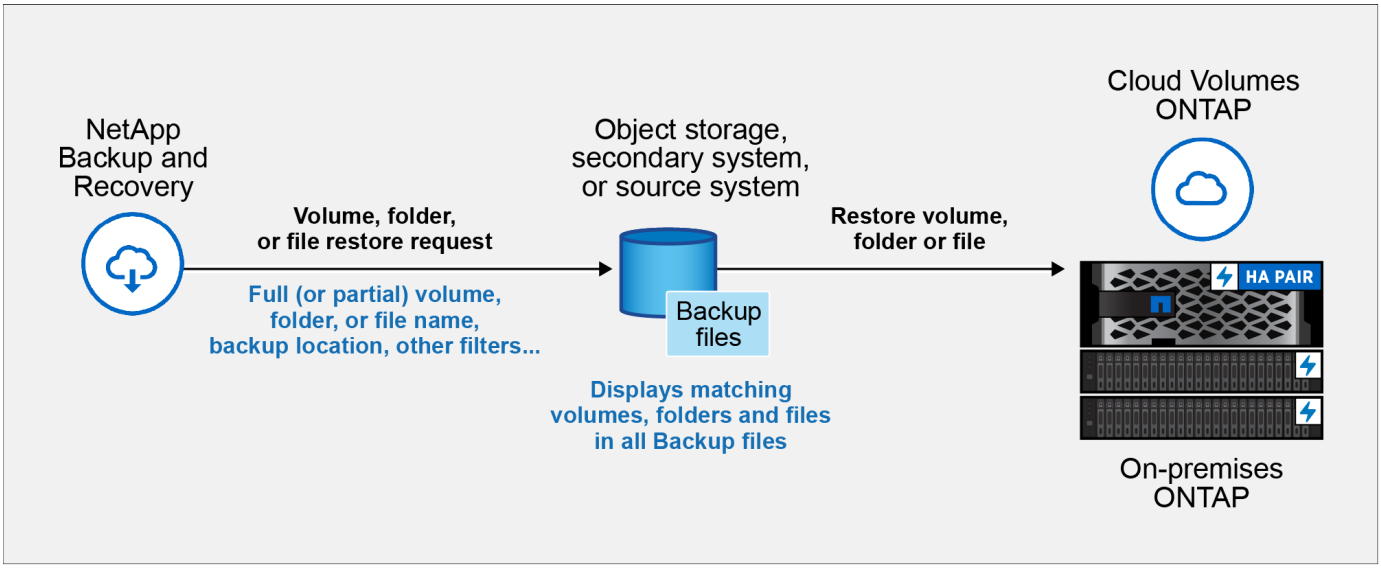
検索と復元のプロセス

プロセスは次のようになります。

1. 検索と復元を使用する前に、ボリューム データを復元する各ソース システムで「インデックス作成」を有効にする必要があります。これにより、インデックス カタログは各ボリュームのバックアップ ファイルを追跡できるようになります。
2. ボリューム バックアップからボリュームまたはファイルを復元する場合は、[検索と復元] で [検索と復元] を選択します。
3. ボリューム名の一部または全部、ファイル名の一部または全部、バックアップ場所、サイズの範囲、作成日の範囲、その他の検索フィルターでボリューム、フォルダー、またはファイルの検索条件を入力し、[検索] を選択します。

   「検索結果」ページには、検索条件に一致するファイルまたはボリュームがあるすべての場所が表示されます。

4. ボリュームまたはファイルの復元に使用する場所の「すべてのバックアップを表示」を選択し、使用する実際のバックアップ ファイルで「復元」を選択します。
5. ボリューム、フォルダー、またはファイルを復元する場所を選択し、「復元」を選択します。
6. ボリューム、フォルダー、またはファイルが復元されます。



名前の一部を知るだけで、 NetApp Backup and Recovery は検索に一致するすべてのバックアップ ファイルを検索します。

各システムでインデックスカタログを有効にする

検索と復元を使用する前に、ボリュームまたはファイルを復元する予定の各ソース システムで「インデックス作成」を有効にする必要があります。これにより、インデックス カタログはすべてのボリュームとすべてのバックアップ ファイルを追跡できるようになり、検索が非常に迅速かつ効率的になります。

インデックス カタログは、システム内のすべてのボリュームとバックアップ ファイルに関するメタデータを保存するデータベースです。これは、復元するデータが含まれているバックアップ ファイルをすばやく見つけるために、検索と復元機能によって使用されます。

インデックスカタログ機能

NetApp Backup and Recovery、インデックス カタログを使用する場合、別のバケットはプロビジョニングされません。代わりに、AWS、Azure、Google Cloud Platform、 StorageGRID、またはONTAP S3 に保存されているバックアップの場合、サービスはコンソール エージェントまたはクラウド プロバイダー環境にスペースをプロビジョニングします。

インデックス カタログは以下をサポートします。

- 3分以内にグローバル検索を効率化
- 最大50億ファイル
- クラスターあたり最大5000ボリューム
- ボリュームあたり最大10万個のスナップショット
- ベースライン インデックスの最大時間は 7 日未満です。実際の時間は環境によって異なります。

システムのインデックス作成を有効にする手順:

システムでインデックス作成がすでに有効になっている場合は、次のセクションに進み、データを復元してください。

まず、カタログ ファイルを保持するための別のボリュームをマウントする必要があります。これにより、スナップショットを保持するファイルのサイズが大きくなりすぎた場合にデータが失われるのを防ぎます。これはすべてのクラスターで必要なわけではなく、環境内の任意のクラスターから任意の 1 つのボリュームをマウントできます。これを行わないと、インデックスが正しく機能しない可能性があります。

マウントされたボリュームについては、次のサイズ設定ガイダンスを使用します。

- NetApp NFSボリュームを使用する
- 300 MB/秒のディスク スループットを備えたAFFストレージを推奨します。スループットが低下すると、検索やその他の操作に影響します。
- NetAppスナップショットを有効にして、カタログバックアップzipファイルに加えてカタログメタデータを保護します。
- 10億ファイルあたり50GB
- カタログデータ用に 20 GB、zip ファイル作成および一時ファイル用の追加スペース

カタログのインデックスを再作成するためにボリュームをマウントする手順

1. ボリュームをマウントする `/opt/application/netapp/cbs` 次のコマンドを入力します。
    - `volume name` カタログファイルが保存されるクラスタ上のボリュームです

- /opt/application/netapp/cbs マウントされているパスです

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

例：

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

インデックスを有効にする手順

1. 次のいずれかを実行します。
   - システムがインデックスされていない場合は、復元ダッシュボードの [検索と復元] で [システムのインデックスを有効にする] を選択します。
   - 少なくとも 1 つのシステムがすでにインデックスされている場合は、復元ダッシュボードの [検索と復元] で [インデックス設定] を選択します。
2. システムに対して*インデックスを有効にする*を選択します。

結果

すべてのサービスがプロビジョニングされ、インデックス カタログがアクティブ化されると、システムは「アクティブ」として表示されます。

システム内のボリュームのサイズと、3 つのバックアップ場所すべてにあるバックアップ ファイルの数によっては、初期のインデックス作成プロセスに最大 1 時間かかる場合があります。その後は、最新の状態を維持するために、1 時間ごとに段階的な変更が透過的に更新されます。

検索と復元を使用してボリューム、フォルダ、ファイルを復元する

完了したらシステムのインデックスを有効にしました、検索と復元を使用してボリューム、フォルダー、およびファイルを復元できます。これにより、幅広いフィルターを使用して、すべてのバックアップ ファイルから復元するファイルまたはボリュームを正確に見つけることができます。

手順

1. コンソール 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. *復元*タブを選択すると、復元ダッシュボードが表示されます。
3. [検索と復元] セクションから、[検索と復元] を選択します。
4. [検索と復元] セクションから、[検索と復元] を選択します。
5. 検索と復元ページから:
   a. 検索バー に、ボリューム名、フォルダー名、またはファイル名の完全または一部を入力します。
   b. リソースの種類を選択します: ボリューム、ファイル、フォルダー、または*すべて*。
   c. [フィルター条件] 領域で、フィルター条件を選択します。たとえば、データが存在するシステムとファイルの種類（.JPEG ファイルなど）を選択できます。または、オブジェクト ストレージ内の利用可能なスナップショットまたはバックアップ ファイル内のみで結果を検索する場合は、バックアップの場所のタイプを選択できます。

6. *検索*を選択すると、検索結果領域に、検索に一致するファイル、フォルダー、またはボリュームを持つすべてのリソースが表示されます。
7. 復元するデータがあるリソースを見つけて、[すべてのバックアップを表示] を選択し、一致するボリューム、フォルダー、またはファイルを含むすべてのバックアップ ファイルを表示します。
8. データの復元に使用するバックアップ ファイルを見つけて、[復元] を選択します。

   結果には、検索したファイルを含むローカル ボリュームのスナップショットとリモートの複製ボリュームが識別されることに注意してください。クラウド バックアップ ファイル、スナップショット、または複製されたボリュームから復元することを選択できます。

9. ボリューム、フォルダー、またはファイルを復元する宛先の場所を選択し、[復元] を選択します。
   - ボリュームの場合、元の宛先システムを選択することも、代替システムを選択することもできます。FlexGroupボリュームを復元する場合は、複数のアグリゲートを選択する必要があります。
   - フォルダーの場合は、元の場所に復元することも、システム、ボリューム、フォルダーなどの別の場所を選択することもできます。
   - ファイルについては、元の場所へ復元することも、システム、ボリューム、フォルダーなどの別の場所を選択することもできます。元の場所を選択するときに、ソース ファイルを上書きするか、新しいファイルを作成するかを選択できます。

     オンプレミスのONTAPシステムを選択し、オブジェクト ストレージへのクラスタ接続をまだ構成していない場合は、追加情報の入力を求められます。

     - Amazon S3 から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を選択し、作成したユーザーのアクセス キーとシークレット キーを入力してONTAPクラスターに S3 バケットへのアクセス権を付与し、オプションで安全なデータ転送のためにプライベート VPC エンドポイントを選択します。"これらの要件の詳細については、こちらをご覧ください。"。
     - Azure Blob から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を選択し、オプションで VNet とサブネットを選択して、安全なデータ転送のためのプライベート エンドポイントを選択します。"これらの要件の詳細については、こちらをご覧ください。"。
     - Google Cloud Storage から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace と、オブジェクト ストレージにアクセスするためのアクセス キーとシークレット キーを選択します。"これらの要件の詳細については、こちらをご覧ください。"。
     - StorageGRIDから復元する場合は、 StorageGRIDサーバーの FQDN と、 ONTAP がStorageGRIDとの HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスタ内の IPspace を入力します。"これらの要件の詳細については、こちらをご覧ください。"。
     - ONTAP S3 からリストアする場合は、 ONTAP S3 サーバーの FQDN と、 ONTAP がONTAP S3 との HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスター内の IPspace を選択します。"これらの要件の詳細については、こちらをご覧ください。"。

結果

ボリューム、フォルダー、またはファイルが復元され、復元ダッシュボードに戻り、復元操作の進行状況を確認できます。また、*ジョブ監視*タブを選択して、復元の進行状況を確認することもできます。見る"ジョブモニターページ"。

NetApp Backup and Recoveryでは、Browse & Restore を使用してONTAPデータを復元します。復元する前に、ソース ボリューム名、ソース システムと SVM、およびバックアップ ファイルの日付をメモします。スナップショット、複製されたボリューム、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ONTAPデータを復元できます。

復元機能はONTAP のバージョンによって異なります。

- フォルダ: ONTAP 9.13.0 以降を使用すると、すべてのファイルとサブフォルダを含むフォルダを復元できます。それ以前のバージョンでは、フォルダ内のファイルのみを復元できます。
- アーカイブ ストレージ: アーカイブ ストレージ (ONTAP 9.10.1 以降で利用可能) からの復元は遅くなり、追加コストが発生する可能性があります。
- 宛先クラスタの要件:
  - ボリュームリストア: ONTAP 9.10.1 以上
  - ファイル復元: ONTAP 9.11.1 以上
  - Google Archive およびStorageGRID: ONTAP 9.12.1 以上
  - フォルダの復元: ONTAP 9.13.1 以上

"AWSアーカイブストレージからの復元の詳細"。"Azure アーカイブ ストレージからの復元の詳細"。"Google アーカイブ ストレージからの復元の詳細"。

Azure アーカイブ ストレージからStorageGRIDシステムにデータを復元する場合、高優先度はサポートされません。

サポートされているシステムとオブジェクト ストレージ プロバイダーを参照および復元する

セカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップ ファイルから、次のシステムにONTAPデータを復元できます。スナップショットはソース システム上に存在し、同じシステムにのみ復元できます。

注: ボリュームはどのタイプのバックアップ ファイルからでも復元できますが、現時点では、フォルダーまたは個々のファイルはオブジェクト ストレージ内のバックアップ ファイルからのみ復元できます。

オブジェクトストアから（バックアップ）	プライマリから（スナップショット）	セカンダリシステムから（レプリケーション）	宛先システムへ
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	Azure ブロブ
Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Google Cloud Storage	Google オンプレミスONTAPシステムのCloud Volumes ONTAP
Google オンプレミスONTAPシステムのCloud Volumes ONTAP	NetAppStorageGRID	オンプレミスのONTAPシステム	オンプレミスのONTAPシステムCloud Volumes ONTAP

オブジェクトストアから（バックアップ）	プライマリから（スナップショット）	セカンダリシステムから（レプリケーション）	宛先システムへ
オンプレミスのONTAPシステムへ	ONTAP S3	オンプレミスのONTAPシステム	オンプレミスのONTAPシステムCloud Volumes ONTAP

参照と復元の場合、コンソール エージェントは次の場所にインストールできます。

- Amazon S3の場合、コンソールエージェントはAWSまたはオンプレミスに導入できます。
- Azure Blobの場合、コンソールエージェントはAzureまたはオンプレミスに展開できます。
- Google Cloud Storage の場合、コンソール エージェントを Google Cloud Platform VPC にデプロイする必要があります。
- StorageGRIDの場合、コンソールエージェントは、インターネットアクセスの有無にかかわらず、お客様の敷地内に導入する必要があります。
- ONTAP S3の場合、コンソールエージェントは、オンプレミス（インターネットアクセスの有無にかかわらず）またはクラウドプロバイダー環境に導入できます。

「オンプレミスのONTAPシステム」への参照には、 FAS、 AFF、およびONTAP Selectシステムが含まれることに注意してください。

システムのONTAPバージョンが 9.13.1 未満の場合、バックアップ ファイルが DataLock & Ransomware で構成されていると、フォルダーまたはファイルを復元できません。この場合、バックアップ ファイルからボリューム全体を復元し、必要なファイルにアクセスできます。

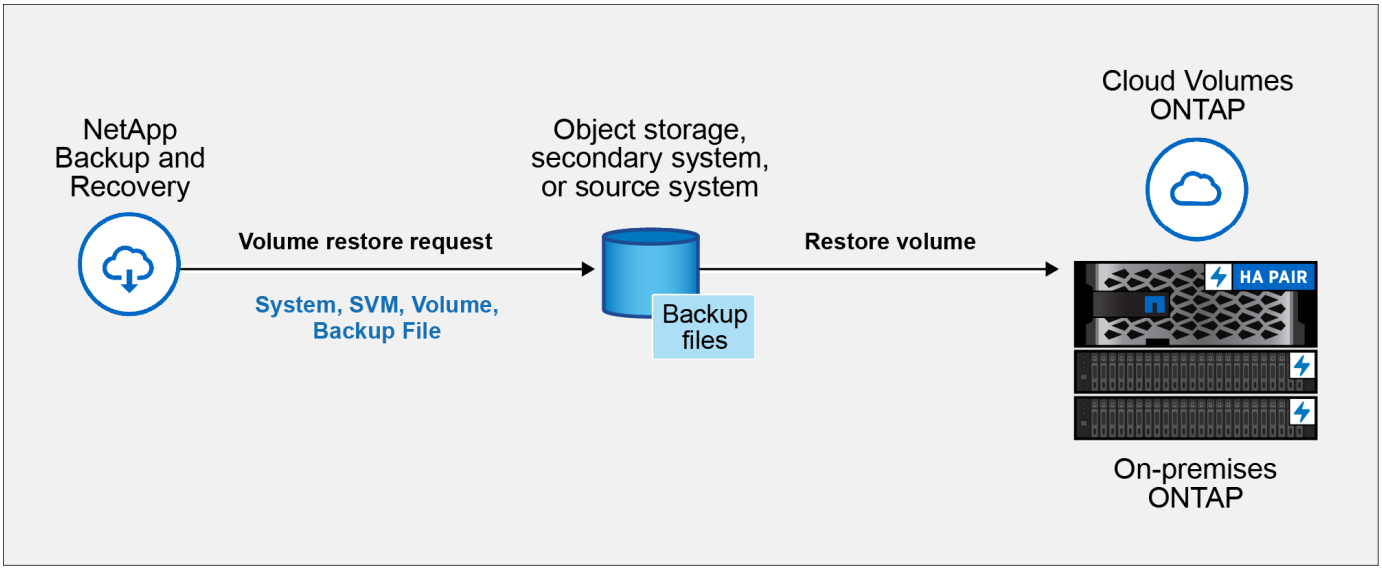
参照と復元を使用してボリュームを復元する

バックアップ ファイルからボリュームを復元すると、 NetApp Backup and Recovery はバックアップのデータを使用して新しいボリュームを作成します。オブジェクト ストレージからのバックアップを使用すると、データを元のシステムのボリューム、ソース システムと同じクラウド アカウントにある別のシステム、またはオンプレミスのONTAPシステムに復元できます。

ONTAP 9.13.0 以降を使用しているCloud Volumes ONTAPシステム、またはONTAP 9.14.1 を実行しているオンプレミスのONTAPシステムにクラウド バックアップを復元する場合は、クイック リストア 操作を実行するオプションがあります。クイック リストアは、ボリュームへのアクセスをできるだけ早く提供する必要がある災害復旧の状況に最適です。クイック リストアでは、バックアップ ファイル全体を復元するのではなく、バックアップ ファイルからボリュームにメタデータを復元します。クイック リストアは、パフォーマンスや待ち時間が重要となるアプリケーションには推奨されません。また、アーカイブ ストレージ内のバックアップではサポートされません。

クイック リストアは、クラウド バックアップが作成されたソース システムでONTAP 9.12.1 以降が実行されている場合にのみ、 FlexGroupボリュームに対してサポートされます。また、ソース システムでONTAP 9.11.0 以降が実行されている場合にのみ、 SnapLockボリュームでサポートされます。

複製されたボリュームから復元する場合、ボリュームを元のシステム、 Cloud Volumes ONTAPまたはオンプレミスのONTAPシステムに復元できます。



ボリュームを復元するには、ソース システム名、ストレージ VM、ボリューム名、およびバックアップ ファイルの日付が必要です。

手順

1. コンソール 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. *復元*タブを選択すると、復元ダッシュボードが表示されます。
3. [参照と復元] セクションから、[ボリュームの復元] を選択します。
4. [ソースの選択] ページで、復元するボリュームのバックアップ ファイルに移動します。復元する日付/タイムスタンプを持つ システム、ボリューム、および バックアップ ファイルを選択します。

   場所 列には、バックアップ ファイル (スナップショット) が ローカル (ソース システム上のスナップショット)、セカンダリ (セカンダリONTAPシステム上の複製されたボリューム)、または オブジェクト ストレージ (オブジェクト ストレージ内のバックアップ ファイル) のいずれであるかが表示されます。復元するファイルを選択します。

5. *次へ*を選択します。

   オブジェクト ストレージ内のバックアップ 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耐性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 とランサムウェア耐性を有効にした場合)、データを復元する前に、バックアップ ファイルに対して追加のランサムウェア スキャンを実行するように求められます。バックアップ ファイルをランサムウェアのスキャン対象とすることをお勧めします。 (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。)

6. [宛先の選択] ページで、ボリュームを復元する システム を選択します。
7. オブジェクト ストレージからバックアップ ファイルを復元するときに、オンプレミスのONTAPシステムを選択し、オブジェクト ストレージへのクラスタ接続をまだ構成していない場合は、追加情報の入力を求められます。

   - Amazon S3 から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を選択し、作成したユーザーのアクセス キーとシークレット キーを入力してONTAPクラスターに S3 バケットへのアクセス権を付与し、オプションで安全なデータ転送のためにプライベート VPC エンドポイントを選択します。
   - Azure Blob から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を選択

し、オブジェクト ストレージにアクセスするための Azure サブスクリプションを選択し、オプションで VNet とサブネットを選択して、安全なデータ転送のためのプライベート エンドポイントを選択します。

- Google Cloud Storage から復元する場合は、Google Cloud プロジェクトとアクセス キーおよびシークレット キーを選択して、オブジェクト ストレージ、バックアップが保存されるリージョン、および宛先ボリュームが存在するONTAPクラスター内の IPspace にアクセスします。
- StorageGRIDから復元する場合は、 StorageGRIDサーバーの FQDN と、 ONTAP がStorageGRIDとの HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスタ内の IPspace を選択します。
- ONTAP S3 からリストアする場合は、 ONTAP S3 サーバーの FQDN と、 ONTAP がONTAP S3 との HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスター内の IPspace を選択します。

8. 復元されたボリュームに使用する名前を入力し、ボリュームが保存されるストレージ VM とアグリゲートを選択します。 FlexGroupボリュームを復元する場合は、複数のアグリゲートを選択する必要があります。デフォルトでは、ボリューム名として **<source_volume_name>_restore** が使用されます。

   オブジェクト ストレージからONTAP 9.13.0 以上を使用するCloud Volumes ONTAPシステム、またはONTAP 9.14.1 を実行するオンプレミスのONTAPシステムにバックアップを復元する場合は、クイック復元操作を実行するオプションがあります。

   また、アーカイブ ストレージ層 (ONTAP 9.10.1 以降で利用可能) にあるバックアップ ファイルからボリュームを復元する場合は、復元優先度を選択できます。

   "AWSアーカイブストレージからの復元の詳細"。"Azure アーカイブ ストレージからの復元の詳細"。"Google アーカイブ ストレージからの復元の詳細"。Google アーカイブ ストレージ層のバックアップ ファイルはほぼ即座に復元されるため、復元の優先順位は必要ありません。

9. [次へ] を選択して、通常の復元プロセスを実行するか、クイック復元プロセスを実行するかを選択します。
   - 通常の復元: 高いパフォーマンスが必要なボリュームでは通常の復元を使用します。復元プロセスが完了するまでボリュームは使用できません。
   - クイック復元: 復元されたボリュームとデータはすぐに利用できるようになります。クイック リストア プロセス中はデータへのアクセスが通常よりも遅くなる可能性があるため、高パフォーマンスが必要なボリュームではこれを使用しないでください。
10. *復元*を選択すると、復元ダッシュボードに戻り、復元操作の進行状況を確認できます。

結果

NetApp Backup and Recovery は、選択したバックアップに基づいて新しいボリュームを作成します。

アーカイブ ストレージにあるバックアップ ファイルからボリュームを復元する場合、アーカイブ層と復元の優先度に応じて数分から数時間かかる場合があることに注意してください。復元の進行状況を確認するには、[ジョブ監視] タブを選択します。

参照と復元を使用してフォルダとファイルを復元する

ONTAPボリューム バックアップから少数のファイルのみを復元する必要がある場合は、ボリューム全体を復元するのではなく、フォルダーまたは個々のファイルを復元することを選択できます。フォルダーとファイルを元のシステムの既存のボリュームに復元することも、同じクラウド アカウントを使用している別のシステ

ムに復元することもできます。オンプレミスのONTAPシステム上のボリュームにフォルダーとファイルを復元することもできます。

> 現時点では、オブジェクト ストレージ内のバックアップ ファイルからのみフォルダーまたは個々のファイルを復元できます。現在、ローカル スナップショットまたはセカンダリ システム (複製されたボリューム) にあるバックアップ ファイルからのファイルとフォルダーの復元はサポートされていません。

複数のファイルを選択した場合、それらは同じ宛先ボリュームに復元されます。ファイルを別のボリュームに復元するには、プロセスを複数回実行します。

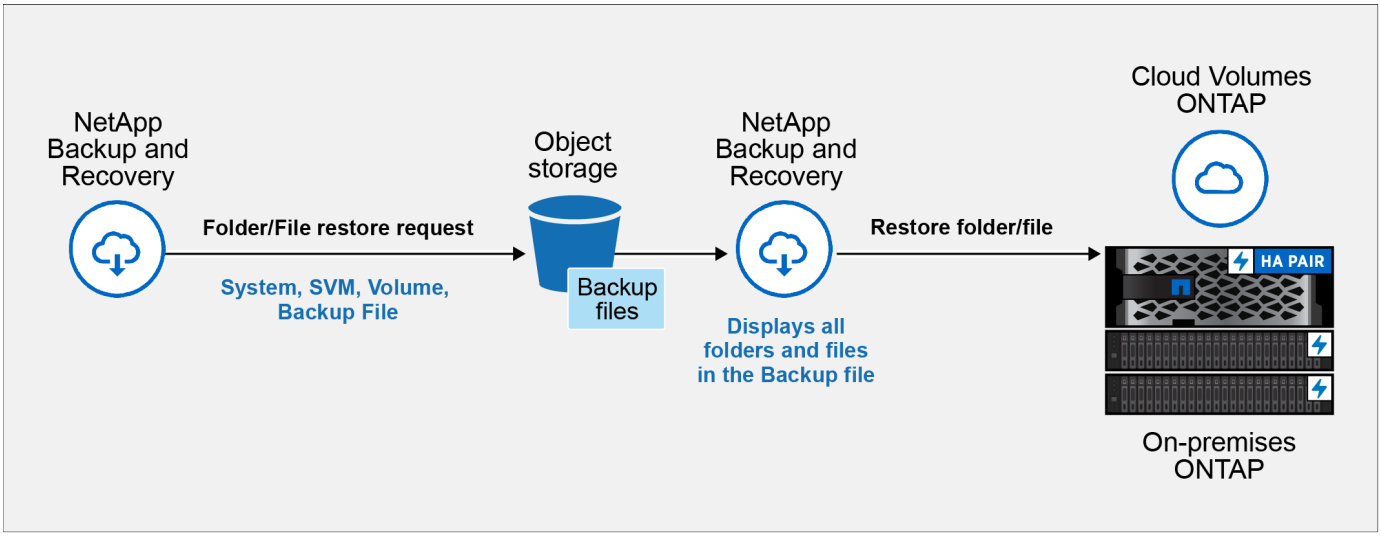
ONTAP 9.13.0 以降を使用している場合は、フォルダーとその中のすべてのファイルおよびサブフォルダーを復元できます。 9.13.0 より前のバージョンのONTAPを使用する場合、そのフォルダのファイルのみが復元され、サブフォルダまたはサブフォルダ内のファイルは復元されません。

- バックアップ ファイルに DataLock および Ransomware 保護が設定されている場合、ONTAPバージョンが 9.13.1 以上の場合にのみフォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、バックアップ ファイルからボリューム全体を復元し、必要なフォルダーとファイルにアクセスできます。
- バックアップ ファイルがアーカイブ ストレージに存在する場合、 ONTAPバージョンが 9.13.1 以上の場合にのみ、フォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、アーカイブされていない新しいバックアップ ファイルからフォルダを復元するか、アーカイブされたバックアップからボリューム全体を復元して、必要なフォルダとファイルにアクセスすることができます。
- ONTAP 9.15.1 では、「参照と復元」オプションを使用してFlexGroupフォルダを復元できます。この機能はテクノロジープレビュー モードです。

  特別なフラグを使用してテストすることができます。 "NetApp Backup and Recovery2024 年 7 月リリース ブログ" 。

フォルダとファイルを復元する

ONTAPボリューム バックアップからボリュームにフォルダーまたはファイルを復元するには、次の手順に従います。フォルダーまたはファイルを復元するために使用するボリュームの名前とバックアップ ファイルの日付を知っておく必要があります。この機能はライブ ブラウジングを使用するため、各バックアップ ファイル内のディレクトリとファイルのリストを表示できます。



開始する前に

- _ファイル_復元操作を実行するには、 ONTAPバージョンが 9.6 以上である必要があります。
- フォルダの復元操作を実行するには、 ONTAPバージョンが 9.11.1 以上である必要があります。データがアーカイブ ストレージにある場合、またはバックアップ ファイルで DataLock およびランサムウェア保護が使用されている場合は、 ONTAPバージョン 9.13.1 が必要です。
- 参照と復元オプションを使用してFlexGroupディレクトリを復元するには、 ONTAPバージョンが 9.15.1 p2 以上である必要があります。

手順

1. コンソール 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. *復元*タブを選択すると、復元ダッシュボードが表示されます。
3. [参照と復元] セクションで、[ファイルまたはフォルダーの復元] を選択します。
4. [ソースの選択] ページで、復元するフォルダーまたはファイルが含まれているボリュームのバックアップ ファイルに移動します。ファイルを復元する日付/タイムスタンプを持つ システム、ボリューム、および バックアップ を選択します。
5. [次へ] を選択すると、ボリューム バックアップのフォルダーとファイルのリストが表示されます。

   アーカイブ ストレージ層にあるバックアップ ファイルからフォルダーまたはファイルを復元する場合は、復元の優先順位を選択できます。

   "AWSアーカイブストレージからの復元の詳細"。"Azure アーカイブ ストレージからの復元の詳細"。"Google アーカイブ ストレージからの復元の詳細"。Google アーカイブ ストレージ層のバックアップ ファイルはほぼ即座に復元されるため、復元の優先順位は必要ありません。

   また、バックアップ ファイルに対して Ransomware Resilience 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 Ransomware Resilience を有効にした場合)、データを復元する前に、バックアップ ファイルに対して追加のランサムウェア スキャンを実行するように求められます。バックアップ ファイルをランサムウェアのスキャン対象とすることをお勧めします。 (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。)

6. [アイテムの選択] ページで、復元するフォルダーまたはファイルを選択し、[続行] を選択します。アイテムを見つける際に役立つ情報:
   - フォルダーまたはファイル名が表示されている場合はそれを選択できます。

- 検索アイコンを選択し、フォルダーまたはファイルの名前を入力すると、アイテムに直接移動できます。
- 行の末尾にある下矢印を使用してフォルダー内の下のレベルに移動し、特定のファイルを見つけることができます。

  ファイルを選択すると、ページの左側に追加されるので、すでに選択したファイルを確認できます。必要に応じて、ファイル名の横にある **x** を選択して、このリストからファイルを削除できます。

7. [宛先の選択] ページで、アイテムを復元する システム を選択します。

   オンプレミス クラスターを選択し、オブジェクト ストレージへのクラスター接続をまだ構成していない場合は、追加情報の入力を求められます。

   - Amazon S3 から復元する場合は、宛先ボリュームが存在するONTAPクラスターの IPspace と、オブジェクト ストレージにアクセスするために必要な AWS アクセス キーとシークレット キーを入力します。クラスターへの接続にプライベート リンク構成を選択することもできます。
   - Azure Blob から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を入力します。クラスターへの接続にプライベート エンドポイント構成を選択することもできます。
   - Google Cloud Storage から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace と、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キーを入力します。
   - StorageGRIDから復元する場合は、 StorageGRIDサーバーの FQDN と、 ONTAP がStorageGRIDとの HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスタ内の IPspace を入力します。
8. 次に、フォルダーまたはファイルを復元する ボリューム と フォルダー を選択します。

   フォルダーやファイルを復元する際の場所についてはいくつかのオプションがあります。

   - 上記のように*ターゲットフォルダーの選択*を選択した場合:
     - 任意のフォルダを選択できます。
     - フォルダーの上にマウスを移動し、行の末尾をクリックしてサブフォルダーにドリルダウンし、フォルダーを選択できます。
   - ソース フォルダ/ファイルが配置されていたのと同じ宛先システムとボリュームを選択した場合は、[ソース フォルダ パスを維持] を選択して、フォルダまたはファイルをソース構造に存在していたのと同じフォルダに復元できます。同じフォルダーとサブフォルダーがすべてすでに存在している必要があります。フォルダーは作成されません。ファイルを元の場所に復元する場合、ソース ファイルを上書きするか、新しいファイルを作成するかを選択できます。
9. 復元 を選択して復元ダッシュボードに戻り、復元操作の進行状況を確認します。

Microsoft SQL Server ワークロードを保護する

NetApp Backup and Recoveryを使用した Microsoft SQL ワークロードの保護の概要

NetApp Backup and Recoveryを使用して、オンプレミスのONTAPシステムから AWS 、Azure、またはStorageGRIDに Microsoft SQL Server アプリケーション データをバックアップします。システムはポリシーに従って、クラウド アカウントにバックアップを

自動的に作成して保存します。 3-2-1 戦略を使用します。つまり、データの 3 つのコピーを 2 つのストレージ システムに保存し、1 つのコピーをクラウドに保存します。

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 は、 NetApp SnapMirrorを使用してスナップショットを作成し、それをバックアップの場所に転送することでバックアップを同期します。

データを保護するために、次の操作を実行できます。

- "SnapCenterからインポートする場合の追加項目を構成する"
- "Microsoft SQL Server 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します"
- "ローカルONTAPプライマリ ストレージ上のローカル スナップショットを使用してワークロードをバックアップします。"
- "ワークロードをONTAPセカンダリストレージに複製する"
- "ワークロードをオブジェクトストアの場所にバックアップする"
- "今すぐワークロードをバックアップ"
- "ワークロードを復元する"
- "クローンワークロード"
- "ワークロードのインベントリを管理する"
- "スナップショットを管理する"

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"詳細についてはこちらをご覧ください。

サポートされているバックアップ先

NetApp Backup and Recovery を使用すると、Microsoft SQL Server インスタンスとデータベースを次のソース システムから次のセカンダリ システムおよびパブリック クラウド プロバイダーとプライベート クラウド プロバイダーのオブジェクト ストレージにバックアップできます。スナップショットはソース システムに存在します。

ソースシステム	セカンダリシステム（レプリケーション）	宛先オブジェクトストア（バックアップ）
AWS のCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	Amazon S3 ONTAP S3
Azure のCloud Volumes ONTAP	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure ブロブONTAP S3
オンプレミスのONTAPシステム	Cloud Volumes ONTAPオンプレミスONTAPシステム	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3

ソースシステム	セカンダリシステム（レプリケーション）	宛先オブジェクトストア（バックアップ）
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	NA

サポートされている復元先

プライマリ ストレージまたはセカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップから、Microsoft SQL Server インスタンスとデータベースを次のシステムに復元できます。スナップショットはソース システム上に存在し、同じシステムにのみ復元できます。

バックアップファイルの場所から		宛先システムへ
オブジェクトストア（バックアップ）	セカンダリシステム（レプリケーション）	
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	AWS オンプレミスのONTAPシステムONTAP S3 の Cloud Volumes
Azure ブロブ	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure のCloud Volumes ONTAPオンプレミスのONTAPシステムONTAP S3
StorageGRID	Cloud Volumes ONTAPオンプレミスONTAPシステム	オンプレミスのONTAPシステムONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	NA

「オンプレミスのONTAPシステム」への参照には、 FASとAFFシステムが含まれます。

プラグイン サービスから**NetApp Backup and Recovery**にインポートするための前提条件

Microsoft SQL Server 用のSnapCenterプラグイン サービスからNetApp Backup and Recoveryにリソースをインポートする場合は、さらにいくつかの項目を構成する必要があります。

まず**NetApp Console**でシステムを作成する

SnapCenterからリソースをインポートする場合は、 SnapCenterからインポートする前に、オンプレミスのすべてのSnapCenterクラスター ストレージをコンソールの [システム] ページに追加する必要があります。これにより、ホスト リソースが正しく検出され、インポートされるようになります。

SnapCenterプラグインをインストールするためのホスト要件を確認する

SnapCenter Plug-in for Microsoft SQL Server からリソースをインポートするには、 SnapCenter Plug-in for Microsoft SQL Server をインストールするためのホスト要件が満たされていることを確認します。

SnapCenterの要件については、"NetApp Backup and Recoveryの前提条件" 。

ユーザーアカウント制御のリモート制限を無効にする

SnapCenterからリソースをインポートする前に、 SnapCenter Windows ホストのユーザー アカウント制御

(UAC) リモート制限を無効にします。ローカル管理者アカウントを使用してSnapCenter Server ホストまたはSQL ホストにリモートで接続する場合は、UAC を無効にします。

セキュリティに関する考慮事項

UAC リモート制限を無効にする前に、次の問題を考慮してください。

- セキュリティ リスク: トークン フィルタリングを無効にすると、特にローカル管理者アカウントが悪意のある人物によって侵害された場合に、システムがセキュリティ上の脆弱性にさらされる可能性があります。
- 注意して使用してください:
  - 管理タスクに不可欠な場合にのみ、この設定を変更してください。
  - 管理者アカウントを保護するために、強力なパスワードやその他のセキュリティ対策が実施されていることを確認します。

代替解決策

- リモート管理アクセスが必要な場合は、適切な権限を持つドメイン アカウントの使用を検討してください。
- リスクを最小限に抑えるために、セキュリティのベストプラクティスに準拠した安全なリモート管理ツールを使用します。

ユーザーアカウント制御のリモート制限を無効にする手順

1. 変更する `LocalAccountTokenFilterPolicy`SnapCenter Windows ホスト上のレジストリ キー。

   次のいずれかを使用してこれを実行してください。手順は次のとおりです。

   - 方法1: レジストリエディター
   - 方法2: PowerShellスクリプト

方法**1:** レジストリエディターを使用してユーザーアカウント制御を無効にする

これは、ユーザー アカウント制御を無効にするために使用できる方法の 1 つです。

手順

1. 次の手順に従って、 SnapCenter Windows ホストでレジストリ エディターを開きます。
   a. プレス `Windows+R`[実行]ダイアログ ボックスを開きます。
   b. タイプ `regedit`押すと `Enter`。
2. ポリシーキーに移動します。

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
   ```

3. 作成または変更 `DWORD`価値：
   a. 場所: `LocalAccountTokenFilterPolicy`
   b. 存在しない場合は、新しいものを作成してください `DWORD`（32ビット）値の名前 `LocalAccountTokenFilterPolicy`。

4. 以下の値がサポートされています。このシナリオでは、値を `1`:
   - `0`(デフォルト): UAC リモート制限が有効になります。ローカル アカウントには、リモート アクセス時にフィルターされたトークンがあります。
   - `1`: UAC リモート制限は無効です。ローカル アカウントはトークン フィルタリングをバイパスし、リモート アクセス時に完全な管理者権限を持ちます。
5. [OK]をクリックします。
6. レジストリ エディターを閉じます。
7. SnapCenter Windows ホストを再起動します。

レジストリの変更例

この例では、LocalAccountTokenFilterPolicy を「1」に設定し、UAC リモート制限を無効にします。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Sys
tem]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

方法**2: PowerShell**スクリプトを使用してユーザーアカウント制御を無効にする

これは、ユーザー アカウント制御を無効にするために使用できる別の方法です。

昇格された権限で PowerShell コマンドを実行すると、システム設定に影響する可能性があります。コマンドを実行する前に、コマンドとその意味を理解していることを確認してください。

手順

1. SnapCenter Windows ホストで管理者権限を使用して PowerShell ウィンドウを開きます。
   a. スタート メニューをクリックします。
   b. **PowerShell 7** または **Windows Powershell** を検索します。
   c. そのオプションを右クリックし、[管理者として実行] を選択します。
2. PowerShell がシステムにインストールされていることを確認してください。インストール後、スタート メニューに表示されます。

   PowerShell は、Windows 7 以降のバージョンにデフォルトで含まれています。
3. UAC リモート制限を無効にするには、次のコマンドを実行して LocalAccountTokenFilterPolicy を「1」に設定します。

   ```
   Set-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
   ```
4. 現在の値が「1」に設定されていることを確認します。 `LocalAccountTokenFilterPolicy``実行して:

```
Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"
```

- 値が 1 の場合、UAC リモート制限は無効になります。
- 値が 0 の場合、UAC リモート制限が有効になります。

5. 変更を適用するには、コンピューターを再起動してください。

UAC リモート制限を無効にする **PowerShell 7** コマンドの例:

値が「1」に設定されているこの例は、UAC リモート制限が無効になっていることを示します。

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Microsoft SQL Server ワークロードを検出し、オプションでNetApp Backup and RecoveryのSnapCenterからインポートします。

NetApp Backup and Recovery、サービスを使用するために、まず Microsoft SQL Server ワークロードを検出する必要があります。 SnapCenterがすでにインストールされている場合は、オプションでSnapCenter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NetApp Consoleロール バックアップおよび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" 。

Microsoft SQL Server 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します

検出中に、 NetApp Backup and Recovery は組織内のシステム内の Microsoft SQL Server インスタンスとデータベースを分析します。

NetApp Backup and Recovery は、 Microsoft SQL Server アプリケーションを評価します。このサービスは、現在のバックアップ保護ポリシー、スナップショット、バックアップおよびリカバリ オプションなどの既存の保護レベルを評価します。

検出は次のように行われます。

- SnapCenterがすでにある場合は、 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がすでにある場合は、まず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、オンプレミスのSnapCenterクラスタ ストレージ システムをNetApp Consoleに追加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がまだない場合は、vCenter を手動で追加して検出を実行することで、ワークロードを検出できます。

SnapCenterがすでにインストールされている場合は、 **SnapCenter**リソースを**NetApp Backup and Recovery**にインポートします。

SnapCenter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リソースをNetApp Backup and Recoveryにインポートします。 NetApp Consoleは、 SnapCenterからリソース、ホスト、資格情報、スケジュールを検出するため、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 2 つの部分から成るプロセスです。

- SnapCenter Server アプリケーションとホスト リソースをインポートする
- 選択したSnapCenterホストリソースを管理する

SnapCenter Server アプリケーションとホスト リソースをインポートする

この最初のステップでは、 SnapCenterからホスト リソースをインポートし、それらのリソースをNetApp Backup and Recoveryインベントリ ページに表示されます。その時点では、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ホスト リソース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. 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。
2. *在庫*を選択します。

3. *リソースの検出*を選択します。
4. 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。
5. * SnapCenterアプリケーションの資格情報*を入力してください:
   a. * SnapCenter FQDN または IP アドレス*: SnapCenterアプリケーション自体の FQDN または IP アドレスを入力します。
   b. ポート: SnapCenterサーバーのポート番号を入力します。
   c. ユーザー名 と パスワード: SnapCenterサーバーのユーザー名とパスワードを入力します。
   d. コンソール エージェント: SnapCenterのコンソール エージェントを選択します。
6. * SnapCenterサーバー 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サーバーを登録します。

SnapCenterサーバー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

インベントリ ページには、MS SQL ホスト、インスタンス、データベースを含むインポートされたSnapCenterリソースが表示されます。

インポートされたSnapCenterリソースの詳細を表示するには、[アクション] メニューから [詳細の表示] オプションを選択します。

SnapCenterホストリソースの管理

SnapCenterリソースをインポートした後、 NetApp Backup and Recoveryでそれらのホスト 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SnapCenterから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。これらのリソースはSnapCenter Server では管理できなくなります。

手順

1. SnapCenter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SnapCenterホストを選択します。
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、ホストの管理ページを表示します。
5. *管理*を選択します。
6. [ホストの管理] ページで、既存の vCenter を使用するか、新しい vCenter を追加するかを選択します。

7. *管理*を選択します。

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

オプションで、[アクション] メニューから [レポートの生成] オプションを選択して、管理対象リソースのレポートを作成することもできます。

インベントリページから検出後に**SnapCenter**リソースをインポートする

すでにリソースを検出している場合は、インベントリ ページからSnapCenterリソースをインポートできます。

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. インベントリ ページで、* SnapCenterリソースのインポート*を選択します。
4. SnapCenterリソースをインポートするには、上記の * SnapCenterリソースのインポート* セクションの手順に従います。

SnapCenterが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 情報を追加して、 NetAppバックアップおよびリカバリでワークロードを検出できます。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。

VMware 環境がある場合、これはオプションです。

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。

   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: このバージョンでは、Microsoft SQL Server のみが利用可能です。
   b. **vCenter** 設定: 既存の vCenter を選択するか、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: 資格情報の追加 を選択し、検出するワークロードを含むホストに関する情報を入力します。

vCenter サーバーではなくスタンドアロン サーバーを追加する場合は、ホスト情報のみを入力します。

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。

5. 詳細設定に進みます。

検出中に詳細設定オプションを設定し、プラグインをインストールします

詳細設定を使用すると、登録されているすべてのサーバーにプラグイン エージェントを手動でインストールできます。これにより、すべてのSnapCenterワークロードをNetApp Backup and Recoveryにインポートして、そこでバックアップとリストアを管理できるようになります。 NetApp Backup and Recovery、プラグインをインストールするために必要な手順が示されています。

手順

1. 「リソースの検出」ページで、右側の下矢印をクリックして「詳細設定」に進みます。
2. 「ワークロード リソースの検出」ページで、次の情報を入力します。
   - プラグインのポート番号を入力: プラグインが使用するポート番号を入力します。
   - インストール パス: プラグインをインストールするパスを入力します。
3. SnapCenterエージェントを手動でインストールする場合は、次のオプションのチェックボックスをオンにします。
   - 手動インストールを使用する: プラグインを手動でインストールするには、このボックスをオンにします。
   - クラスター内のすべてのホストを追加: 検出中にクラスター内のすべてのホストをNetApp Backup and Recoveryに追加するには、このボックスをオンにします。
   - オプションのインストール前チェックをスキップ: オプションのインストール前チェックをスキップするには、このチェックボックスをオンにします。たとえば、メモリやスペースの考慮事項が近い将来に変更されることがわかっていて、今すぐプラグインをインストールしたい場合などに、これを実行することができます。
4. *Discover*を選択します。

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

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。

"ダッシュボードに表示される内容を学ぶ"。

NetApp Backup and Recoveryで Microsoft SQL Server 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、Microsoft Azure、またはStorageGRIDに Microsoft SQL Server アプリケーション データをバックアップします。システムは自動的にバックアップを作成し、データ保護のためにクラウド アカウント内のオブジェクト ストアに保存します。

- 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。
- バックアップを開始する前に、検出されたホストのログ ディレクトリを構成します。
- 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)。

ワークロード保護ステータスの表示

バックアップを開始する前に、ワークロードの保護ステータスを表示します。

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、バックアップおよびリカバリ リストア管理者、バックアップおよびリカバリ クローン管理者、またはバックアップおよびリカバリ ビューアー ロール。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" 。

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. ホスト、保護グループ、可用性グループ、インスタンス、およびデータベースのタブで詳細を確認します。

検出されたホストのログディレクトリを構成する

ワークロードをバックアップする前に、検出されたホストのアクティビティ ログ パスを設定して操作ステータスを追跡します。

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、またはバックアップおよびリカバリ リストア管理者のロール。 "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. ホストを選択します。
5. アクションアイコンを選択します > ログディレクトリを設定します。
6. ホスト パスを入力するか、ホストまたはノードのリストを参照して、ホスト ログを保存する場所を見つ

けます。

7. ログを保存するものを選択します。

   表示されるフィールドは、フェールオーバー クラスター インスタンスやスタンドアロンなど、選択した展開モデルによって異なります。

8. *保存*を選択します。

保護グループを作成する

複数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。保護グループは、ワークロードの論理的なグループです。

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. 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. 保護グループに含めるインスタンスまたはデータベースを選択します。
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。

   ポリシーを作成する場合は、「新しいポリシーの作成」を選択し、指示に従ってポリシーを作成します。見る"ポリシーを作成"詳細についてはこちらをご覧ください。

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。

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

システムに変更を加える前にオンデマンド バックアップを実行して、データが保護されていることを確認してください。

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. 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、インスタンス、または*データベース*タブを選択します。
5. バックアップするインスタンスまたはデータベースを選択します。
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。
7. バックアップに適用するポリシーを選択します。
8. スケジュール層を選択します。
9. *今すぐバックアップ*を選択します。

バックアップスケジュールを一時停止する

メンテナンスやトラブルシューティング中にバックアップを一時的に停止するには、スケジュールを一時停止します。

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. 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、インスタンス、または*データベース*タブを選択します。
5. 一時停止する保護グループ、インスタンス、またはデータベースを選択します。
6. アクションアイコンを選択します ••• > 一時停止。

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。

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. 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 ••• > 保護グループを削除します。

ワークロードから保護を削除する

ワークロードのバックアップが不要になった場合、またはNetApp Backup and Recoveryでの管理を停止する場合は、ワークロードから保護を削除できます。

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、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. 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、インスタンス、または*データベース*タブを選択します。
5. 保護グループ、インスタンス、またはデータベースを選択します。
6. アクションアイコンを選択します > 保護を解除。
7. [保護の削除] ダイアログ ボックスで、バックアップとメタデータを保持するか削除するかを選択します。
8. 操作を確認するには、[削除] を選択します。

NetApp Backup and Recoveryを使用して **Microsoft SQL Server** のワークロードを復元する

NetApp Backup and Recoveryを使用して Microsoft SQL Server ワークロードを復元します。スナップショット、セカンダリ ストレージに複製されたバックアップ、またはオブジェクト ストレージ内のバックアップを使用します。ワークロードを元のシステム、同じクラウド アカウントを持つ別のシステム、またはオンプレミスのONTAPシステムに復元します。

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から復元
- 複製されたリソースから復元する
- オブジェクトストアのバックアップから復元する

これらのポイントに復元する

データを最新のスナップショットまたは以下のポイントに復元できます。

- スナップショットからの復元
- ファイル名、場所、最終有効日が分かっている場合は、特定の時点に復元します。
- 最新のバックアップに復元する

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 ストレージ内のバックアップ ファイルを選択し、そのバックアップに対して Ransomware

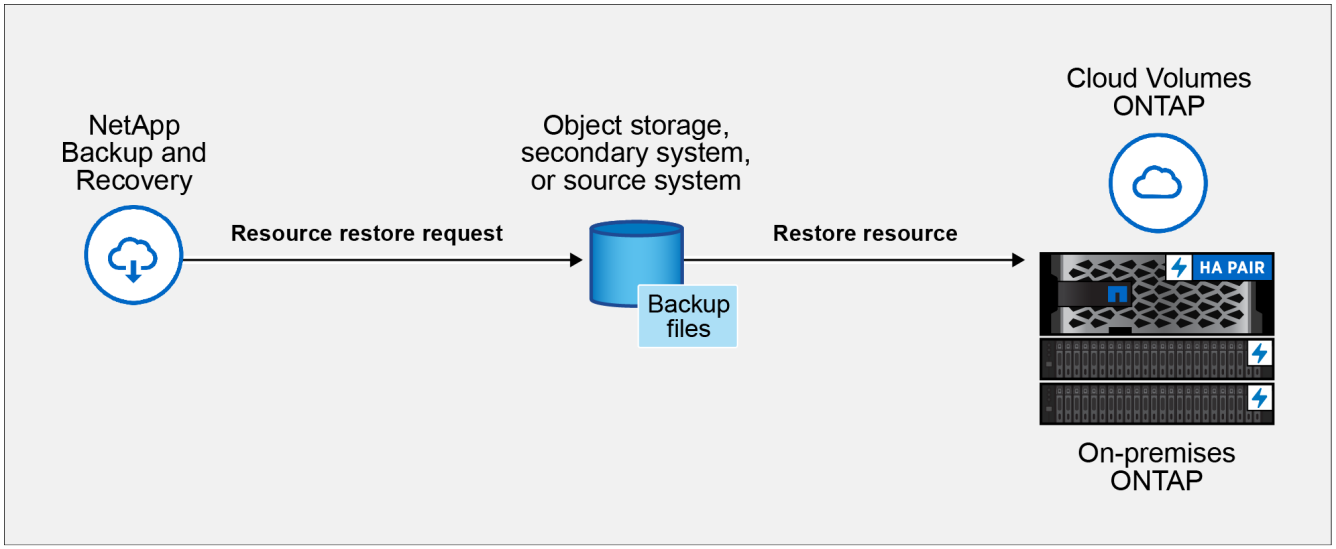
Resilience がアクティブになっている場合 (バックアップ ポリシーで DataLock と Ransomware Resilience を有効にした場合)、データを復元する前に、バックアップ ファイルに対して追加の整合性チェックを実行するように求められます。スキャンを実行することをお勧めします。

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。

- 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。



- 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。

復元方法

次のいずれかの方法を使用してワークロードを復元します。

- 復元ページから: リソースの名前、場所、または最終有効日がわからない場合に、このオプションを使用してリソースを復元します。フィルターを使用してスナップショットを検索します。
- インベントリ ページから: 特定のリソースの名前、場所、最終有効日がわかっている場合は、このオプションを使用してそのリソースを復元します。リストを参照してリソースを見つけます。

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" 。

復元オプション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データベース ワークロードを復元します。

手順

1. NetApp Backup and Recoveryメニューから、[復元] を選択します。
2. 復元するデータベースを選択します。フィルターを使用して検索します。
3. 復元オプションを選択します:
   - スナップショットからの復元
   - ファイル名、場所、最終有効日が分かっている場合は、特定の時点に復元します。
   - 最新のバックアップに復元する

スナップショットからワークロードを復元する

1. 復元オプション ページから続行して、*スナップショットからの復元*を選択します。

   スナップショットのリストが表示されます。

2. 復元するスナップショットを選択します。
3. *次へ*を選択します。

   次に、宛先オプションが表示されます。

4. 宛先の詳細ページで、次の情報を入力します。
   - 宛先設定: データを元の場所に復元するか、別の場所に復元するかを選択します。別の場所の場合は、ホスト名とインスタンスを選択し、データベース名を入力して、スナップショットを復元する宛先パスを入力します。
   - 復元前のオプション:
     - 復元中に同じ名前のデータベースを上書きする: 復元中、元のデータベース名は保持されます。
     - **SQL** データベースのレプリケーション設定を保持: 復元操作後も SQL データベースのレプリケーション設定を保持します。
     - 復元前にトランザクション ログのバックアップを作成する: 復元操作の前にトランザクション ログのバックアップを作成します。* 復元前のトランザクション ログ バックアップが失敗した場合は復元を終了: トランザクション ログ バックアップが失敗した場合は復元操作を停止します。
     - **Prescript**: 復元操作の前に実行するスクリプトの完全なパス、スクリプトが取る引数、およびスクリプトが完了するまでの待機時間を入力します。
   - 復元後のオプション:
     - *動作可能*ですが、追加のトランザクション ログを復元するためには使用できません。これにより、トランザクション ログ バックアップが適用された後、データベースがオンラインに戻ります。
     - *非動作*ですが、追加のトランザクション ログを復元するために使用できます。トランザクション ログ バックアップを復元しながら、復元操作後にデータベースを非動作状態に維持します。このオプションは、追加のトランザクション ログを復元するのに役立ちます。
     - *読み取り専用モード*で、追加のトランザクション ログを復元できます。データベースを読み取

り専用モードで復元し、トランザクション ログ バックアップを適用します。

- **Postscript**: 復元操作後に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。

特定の時点に復元する

NetApp Backup and Recovery は、ログと最新のスナップショットを使用して、データのポイントインタイム リストアを作成します。

1. 復元オプション ページから続行して、*特定の時点に復元*を選択します。
2. *次へ*を選択します。
3. 「特定の時点への復元」ページで、次の情報を入力します。
   - データ復元の日時: 復元するデータの正確な日時を入力します。この日付と時刻は、Microsoft SQL Server データベース ホストからのものです。
4. *検索*を選択します。
5. 復元するスナップショットを選択します。
6. *次へ*を選択します。
7. 宛先の詳細ページで、次の情報を入力します。
   - 宛先設定: データを元の場所に復元するか、別の場所に復元するかを選択します。別の場所の場合は、ホスト名とインスタンスを選択し、データベース名を入力して、宛先パスを入力します。
   - 復元前のオプション:
     - 元のデータベース名を保持: 復元中に、元のデータベース名が保持されます。
     - **SQL** データベースのレプリケーション設定を保持: 復元操作後も SQL データベースのレプリケーション設定を保持します。
     - **Prescript**: 復元操作の前に実行するスクリプトの完全なパス、スクリプトが取る引数、およびスクリプトが完了するまでの待機時間を入力します。
   - 復元後のオプション:
     - *動作可能*ですが、追加のトランザクション ログを復元するためには使用できません。これにより、トランザクション ログ バックアップが適用された後、データベースがオンラインに戻ります。
     - *非動作*ですが、追加のトランザクション ログを復元するために使用できます。トランザクション ログ バックアップを復元しながら、復元操作後にデータベースを非動作状態に維持します。このオプションは、追加のトランザクション ログを復元するのに役立ちます。
     - *読み取り専用モード*で、追加のトランザクション ログを復元できます。データベースを読み取り専用モードで復元し、トランザクション ログ バックアップを適用します。
     - **Postscript**: 復元操作後に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。
8. *復元*を選択します。

最新のバックアップに復元する

このオプションは、最新の完全バックアップとログ バックアップを使用して、データを最後の正常な状態に復元します。システムは最後のスナップショットから現在までのログをスキャンします。このプロセスでは、変更とアクティビティを追跡して、データの最新かつ正確なバージョンを復元します。

1. 復元オプション ページから続行して、*最新のバックアップに復元*を選択します。

   NetApp Backup and Recovery、復元操作に使用できるスナップショットが表示されます。

2. 「最新の状態に復元」ページで、ローカル、セカンダリ ストレージ、またはオブジェクト ストレージのスナップショットの場所を選択します。
3. *次へ*を選択します。
4. 宛先の詳細ページで、次の情報を入力します。
   - 宛先設定: データを元の場所に復元するか、別の場所に復元するかを選択します。別の場所の場合は、ホスト名とインスタンスを選択し、データベース名を入力して、宛先パスを入力します。
   - 復元前のオプション:
     - 復元中に同じ名前のデータベースを上書きする: 復元中、元のデータベース名は保持されます。
     - **SQL** データベースのレプリケーション設定を保持: 復元操作後も SQL データベースのレプリケーション設定を保持します。
     - 復元前にトランザクション ログ バックアップを作成する: 復元操作の前にトランザクション ログ バックアップを作成します。
     - 復元前のトランザクション ログ バックアップが失敗した場合は復元を終了: トランザクション ログ バックアップが失敗した場合は復元操作を停止します。
     - **Prescript**: 復元操作の前に実行するスクリプトの完全なパス、スクリプトが取る引数、およびスクリプトが完了するまでの待機時間を入力します。
   - 復元後のオプション:
     - *動作可能*ですが、追加のトランザクション ログを復元するためには使用できません。これにより、トランザクション ログ バックアップが適用された後、データベースがオンラインに戻ります。
     - *非動作*ですが、追加のトランザクション ログを復元するために使用できます。トランザクション ログ バックアップを復元しながら、復元操作後にデータベースを非動作状態に維持します。このオプションは、追加のトランザクション ログを復元するのに役立ちます。
     - *読み取り専用モード*で、追加のトランザクション ログを復元できます。データベースを読み取り専用モードで復元し、トランザクション ログ バックアップを適用します。
     - **Postscript**: 復元操作後に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。

インベントリオプションからワークロードデータを復元する

インベントリ ページからデータベース ワークロードを復元します。インベントリ オプションを使用すると、インスタンスではなくデータベースのみを復元できます。

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. 復元するリソースが配置されているホストを選択します。
3. *アクション*を選択します ••• アイコンをクリックし、[詳細を表示] を選択します。
4. Microsoft SQL Server ページで、データベース タブを選択します。
5. 「データベース」メニューで、「保護」ステータスのデータベースを選択します。
6. *アクション*を選択します ••• アイコンをクリックし、[復元] を選択します。

   「復元」ページから復元する場合と同じ 3 つのオプションが表示されます。

   - スナップショットからの復元
   - 特定の時点に復元する
   - 最新のバックアップに復元する
7. 復元ページから復元オプションについて同じ手順を続行します。

NetApp Backup and Recoveryを使用して Microsoft SQL Server ワークロードをクローンする

NetApp Backup and Recoveryを使用して、開発、テスト、または保護のために Microsoft SQL Server アプリケーション データを VM に複製します。 SQL Server ワークロードのインスタント スナップショットまたは既存のスナップショットからクローンを作成します。

次のクローンの種類から選択します。

- インスタント スナップショットとクローン: バックアップから作成されたソース データのポイントインタイム コピーであるインスタント スナップショットから、Microsoft SQL Server ワークロードのクローンを作成できます。クローンは、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。データが失われたり破損したりした場合に、クローンを使用してワークロードを復元できます。
- 既存のスナップショットからのクローン作成: ワークロードで使用可能なスナップショットのリストから既存のスナップショットを選択できます。このオプションは、特定の時点からクローンを作成する場合に便利です。プライマリ ストレージまたはセカンダリ ストレージにクローンを作成します。

次の保護目標を達成できます。

- クローンを作成する
- クローンの更新
- クローンのスプリット
- クローンを削除する

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" 。

クローンを作成する

Microsoft SQL Server ワークロードのクローンを作成できます。クローンとは、バックアップから作成されたソース データのコピーです。クローンは、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。データが失われたり破損したりした場合に、クローンを使用してワークロードを復元できます。

既存のスナップショットまたはインスタント スナップショットからクローンを作成できます。インスタント スナップショットは、バックアップから作成されたソース データの特定時点のコピーです。データが失われたり破損したりした場合に、クローンを使用してワークロードを復元できます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. *新しいクローンを作成*を選択します。
3. クローンの種類を選択します:
   - 既存のスナップショットからのクローン作成とデータベースの更新: スナップショットを選択し、クローン オプションを構成します。
   - インスタント スナップショットとクローン: ソース データのスナップショットを今すぐ作成し、そのスナップショットからクローンを作成します。このオプションは、ソース ワークロードの最新データからクローンを作成する場合に便利です。
4. データベース ソース セクションを完了します。
   - 単一クローンまたは一括クローン: 単一クローンを作成するか、複数クローンを作成するかを選択します。 *一括クローン*を選択すると、既に作成した保護グループを使用して一度に複数のクローンを作成できます。このオプションは、異なるワークロードに対して複数のクローンを作成する場合に便利です。
   - ソース データベース ホスト、インスタンス、および名前: クローンのソース データベース ホスト、インスタンス、および名前を選択します。ソース データベースは、クローンの作成元となるデータベースです。
5. データベース ターゲット セクションを完了します。
   - ターゲット データベース ホスト、インスタンス、および名前: クローンのターゲット データベース ホスト、インスタンス、および名前を選択します。ターゲット データベースは、クローンが作成される場所です。

     必要に応じて、ターゲット名のドロップダウン リストから サフィックス を選択し、クローンされたデータベース名にサフィックスを追加します。サフィックスを追加しない場合、クローンされたデータベース名はソース データベース名と同じになります。

   - **QoS (**最大スループット**)**: クローンのサービス品質 (QoS) 最大スループットを MBps 単位で選択します。 QoS は、最大スループットや IOPS など、クローンのパフォーマンス特性を定義します。
6. *マウント*セクションを完了します。
   - マウント ポイントの自動割り当て: オブジェクト ストア内のクローンのマウント ポイントを自動的に割り当てます。
   - マウント ポイント パスの定義: クローンのマウント ポイントを入力します。マウント ポイントは、オブジェクト ストア内でクローンがマウントされる場所です。ドライブ文字を選択し、データ ファイルのパスを入力し、ログ ファイルのパスを入力します。
7. *次へ*を選択します。

8. 復元ポイントを選択します:
    - 既存のスナップショット: ワークロードで使用可能なスナップショットのリストから既存のスナップショットを選択します。このオプションは、特定の時点からクローンを作成する場合に便利です。
    - インスタント スナップショットとクローン: ワークロードで使用可能なスナップショットのリストから最新のスナップショットを選択します。このオプションは、ソース ワークロードの最新データからクローンを作成する場合に便利です。
9. *インスタント スナップショットとクローン*の作成を選択した場合は、クローンの保存場所を選択します。
    - ローカル ストレージ: ONTAPシステムのローカル ストレージにクローンを作成するには、このオプションを選択します。ローカル ストレージは、 ONTAPシステムに直接接続されたストレージです。
    - セカンダリ ストレージ: ONTAPシステムのセカンダリ ストレージにクローンを作成するには、このオプションを選択します。セカンダリ ストレージは、バックアップおよびリカバリのワークロードに使用されるストレージです。
10. データとログの保存先を選択します。
11. *次へ*を選択します。
12. *詳細オプション*セクションを完了します。
13. インスタント スナップショットとクローン を選択した場合は、次のオプションを完了します。
    - クローンの更新スケジュールと有効期限: インスタントクローン を選択した場合は、クローンの更新を開始する日付を入力します。クローン スケジュールは、クローンがいつ作成されるかを定義します。
        - スケジュールの有効期限が切れたらクローンを削除: クローンの有効期限が切れたらクローンを削除する場合。
        - クローンの更新間隔: クローンを更新する頻度を選択します。クローンを毎時、毎日、毎週、毎月、または四半期ごとに更新することを選択できます。このオプションは、クローンをソース ワークロードに合わせて最新の状態に保つ場合に便利です。
    - プレスクリプトとポストスクリプト: オプションで、クローンの作成前と作成後に実行するスクリプトを追加します。これらのスクリプトは、クローンの設定や通知の送信などの追加タスクを実行できます。
    - 通知: オプションで、ジョブ レポートとともにクローン作成ステータスに関する通知を受信する電子メール アドレスを指定します。クローン作成ステータスに関する通知を受信するための Webhook URL を指定することもできます。成功通知と失敗通知の両方、またはどちらか一方のみの通知を指定することができます。
    - タグ: 後でリソース グループを検索する際に役立つラベルを選択し、[適用] を選択します。たとえば、複数のリソース グループに「HR」をタグとして追加すると、後で「HR」タグに関連付けられているすべてのリソース グループを見つけることができます。
14. *作成*を選択します。
15. クローンが作成されると、*インベントリ*ページで確認できます。

クローンの更新

Microsoft SQL Server ワークロードのクローンを更新できます。クローンを更新すると、クローンはそのソース ワークロードの最新データで更新されます。これは、クローンをソース ワークロードに合わせて最新の状態に保つ場合に便利です。

データベース名を変更したり、最新のインスタント スナップショットを使用したり、既存の運用スナップショットから更新したりすることができます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. 更新する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 ••• > クローンを更新。
4. *詳細設定*セクションを完了します。
   - 回復範囲: すべてのログ バックアップを回復するか、特定の時点までのログ バックアップを回復するかを選択します。このオプションは、クローンを特定の時点に復元する場合に便利です。
   - クローンの更新スケジュールと有効期限: インスタントクローン を選択した場合は、クローンの更新を開始する日付を入力します。クローン スケジュールは、クローンがいつ作成されるかを定義します。
     - スケジュールの有効期限が切れたらクローンを削除: クローンの有効期限が切れたらクローンを削除する場合。
     - クローンの更新間隔: クローンを更新する頻度を選択します。クローンを毎時、毎日、毎週、毎月、または四半期ごとに更新することを選択できます。このオプションは、クローンをソース ワークロードに合わせて最新の状態に保つ場合に便利です。
   - **iGroup** 設定: クローンの iGroup を選択します。iGroup は、クローンへのアクセスに使用されるイニシエーターの論理グループです。既存の iGroup を選択するか、新しい iGroup を作成することができます。プライマリまたはセカンダリONTAPストレージ システムから iGroup を選択します。
   - プレスクリプトとポストスクリプト: オプションで、クローンの作成前と作成後に実行するスクリプトを追加します。これらのスクリプトは、クローンの設定や通知の送信などの追加タスクを実行できます。
   - 通知: オプションで、ジョブ レポートとともにクローン作成ステータスに関する通知を受信する電子メール アドレスを指定します。クローン作成ステータスに関する通知を受信するための Webhook URL を指定することもできます。成功通知と失敗通知の両方、またはどちらか一方のみの通知を指定することができます。
   - タグ: 後でリソース グループを検索するときに役立つ 1 つ以上のラベルを入力します。たとえば、複数のリソース グループに「HR」をタグとして追加すると、後で HR タグに関連付けられているすべてのリソース グループを見つけることができます。
5. 続行するには、更新確認ダイアログボックスで「更新」を選択します。

クローンの更新をスキップする

クローンを変更せずに維持するには、クローンの更新をスキップします。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. 更新をスキップする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 ••• > 更新をスキップ。
4. [更新をスキップする] 確認ダイアログ ボックスで、次の操作を行います。
   a. 次の更新スケジュールのみをスキップするには、[次の更新スケジュールのみをスキップ] を選択します。

b. 続行するには、[スキップ] を選択します。

クローンのスプリット

Microsoft SQL Server ワークロードのクローンを分割できます。クローンを分割すると、クローンから新しいバックアップが作成されます。新しいバックアップを使用してワークロードを復元できます。

クローンを独立したクローンまたは長期クローンとして分割することを選択できます。ウィザードには、SVM の一部であるアグリゲートのリスト、それらのサイズ、およびクローン ボリュームが存在する場所が表示されます。 NetApp Backup and Recovery は、クローンを分割するのに十分なスペースがあるかどうかも示します。クローンを分割すると、クローンはその保護のために独立したデータベースになります。

クローンジョブは削除されず、他のクローンに再度再利用できます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. 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. 分割クローンの詳細を確認し、「分割」を選択します。
5. 分割クローンが作成されると、*インベントリ*ページで確認できます。

クローンを削除する

Microsoft SQL Server ワークロードのクローンを削除できます。クローンを削除すると、オブジェクト ストアからクローンが削除され、ストレージ領域が解放されます。

ポリシーによってクローンが保護されている場合、クローンおよび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ます > クローンを削除。
4. クローンの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。
   a. クローンまたはそのストレージにアクセスできない場合でも、クローンされたリソースをSnapCenterから削除するには、[強制削除] を選択します。
   b. *削除*を選択します。
5. 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。

NetApp Backup and Recoveryで Microsoft SQL Server のインベントリを管理する

NetApp Backup and Recovery は、 Microsoft SQL Server ホスト、データベース、インスタンスの管理に役立ちます。インベントリの保護設定を表示、変更、または削除できます。

在庫管理に関連する次のタスクを実行できます。

- ホスト情報の管理
  - スケジュールを中断
  - ホストを編集または削除する
- インスタンス情報の管理
  - 資格情報をリソースに関連付ける
  - オンデマンドバックアップを開始して今すぐバックアップ
  - 保護設定を編集する
- データベース情報の管理
  - データベースを保護する
  - データベースを復元する
  - 保護設定を編集する
  - オンデマンドバックアップを開始して今すぐバックアップ
- ログ ディレクトリを構成します ([インベントリ] > [ホスト])。スナップショット内のデータベース ホストのログをバックアップする場合は、まずNetApp Backup and Recoveryでログを構成します。詳細については、"NetApp Backup and Recovery設定を構成する" 。

ホスト情報の管理

ホスト情報を管理して、適切なホストが保護されるようにすることができます。ホスト情報を表示、編集、削除できます。

必要な**NetApp Console**ロール ストレージ ビューア、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、バックアップおよびリカバリ リストア管理者、またはバックアップおよびリカバリ クローン管理者のロール。 "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" 。

- ログディレクトリを構成します。詳細については、"NetApp Backup and Recovery設定を構成する" 。
- スケジュールを中断
- ホストを編集する
- ホストを削除する

ホストの管理

システム内で検出されたホストを管理できます。個別に、またはグループとして管理できます。

「ホスト」列で「管理対象外」ステータスのホストを管理できます。 NetApp Backup and Recovery はすでに「管理対象」ステータスのホストを管理しています。

NetApp Backup and Recoveryでホストを管理すると、 SnapCenterそれらのホスト上のリソースは管理されなくなります。

必要な**NetApp Console**ロール ストレージ ビューアー、またはバックアップおよび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. 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. *ホスト*タブを選択します。
5. 1 つ以上のホストを選択します。複数のホストを選択した場合は、一括操作オプションが表示され、*管理（最大 5 台のホスト）*を選択できます。
6. アクションアイコンを選択します ••• > 管理。
7. ホストの依存関係を確認します。
   - vCenter が表示されない場合は、鉛筆アイコンを選択して、vCenter の詳細を追加または編集します。
   - vCenter を追加する場合は、[vCenter の登録] を選択して vCenter も登録する必要があります。
8. 設定をテストするには、「設定の検証」を選択します。
9. ホストを管理するには、[管理] を選択します。

スケジュールを中断

ホストのメンテナンス中にバックアップおよび復元操作を停止するには、スケジュールを一時停止します。

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. スケジュールを一時停止するホストを選択します。
3. アクション*を選択します ••• アイコンをクリックし、**[*スケジュールの一時停止]を選択します。
4. 確認ダイアログボックスで、[一時停止] を選択します。

ホストを編集する

vCenter サーバー情報、ホスト登録資格情報、および詳細設定オプションを変更できます。

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. 編集するホストを選択します。
3. *アクション*を選択します ••• アイコンをクリックし、[ホストの編集] を選択します。
4. ホスト情報を編集します。
5. *完了*を選択します。

ホストを削除する

ホスト情報を削除すると、サービス料金を停止できます。

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. 削除するホストを選択します。

3. *アクション*を選択します ••• アイコンをクリックし、[ホストの削除] を選択します。
4. 確認情報を確認し、「削除」を選択します。

インスタンス情報の管理

次の方法でインスタンス情報を管理し、リソース保護のための適切な資格情報を割り当て、リソースをバックアップすることができます。

- インスタンスを保護する
- アソシエイト資格
- 資格情報の関連付けを解除する
- 編集保護
- 今すぐバックアップ

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" 。

データベースインスタンスを保護する

リソース保護のスケジュールと保持を管理するポリシーを使用して、データベース インスタンスにポリシーを割り当てることができます。

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. 表示するワークロードを選択し、[表示] を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[保護] を選択します。
6. ポリシーを選択するか、新しいポリシーを作成します。

   ポリシー作成の詳細については、"ポリシーを作成します。" 。

7. バックアップの前後に実行するスクリプトに関する情報を提供します。
   - 事前スクリプト: 保護アクションがトリガーされる前にスクリプトを自動的に実行するには、スクリプトのファイル名と場所を入力します。これは、保護ワークフローの前に実行する必要がある追加のタスクや構成を実行するのに役立ちます。
   - 事後スクリプト: 保護アクションが完了した後にスクリプトを自動的に実行するには、スクリプトのファイル名と場所を入力します。これは、保護ワークフローの後に実行する必要がある追加のタスクや構成を実行するのに役立ちます。
8. スナップショットを検証する方法についての情報を提供します。
   - 保存場所: 検証スナップショットを保存する場所を選択します。
   - 検証リソース: 検証するリソースがローカル スナップショット上にあるか、 ONTAPセカンダリ ストレージ上にあるかを選択します。

- 検証スケジュール: 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。

資格情報をリソースに関連付ける

保護が行われるように、資格情報をリソースに関連付けることができます。

詳細については、"資格情報を含むNetApp Backup and Recoveryの設定を構成する" 。

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. 表示するワークロードを選択し、[表示] を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[資格情報の関連付け] を選択します。
6. 既存の資格情報を使用するか、新しい資格情報を作成します。

保護設定を編集する

ポリシーを変更したり、新しいポリシーを作成したり、スケジュールを設定したり、保持設定を設定したりできます。

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. 表示するワークロードを選択し、[表示] を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[保護の編集] を選択します。

   ポリシー作成の詳細については、"ポリシーを作成します。" 。

今すぐバックアップ

データをすぐに保護するために今すぐバックアップしてください。

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. 表示するワークロードを選択し、[表示] を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[今すぐバックアップ] を選択します。
6. バックアップの種類を選択し、スケジュールを設定します。

   アドホックバックアップの作成の詳細については、"ポリシーを作成します。" 。

データベース情報の管理

データベース情報は次の方法で管理できます。

- データベースを保護する
- データベースを復元する
- 保護の詳細を表示
- 保護設定を編集する
- 今すぐバックアップ

データベースを保護する

ポリシーを変更したり、新しいポリシーを作成したり、スケジュールを設定したり、保持設定を設定したりできます。

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 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. 表示するワークロードを選択し、[表示] を選択します。
3. *データベース*タブを選択します。
4. データベースを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[保護] を選択します。

   ポリシー作成の詳細については、"ポリシーを作成します。" 。

データベースを復元する

データを保護するためにデータベースを復元します。

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" 。

1. *データベース*タブを選択します。
2. データベースを選択します。
3. *アクション*を選択します ••• アイコンをクリックし、[復元] を選択します。

   ワークロードの復元については、以下を参照してください。"ワークロードを復元する" 。

保護設定を編集する

ポリシーを変更したり、新しいポリシーを作成したり、スケジュールを設定したり、保持設定を設定したりできます。

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 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. 表示するワークロードを選択し、[表示] を選択します。
3. *データベース*タブを選択します。
4. データベースを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[保護の編集] を選択します。

   ポリシー作成の詳細については、"ポリシーを作成します。" 。

今すぐバックアップ

今すぐ Microsoft SQL Server インスタンスとデータベースをバックアップして、データを保護できます。

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 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. 表示するワークロードを選択し、[表示] を選択します。
3. *インスタンス*または*データベース*タブを選択します。
4. インスタンスまたはデータベースを選択します。
5. *アクション*を選択します ••• アイコンをクリックし、[今すぐバックアップ] を選択します。

NetApp Backup and Recoveryで Microsoft SQL Server スナップショットを管理する

Microsoft SQL Server スナップショットは、NetApp Backup and Recoveryから削除することで管理できます。

スナップショットを削除する

削除できるのはローカル スナップショットのみです。

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で、**Inventory** を選択します。
2. ワークロードを選択し、[表示] を選択します。
3. *データベース*タブを選択します。

4. スナップショットを削除するデータベースを選択します。
5. [アクション] メニューから、[保護の詳細を表示] を選択します。
6. 削除するローカル スナップショットを選択します。

   その行の 場所 列のローカル スナップショット アイコンが青色で表示されていることを確認します。

7. *アクション*を選択しますアイコンをクリックし、[ローカル スナップショットの削除] を選択します。
8. 確認ダイアログボックスで、[削除] を選択します。

NetApp Backup and Recoveryで Microsoft SQL Server ワークロードのレポートを作成する

NetApp Backup and Recoveryでは、Microsoft SQL Server ワークロードのレポートを作成して、成功したバックアップと失敗したバックアップの数、バックアップの種類、ストレージ システム、タイムスタンプなどのバックアップの状態と詳細を表示します。

レポートを作成する

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、バックアップおよびリカバリ リストア管理者、バックアップおよびリカバリ クローン管理者。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" 。

1. NetApp Backup and Recoveryメニューから、レポート オプションを選択します。
2. *レポートの作成*を選択します。
3. レポート範囲の詳細を入力します:
   - レポート名: レポートの一意の名前を入力します。
   - レポート タイプ: アカウント別またはワークロード (Microsoft SQL Server) 別にレポートを作成するかどうかを選択します。
   - ホストを選択: ワークロードで選択した場合は、レポートを生成するホストを選択します。
   - コンテンツの選択: レポートにすべてのバックアップの概要を含めるか、各バックアップの詳細を含めるかを選択します。 （「アカウント別」を選択した場合）
4. レポート範囲を入力: レポートに過去 1 日、過去 7 日間、過去 30 日間、前四半期、または前年度のデータを含めるかどうかを選択します。
5. レポート配信の詳細を入力します。レポートを電子メールで配信する場合は、[電子メールを使用してレポートを送信] をオンにします。レポートを送信するメールアドレスを入力します。

   設定ページで電子メール通知を構成します。電子メール通知の設定の詳細については、"設定を構成する" 。

VMwareワークロードを保護する（SnapCenter Plug-in for VMware不使用）

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

NetApp Backup and Recoveryを使用して VMware VM と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が高く、クラッシュ整合性と VM 整合性を備えたバックアップおよび復元操作を提供します。VMware ワークロードを Amazon Web Services S3 またはStorageGRIDにバックアップし、VMware ワークロードをオンプレミスの VMware ホストに復元できます。

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 UIのバージョンを切り替えるには、"以前のNetApp Backup and RecoveryUIに切り替える" 。

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。

- 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"VMwareワークロードを今すぐバックアップ"。
- 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。

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" 。

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. 保護グループに含める VM またはデータベースを選択します。
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。

   ポリシーを作成する場合は、「新しいポリシーの作成」を選択し、指示に従ってポリシーを作成します。見る"ポリシーを作成"詳細についてはこちらをご覧ください。

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 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。

- 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 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"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

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. 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、データストア、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。

> バックアップに適用されるポリシーは、保護グループ、データストア、または仮想マシン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。

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。

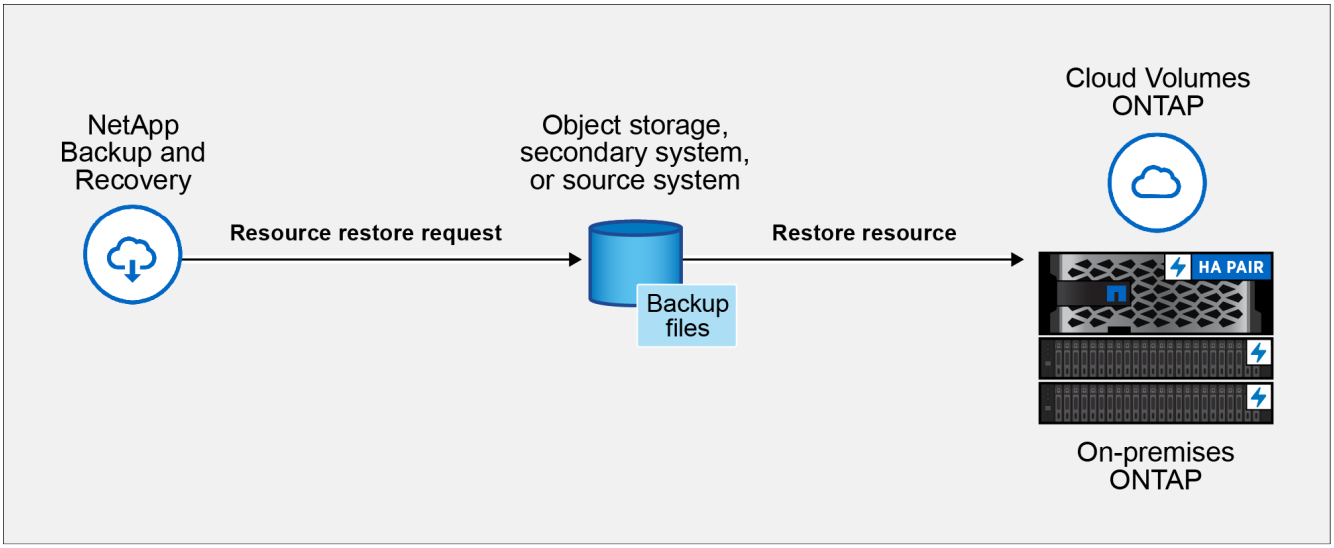
オブジェクトストレージからの復元に関する考慮事項

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 Ransomware Resilience が有効になっている場合は、復元する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。
   - *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。

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。

ゲストファイルとフォルダを復元する

WindowsゲストOSの仮想マシン ディスク（VMDK）からファイルやフォルダをリストアできます。

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 に接続し、ゲスト ファイルの復元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

   VMDK ファイルを参照し、復元する 1 つ以上のファイルまたはフォルダーを選択します。

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

Windows ゲスト OS 上の VMDK からファイルまたはフォルダーを復元する前に、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 ツールからの情報を使用して、VMware ゲスト OS への接続を確立します。

- 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。

- 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。

  NetApp Backup and Recovery、復元するファイルまたはフォルダの検索はサポートされていません。始

める前に、スナップショット内のファイルまたはフォルダーと対応する VMDK の場所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。

- 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 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。
- LinuxゲストOSからはリストアできません。

  LinuxゲストOSを実行しているVMからファイルやフォルダをリストアすることはできません。ただし、VMDKを接続し、ファイルとフォルダを手動でリストアすることもできます。サポートされているゲストOSの最新情報については、 "NetApp Interoperability Matrix Tool（IMT）" 。

- 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。

VMDKからのゲスト ファイルとフォルダのリストア

WindowsゲストOSのVMDKから1つ以上のファイルまたはフォルダをリストアできます。

開始する前に

ゲスト VM からファイルやフォルダを復元する前に、 NetApp Backup and Recoveryでゲスト VM の資格情報を作成する必要があります。NetApp Backup and Recovery は、仮想ディスクを接続するときに、これらの資格情報を使用してゲスト VM を認証します。

タスク概要

ゲスト ファイルまたはフォルダのリストア パフォーマンスは、リストアするファイル/ /フォルダのサイズと、リストアするファイル / フォルダの数という2つの要因によって決まります。リストア対象のデータ セットのサイズが同じ場合、サイズの小さいファイルを多数リストアするのにかかる時間は、サイズの大きいファイルを少数リストアするのにかかる時間と比較して、想定よりも長くなることがあります。

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。

ゲスト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ー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保持されません。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。

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. *仮想マシン*メニューを選択します。
3. 復元するファイルが含まれているリストから仮想マシンを選択します。
4. アクションアイコンを選択します ••• その VM に対して。
5. *ファイルとフォルダの復元*を選択します。
6. 復元するスナップショットを選択し、[次へ] を選択します。
7. 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。
8. *次へ*を選択します。
9. VM に接続する仮想ディスクをリストから選択し、[次へ] を選択します。
10. [仮想マシンの資格情報の選択] ページで、ゲスト 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、次の操作を行います。
    a. 資格情報名: 資格情報の名前を入力します。
    b. 認証モード: **Windows** を選択します。
    c. エージェント: NetApp Backup and Recoveryとこのホスト間の通信を処理するコンソール エージェントをリストから選択します。
    d. ドメインとユーザー名: 資格情報の NetBIOS またはドメイン FQDN とユーザー名を入力します。
    e. パスワード: 資格情報のパスワードを入力します。
    f. *追加*を選択します。
11. ゲスト VM での認証に使用する仮想マシン資格情報を選択します。

NetApp Backup and Recovery は仮想ディスクを VM に接続し、隠しファイルも含めたすべてのファイルとフォルダを表示します。システム予約済み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。

選択したファイルとフォルダは画面の右側のペインに表示されます。

12. *次へ*を選択します。
13. 選択したファイルをリストアするゲストへのUNC共有パスを入力します。
    - IPv4アドレスの例: `\\10.60.136.65\c$`
    - IPv6アドレスの例: `\\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。
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。

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 system and account used is 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。

KVM ワークロードを保護する（プレビュー）

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 UIのバージョンを切り替えるには、"以前のNetApp Backup and RecoveryUIに切り替える" 。

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. 保護グループに含める VM またはストレージ プールを選択します。
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。

   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" 。

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

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 Ransomware Resilience を有効にしている場合)、データを復元する前に、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お勧めします。

> 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 (検索と復元とも呼ばれます) からは、VM の正確な名前、VM が存在する場所、VM が最後に正常な状態であった日付を覚えていなくても、VM 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。

復元オプション（検索と復元）から**VM**を復元する

復元オプションを使用して KVM 仮想マシンを復元します。スナップショットは、名前またはフィルター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

1. クイック復元を有効にする: クイック復元操作を実行するにはこれを選択します。復元されたボリュームとデータはすぐに利用できるようになります。クイック リストア プロセス中はデータへのアクセスが通常よりも遅くなる可能性があるため、高パフォーマンスが必要なボリュームではこれを使用しないでください。
2. 復元前オプション: 復元操作の前に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. 復元後のオプション:
   - **VM** の再起動: 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 VM を再起動するには、これを選択します。
   - **Postscript**: 復元操作後に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. *通知*セクション:
   - 電子メール通知を有効にする: 復元操作に関する電子メール通知を受信し、受信する通知の種類を指定するには、これを選択します。
5. *復元*を選択します。

別の場所へのリストア

KVM ワークロード プレビューでは使用できません。

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 UIのバージョンを切り替えるには、"以前のNetApp Backup and RecoveryUIに切り替える" 。

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" 。

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。
7. 保護グループの名前やグループ内の仮想マシンなどの設定を変更します。
8. *次へ*を選択します。
9. 必要に応じて保護ポリシーを変更します。完了したら、[次へ] を選択します。
10. 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 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。

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 ストレージ内のバックアップ 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 Ransomware Resilience を有効にしている場合)、データを復元する前に、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お勧めします。

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 (検索と復元とも呼ばれます) からは、リソースの正確な名前、リソースが存在する場所、リソースが最後に良好な状態であっ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。

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 Hyper-V ワークロードを復元します。スナップショットは、名前またはフィルター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

元の場所に復元する場合、[宛先設定] セクションを展開して宛先設定を表示することはできますが、変更することはできません。

1. 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。
2. *復元*を選択します。

別の場所へのリストア

1. 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。
2. 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。
3. *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。
4. *復元*を選択します。

Oracle Database ワークロードの保護（プレビュー）

Oracle Databaseワークロードの保護の概要

NetApp Backup and Recoveryを使用してOracleデータベースとログを保護します。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）」の状態およびデータベース整合性のあるバックアップとリストアを実現します。Oracle DatabaseワークロードをAWS S3、NetApp StorageGRID、Azure Blob Storage、またはONTAP S3にバックアップします。バックアップをオンプレミスのOracleホストにリストアします。

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 UIのバージョンを切り替えるには、"以前のNetApp Backup and RecoveryUIに切り替える" 。

NetApp Backup and Recoveryを使用して、Oracleデータベースワークロードに関連する次のタスクを実行できます：

- "Oracle Databaseワークロードを検出"
- "Oracle Database ワークロードの保護グループの作成と管理"
- "Oracle Databaseワークロードのバックアップ"
- "Oracle Database ワークロードのリストア"

NetApp Backup and RecoveryでOracle Databaseワークロードを検出

NetApp Backup and Recovery、まず Oracle データベースを検出して保護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" 。

Oracleホストを追加してリソースを検出する

Oracle 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。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、*Oracle*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: **Oracle** を選択します。
   b. この Oracle 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: 新しい Oracle ホストを追加します。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

Oracle 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

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を使用した**Oracle Database**ワークロードの保護グループの作成と管理

保護グループを作成して、Oracle Database リソース セットのバックアップ操作を管理します。保護グループとは、まとめて保護するデータベースなどのリソースの論理的なグループです。 Oracle データベース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。"Oracle Databaseの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. 保護グループに含める VM またはストレージ プールを選択します。
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。

   ポリシーを作成する場合は、「新しいポリシーの作成」を選択し、指示に従ってポリシーを作成します。見る"ポリシーを作成"詳細についてはこちらをご覧ください。

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 ••• > 保護を解除。
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を使用したOracle Databaseワークロードのバックアップ

NetApp Backup and Recoveryを使用して、オンプレミスのONTAPシステムから Amazon S3、 NetApp StorageGRID、Microsoft Azure Blob Storage、 ONTAP S3 などのクラウド ストレージに Oracle Database 保護グループまたはデータベースをバックアップします。 NetApp Backup and Recovery は、各保護グループ内のデータベースとログデータをバックアップします。

保護グループまたは単一のデータベース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。"NetApp Backup and Recoveryを使用したOracle Database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。
- 保護グループを今すぐバックアップします (オンデマンド バックアップを今すぐ作成します)。
- 今すぐデータベースをバックアップします。

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

システムを変更する前にオンデマンド バックアップを実行して、データが保護されていることを確認します。

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 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、*Oracle*タイルを選択します。
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。

   NetApp Backup and Recovery、バックアップと保護グループの両方に同じポリシーが使用されます。

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。

オンデマンドバックアップで今すぐデータベースをバックアップ

単一のデータベースのオンデマンド バックアップを実行できます。

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" 。

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、*Oracle*タイルを選択します。
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. *データベース*タブを選択します。
7. バックアップするデータベースを選択します。
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。
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でOracleデータベースを復元する

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 Oracle データベースを復元します。

これらの場所から復元

異なる開始場所からデータベースを復元できます。

- 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

データを元の場所に復元することはできますが、このプライベート プレビュー リリースでは別の場所に復元することはできません。

- 元の場所に復元する

Oracleデータベースの復元の仕組み

Oracle データベースを復元すると、次のことが起こります。

- ローカル スナップショットからデータベースを復元すると、 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。

- 複製されたストレージから復元する場合は、元の場所に復元できます。
- 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、データをソース ストレージまたはオンプレミスのONTAPシステムに復元し、そこからデータベースを回復できます。

[復元] ページ (検索と復元とも呼ばれます) からは、データベースの正確な名前、データベースが存在する場所、データベースが最後に正常な状態であった日付を覚えていなくても、データベースを復元できます。フィルターを使用してデータベースを検索できます。

Oracleデータベースを復元する

ニーズに応じて、Oracle データベースを特定の時点、特定のシステム変更番号 (SCN)、または最後の正常な状態に復元します。また、スナップショットからデータベースを復元し、自動回復プロセスをスキップすることもできます。手動で回復を実行する場合は、自動回復プロセスをスキップすることができます。データベースは、名前または特定のフィルター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、**Oracle** を選択します。
4. 復元するデータベースの名前を入力するか、復元するデータベースが配置されているデータベース ホスト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. 復元するデータベースの*復元*ボタンを選択します。
6. 復元オプションを選択します:

特定の時点に復元する

a. *特定の時点に復元*を選択します。
b. *次へ*を選択します。
c. ドロップダウンから日付を選択し、「検索」を選択します。

   指定された日付に一致するスナップショットのリストが表示されます。

特定のシステム変更番号 **(SCN)** に復元する

a. *特定のシステム変更番号 (SCN) に復元*を選択します。
b. *次へ*を選択します。
c. 復元ポイントとして使用する SCN を入力し、[検索] を選択します。

   指定された SCN に一致するスナップショットのリストが表示されます。

最新のバックアップ（最後の正常な状態）に復元する

a. *最新のバックアップに復元*を選択します。
b. *次へ*を選択します。

   最新の完全バックアップとログバックアップが表示されます。

リカバリなしでスナップショットから復元

a. *リカバリなしでスナップショットから復元*を選択します。
b. *次へ*を選択します。

   一致するスナップショットが表示されます。

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

1. 宛先設定:
   - データベース全体を復元するか、データベースの表領域のみを復元するかを選択します。
   - 制御ファイル: オプションで、このオプションを有効にすると、データベース制御ファイルも復元されます。
2. 復元前のオプション:
   - 必要に応じて、このオプションを有効にし、復元操作の前に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。
   - スクリプトのタイムアウト値を選択します。この期間内にスクリプトの実行に失敗した場合、復元は続行されます。
3. 復元後のオプション:
   - **Postscript**: 必要に応じて、このオプションを有効にし、復元操作後に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。
   - リカバリ後にデータベースまたはコンテナ データベースを読み取り/書き込みモードで開きます: 復元操作が完了すると、バックアップとリカバリによってデータベースの読み取り/書き込みモードが有効になります。
4. *通知*セクション:
   - 電子メール通知を有効にする: 復元操作に関する電子メール通知を受信し、受信する通知の種類を指定するには、これを選択します。
5. *復元*を選択します。

別の場所へのリストア

Oracle Database ワークロード プレビューでは使用できません。

NetApp Backup and Recoveryを使用して **Oracle** データベースのリカバリ ポイントをマウントおよびアンマウントする

リカバリ操作を実行するために制御された状態でデータベースにアクセスする必要がある場合は、Oracle データベースのリカバリ ポイントをマウントすることをお勧めします。

Oracle データベースの復元ポイントをマウントする

データベースの保護ポリシーを構成してアーカイブ ログを保持すると、回復ポイントをマウントしてデータベースの変更履歴を表示できます。

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. Oracle タイルを選択します。
3. [バックアップとリカバリ] メニューで、[インベントリ] を選択します。
4. リスト内の Oracle Database ワークロードについては、「表示」を選択します。

5. *データベース*メニューを選択します。
6. リストからデータベースを選択し、アクションアイコンを選択します ••• > 保護の詳細を表示。

   そのデータベースの回復ポイントのリストが表示されます。

7. リストから回復ポイントを選択し、アクションアイコンを選択します ••• > マウント。
8. 表示されるダイアログで、次の操作を行います。
   a. リストからリカバリポイントをマウントするホストを選択します。
   b. バックアップとリカバリがリカバリポイントをマウントするために使用する場所を選択します。プレビュー リリースでは、オブジェクト ストアからのマウントはサポートされていません。

      バックアップとリカバリで使用するマウント パスが表示されます。

9. *マウント*を選択します。

   リカバリ ポイントは Oracle ホストにマウントされます。

Oracleデータベースの復元ポイントをアンマウントする

データベースに加えられた変更を表示する必要がなくなった場合は、回復ポイントをマウント解除します。

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. Oracle タイルを選択します。
3. [バックアップとリカバリ] メニューで、[インベントリ] を選択します。
4. リスト内の Oracle ワークロードについては、「表示」を選択します。
5. *データベース*メニューを選択します。
6. リストからデータベースを選択し、アクションアイコンを選択します ••• > 保護の詳細を表示。

   そのデータベースの回復ポイントのリストが表示されます。

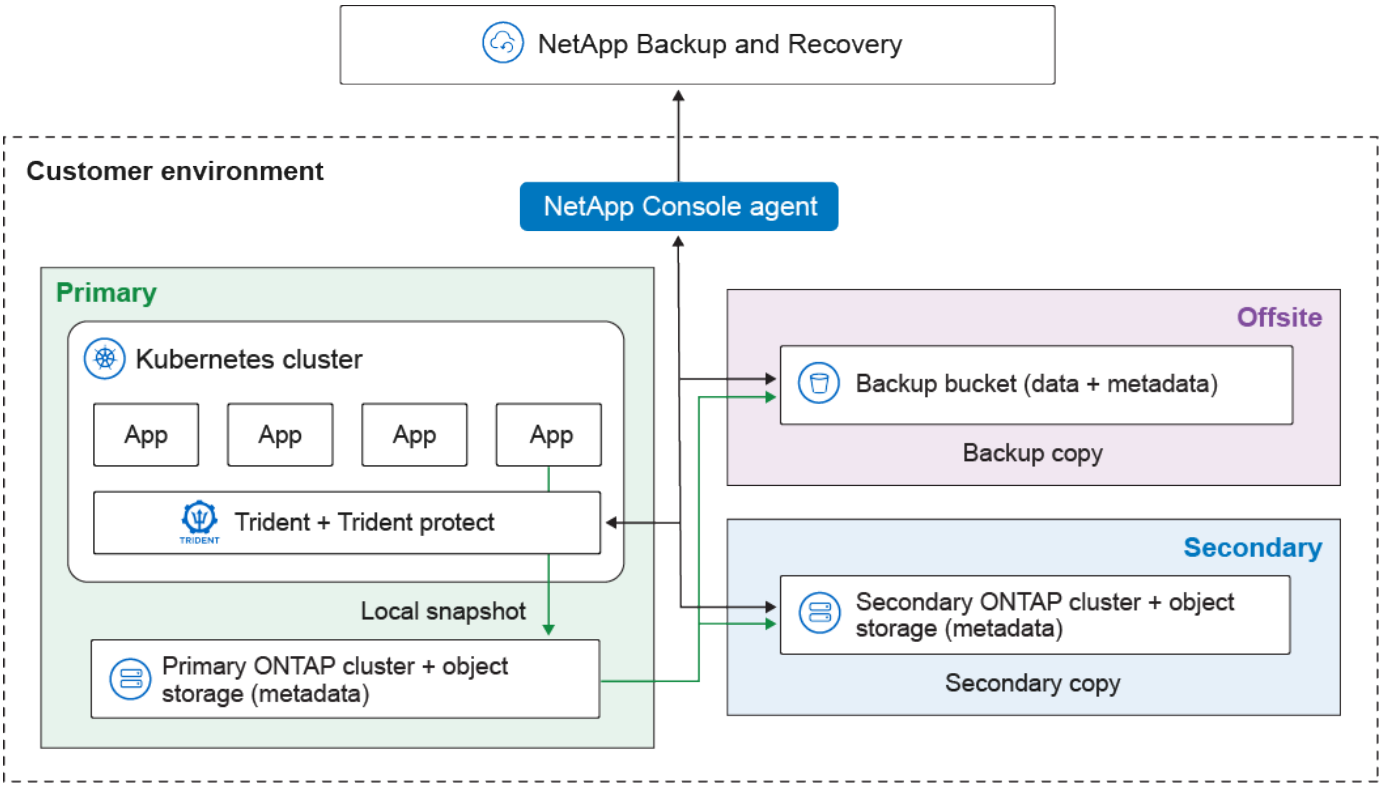
7. リストから回復ポイントを選択し、アクションアイコンを選択します ••• > アンマウント。
8. *アンマウント*を選択してアクションを確認します。

Kubernetes ワークロードを保護する（プレビュー）

Kubernetes ワークロードの管理の概要

NetApp Backup and Recoveryで Kubernetes ワークロードを管理することで、Kubernetes クラスターとアプリケーションをすべて 1 か所で検出、管理、保護できるようになります。クラスタでホストされているリソースとアプリケーションを管理できます。また、単一のインターフェースを使用して、Kubernetesワークロードに保護ポリシーを作成し、関連付けることもできます。

次の図は、Kubernetes ワークロードのバックアップとリカバリのコンポーネントと基本アーキテクチャ、およびデータの異なるコピーを異なる場所に保存する方法を示しています。



NetApp Backup and Recovery は、 Kubernetes ワークロードの管理に次の利点をもたらします。

- 複数の Kubernetes クラスターで実行されるアプリケーションを保護するための単一のコントロールプレーン。これらのアプリケーションには、Kubernetes クラスターで実行されるコンテナや仮想マシンが含まれます。
- NetApp SnapMirrorとのネイティブ統合により、すべてのバックアップおよびリカバリ ワークフローのストレージ オフロード機能が有効になります。
- Kubernetes アプリケーションの永久増分バックアップにより、復旧ポイント目標 (RPO) と復旧時間目標 (RTO) が低下します。

このドキュメントはテクノロジープレビューとして提供されています。プレビュー期間中は、Kubernetes 機能は本番環境のワークロードには推奨されません。このプレビュー オファリングでは、 NetApp は一般提供開始前にオファリングの詳細、内容、およびタイムラインを変更する権利を留保します。

Kubernetes ワークロードの管理に関連する次のタスクを実行できます。

- "Kubernetes ワークロードを発見する"。
- "Kubernetes クラスターを管理する"。
- "Kubernetes アプリケーションの追加と保護"。
- "Kubernetes アプリケーションを管理する"。
- "Kubernetesアプリケーションを復元する"。

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

NetApp Backup and Recovery、 Kubernetes ワークロードを保護する前に検出する必要があります。

必要なNetApp Consoleロール バックアップおよび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" 。

Kubernetes ワークロードを発見する

バックアップとリカバリのインベントリで、環境内の Kubernetes ワークロードを検出します。ワークロードを追加すると、NetApp Backup and Recoveryに Kubernetes クラスターが追加されます。その後、アプリケーションを追加し、クラスター リソースを保護できます。

> ⓘ 現在Trident Protectで保護されているクラスタを検出すると、Trident Protectで使用されていたバックアップスケジュールは検出プロセス中に無効になります（Trident Protectのバックアップスケジュールはバックアップおよびリカバリと互換性がありません）。クラスタのアプリケーションを保護するには、"新しい保護ポリシーを作成する"または、アプリケーションを既存のポリシーに関連付けます。その後、必要に応じてTrident Protectのバックアップスケジュールを削除できます。

手順

1. 次のいずれかを実行します。
   - Kubernetes ワークロードを初めて検出する場合は、 NetApp Backup and Recovery の*ワークロード*で、**Kubernetes** タイルを選択します。
   - Kubernetes ワークロードをすでに検出している場合は、 NetApp Backup and Recoveryで インベントリ > ワークロード を選択し、リソースの検出 を選択します。
2. **Kubernetes** ワークロード タイプを選択します。
3. クラスター名を入力し、クラスターで使用するコネクタを選択します。
4. 表示されるコマンド ラインの指示に従います。
   - Trident Protect ネームスペースを作成する
   - Kubernetesシークレットを作成する
   - Helmリポジトリを追加する
   - Trident Protectおよび Trident Protect コネクタのインストールまたはアップグレード

     これらの手順により、 NetApp Backup and Recovery がクラスターと対話できるようになります。
5. 手順を完了したら、[検出] を選択します。

   クラスターがインベントリに追加されます。
6. 関連付けられている Kubernetes ワークロードで [表示] を選択すると、そのワークロードのアプリケーション、クラスター、および名前空間のリストが表示されます。

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

NetApp Backup and Recoveryダッシュボードを表示するには、次の手順に従います。

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。

   "ダッシュボードに表示される内容を学ぶ"。

Kubernetes アプリケーションの追加と保護

Kubernetes アプリケーションの追加と保護

NetApp Backup and Recovery を使用すると、kubeconfig ファイルを生成してアップロードしなくても、Kubernetes クラスターを簡単に検出できます。 NetApp Consoleのユーザー インターフェイスからコピーした簡単なコマンドを使用して、Kubernetes クラスターを接続し、必要なソフトウェアをインストールできます。

必要なNetApp Consoleロール

組織管理者またはSnapCenter管理者。"NetApp Backup and Recoveryのアクセス ロールについて学習します"。 "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" 。

新しいKubernetesアプリケーションを追加して保護する

Kubernetes アプリケーションを保護するための最初のステップは、NetApp Backup and Recovery内にアプリケーションを作成することです。アプリケーションを作成すると、Kubernetes クラスター上で実行中のアプリケーションがコンソールに認識されます。

開始する前に

Kubernetesアプリケーションを追加して保護する前に、"Kubernetesワークロードを発見する" 。

Web UI を使用してアプリケーションを追加する

手順

1. NetApp Backup and Recoveryで、**Inventory** を選択します。
2. Kubernetes インスタンスを選択し、[表示] を選択して、そのインスタンスに関連付けられているリソースを表示します。
3. *アプリケーション*タブを選択します。
4. *アプリケーションの作成*を選択します。
5. アプリケーションの名前を入力します。
6. 必要に応じて、次のいずれかのフィールドを選択して、保護するリソースを検索します。
   - 関連クラスター
   - 関連する名前空間
   - リソースの種類
   - ラベルセレクター
7. 必要に応じて、「クラススコープリソース」を選択して、クラスターレベルでスコープ指定されたリソースを選択します。これらのリソースを含めると、アプリケーションの作成時にアプリケーションに追加されます。
8. 必要に応じて、「検索」を選択し、検索条件に基づいてリソースを検索します。

   コンソールには検索パラメータや結果は保存されません。パラメータは、選択した Kubernetes クラスターでアプリケーションに含めることができるリソースを検索するために使用されます。

9. コンソールには、検索条件に一致するリソースのリストが表示されます。
10. 保護するリソースがリストに含まれている場合は、[次へ] を選択します。
11. 必要に応じて、「ポリシー」領域で、アプリケーションを保護するための既存の保護ポリシーを選択するか、新しいポリシーを作成します。ポリシーを選択しない場合、アプリケーションは保護ポリシーなしで作成されます。あなたはできる"保護ポリシーを追加する"後で。
12. *プレスクリプトとポストスクリプト*領域で、バックアップ操作の前または後に実行するプレスクリプトまたはポストスクリプトの実行フックを有効にして構成します。プレスクリプトまたはポストスクリプトを有効にするには、少なくとも1つ作成しておく必要があります。"実行フックテンプレート" 。
13. *作成*を選択します。

結果

アプリケーションが作成され、Kubernetes インベントリの アプリケーション タブのアプリケーションリストに表示されます。 NetApp Consoleは設定に基づいてアプリケーションの保護を有効にし、バックアップとリカバリの 監視 領域で進行状況を監視できます。

CRを使用してアプリケーションを追加する

手順

1. デスティネーション アプリケーションの CR ファイルを作成します：

a. カスタムリソース（CR）ファイルを作成し、名前を付けます（例： `my-app-name.yaml`）。

b. 次の属性を設定します：

- **metadata.name**：（必須）アプリケーションのカスタム リソースの名前。保護操作に必要な他の CR ファイルはこの値を参照するため、選択した名前を書き留めておいてください。
- **spec.includedNamespaces**：（必須）ネームスペースとラベルセレクタを使用して、アプリケーションが使用するネームスペースとリソースを指定します。アプリケーションネームスペースはこのリストに含まれている必要があります。ラベルセレクタはオプションであり、指定された各ネームスペース内のリソースをフィルタリングするために使用できます。
- **spec.includedClusterScopedResources**：（オプション）この属性を使用して、アプリケーション定義に含めるクラスタスコープのリソースを指定します。この属性を使用すると、グループ、バージョン、種類、ラベルに基づいてこれらのリソースを選択できます。
  - **groupVersionKind**：（必須）クラスタースコープのリソースの API グループ、バージョン、および種類を指定します。
  - **labelSelector**：（オプション）ラベルに基づいてクラスタースコープのリソースをフィルタリングします。

c. 必要に応じて、次のアノテーションを設定します：

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**：（オプション）このアノテーションは、KubeVirt環境など、スナップショットの前にファイルシステムのフリーズが発生する仮想マシンから定義されたアプリケーションにのみ適用されます。スナップショット中にこのアプリケーションがファイルシステムに書き込むことができるかどうかを指定します。trueに設定すると、アプリケーションはグローバル設定を無視し、スナップショット中にファイルシステムに書き込むことができます。falseに設定すると、アプリケーションはグローバル設定を無視し、スナップショット中にファイルシステムがフリーズされます。指定されていても、アプリケーション定義にアプリケーションの仮想マシンがない場合、アノテーションは無視されます。指定されていない場合、アプリケーションは"グローバル ファイルシステム フリーズ設定"に従います。
- **protect.trident.netapp.io/protection-command**：（オプション）この注釈を使用して、NetApp Backup and Recoveryにアプリケーションの保護または保護の停止を指示します。指定可能な値は `protect`または `unprotect`です。
- **protect.trident.netapp.io/protection-policy-name**：（オプション）このアノテーションを使用して、このアプリケーションを保護するために使用するNetApp Backup and Recovery保護ポリシーの名前を指定します。この保護ポリシーは、NetApp Backup and Recoveryにすでに存在している必要があります。

アプリケーションがすでに作成された後にこのアノテーションを適用する必要がある場合は、次のコマンドを使用できます：

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
YAMLの例：

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. （オプション）特定のラベルでマークされたリソースを含めるか除外するかを指定するフィルタリングを追加します：

   - **resourceFilter.resourceSelectionCriteria**：（フィルタリングに必須）`Include`または`Exclude`を使用して、resourceMatchersで定義されたリソースを含めるか除外します。含めるまたは除外するリソースを定義するには、以下のresourceMatchersパラメータを追加します：

     - **resourceFilter.resourceMatchers**：resourceMatcherオブジェクトの配列。この配列に複数の要素を定義すると、それらはOR演算として一致し、各要素内のフィールド（グループ、種類、バージョン）はAND演算として一致します。

       - **resourceMatchers[].group**：（オプション）フィルタリングするリソースのグループ。
       - **resourceMatchers[].kind**：（オプション）フィルタリングするリソースの種類。

- **resourceMatchers[].version**：（オプション）フィルタリングするリソースのバージョン。
- **resourceMatchers[].names**：（オプション）フィルタリングするリソースのKubernetes metadata.name フィールド内の名前。
- **resourceMatchers[].namespaces**：（オプション）フィルタリングするリソースのKubernetes metadata.name フィールド内の名前空間。
- **resourceMatchers[].labelSelectors**：（オプション） "Kubernetesドキュメント"で定義されているリソースのKubernetesメタデータ.nameフィールドのラベルセレクタ文字列。例： `"trident.netapp.io/os=linux"`。

> ⓘ `resourceFilter`と `labelSelector`の両方が使用される場合、`resourceFilter`が最初に実行され、次に `labelSelector`が結果のリソースに適用されます。

例：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. 環境に合わせてアプリケーション CR を作成したら、CR を適用します。例：

```
kubectl apply -f my-app-name.yaml
```

Backup and Recovery Web UIを使用してKubernetesアプリケーションを今すぐバックアップ

NetApp Backup and Recovery を使用すると、Web インターフェースを使用して Kubernetes アプリケーションを手動でバックアップできます。

必要な**NetApp Console**ロール

組織管理者またはSnapCenter管理者。"NetApp Backup and Recoveryのアクセス ロールについて学習します" 。 "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" 。

Web UI を使用して Kubernetes アプリケーションを今すぐバックアップする

将来のバックアップとスナップショットのベースラインを確立するため、または最新のデータが保護されていることを確認するために、Kubernetes アプリケーションのバックアップを手動で作成します。

手順

1. NetApp Backup and Recoveryで、**Inventory** を選択します。
2. Kubernetes インスタンスを選択し、[表示] を選択して、そのインスタンスに関連付けられているリソースを表示します。
3. *アプリケーション*タブを選択します。
4. アプリケーションのリストで、バックアップするアプリケーションを選択し、関連する [アクション] メニューを選択します。
5. *今すぐバックアップ*を選択します。
6. 正しいアプリケーション名が選択されていることを確認してください。
7. *バックアップ*を選択します。

結果

コンソールはアプリケーションのバックアップを作成し、バックアップとリカバリの 監視 領域に進行状況を表示します。バックアップは、アプリケーションに関連付けられた保護ポリシーに基づいて作成されます。

Backup and Recoveryのカスタム リソースを使用して、Kubernetesアプリケーションを今すぐバックアップ

NetApp Backup and Recovery では、カスタムリソース（CR）を使用して Kubernetes アプリケーションを手動でバックアップできます。

カスタムリソースを使用してKubernetesアプリケーションを今すぐバックアップ

将来のバックアップとスナップショットのベースラインを確立するため、または最新のデータが保護されていることを確認するために、Kubernetes アプリケーションのバックアップを手動で作成します。

> クラスタを対象としたリソースは、アプリケーション定義で明示的に参照されている場合、またはいずれかのアプリケーション名前空間への参照がある場合、バックアップ、Snapshot、またはクローンに含まれます。

開始する前に

AWS セッショントークンの有効期限が、長時間実行される s3 バックアップ処理に十分であることを確認します。バックアップ処理中にトークンの有効期限が切れると、処理が失敗する可能性があります。

- 現在のセッショントークンの有効期限を確認する方法の詳細については、 "AWS API ドキュメント"を参照してください。
- "AWS IAM ドキュメント"AWS リソースの認証情報の詳細については、こちらを参照してください。

カスタムリソースを使用してローカルスナップショットを作成する

Kubernetes アプリケーションのスナップショットを作成してローカルに保存するには、特定の属性を持つ Snapshot カスタム リソースを使用します。

手順

1. カスタムリソース（CR）ファイルを作成し、名前を付けます `local-snapshot-cr.yaml`。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。
   - **spec.applicationRef**：スナップショットを作成するアプリケーションの Kubernetes 名。
   - **spec.appVaultRef**：（必須）スナップショットの内容（メタデータ）を保存するAppVaultの名前。
   - **spec.reclaimPolicy**：（オプション）スナップショット CR が削除されたときに、スナップショットの AppArchive に対して何が起こるかを定義します。つまり、 `Retain`に設定されている場合でも、スナップショットは削除されます。有効なオプション：
     - `Retain`（デフォルト）
     - `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: local-snapshot-cr
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Retain
```

3. `local-snapshot-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f local-snapshot-cr.yaml
```

カスタム リソースを使用してアプリケーションをオブジェクト ストアにバックアップする

アプリケーションをオブジェクト ストアにバックアップするには、特定の属性を持つバックアップ CR を作成します。

手順

1. カスタムリソース（CR）ファイルを作成し、名前を `object-store-backup-cr.yaml`とします。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。

- **spec.applicationRef**：（必須）バックアップするアプリケーションの Kubernetes 名。
- **spec.appVaultRef**：（必須、*spec.appVaultTargetsRef*とは相互排他）スナップショットとバックアップの保存に同じバケットを使用する場合、これはバックアップコンテンツを保存するAppVaultの名前です。
- **spec.appVaultTargetsRef**：（必須、*spec.appVaultRef*とは相互排他）スナップショットとバックアップを保存するために別のバケットを使用する場合、これはバックアップコンテンツを保存するAppVaultの名前です。
- **spec.dataMover**：（オプション）バックアップ操作に使用するバックアップツールを示す文字列。値は大文字と小文字が区別され、 `CBS`である必要があります。
- **spec.reclaimPolicy**：（オプション）Backup CR が削除されたときにバックアップコンテンツ（メタデータ / ボリュームデータ）に何が起こるかを定義します。使用可能な値：
  - `Delete`
  - `Retain`（デフォルト）
- **spec.cleanupSnapshot**：（必須）バックアップ CR によって作成された一時スナップショットが、バックアップ処理の完了後に削除されないようにします。推奨値： `false`。

同じバケットを使用してスナップショットとバックアップを保存する場合の YAML の例：

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

スナップショットとバックアップを保存するために異なるバケットを使用する場合の YAML の例：

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. `object-store-backup-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f object-store-backup-cr.yaml
```

カスタムリソースを使用して **3-2-1** ファンアウト バックアップを作成する

3-2-1 ファンアウト アーキテクチャを使用してバックアップすると、バックアップがオブジェクト ストアだけでなくセカンダリ ストレージにもコピーされます。3-2-1 ファンアウト バックアップを作成するには、特定の属性を持つバックアップ CR を作成します。

手順

1. カスタムリソース（CR）ファイルを作成し、名前を付けます `3-2-1-fanout-backup-cr.yaml`。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。
   - **spec.applicationRef**：（必須）バックアップするアプリケーションの Kubernetes 名。
   - **spec.appVaultTargetsRef**：（必須）バックアップコンテンツを保存するAppVaultの名前。
   - **spec.dataMover**：（オプション）バックアップ操作に使用するバックアップツールを示す文字列。値は大文字と小文字が区別され、 `CBS`である必要があります。
   - **spec.reclaimPolicy**：（オプション）Backup CR が削除されたときにバックアップコンテンツ（メタデータ / ボリュームデータ）に何が起こるかを定義します。使用可能な値：
     - `Delete`
     - `Retain`（デフォルト）
   - **spec.cleanupSnapshot**：（必須）バックアップ CR によって作成された一時スナップショットが、バックアップ処理の完了後に削除されないようにします。推奨値： `false`。
   - **spec.replicateSnapshot**：（必須）NetApp Backup and Recoveryにスナップショットをセカンダリストレージにレプリケートするように指示します。必要な値： `true`。
   - **spec.replicateSnapshotReclaimPolicy**：（オプション）レプリケートされたSnapshotが削除されたときの動作を定義します。使用可能な値：
     - `Delete`
     - `Retain`（デフォルト）

     YAMLの例：

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. `3-2-1-fanout-backup-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

サポートされているバックアップアノテーション

次の表では、バックアップ CR を作成するときに使用できる注釈について説明します。

注釈	タイプ	説明	デフォルト値
protect.trident.netapp.io/full-backup	string	バックアップを非増分にするかどうかを指定します。 `true`に設定すると、非増分バックアップが作成されます。ベストプラクティスとしては、定期的にフル バックアップを実行し、フル バックアップの間に増分バックアップを実行して、リストアに伴うリスクを最小限に抑えることです。	"false"
protect.trident.netapp.io/snapshot-completion-timeout	string	スナップショット処理全体が完了するまでに許容される最大時間。	"60m"
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	string	ボリューム スナップショットが使用可能状態になるまでに許容される最大時間。	"30分"
protect.trident.netapp.io/ボリュームスナップショット作成タイムアウト	string	ボリューム スナップショットの作成に許可される最大時間。	「5m」
protect.trident.netapp.io/pvc-bind-timeout-sec	string	新しく作成されたPersistentVolumeClaims（PVC）が `Bound`フェーズに到達するまで待機する最大時間（秒単位）。この時間を超えると操作は失敗します。	「1200」（20分）

Kubernetesアプリケーションを復元する

Web UI を使用して Kubernetes アプリケーションをリストアする

NetApp Backup and Recovery を使用すると、保護ポリシーで保護したアプリケーションを復元できます。アプリケーションを復元するには、少なくとも 1 つの復元ポイントが必要です。復元ポイントは、ローカル スナップショットまたはオブジェクト ストアへのバックアップ（あるいはその両方）で構成されます。アプリケーションは、ローカル アーカイブ、セカンダリ アーカイブ、またはオブジェクト ストア アーカイブを使用して復元できます。

開始する前に

Trident Protect を使用してバックアップされたアプリケーションを復元する場合は、Trident Protect がソース クラスタとデスティネーション クラスタの両方にインストールされていることを確認してください。

必要なNetApp Consoleロール

組織管理者またはSnapCenter管理者。"NetApp Backup and Recoveryのアクセス ロールについて学習します" 。 "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メニューで、*リストア*を選択します。
2. リストから Kubernetes アプリケーションを選択し、そのアプリケーションの * 表示と復元 * を選択します。

   復元ポイントのリストが表示されます。
3. 使用する復元ポイントの*Restore*ボタンを選択します。

一般設定

1. 復元元のソースの場所を選択します。
2. クラスター リストから宛先クラスターを選択します。

   Trident Protectで作成したローカルスナップショットを別のクラスターにリストアすることは、現時点ではサポートされていません。
3. 元のネームスペースに復元するか、新しいネームスペースに復元するかを選択します。
4. 新しいネームスペースにリストアすることを選択した場合は、使用するデスティネーションネームスペースを入力します。
5. *次へ*を選択します。

リソースの選択

1. アプリケーションに関連付けられているすべてのリソースを復元するか、フィルターを使用して復元する特定のリソースを選択するかを選択します。

すべてのリソースを復元する

1. *すべてのリソースを復元*を選択します。
2. *次へ*を選択します。

特定のリソースを復元する

1. *選択的リソース*を選択します。
2. リソース フィルターの動作を選択します。 *含める*を選択すると、選択したリソースが復元されます。 *除外*を選択した場合、選択したリソースは復元されません。
3. リソースを選択するためのフィルターを定義するルールを追加するには、[ルールの追加] を選択します。リソースをフィルタリングするには、少なくとも 1 つのルールが必要です。

   各ルールは、リソースの名前空間、ラベル、グループ、バージョン、種類などの基準でフィルタリングできます。

4. 各ルールを保存するには、[保存] を選択します。
5. 必要なルールをすべて追加したら、「検索」を選択して、フィルター条件に一致するバックアップ アーカイブ内の利用可能なリソースを表示します。

   表示されるリソースは、クラスター上に現在存在するリソースです。

6. 結果に満足したら、[次へ] を選択します。

宛先設定

1. *Destination settings*セクションを展開し、デフォルトのストレージクラス、別のストレージクラスのいずれかに復元するか、別のクラスタに復元する場合は、ストレージクラスをデスティネーション クラスタにマッピングするかを選択します。
2. 別のストレージ クラスにリストアすることを選択した場合は、各ソース ストレージ クラスに一致するデスティネーション ストレージ クラスを選択します。
3. オプションで、Trident Protect を使用して作成されたバックアップまたは Snapshot をリストアする場合は、リストア処理のストレージバケットとして使用される AppVault の詳細を表示します。環境または AppVault のステータスに変更がある場合は、* App Vault を同期*を選択して詳細を更新します。

   Trident Protectを使用して作成されたバックアップまたはスナップショットの復元を容易にするために、Kubernetesクラスタ上にAppVaultを作成する必要がある場合は、 "Trident Protect AppVaultオブジェクトを使用してバケットを管理する"を参照してください。

4. 必要に応じて、[復元スクリプト] セクションを展開し、[**Postscript**] オプションを有効にして、復元操作の完了後に実行される実行フック テンプレートを選択します。必要に応じて、スクリプトに必要な引数を入力し、ラベル セレクタを追加して、リソース ラベルに基づいてリソースをフィルタします。
5. *復元*を選択します。

カスタムリソースを使用した **Kubernetes** アプリケーションのリストア

カスタム リソースを使用して、スナップショットまたはバックアップからアプリケーシ

ョンを復元できます。アプリケーションを同じクラスタに復元する場合、既存のスナップショットからの復元の方が高速になります。

- アプリケーションを復元すると、アプリケーションに対して設定されているすべての実行フックもアプリとともに復元されます。復元後の実行フックが存在する場合、復元操作の一部として自動的に実行されます。
- バックアップから別の名前空間または元の名前空間への復元は、qtree ボリュームでサポートされています。ただし、スナップショットから別の名前空間または元の名前空間への復元は、qtree ボリュームではサポートされていません。
- 詳細設定を使用して復元操作をカスタマイズできます。詳細については、"高度なカスタムリソースのリストア設定を使用する"を参照してください。

バックアップを別の名前空間に復元する

BackupRestore CR を使用して異なる名前空間にバックアップを復元すると、NetApp Backup and Recovery はアプリケーションを新しい名前空間に復元し、復元されたアプリケーションのアプリケーション CR を作成します。復元されたアプリケーションを保護するには、オンデマンドバックアップまたはスナップショットを作成するか、保護スケジュールを確立します。

- 既存のリソースを含む別の名前空間にバックアップをリストアしても、バックアップ内のリソースと名前を共有するリソースは変更されません。バックアップ内のすべてのリソースをリストアするには、ターゲット名前空間を削除して再作成するか、バックアップを新しい名前空間にリストアします。
- CR を使用して新しい名前空間に復元する場合は、CR を適用する前に、デスティネーション名前空間を手動で作成する必要があります。NetApp Backup and Recovery では、CLI を使用する場合にのみ名前空間が自動的に作成されます。

開始する前に

AWS セッショントークンの有効期限が、長時間実行される s3 復元処理に十分であることを確認します。復元処理中にトークンの有効期限が切れると、処理が失敗する可能性があります。

- 現在のセッショントークンの有効期限を確認する方法の詳細については、 "AWS API ドキュメント"を参照してください。
- "AWS IAM ドキュメント"AWS リソースの認証情報の詳細については、こちらを参照してください。

Kopia をデータ ムーバーとして使用してバックアップを復元する場合、オプションで CR に注釈を指定して、Kopia が使用する一時ストレージの動作を制御できます。 "Kopiaのドキュメント"設定できるオプションの詳細については、こちらを参照してください。

手順

1. カスタムリソース（CR）ファイルを作成し、名前を付けます `trident-protect-backup-restore-cr.yaml`。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。
   - **spec.appArchivePath**：AppVault内でバックアップコンテンツが保存されるパス。このパスを見つけるには、次のコマンドを使用できます：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**：（必須）バックアップコンテンツが保存されるAppVaultの名前。
- **spec.namespaceMapping**：リストア処理のソースネームスペースからデスティネーションネームスペースへのマッピング。 `my-source-namespace`と `my-destination-namespace`を環境の情報に置き換えます。

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. （オプション）復元するアプリケーションの特定のリソースのみを選択する必要がある場合は、特定のラベルでマークされたリソースを含めるか除外するフィルタリングを追加します：

> Trident Protect は、選択したリソースとの関係に基づいて、一部のリソースを自動的に選択します。たとえば、永続ボリュームクレームリソースを選択し、それに関連付けられたポッドがある場合、Trident Protect は関連付けられているポッドも復元します。

- **resourceFilter.resourceSelectionCriteria**：（フィルタリングに必須） `Include`または `Exclude`を使用して、resourceMatchersで定義されたリソースを含めるか除外します。含めるまたは除外するリソースを定義するには、以下のresourceMatchersパラメータを追加します：
  - **resourceFilter.resourceMatchers**：resourceMatcherオブジェクトの配列。この配列に複数の要素を定義すると、それらはOR演算として一致し、各要素内のフィールド（グループ、種類、バージョン）はAND演算として一致します。
    - **resourceMatchers[].group**：（オプション）フィルタリングするリソースのグループ。
    - **resourceMatchers[].kind**：（オプション）フィルタリングするリソースの種類。
    - **resourceMatchers[].version**：（オプション）フィルタリングするリソースのバージョン。
    - **resourceMatchers[].names**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前。
    - **resourceMatchers[].namespaces**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前空間。
    - **resourceMatchers[].labelSelectors**：（オプション） "Kubernetesドキュメント"で定義されているリソースのKubernetesメタデータ.nameフィールドのラベルセレクタ文字列。例：`"trident.netapp.io/os=linux"`。

例：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. `trident-protect-backup-restore-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

バックアップを元の名前空間に復元する

いつでもバックアップを元の名前空間に復元できます。

開始する前に

AWS セッショントークンの有効期限が、長時間実行される s3 復元処理に十分であることを確認します。復元処理中にトークンの有効期限が切れると、処理が失敗する可能性があります。

- 現在のセッショントークンの有効期限を確認する方法の詳細については、 "AWS API ドキュメント"を参照してください。
- "AWS IAM ドキュメント"AWS リソースの認証情報の詳細については、こちらを参照してください。

Kopia をデータ ムーバーとして使用してバックアップを復元する場合、オプションで CR に注釈を指定して、Kopia が使用する一時ストレージの動作を制御できます。 "Kopiaのドキュメント"設定できるオプションの詳細については、こちらを参照してください。

手順

1. カスタムリソース（CR）ファイルを作成し、名前を `trident-protect-backup-ipr-cr.yaml`とします。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。

- **spec.appArchivePath**：AppVault内でバックアップコンテンツが保存されるパス。このパスを見つけるには、次のコマンドを使用できます：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**：（必須）バックアップコンテンツが保存されるAppVaultの名前。

  例：

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. （オプション）復元するアプリケーションの特定のリソースのみを選択する必要がある場合は、特定のラベルでマークされたリソースを含めるか除外するフィルタリングを追加します：

> Trident Protect は、選択したリソースとの関係に基づいて、一部のリソースを自動的に選択します。たとえば、永続ボリュームクレームリソースを選択し、それに関連付けられたポッドがある場合、Trident Protect は関連付けられているポッドも復元します。

- **resourceFilter.resourceSelectionCriteria**：（フィルタリングに必須） `Include`または `Exclude`を使用して、resourceMatchersで定義されたリソースを含めるか除外します。含めるまたは除外するリソースを定義するには、以下のresourceMatchersパラメータを追加します：
  - **resourceFilter.resourceMatchers**：resourceMatcherオブジェクトの配列。この配列に複数の要素を定義すると、それらはOR演算として一致し、各要素内のフィールド（グループ、種類、バージョン）はAND演算として一致します。
    - **resourceMatchers[].group**：（オプション）フィルタリングするリソースのグループ。
    - **resourceMatchers[].kind**：（オプション）フィルタリングするリソースの種類。
    - **resourceMatchers[].version**：（オプション）フィルタリングするリソースのバージョン。
    - **resourceMatchers[].names**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前。
    - **resourceMatchers[].namespaces**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前空間。
    - **resourceMatchers[].labelSelectors**：（オプション） "Kubernetesドキュメント"で定義されているリソースのKubernetesメタデータ.nameフィールドのラベルセレクタ文字列。例：`"trident.netapp.io/os=linux"`。

      例：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. `trident-protect-backup-ipr-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

バックアップを別のクラスタにリストアする

元のクラスタに問題がある場合は、バックアップを別のクラスタにリストアできます。

- Kopia をデータ ムーバーとして使用してバックアップを復元する場合、オプションで CR に注釈を指定して、Kopia が使用する一時ストレージの動作を制御できます。 "Kopiaのドキュメント"設定できるオプションの詳細については、こちらを参照してください。
- CR を使用して新しいネームスペースにリストアする場合は、CR を適用する前に、デスティネーションネームスペースを手動で作成する必要があります。

開始する前に

次の前提条件が満たされていることを確認してください：

- デスティネーション クラスタに Trident Protect がインストールされている。
- デスティネーション クラスタは、バックアップが保存されているソース クラスタと同じAppVaultのバケット パスにアクセスできます。
- AWS セッション トークンの有効期限が、長時間実行される復元操作に十分であることを確認します。復元操作中にトークンの有効期限が切れると、操作が失敗する可能性があります。
  - 現在のセッショントークンの有効期限を確認する方法の詳細については、 "AWS API ドキュメント"を参照してください。
  - AWS リソースの認証情報の詳細については、 "AWSのドキュメント"を参照してください。

手順

1. Trident Protect CLIプラグインを使用して、デスティネーション クラスタ上のAppVault CRの可用性を確認します：

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

アプリケーションのリストアに使用する名前空間がデスティネーション クラスタに存在することを確認します。

2. デスティネーション クラスタから利用可能なAppVaultのバックアップコンテンツを表示します：

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

このコマンドを実行すると、AppVault内の利用可能なバックアップが表示されます。これには、元のクラスタ、対応するアプリケーション名、タイムスタンプ、アーカイブ パスが含まれます。

出力例：

```
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |         TIMESTAMP
|    PATH     |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
```

3. AppVault名前とアーカイブパスを使用して、アプリケーションをデスティネーション クラスタに復元します：

4. カスタムリソース（CR）ファイルを作成し、名前を付けます `trident-protect-backup-restore-cr.yaml`。

5. 作成したファイルで、次の属性を設定します：

   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。
   - **spec.appVaultRef**：（必須）バックアップコンテンツが保存されるAppVaultの名前。

- **spec.appArchivePath**：AppVault内でバックアップコンテンツが保存されるパス。このパスを見つけるには、次のコマンドを使用できます：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

> BackupRestore CR が利用できない場合は、手順 2 に記載されているコマンドを使用してバックアップの内容を表示できます。

- **spec.namespaceMapping**：リストア処理のソースネームスペースからデスティネーションネームスペースへのマッピング。 `my-source-namespace`と `my-destination-namespace`を環境の情報に置き換えます。

  例：

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. `trident-protect-backup-restore-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

スナップショットを別のネームスペースにリストアする

カスタム リソース (CR) ファイルを使用して、スナップショットからデータを別の名前空間または元のソース名前空間に復元できます。SnapshotRestore CR を使用してスナップショットを別の名前空間に復元すると、Backup and Recovery はアプリケーションを新しい名前空間に復元し、復元されたアプリケーションのアプリケーション CR を作成します。復元されたアプリケーションを保護するには、オンデマンド バックアップまたはスナップショットを作成するか、保護スケジュールを設定します。

> - SnapshotRestoreは `spec.storageClassMapping`属性をサポートしていますが、ソース ストレージ クラスとデスティネーション ストレージ クラスが同じストレージ バックエンドを使用する場合のみです。異なるストレージ バックエンドを使用する `StorageClass`に復元しようとすると、復元処理は失敗します。
> - CR を使用して新しいネームスペースにリストアする場合は、CR を適用する前に、デスティネーションネームスペースを手動で作成する必要があります。

開始する前に

AWS セッショントークンの有効期限が、長時間実行される s3 復元処理に十分であることを確認します。復元処理中にトークンの有効期限が切れると、処理が失敗する可能性があります。

- 現在のセッショントークンの有効期限を確認する方法の詳細については、 "AWS API ドキュメント"を参照してください。
- "AWS IAM ドキュメント"AWS リソースの認証情報の詳細については、こちらを参照してください。

手順

1. カスタムリソース（CR）ファイルを作成し、名前を `trident-protect-snapshot-restore-cr.yaml`とします。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。
   - **spec.appVaultRef**：（必須）スナップショットの内容が保存されるAppVaultの名前。
   - **spec.appArchivePath**：AppVault内のパスで、スナップショットの内容が保存される場所。このパスを見つけるには、次のコマンドを使用できます：

     ```
     kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.namespaceMapping**：リストア処理のソースネームスペースからデスティネーションネームスペースへのマッピング。 `my-source-namespace`と `my-destination-namespace`を環境の情報に置き換えます。

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
       namespaceMapping: [{"source": "my-source-namespace", "destination":
     "my-destination-namespace"}]
     ```

3. （オプション）復元するアプリケーションの特定のリソースのみを選択する必要がある場合は、特定のラベルでマークされたリソースを含めるか除外するフィルタリングを追加します：

   Trident Protect は、選択したリソースとの関係に基づいて、一部のリソースを自動的に選択します。たとえば、永続ボリュームクレームリソースを選択し、それに関連付けられたポッドがある場合、Trident Protect は関連付けられているポッドも復元します。

   - **resourceFilter.resourceSelectionCriteria**：（フィルタリングに必須） `Include`または `Exclude`を使用して、resourceMatchersで定義されたリソースを含めるか除外します。含めるまたは除外するリ

ソースを定義するには、以下のresourceMatchersパラメータを追加します：

- **resourceFilter.resourceMatchers**：resourceMatcherオブジェクトの配列。この配列に複数の要素を定義すると、それらはOR演算として一致し、各要素内のフィールド（グループ、種類、バージョン）はAND演算として一致します。
  - **resourceMatchers[].group**：（オプション）フィルタリングするリソースのグループ。
  - **resourceMatchers[].kind**：（オプション）フィルタリングするリソースの種類。
  - **resourceMatchers[].version**：（オプション）フィルタリングするリソースのバージョン。
  - **resourceMatchers[].names**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前。
  - **resourceMatchers[].namespaces**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前空間。
  - **resourceMatchers[].labelSelectors**：（オプション） "Kubernetesドキュメント"で定義されているリソースのKubernetesメタデータ.nameフィールドのラベルセレクタ文字列。例：`"trident.netapp.io/os=linux"`。

    例：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. `trident-protect-snapshot-restore-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

スナップショットを元の名前空間に復元する

いつでもスナップショットを元の名前空間にリストアできます。

開始する前に

AWS セッショントークンの有効期限が、長時間実行される s3 復元処理に十分であることを確認します。復元処理中にトークンの有効期限が切れると、処理が失敗する可能性があります。

- 現在のセッショントークンの有効期限を確認する方法の詳細については、 "AWS API ドキュメント"を参照してください。
- "AWS IAM ドキュメント"AWS リソースの認証情報の詳細については、こちらを参照してください。

手順

1. カスタムリソース（CR）ファイルを作成し、 `trident-protect-snapshot-ipr-cr.yaml`という名前を付けます。
2. 作成したファイルで、次の属性を設定します：
   - **metadata.name**：（必須）このカスタム リソースの名前。環境に合わせて一意かつ適切な名前を選択してください。
   - **spec.appVaultRef**：（必須）スナップショットの内容が保存されるAppVaultの名前。
   - **spec.appArchivePath**：AppVault内のパスで、スナップショットの内容が保存される場所。このパスを見つけるには、次のコマンドを使用できます：

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
```

3. （オプション）復元するアプリケーションの特定のリソースのみを選択する必要がある場合は、特定のラベルでマークされたリソースを含めるか除外するフィルタリングを追加します：

> Trident Protect は、選択したリソースとの関係に基づいて、一部のリソースを自動的に選択します。たとえば、永続ボリュームクレームリソースを選択し、それに関連付けられたポッドがある場合、Trident Protect は関連付けられているポッドも復元します。

   - **resourceFilter.resourceSelectionCriteria**：（フィルタリングに必須） `Include`または `Exclude`を使用して、resourceMatchersで定義されたリソースを含めるか除外します。含めるまたは除外するリソースを定義するには、以下のresourceMatchersパラメータを追加します：
     - **resourceFilter.resourceMatchers**：resourceMatcherオブジェクトの配列。この配列に複数の要素を定義すると、それらはOR演算として一致し、各要素内のフィールド（グループ、種類、バージョン）はAND演算として一致します。
       - **resourceMatchers[].group**：（オプション）フィルタリングするリソースのグループ。

- **resourceMatchers[].kind**：（オプション）フィルタリングするリソースの種類。
- **resourceMatchers[].version**：（オプション）フィルタリングするリソースのバージョン。
- **resourceMatchers[].names**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前。
- **resourceMatchers[].namespaces**：（オプション）フィルタリングするリソースの Kubernetes metadata.name フィールド内の名前空間。
- **resourceMatchers[].labelSelectors**：（オプション） "Kubernetesドキュメント"で定義されているリソースのKubernetesメタデータ.nameフィールドのラベルセレクタ文字列。例：`"trident.netapp.io/os=linux"`。

  例：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. `trident-protect-snapshot-ipr-cr.yaml`ファイルに正しい値を入力したら、CRを適用します：

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

高度なカスタムリソースのリストア設定を使用する

注釈、名前空間設定、ストレージ オプションなどの詳細設定を使用して、特定の要件を満たすように復元操作をカスタマイズできます。

リストアおよびフェイルオーバー処理中のネームスペースのアノテーションとラベル

復元およびフェイルオーバー処理中に、デスティネーションネームスペースのラベルとアノテーションは、ソースネームスペースのラベルとアノテーションと一致するように作成されます。デスティネーションネームスペースに存在しないソースネームスペースのラベルまたはアノテーションが追加され、既存のラベルまたはアノテーションはソースネームスペースの値と一致するように上書きされます。デスティネーションネームスペ

ースにのみ存在するラベルまたはアノテーションは変更されません。

> Red Hat OpenShiftを使用する場合は、OpenShift環境における名前空間アノテーションの重要な役割に注意することが重要です。名前空間アノテーションにより、リストアされたポッドがOpenShiftセキュリティコンテキスト制約（SCC）で定義された適切な権限とセキュリティ設定に準拠し、権限の問題なくボリュームにアクセスできるようになります。詳細については、"OpenShiftセキュリティコンテキスト制約ドキュメント"を参照してください。

リストアまたはフェイルオーバー処理を実行する前にKubernetes環境変数 `RESTORE_SKIP_NAMESPACE_ANNOTATIONS`を設定することで、デスティネーションネームスペース内の特定のアノテーションが上書きされるのを防ぐことができます。例：

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

> 復元またはフェイルオーバー操作を実行する場合、 `restoreSkipNamespaceAnnotations`および `restoreSkipNamespaceLabels`で指定されたネームスペースのアノテーションとラベルは、復元またはフェイルオーバー操作から除外されます。これらの設定がHelmの初期インストール時に構成されていることを確認してください。詳細については、"追加のTrident Protectヘルムチャート設定を構成する"を参照してください。

Helm を使用して `--create-namespace`フラグを指定してソースアプリケーションをインストールした場合、 `name`ラベルキーには特別な処理が適用されます。リストアまたはフェイルオーバープロセス中に、 Trident Protect はこのラベルをデスティネーションネームスペースにコピーしますが、ソースからの値がソースネームスペースと一致する場合は、値をデスティネーションネームスペースの値に更新します。この値がソースネームスペースと一致しない場合は、変更されずにデスティネーションネームスペースにコピーされます。

例

次の例は、それぞれ異なる注釈とラベルを持つソース名前空間と宛先名前空間を示しています。操作の前後の宛先名前空間の状態や、宛先名前空間で注釈とラベルがどのように結合または上書きされるかを確認できます。

リストアまたはフェイルオーバー処理の前に

次の表は、リストアまたはフェイルオーバー処理前のサンプルのソースネームスペースとデスティネーションネームスペースの状態を示しています：

ネームスペース	アノテーション	ラベル
ネームスペースns-1（ソース）	• annotation.one/key："updatedvalue" • annotation.two/key："true"	• environment=production • コンプライアンス＝hipaa • name=ns-1

ネームスペース	アノテーション	ラベル
ネームスペースns-2（宛先）	• annotation.one/key："true" • annotation.three/key："false"	• ロール＝database

リストア処理後

次の表は、復元またはフェイルオーバー操作後の宛先名前空間の例の状態を示しています。いくつかのキーが追加され、いくつかは上書きされ、 `name`ラベルは宛先名前空間と一致するように更新されました：

ネームスペース	アノテーション	ラベル
ネームスペースns-2（宛先）	• annotation.one/key："updatedvalue" • annotation.two/key："true" • annotation.three/key："false"	• name=ns-2 • コンプライアンス＝hipaa • environment=production • ロール＝database

サポートされているフィールド

このセクションでは、復元操作に使用できる追加のフィールドについて説明します。

ストレージクラスのマッピング

`spec.storageClassMapping`属性は、ソース アプリケーションに存在するストレージクラスからターゲット クラスタ上の新しいストレージクラスへのマッピングを定義します。異なるストレージクラスを持つクラスタ間でアプリケーションを移行する場合や、`BackupRestore`操作のストレージバックエンドを変更する場合にこれを使用できます。

例：

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

サポートされているアノテーション

このセクションでは、システム内のさまざまな動作を構成するためにサポートされているアノテーションを一覧表示します。ユーザーがアノテーションを明示的に設定しない場合、システムはデフォルト値を使用します。

注釈	タイプ	説明	デフォルト値
protect.trident.netapp.io/data-mover-timeout-sec	string	データ ムーバー処理が停止する最大時間（秒単位）。	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	string	Kopia コンテンツ キャッシュの最大サイズ制限（メガバイト単位）。	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	string	新しく作成されたPersistentVolumeClaims（PVC）が`Bound`フェーズに到達するまで待機する最大時間（秒単位）。この時間を超えると処理は失敗します。環境：すべてのリストアCRタイプ（BackupRestore、BackupInplaceRestore、SnapshotRestore、SnapshotInplaceRestore）。ストレージバックエンドまたはクラスターで処理に時間がかかることが多い場合は、より大きい値を使用してください。	「1200」（20分）

Kubernetes クラスターを管理する

NetApp Backup and Recovery を使用すると、Kubernetes クラスターを検出して管理できるため、クラスターによってホストされるリソースを保護できます。

必要なNetApp Consoleロール

組織管理者またはSnapCenter管理者。"NetApp Backup and Recoveryのアクセス ロールについて学習します"。 "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"。

Kubernetesクラスターを発見するには、以下を参照してください。"Kubernetes ワークロードを発見する"。

Kubernetes クラスターの情報を編集する

名前を変更する必要がある場合は、クラスターを編集できます。

手順

1. NetApp Backup and Recoveryで、インベントリ > クラスタ を選択します。
2. クラスターのリストで、編集するクラスターを選択し、関連する [アクション] メニューを選択します。
3. *クラスターの編集*を選択します。
4. クラスター名に必要な変更を加えます。クラスター名は、検出プロセス中にHelmコマンドで使用した名前と一致する必要があります。
5. *完了*を選択します。

Kubernetes クラスターを削除する

Kubernetes クラスターの保護を停止するには、保護を無効にして関連付けられているアプリケーションを削除し、 NetApp Backup and Recoveryからクラスターを削除します。 NetApp Backup and Recovery、クラスタまたはそのリソースは削除されません。NetAppNetApp Consoleインベントリからクラスタが削除されるだ

けです。

手順

1. NetApp Backup and Recoveryで、インベントリ > クラスタ を選択します。
2. クラスターのリストで、編集するクラスターを選択し、関連する [アクション] メニューを選択します。
3. *クラスターの削除*を選択します。
4. 確認ダイアログボックスの情報を確認し、「削除」を選択します。

Kubernetes アプリケーションを管理する

NetApp Backup and Recovery を使用すると、Kubernetes アプリケーションと関連リソースの保護を解除したり削除したりできます。

必要な**NetApp Console**ロール

組織管理者またはSnapCenter管理者。"NetApp Backup and Recoveryのアクセス ロールについて学習します" 。 "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" 。

Kubernetes アプリケーションの保護を解除する

アプリケーションを保護する必要がなくなった場合は、保護を解除できます。アプリケーションの保護を解除すると、 NetApp Backup and Recovery はアプリケーションの保護を停止しますが、関連するすべてのバックアップとスナップショットは保持されます。

保護操作が実行中の間は、アプリケーションの保護を解除することはできません。操作が完了するまで待つか、回避策として、実行中の保護操作が使用しているリストアポイントを削除するを削除します。その後、アプリケーションの保護を解除できます。

手順

1. NetApp Backup and Recoveryで、**Inventory** を選択します。
2. Kubernetes インスタンスを選択し、[表示] を選択して、そのインスタンスに関連付けられているリソースを表示します。
3. *アプリケーション*タブを選択します。
4. アプリケーションのリストで、保護を解除するアプリケーションを選択し、関連する [アクション] メニューを選択します。
5. *保護解除*を選択します。
6. 通知を読み、準備ができたら [保護解除] を選択します。

Kubernetes アプリケーションを削除する

不要になったアプリケーションを削除します。 NetApp Backup and Recovery は保護を停止し、削除されたアプリケーションのバックアップとスナップショットをすべて削除します。

手順

1. NetApp Backup and Recoveryで、**Inventory** を選択します。
2. Kubernetes インスタンスを選択し、[表示] を選択して、そのインスタンスに関連付けられているリソース

を表示します。

3. *アプリケーション*タブを選択します。
4. アプリケーションのリストで、削除するアプリケーションを選択し、関連する [アクション] メニューを選択します。
5. *削除*を選択します。
6. スナップショットとバックアップの削除 を有効にすると、アプリケーションのすべてのスナップショットとバックアップが削除されます。

   これらのスナップショットとバックアップを使用してアプリケーションを復元することはできなくなります。

7. 操作を確認し、[削除] を選択します。

Kubernetes アプリケーションの復元ポイントを削除する

アプリケーションの保護を解除する必要があり、現在保護操作が実行中の場合は、アプリケーションの復元ポイントを削除する必要がある場合があります。

手順

1. NetApp Backup and Recoveryメニューで、*リストア*を選択します。
2. リストから Kubernetes アプリケーションを選択し、そのアプリケーションの * 表示と復元 * を選択します。

   復元ポイントのリストが表示されます。

3. 削除するリカバリポイントを選択し、アクションアイコン>*リカバリポイントの削除*を選択して削除します。

Kubernetes ワークロード用の**NetApp Backup and Recovery**実行フック テンプレートを管理する

実行フックは、管理された Kubernetes アプリケーションのデータ保護操作で実行されるカスタム アクションです。たとえば、実行フックを使用してスナップショットの前にデータベース トランザクションを一時停止し、スナップショット後に再開することで、アプリケーション整合性のあるスナップショットを作成します。実行フック テンプレートを作成するときは、フックの種類、実行するスクリプト、およびターゲット コンテナーのフィルターを指定します。テンプレートを使用して、実行フックをアプリケーションにリンクします。

NetApp Backup and Recoveryは、データ保護中にKubeVirtなどのアプリケーションのファイルシステムをフリーズおよびアンフリーズします。Trident Protectのドキュメントを使用して、この動作をグローバルに無効にすることも、特定のアプリケーションに対して無効にすることもできます：

- すべてのアプリケーションでこの動作を無効にするには、 "KubeVirt VM によるデータ保護" 。
- 特定のアプリケーションでこの動作を無効にするには、 "アプリケーションを定義する" 。

必要な**NetApp Console**ロール

組織管理者またはSnapCenter管理者。"NetApp Backup and Recoveryのアクセス ロールについて学習します" 。 "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" 。

実行フックの種類

NetApp Backup and Recovery は、実行できるタイミングに基づいて、次のタイプの実行フックをサポートしています。

- 事前スナップショット
- スナップショット後
- バックアップ前
- バックアップ後
- 復元後

実行順序

データ保護操作が実行されると、実行フック イベントが次の順序で発生します。

1. 適用可能なカスタム操作前実行フックは、適切なコンテナで実行されます。複数のカスタム事前操作フックを作成できますが、その実行順序は保証されず、構成もできません。
2. 該当する場合、ファイルシステムのフリーズが発生します。
3. データ保護操作が実行されます。
4. 該当する場合、凍結されたファイルシステムは凍結解除されます。
5. NetApp Backup and Recovery は、適切なコンテナで適用可能なカスタム操作前実行フックを実行します。複数のカスタム操作後フックを作成できますが、その実行順序は保証されず、構成もできません。

同じタイプのフックを複数作成した場合、それらの実行順序は保証されません。異なるタイプのフックは常に指定された順序で実行されます。たとえば、さまざまな種類のフックがすべて含まれる構成の実行順序は次のとおりです。

1. スナップショット前のフックが実行されました
2. スナップショット後のフックが実行されました
3. バックアップ前のフックが実行されました
4. バックアップ後のフックが実行されました

実行フック スクリプトを本番環境で有効にする前にテストします。 「kubectl exec」を使用してスクリプトをテストし、アプリを一時的な名前空間に複製して復元することで、スナップショットとバックアップを検証します。

スナップショット前の実行フックによって Kubernetes リソースが追加、変更、または削除された場合、それらの変更はスナップショットまたはバックアップと、その後のすべての復元操作に含まれます。

カスタム実行フックに関する重要な注意事項

アプリの実行フックを計画するときは、次の点を考慮してください。

- 実行フックは、アクションを実行するためにスクリプトを使用する必要があります。複数の実行フックが同じスクリプトを参照できます。
- 実行フックは、実行可能なシェル スクリプトの形式で記述する必要があります。
- スクリプトのサイズは 96 KB に制限されています。
- 実行フックの設定と一致基準は、スナップショット、バックアップ、または復元操作に適用可能なフックを決定するために使用されます。

実行フックにより、アプリケーションの機能が低下したり、無効になったりする可能性があります。カスタムフックをできるだけ早く実行するようにします。関連する実行フックを使用してバックアップまたはスナップショット操作を開始したが、その後キャンセルした場合でも、バックアップまたはスナップショット操作がすでに開始されている場合は、フックは引き続き実行できます。つまり、バックアップ後の実行フックで使用されるロジックでは、バックアップが完了したと想定することはできません。

実行フックフィルター

アプリケーションの実行フックを追加または編集するときに、実行フックにフィルターを追加して、フックが一致するコンテナーを管理できます。フィルターは、すべてのコンテナーで同じコンテナー イメージを使用するが、各イメージを異なる目的で使用する可能性があるアプリケーション (Elasticsearch など) に役立ちます。フィルターを使用すると、実行フックが必ずしもすべての同一コンテナーではなく一部のコンテナーで実行されるシナリオを作成できます。単一の実行フックに対して複数のフィルターを作成すると、それらは論理 AND 演算子で結合されます。実行フックごとに最大 10 個のアクティブ フィルターを設定できます。

実行フックに追加する各フィルターは、正規表現を使用してクラスター内のコンテナを照合します。フックがコンテナに一致すると、フックはそのコンテナ上で関連付けられたスクリプトを実行します。フィルターの正規表現では正規表現 2 (RE2) 構文が使用されますが、一致リストからコンテナーを除外するフィルターの作成はサポートされていません。 NetApp Backup and Recoveryが実行フックフィルタの正規表現でサポートする構文については、以下を参照してください。 "正規表現2（RE2）構文のサポート" 。

復元またはクローン操作後に実行される実行フックに名前空間フィルターを追加し、復元またはクローンのソースと宛先が異なる名前空間にある場合、名前空間フィルターは宛先の名前空間にのみ適用されます。

実行フックの例

訪問 "NetApp Verda GitHub プロジェクト"Apache Cassandra や Elasticsearch などの一般的なアプリの実際の実行フックをダウンロードします。また、例を参照したり、独自のカスタム実行フックを構成するためのア

イデアを入手したりすることもできます。

実行フックテンプレートを作成する

アプリケーションでのデータ保護操作の前後にアクションを実行するために使用できるカスタム実行フックテンプレートを作成できます。

ここで作成するテンプレートは、Kubernetes ワークロードを保護する場合にのみ使用できます。

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. *設定*タブを選択します。
3. 実行フック テンプレート セクションを展開します。
4. *実行フックテンプレートの作成*を選択します。
5. 実行フックの名前を入力します。
6. 必要に応じて、フックの種類を選択します。たとえば、復元後フックは復元操作が完了した後に実行されます。
7. スクリプト テキスト ボックスに、実行フック テンプレートの一部として実行する実行可能シェル スクリプトを入力します。必要に応じて、*スクリプトのアップロード*を選択して、代わりにスクリプト ファイルをアップロードすることもできます。
8. *作成*を選択します。

   テンプレートを作成すると、実行フック テンプレート セクションのテンプレートのリストに表示されます。

NetApp Backup and Recoveryのジョブを監視する

NetApp Backup and Recoveryを使用すると、ローカル スナップショット、レプリケーション、および開始したバックアップ ジョブを監視します。開始した復元ジョブを追跡します。完了したジョブ、進行中のジョブ、失敗したジョブを表示して、問題の診断に役立ちます。 NetApp Console通知センターで電子メール通知を有効にすると、ログインしていないときでもシステム アクティビティに関する最新情報を入手できます。コンソール タイムラインを使用して、UI または API から開始されたすべてのアクションの詳細を表示します。

NetApp Backup and Recovery はジョブ情報を 15 日間保持し、その後ジョブ情報を削除してジョブ モニターから除去します。

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、バックアップおよびリカバリ リストア管理者、バックアップおよびリカバリ クローン管理者、またはバックアップおよびリカバリ ビューアー ロール。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" 。

ジョブモニターでジョブのステータスを表示する

ジョブ監視 タブでは、すべてのスナップショット、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、および復元操作とその現在のステータスのリストを表示できます。これには、 Cloud Volumes ONTAP、オンプレミスのONTAP、アプリケーション、仮想マシンからの操作が含まれます。各操作またはジョブには、一意の ID とステータスがあります。

ステータスは次のようになります。

- 成功
- 実行中
- キューに登録
- 警告
- 失敗

NetApp Backup and Recovery UI および API から開始したスナップショット、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、および復元操作は、[ジョブ監視] タブで利用できます。

ONTAPシステムを 9.13.x にアップグレードし、ジョブ モニターに進行中のスケジュールされたバックアップ操作が表示されない場合は、 NetApp Backup and Recoveryを再起動してください。"NetApp Backup and Recoveryを再起動する方法を学ぶ"。

手順

1. NetApp Backup and Recoveryメニューから、監視 を選択します。
2. 追加の列 (システム、SVM、ユーザー名、ワークロード、ポリシー名、スナップショット ラベル) を表示するには、プラス記号を選択します。

求人リストを検索してフィルタリングする

ポリシー、スナップショット ラベル、操作の種類 (保護、復元、保持など)、保護の種類 (ローカル スナップショット、レプリケーション、クラウドへのバックアップ) などのいくつかのフィルターを使用して、[ジョブ監視] ページで操作をフィルターできます。

デフォルトでは、ジョブ監視ページには過去 24 時間の保護ジョブと回復ジョブが表示されます。タイムフレーム フィルターを使用してタイムフレームを変更できます。

手順

1. NetApp Backup and Recoveryメニューから、監視 を選択します。
2. 結果を異なる方法で並べ替えるには、各列見出しを選択し、ステータス、開始時刻、リソース名などで並べ替えます。
3. 特定の求人を探している場合は、「詳細検索とフィルタリング」領域を選択して検索パネルを開きます。

   このパネルを使用して、任意のリソースのフリーテキスト検索を入力します (例:「ボリューム 1」または「アプリケーション 3」)。ドロップダウン メニューの項目に応じてジョブ リストをフィルターすることもできます。

   ほとんどのフィルターは説明を要しません。「ワークロード」のフィルターを使用すると、次のカテゴリのジョブを表示できます。

- ONTAPボリューム (Cloud Volumes ONTAPおよびオンプレミスのONTAPボリューム)
- Microsoft SQL Server
- 仮想マシン
- Kubernetes

- 最初にシステムを選択した場合にのみ、特定の「SVM」内のデータを検索できます。
- 「タイプ」で「保護」を選択した場合のみ、「保護タイプ」フィルターを使用して検索できます。

4. ページをすぐに更新するには、  ボタン。それ以外の場合、このページは 15 分ごとに更新され、常に最新のジョブ ステータスの結果が表示されます。

求人の詳細を見る

特定の完了したジョブに対応する詳細を表示できます。特定のジョブの詳細を JSON 形式でエクスポートできます。

ジョブ タイプ (スケジュールまたはオンデマンド)、 SnapMirrorバックアップ タイプ (初期または定期) の開始時刻と終了時刻、期間、システムからオブジェクト ストレージに転送されたデータの量、平均転送速度、ポリシー名、有効な保持ロック、実行されたランサムウェア スキャン、保護ソースの詳細、保護ターゲットの詳細などの詳細を表示できます。

復元ジョブでは、バックアップ ターゲット プロバイダー (Amazon Web Services、Microsoft Azure、Google Cloud、オンプレミス)、S3 バケット名、SVM 名、ソース ボリューム名、宛先ボリューム、スナップショット ラベル、復元されたオブジェクトの数、ファイル名、ファイル サイズ、最終変更日、完全なファイル パスなどの詳細が表示されます。

手順

1. NetApp Backup and Recoveryメニューから、監視 を選択します。
2. ジョブの名前を選択します。
3. アクションメニューを選択します•••[詳細を表示]を選択します。
4. 各セクションを展開すると詳細が表示されます。

ジョブ監視の結果をレポートとしてダウンロードする

結果をフィルタリングまたは並べ替えた後、メインのジョブ監視ページの内容をレポートとしてダウンロードできます。NetApp Backup and Recovery は、必要に応じて確認したり他のグループに送信したりできる .CSV ファイルを生成してダウンロードします。.CSV ファイルには最大 10,000 行のデータが含まれます。

ジョブ監視の詳細情報から、単一のジョブの詳細を含む JSON ファイルをダウンロードできます。

手順

1. NetApp Backup and Recoveryメニューから、監視 を選択します。
2. すべてのジョブの CSV ファイルをダウンロードするには、[ダウンロード] ボタンを選択し、ダウンロード ディレクトリでファイルを見つけます。
3. 単一のジョブのJSONファイルをダウンロードするには、[アクション]メニューを選択します。•••ジョブの場合は、*JSON ファイルのダウンロード*を選択し、ダウンロード ディレクトリでファイルを見つけま

す。

保持（バックアップ ライフサイクル）ジョブを確認する

保持（バックアップ ライフサイクル）フローを監視して、バックアップを確認し、安全に保ち、監査をサポートします。ライフサイクルを追跡するために、バックアップ コピーの有効期限を特定します。

バックアップ ライフサイクル ジョブは、削除されたスナップショット、または削除待ちのキューにあるスナップショットをすべて追跡します。ONTAP 9.13 以降では、「ジョブ監視」ページで「保持」と呼ばれるすべてのジョブ タイプを表示できます。

「保持」ジョブ タイプは、NetApp Backup and Recoveryによって保護されているボリューム上で開始されたすべてのスナップショット削除ジョブをキャプチャします。

手順

1. NetApp Backup and Recoveryメニューから、監視 を選択します。
2. *高度な検索とフィルタリング*領域を選択して、検索パネルを開きます。
3. ジョブタイプとして「保持」を選択します。

NetApp Console通知センターでバックアップとリストアのアラートを確認する

NetApp Console通知センターは、開始したバックアップおよび復元ジョブの進行状況を追跡し、操作が成功したかどうかを確認できます。

通知センターでアラートを表示し、ログインしていない場合でも重要なシステム アクティビティに関する電子メール アラートを送信するようにコンソールを構成することができます。 "通知センターの詳細と、バックアップおよび復元ジョブのアラートメールを送信する方法を学びます" 。

通知センターには、多数のスナップショット、レプリケーション、クラウドへのバックアップ、復元イベントが表示されますが、電子メールアラートをトリガーするのは特定のイベントのみです。

処理のタイプ	イベント	アラートが生成されました	メールが送信されました
アクティベーション	システムのバックアップとリカバリのアクティベーションに失敗しました	はい	はい
アクティベーション	システムのバックアップとリカバリの編集に失敗しました	はい	はい
アクティベーション	ボリュームがスナップショットポリシーに関連付けられました	はい	はい
アクティベーション	ボリュームのバックアップまたは状態の変更	はい	はい
アクティベーション	システムのバックアップとリカバリのアクティベーションが成功しました	はい	はい
アクティベーション	アドホックボリュームのバックアップに失敗しました	はい	はい
アクティベーション	アドホックボリュームのバックアップが成功しました	はい	いいえ

処理のタイプ	イベント	アラートが生成されました	メールが送信されました
アクティベーション	マルチボリュームバックアップに失敗しました	はい	はい
Cron操作	欠落しているスナップショットラベルの確認	はい	はい
Cron操作	このシステムのONTAPにセキュリティ トークンを送信できませんでした	はい	はい
Pub/Subイベント	接続失敗	はい	いいえ
Pub/Subイベント	スケジュールされたスナップショットを削除できませんでした	はい	いいえ
Pub/Subイベント	ボリュームのスケジュールされたバックアップに失敗しました	はい	いいえ
Pub/Subイベント	ボリュームの復元に成功しました	はい	いいえ
Pub/Subイベント	ボリュームの復元に失敗しました	はい	いいえ
ランサムウェア	バックアップコピーで潜在的なランサムウェア攻撃が検出されました	はい	はい
ランサムウェア	このシステムのバックアップコピーで潜在的なランサムウェア攻撃が検出されました	はい	はい
ローカルスナップショット	NetApp Backup and Recovery のアドホック スナップショット作成ジョブの失敗	はい	はい
レプリケーション	ボリューム障害のレプリケーション関係の変更	はい	はい
レプリケーション	NetApp Backup and Recovery のアドホック レプリケーション ジョブの失敗	はい	はい
レプリケーション	NetApp Backup and Recoveryのレプリケーション一時停止ジョブの失敗	はい	いいえ
レプリケーション	NetApp Backup and Recoveryのレプリケーションによるジョブの中断の失敗	はい	いいえ
レプリケーション	NetApp Backup and Recoveryのレプリケーション再同期ジョブの失敗	はい	いいえ
レプリケーション	NetApp Backup and Recoveryのレプリケーション停止ジョブの失敗	はい	いいえ
レプリケーション	NetApp Backup and Recoveryレプリケーション逆再同期ジョブの失敗	はい	はい
レプリケーション	NetApp Backup and Recovery のレプリケーション削除ジョブの失敗	はい	はい
ターゲット操作	ローカルまたはクラウドへの復元の失敗	はい	はい
ターゲット操作	オンデマンド復元の失敗	はい	はい
システム操作	アドホックボリュームスナップショットの作成失敗	はい	はい

ONTAP 9.13.0 以降では、 Cloud Volumes ONTAPおよびオンプレミスのONTAPシステムのすべてのアラートが表示されます。 Cloud Volumes ONTAP 9.13.0 およびオンプレミスのONTAPを搭載したシステムの場合、「復元ジョブは完了しましたが、警告があります」に関連するアラートのみが表示されます。

デフォルトでは、 NetApp Consoleの組織およびアカウント管理者は、すべての「重大」および「推奨事項」アラートに関するメールを受信します。デフォルトでは、システムは他のユーザーや受信者が通知メールを受信するように設定しません。 NetAppクラウド アカウントのコンソール ユーザー、またはバックアップと復元のアクティビティについて知る必要があるその他の受信者への電子メール アラートを構成します。

NetApp Backup and Recovery の電子メールアラートを受信するには、通知設定ページで通知の重大度タイプとして「重大」、「警告」、「エラー」を選択する必要があります。

"バックアップおよび復元ジョブのアラートメールを送信する方法を学びます"。

手順

1. コンソールメニューから（ ）。
2. 通知を確認します。

コンソールタイムラインで操作アクティビティを確認する

コンソール タイムラインでバックアップおよび復元操作の詳細を表示して、さらに調査することができます。コンソール タイムラインには、ユーザーが開始したものかシステムが開始したものかに関係なく、各イベントの詳細が提供され、UI または API 経由で開始されたアクションが表示されます。

"タイムラインと通知センターの違いについて学びましょう"。

NetApp Backup and Recoveryを再起動します

NetApp Backup and Recovery を再起動しなければならない場合があります。

コンソール エージェントには、NetApp Backup and Recovery機能が含まれています。

手順

1. コンソール エージェントが実行されている Linux システムに接続します。

コンソールエージェントの場所	手順
クラウド展開	指示に従ってください "コンソールエージェントLinux仮想マシンへの接続"使用しているクラウド プロバイダーによって異なります。
手動インストール	Linux システムにログインします。

2. サービスを再起動するコマンドを入力します。

コンソールエージェントの場所	**Docker**コマンド	ポッドマンコマンド
クラウド展開	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`

コンソールエージェントの場所	**Docker**コマンド	ポッドマンコマンド
インターネットアクセスによる手動インストール	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
インターネットアクセスなしでの手動インストール	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`