



# 保護関係の作成、監視、およびトラブルシューティング

## OnCommand Unified Manager 9.5

NetApp  
December 20, 2023

# 目次

保護関係の作成、監視、およびトラブルシューティング .....	1
SnapMirror 保護のタイプ .....	1
Unified Manager で保護関係をセットアップする .....	2
保護関係のフェイルオーバーとフェイルバックを実行する .....	8
保護ジョブの失敗を解決する .....	13
遅延の問題を解決する .....	16

# 保護関係の作成、監視、およびトラブルシューティング

Unified Manager では、保護関係の作成、管理対象クラスタに保存されているデータのミラー保護とバックアップ保護の監視とトラブルシューティング、および上書きされたデータや失われたデータのリストアを実行できます。

## SnapMirror 保護のタイプ

導入するデータストレージのトポロジに応じて、複数のタイプの SnapMirror 保護関係を Unified Manager で設定できます。すべての種類の SnapMirror 保護では、フェイルオーバーによるディザスタリカバリ保護が提供されますが、パフォーマンス、バージョン依存性の解消、および複数のバックアップコピーによる保護については、提供される機能が異なります。

### 従来型の SnapMirror 非同期保護関係

従来型の SnapMirror 非同期保護では、ソースボリュームとデスティネーションボリューム間のブロックレプリケーションによるミラー保護が提供されます。

従来型の SnapMirror 関係では、ブロックレプリケーションに基づいてミラー処理が行われるため、他の SnapMirror 関係よりも高速なミラー処理が可能です。ただし、従来型の SnapMirror 保護では、デスティネーションボリュームで実行されている ONTAP ソフトウェアのマイナーバージョンがソースボリュームと同じかそれよりも新しい必要があります（バージョン 8.x から 8.x、9.x から 9.x など）。

### バージョンに依存しないレプリケーションを使用した SnapMirror 非同期保護

バージョンに依存しないレプリケーションを使用した SnapMirror 非同期保護では、ソースボリュームとデスティネーションボリューム間に論理レプリケーションによるミラー保護が提供されます。ボリュームで異なるバージョンの ONTAP 8.3 以降のソフトウェアを実行している場合でも同様です（バージョン 8.3 から 8.3、8.3 から 9.1、9.0 から 8.3 など）。

バージョンに依存しないレプリケーションを使用した SnapMirror 関係では、ミラー処理が従来型の SnapMirror 関係ほど高速ではありません。

実行速度が遅いため、バージョンに依存しないレプリケーション保護を使用する SnapMirror は、次の状況のどちらにも適していません。

- ・ソースオブジェクトには、保護対象のファイルが 1、000 万を超えています。
- ・保護対象データの目標復旧時点が 2 時間以下である。（つまり、ソースのデータからの遅れが 2 時間未満のリカバリ可能なミラーデータが常にデスティネーションに含まれている必要があります）。

これらのいずれかの状況では、デフォルトの SnapMirror 保護をより高速なブロックレプリケーションベースで実行する必要があります。

## バージョンに依存しないレプリケーションとバックアップオプションを使用した SnapMirror 非同期保護

バージョンに依存しないレプリケーションとバックアップオプションを使用した SnapMirror 非同期保護では、ソースボリュームとデスティネーションボリューム間のミラー保護およびミラーデータの複数のコピーをデスティネーションに格納する機能が提供されます。

ストレージ管理者は、ソースからデスティネーションにミラーリングする Snapshot コピーを指定したり、ソースで削除されたコピーをデスティネーションに保持する期間を指定したりできます。

バージョンに依存しないレプリケーションとバックアップオプションを使用した SnapMirror 関係では、ミラー処理が従来型の SnapMirror 関係ほど高速ではありません。

## 厳密な同期を使用した SnapMirror 同期保護

「stict」同期を使用した SnapMirror 同期保護では、プライマリボリュームとセカンダリボリュームが常に相互の完全なコピーになります。セカンダリボリュームへのデータの書き込みでレプリケーションエラーが発生すると、プライマリボリュームに対するクライアント I/O が中断されます。

## 通常の同期を使用した SnapMirror 同期保護

「ル」同期を使用した SnapMirror 同期保護では、プライマリボリュームとセカンダリボリュームが常に相互の完全なコピーである必要はないため、プライマリボリュームの可用性が確保されます。セカンダリボリュームへのデータの書き込みでレプリケーションエラーが発生すると、プライマリボリュームとセカンダリボリュームが同期されていない状態のまま、プライマリボリュームに対するクライアント I/O が継続されます。



同期保護関係を健全性/ボリュームのインベントリページまたは健全性/ボリュームの詳細ページから監視する場合は、リストアボタンと関係操作ボタンは使用できません。

## Unified Manager で保護関係をセットアップする

Unified Manager と OnCommand Workflow Automation を使用してデータを保護するための SnapMirror 関係と SnapVault 関係をセットアップするには、いくつかの手順を実行する必要があります。

### 作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- 2 つのクラスタまたは 2 つの Storage Virtual Machine (SVM) 間にピア関係を確立しておく必要があります。
- OnCommand Workflow Automation を Unified Manager に統合する必要があります。
  - [OnCommand Workflow Automation をセットアップする](#)
  - [Workflow Automation での Unified Manager データソースのキャッシングの確認](#)

### 手順

1. 作成する保護関係のタイプに応じて、次のいずれかを実行します。

- SnapMirror 保護関係を作成する。
  - SnapVault 保護関係を作成する。
2. 関係のポリシーを作成する場合は、作成する関係タイプに応じて、次のいずれかを実行します。
- SnapVault ポリシーを作成する。
  - SnapMirror ポリシーを作成する。
3. SnapMirror または SnapVault スケジュールを作成します。

## Workflow Automation と Unified Manager の間の接続の設定

OnCommand Workflow Automation （ WFA ） と Unified Manager の間にセキュアな接続を確立することができます。Workflow Automation に接続することで、 SnapMirror や SnapVault の設定ワークフロー、 SnapMirror 関係の管理用コマンドなどの保護機能を使用できるようになります。

作業を開始する前に

- バージョン4.2以降のWorkflow Automationがインストールされている必要があります。
- WFAサーバに「WFA pack for managing Clustered Data ONTAP」バージョン9.5.0以上がインストールされている必要があります。これらは、NetAppStorage Automation Storeからダウンロードできます。


### "ONTAP を管理するための WFA パック"

- WFA と Unified Manager の接続をサポートするために Unified Manager で作成したデータベースユーザの名前を確認しておく必要があります。

このデータベースユーザには、統合スキーマユーザロールが割り当てられている必要があります。

- Workflow Automation で Administrator ロールまたは Architect のロールが割り当てられている必要があります。
- ホストアドレス、ポート番号 443 、および Workflow Automation セットアップのユーザ名とパスワードが必要です。
- OnCommand 管理者またはストレージ管理者のロールが必要です。

手順

1. ツールバーで、をクリックします  \*をクリックし、左の[セットアップ]メニューの[ Workflow Automation\*]をクリックします。
2. OnCommand Unified Managerの[データベースユーザ\*]領域の[セットアップ/ Workflow Automation \*]ページで、名前を選択し、Unified Manager接続とWorkflow Automation接続をサポートするために作成したデータベースユーザのパスワードを入力します。
3. Setup/Workflow Automation ページの OnCommand Workflow Automation クリデンシャル\*領域に、ホスト名またはIPアドレス（IPv4またはIPv6） 、およびWorkflow Automationセットアップのユーザー名とパスワードを入力します。

Unified Managerサーバのポート（ポート443）を使用する必要があります。

4. [ 保存 ( Save ) ] をクリックします。
5. 自己署名証明書を使用する場合は、[\* はい] をクリックしてセキュリティ証明書を承認します。

Setup/Workflow Automation ページが表示されます。

6. Web UI をリロードして Workflow Automation の機能を追加するには、「\* Yes 」をクリックします。

## Workflow Automation での Unified Manager データソースのキャッシングの確認

Unified Manager データソースのキャッシングが正しく機能しているかどうかを判別するには、Workflow Automation でデータソースの取得が正常に行われているかどうかを確認します。Workflow Automation を Unified Manager に統合する際にこの操作を実行して、統合後に Workflow Automation の機能が利用可能になることを確認できます。

作業を開始する前に

このタスクを実行するには、Workflow Automation で Administrator ロールまたは Architect ロールが割り当てられている必要があります。

手順

1. Workflow Automation の UI から、\* Execution \* > \* Data Sources \* を選択します。
2. Unified Manager データソースの名前を右クリックし、\* 今すぐ取得 \* を選択します。
3. 取得が正常に完了してエラーが発生しないことを確認します

Workflow Automation を Unified Manager に統合するためには、収集エラーを解決する必要があります。

## ケンセンセイ/ホリユウムノシヨウサイヘエシテ**SnapMirror**ホコカンケイヲサクセイ

データレプリケーションを有効にしてデータを保護するために、健全性/ボリュームの詳細ページを使用して SnapMirror 関係を作成することができます。SnapMirror レプリケーションを使用すると、ソースでデータ損失が発生した場合にデスティネーションボリュームからデータをリストアできます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

このタスクについて

次の場合、\* Protect \* メニューは表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリュームが FlexGroup ボリュームの場合
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出さ

れていない場合など

保護ジョブは、パフォーマンスに影響を及ぼすことなく最大 10 件まで同時に実行できます。11~30 件のジョブを同時に実行すると、パフォーマンスが低下することがあります。30 を超えるジョブを同時に実行することは推奨されません。

## 手順

1. \*正常性/ボリューム\*の詳細ページの\*保護\*タブで、保護するボリュームの名前をトポロジビューで右クリックします。
2. メニューから \* Protect \* > \* SnapMirror \* を選択します。

Configure Protection（保護の設定）ダイアログボックスが表示されます。

3. 「\* SnapMirror \*」をクリックして、「\* SnapMirror \*」タブを表示し、デスティネーション情報を設定します。
4. 必要に応じて「\* 詳細設定 \*」をクリックしてスペースギャランティを設定し、「\* 適用 \*」をクリックします。
5. [ 保護の設定 \*] ダイアログボックスの [ 接続先情報 \*] 領域と [ 関係設定 \*] 領域に入力します。
6. [ 適用（Apply） ] をクリックします。

健全性とボリュームの詳細ページに戻ります。

7. 「\* Health / Volume \* details」 ページの上部にある保護設定ジョブのリンクをクリックします。

ジョブのタスクと詳細が保護/ジョブの詳細ページに表示されます。

8. [\*保護/ジョブ\*の詳細] ページで、[\*更新] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。
9. ジョブのタスクが完了したら、ブラウザの\*戻る\*をクリックして\*正常性/ボリューム\*の詳細ページに戻ります。

新しい関係は、健全性/ボリュームの詳細ページのトポロジビューに表示されます。

## 結果

設定で指定したデスティネーション SVM と詳細設定で有効にしたオプションに応じて、次のいずれかの SnapMirror 関係が作成されます。

- ソースボリュームと同じかそれよりも新しいバージョンの ONTAP で実行されているデスティネーション SVM を指定した場合、デフォルトではブロックレプリケーションベースの SnapMirror 関係が作成されます。
- ソースボリュームと同じかそれよりも新しいバージョン（バージョン 8.3 以降）の ONTAP で実行されているデスティネーション SVM を指定し、詳細設定でバージョンに依存しないレプリケーションを有効にした場合、バージョンに依存しないレプリケーションを使用した SnapMirror 関係が作成されます。
- ONTAP 8.3 の以前のバージョン、またはソースボリュームよりも新しいバージョンで実行されているデスティネーション SVM を指定した場合、以前のバージョンでバージョンに依存しないレプリケーションがサポートされていれば、バージョンに依存しないレプリケーションを使用した SnapMirror 関係が自動で作成されます。

## ケンセンセイ/ホリユウムノシヨウサイヘエシテノ**SnapVault** ホコカンケイノサクセイ

ボリュームでデータバックアップを有効にして保護するために、健全性/ボリュームの詳細ページを使用してSnapVault 関係を作成することができます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- このタスクを実行するには、Workflow Automation をセットアップしておく必要があります。

このタスクについて

次の場合、\* Protect \* メニューは表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など

手順

1. \*正常性/ボリューム\*の詳細ページの\*保護\*タブで、保護するボリュームをトポロジビューで右クリックします。
2. メニューから \* Protect \* > \* SnapVault \* を選択します。

Configure Protection （保護の設定）ダイアログボックスが開きます。

3. SnapVault \* をクリックして、\* SnapVault \* タブを表示し、セカンダリ・リソース情報を設定します。
4. [\* 詳細設定 \*] をクリックして、必要に応じて重複排除、圧縮、自動拡張、およびスペースギャランティを設定し、[\* 適用 \*] をクリックします。
5. [保護の設定 \*] ダイアログボックスの[接続先情報 \*] 領域と[関係設定 \*] 領域に入力します。
6. [適用（Apply）] をクリックします。

健全性とボリュームの詳細ページに戻ります。

7. 「\* Health / Volume \* details」 ページの上部にある保護設定ジョブのリンクをクリックします。

保護/ジョブの詳細ページが表示されます。

8. 保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認するには、[\* Refresh] をクリックします。

ジョブのタスクが完了すると、新しい関係が正常性/ボリュームの詳細ページのトポロジビューに表示されます。

## 転送効率を最大化するための **SnapVault** ポリシーを作成する

新しい SnapVault ポリシーを作成して SnapVault 転送の優先度を設定できます。ポリシ



ーを使用することで、保護関係におけるプライマリからセカンダリへの転送効率を最大化できます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- [ 保護の設定 ] ダイアログボックスの [ 接続先情報 ] 領域が既に完了している必要があります。

手順

1. [ 保護の設定 \* ] ダイアログボックスの [ SnapVault ポリシーの作成 \* ] タブで、[ 関係設定 \* ] 領域の [ ポリシーの作成 \* ] リンクをクリックします。

SnapVault タブが表示されます。

2. [ \* ポリシー名 \* ] フィールドに、ポリシーに付ける名前を入力します。
3. [ \* 転送優先度 \* ] フィールドで、ポリシーに割り当てる転送優先度を選択します。
4. [ \* Comment \* (コメント) ] フィールドに、ポリシーのコメントを入力します。
5. レプリケーションラベル \* 領域で、必要に応じてレプリケーションラベルを追加または編集します。
6. [ 作成 ( Create ) ] をクリックします。

新しいポリシーが [Create Policy] ドロップダウンリストに表示されます。

転送効率を最大化するために、 **SnapMirror** ポリシーを作成します

SnapMirror ポリシーを作成して、保護関係における SnapMirror 転送の優先順位を指定することができます。SnapMirror ポリシーで優先度を割り当てて、優先度が低い転送を通常の優先度の転送よりもあとに実行するようにスケジュールすることで、ソースからデスティネーションへの転送効率を最大化できます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- このタスクでは、[ 保護の設定 ] ダイアログボックスの [ 宛先情報 ] 領域がすでに完了していることを前提としています。

手順

1. Configure Protection \* (保護の設定) ダイアログボックスの \* SnapMirror \* タブで、\* Relationship Settings \* (関係設定 \*) 領域の \* Create Policy \* (ポリシーの作成) リンクをクリックします。

SnapMirror ポリシーの作成ダイアログボックスが表示されます。

2. [ \* ポリシー名 \* ] フィールドに、ポリシーに付ける名前を入力します。

3. [\* 転送優先度 \*] フィールドで、ポリシーに割り当てる転送優先度を選択します。
4. [\* コメント \* ( \* Comment \* ) ] フィールドに、ポリシーのオプションのコメントを入力します。
5. [ 作成 ( Create ) ] をクリックします。

新しいポリシーが SnapMirror ポリシーのドロップダウンリストに表示されます。

## SnapMirror スケジュールと SnapVault スケジュールを作成

SnapMirror および SnapVault の基本または詳細スケジュールを作成して、ソースボリュームまたはプライマリボリュームで自動データ保護転送を有効にすることができます。ボリュームでのデータ変更の頻度に応じて、転送の実行頻度を調整することができます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- [ 保護の設定 ] ダイアログボックスの [ 宛先情報 ] 領域に、すでに入力されている必要があります。
- このタスクを実行するには、Workflow Automation をセットアップしておく必要があります。

手順

1. [ 保護の設定 ] ダイアログ・ボックスの [\* SnapMirror \*] タブまたは [\* SnapVault \*] タブで、[\* 関係設定 \*] 領域の [\* スケジュールの作成 ] リンクをクリックします。

Create Schedule (スケジュールの作成) ダイアログボックスが表示されます。

2. [\* スケジュール名 \*] フィールドに、スケジュールに付ける名前を入力します。
3. 次のいずれかを選択します。

- \* 基本 \*

間隔で指定する基本的なスケジュールを作成する場合に選択します。

- \* 詳細 \*

cron 形式のスケジュールを作成する場合に選択します。

4. [ 作成 ( Create ) ] をクリックします。

新しいスケジュールは、SnapMirror Schedule または SnapVault Schedule ドロップダウンリストに表示されます。

## 保護関係のフェイルオーバーとフェイルバックを実行する

ハードウェア障害や災害が原因で保護関係のソースボリュームが無効になっている場合は、Unified Manager の保護関係機能を使用して保護デスティネーションの読み取り / 書き込みアクセスを可能にし、ソースがオンラインに戻るまでそのボリュームにフェイ

ルオーバーすることができます。その後、データの提供に使用できる元のソースにフェイルバックできます。

## 作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- この処理を実行するには、OnCommand Workflow Automation をセットアップしておく必要があります。

## 手順

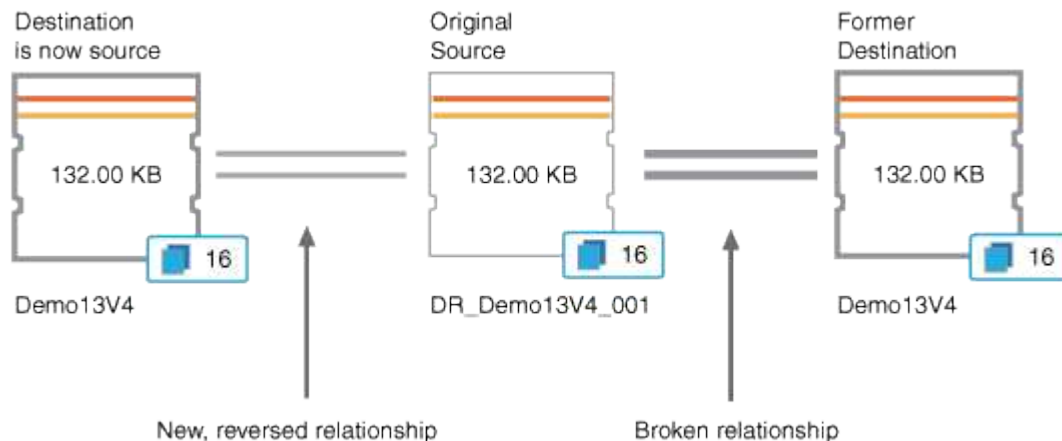
### 1. SnapMirror 関係を解除。

デスティネーションをデータ保護ボリュームから読み書き可能ボリュームに変換する前、および関係を反転する前に、関係を解除する必要があります。

### 2. 保護関係を反転する。

元のソースボリュームが再び使用可能になったら、ソースボリュームをリストアして元の保護関係を再確立できます。ソースをリストアする前に、以前のデスティネーションに書き込まれたデータとソースを同期させる必要があります。逆再同期処理を使用して新しい保護関係を作成するには、元の関係のロールを反転し、ソースボリュームと以前のデスティネーションを同期させます。新しい関係に対して新しいベースライン Snapshot コピーが作成されます。

反転関係は、カスケード関係に似ています。



### 3. 反転する SnapMirror 関係を解除する。

元のソースボリュームが再同期され、再びデータを提供できるようになったら、解除処理を使用して反転関係を解除します。

### 4. 関係を削除します。

反転関係が不要になった場合は、元の関係を再確立する前に反転関係を削除する必要があります。

### 5. 関係を再同期します。

再同期処理を使用して、ソースからデスティネーションにデータを同期し、元の関係を再確立します。

## 健全性/ボリュームの詳細ページから**SnapMirror**関係を解除します

保護関係を健全性/ボリュームの詳細ページから解除して、SnapMirror関係にあるソースボリュームとデスティネーションボリュームの間のデータ転送を停止することができます。関係の解除は、データを移行する場合、ディザスタリカバリやアプリケーションのテストなどの目的で行うことがあります。デスティネーションボリュームは読み書き可能ボリュームに変わります。SnapVault 関係を解除することはできません。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. 健全性/ボリューム\*の詳細ページの\*保護\*タブで、解除するSnapMirror関係をトポロジから選択します。
2. 目的地を右クリックして、メニューから \* ブレーク \* を選択します。

[ 関係の解除 ( Break Relationship ) ] ダイアログボックスが表示されます。

3. 「 \* Continue \* 」をクリックして関係を解除します。
4. トポロジで、関係が解除されていることを確認します。

## ケンセンセイ/ホリユウムノシヨウサイヘエシテノホコカンケイノハンテン

災害によって保護関係のソースボリュームが機能しなくなった場合は、ソースの修理や交換を行う間、デスティネーションボリュームを読み書き可能に変換してデータの提供を継続することができます。ソースがデータを受信できる状態に戻ったら、逆再同期処理を使用して逆方向の関係を確立し、ソースのデータを読み書き可能なデスティネーションのデータと同期できます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- SnapVault 関係は使用できません。
- 保護関係がすでに存在している必要があります。
- 保護関係が解除されている必要があります。
- ソースとデスティネーションの両方がオンラインになっている必要があります。
- ソースが別のデータ保護ボリュームのデスティネーションになっていることはできません。

このタスクについて

- このタスクを実行すると、共通の Snapshot コピーのデータよりも新しいソースのデータは削除されます。

- 逆再同期した関係に対して作成されるポリシーとスケジュールは、元の保護関係と同じになります。

ポリシーとスケジュールが存在しない場合は作成されます。

## 手順

1. 健全性/ボリューム\*の詳細ページの\*保護\*タブで、ソースとデスティネーションを反転するSnapMirror関係をトポロジから探して右クリックします。
2. メニューから \* 逆再同期 \* を選択します。

逆再同期（ Reverse Resync ） ダイアログボックスが表示されます。

3. 逆再同期を実行する関係が \* 逆再同期 \* （ Reverse Resync \* ） ダイアログボックスに表示されていることを確認し、 \* 送信 \* （ Submit \* ） をクリックします。

逆再同期（Reverse Resync）ダイアログボックスが閉じ、健全性/ボリュームの詳細ページの上部にジョブのリンクが表示されます。

4. 各逆再同期ジョブのステータスを追跡するには、\*健全性/ボリューム\*の詳細ページで\*ジョブの表示\*をクリックします。

フィルタリングされたジョブのリストが表示されます。

5. ブラウザの戻る矢印をクリックして、\*正常性/ボリューム\*の詳細ページに戻ります。

すべてのタスクが正常に完了すれば逆再同期処理は終了です。

## 健全性/ボリュームの詳細ページから保護関係を削除しています

保護関係を削除すると、選択したソースとデスティネーションの間の既存の関係を完全に削除することができます。これは、たとえば別のデスティネーションを使用して関係を作成する場合などに行います。この処理ではすべてのメタデータが削除され、元に戻すことはできません。

### 作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

## 手順

1. 健全性/ボリューム\*の詳細ページの\*保護\*タブで、削除するSnapMirror関係をトポロジから選択します。
2. 目的地の名前を右クリックし、メニューから \* 削除 \* を選択します。

[ 関係の削除（ Remove Relationship ） ] ダイアログボックスが表示されます。

3. [\* 続行 ] をクリックして、関係を削除します。

健全性/ボリュームの詳細ページから関係が削除されます。

健全性/ボリュームの詳細ページから保護関係を再同期しています

SnapMirror 関係や SnapVault 関係を解除してデスティネーションが読み書き可能になったあとに、ソースのデータとデスティネーションのデータが一致するようにデータを再同期することができます。再同期は、必要な共通の Snapshot コピーがソースボリュームで削除されたために SnapMirror や SnapVault の更新が失敗する場合にも実行することができます。

作業を開始する前に

- OnCommand 管理者またはストレージ管理者のロールが必要です。
- OnCommand Workflow Automation のセットアップが完了している必要があります。

手順

1. \* Health/Volume の詳細ページの Protection \* タブで、再同期する保護関係をトポロジから探して右クリックします。
2. メニューから \* Resynchronize \* を選択します。

または、\* Actions \* メニューから \* Relationship \* > \* Resynchronize \* を選択して、現在詳細を表示している関係を再同期します。

再同期化ダイアログボックスが表示されます。

3. [\* Resynchronization Options] \* タブで、転送の優先順位と最大転送速度を選択します。
4. [\* ソース Snapshot コピー \*] をクリックし、[\* Snapshot コピー \*] 列で [\* デフォルト \*] をクリックします。

Select Source Snapshot Copy (ソース Snapshot コピーの選択) ダイアログボックスが表示されます。

5. デフォルトの Snapshot コピーを転送するのではなく、既存の Snapshot コピーを指定する場合は、\* 既存の Snapshot コピー \* をクリックし、リストから Snapshot コピーを選択します。
6. [Submit (送信)] をクリックします。

再同期ダイアログボックスに戻ります。

7. 再同期するソースを複数選択した場合は、既存の Snapshot コピーを指定する次のソースに対して \* Default \* をクリックします。
8. Submit \* をクリックして、再同期ジョブを開始します。

再同期ジョブが開始されると、健全性/ボリュームの詳細ページに戻り、ページの上部にジョブのリンクが表示されます。

9. 各再同期ジョブのステータスを追跡するには、\* 健全性/ボリューム \* の詳細ページで \* ジョブの表示 \* をクリックします。

フィルタリングされたジョブのリストが表示されます。

10. ブラウザの戻る矢印をクリックして、\* 健全性/ボリューム \* の詳細ページに戻ります。

すべてのタスクが正常に完了すれば再同期ジョブは終了です。

## 保護ジョブの失敗を解決する

このワークフローでは、Unified Manager のダッシュボードで保護ジョブの失敗を特定して解決する方法の例を示します。

### 作業を開始する前に

このワークフローの一部のタスクはOnCommand 管理者ロールでログインする必要があるため、の説明に従って、さまざまな機能を使用するために必要なロールを把握しておく必要があります [Unified Manager のユーザロールと機能](#)。

### このタスクについて

このシナリオでは、[ダッシュボード/概要]ページにアクセスして、保護ジョブに問題がないかどうかを確認します。保護インシデント領域には、ボリュームで保護ジョブの失敗エラーが表示され、ジョブ終了インシデントがあることがわかりました。このエラーを調査して、原因と潜在的な解決策を特定します。

### 手順

1. [ダッシュボード\*未解決のインシデントとリスク\*]領域の[保護インシデント\*]パネルで、[保護ジョブ失敗\*]イベントをクリックします。



イベントのリンクされたテキストがフォームに書き込まれます

object\_name:/object\_name - Error Name`など

`cluster2\_src\_svm:/cluster2\_src\_vol2 - Protection Job Failed。

失敗した保護ジョブのイベントの詳細ページが表示されます。

2. 「概要」エリアの「原因」フィールドのエラーメッセージを確認して、問題を特定し、考えられる対処方法を評価します。

を参照してください [保護ジョブが失敗した場合の問題の特定と対処策の実施](#)。

### 保護ジョブが失敗した場合の問題の特定と対処策の実施

原因の詳細ページでジョブエラーのエラーメッセージを確認し、Snapshot コピーのエラーが原因でジョブが失敗したことを確認します。その後、健全性/ボリュームの詳細ページに進み、詳細情報を収集します。

### 作業を開始する前に

OnCommand 管理者のロールが必要です。

## このタスクについて

イベントの詳細ページの原因フィールドに表示されるエラーメッセージには、失敗したジョブに関する次のテキストが含まれています。

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure..)
*Job Details*
```

このメッセージには次の情報が表示されます。

- バックアップジョブまたはミラージョブが正常に完了しませんでした。

ジョブにソースボリューム間の保護関係が関係しています cluster2\_src\_vol2 仮想サーバ cluster2\_src\_svm デスティネーションボリュームを指定します managed\_svc2\_vol3 という名前の仮想サーバ上にある cluster3\_dst\_svm。

- に対する Snapshot コピージョブが失敗しました 0426cluster2\_src\_vol2snap ソースボリューム cluster2\_src\_svm:/cluster2\_src\_vol2。

このシナリオでは、ジョブが失敗した場合の原因と潜在的な対処策を特定できます。ただし、失敗を解決するには、System Manager Web UI または ONTAP CLI コマンドを使用する必要があります。

## 手順

1. エラーメッセージを確認し、ソースボリュームで Snapshot コピージョブが失敗していることから、おそらくソースボリュームに問題があると判断します。

必要に応じて、エラーメッセージの最後にある \* Job Details \* リンクをクリックしてもかまいませんが、このシナリオでは、そのような操作を行わないように選択します。

2. イベントを解決するために、次の作業を行います。
  - a. [\* Assign to \* (\* への割り当て) ] ボタンをクリックし、メニューから [\* Me\* (\* Me \*) ] を選択します
  - b. [\* Acknowledge \* (確認) ] ボタンをクリックして、イベントにアラートが設定されている場合は、繰り返しアラート通知を受信しないようにします。
  - c. 必要に応じて、イベントに関するメモを追加することもできます。
3. [Summary] \* ペインで [Source] \* フィールドをクリックして、ソース・ボリュームの詳細を表示します。

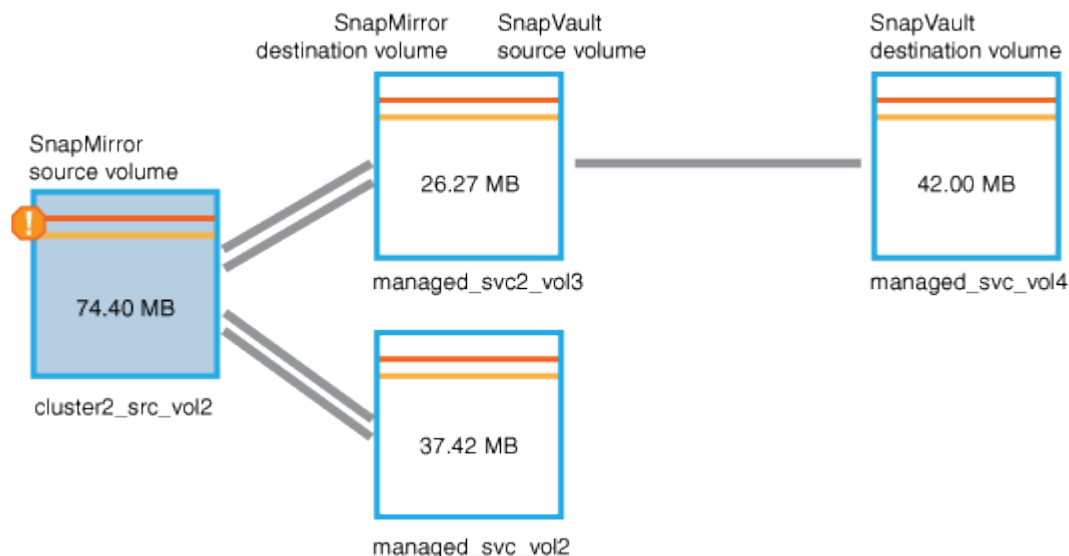
「\* Source \*」フィールドには、ソースオブジェクトの名前が表示されます。この場合は、Snapshot コピージョブがスケジュールされたボリュームが表示されます。

の健全性/ボリュームの詳細ページが表示されます `cluster2\_src\_vol2` をクリックすると、Protection タブの内容が表示されます。



- 保護トポロジのグラフを見ると、トポロジ内の最初のボリューム（ SnapMirror 関係のソースボリューム ）に関連付けられているエラーアイコンが表示されます。

また、ソースボリュームアイコンに水平のバーが表示され、そのボリュームに設定されている警告とエラーのしきい値が表示されます。



- エラーアイコンにカーソルを合わせると、ポップアップダイアログが開いてしきい値の設定が表示され、ボリュームがエラーしきい値を超えて容量の問題を示していることがわかります。
- [ 容量 \* ] タブをクリックします。

ボリュームの容量情報 cluster2\_src\_vol2 を表示します。

- 容量\*ペインの棒グラフに、ボリュームの容量がボリュームに設定されたしきい値のレベルを超えたことを示すエラーアイコンが再び表示されます。
- 容量グラフの下には、ボリュームの自動拡張が無効になっていることと、ボリュームのスペースギャランティが設定されていることが示されています。

自動拡張を有効にすることもできますが、このシナリオの目的上、さらに調査を進めてから、容量の問題を解決する方法を決定することにします。

- 下にスクロールして「 \* Events 」リストを表示し、「 Protection Job Failed 」、「 Volume Days Until Full 」、「 Volume Space Full 」の各イベントが生成されたことを確認します。
- イベントのリストで、「 \* ボリュームスペースがフル \* 」イベントをクリックして詳細を確認します。このイベントは容量問題に最も関連しているように見えます。

イベントの詳細ページには、ソースボリュームで「ボリュームスペースがフル」イベントが表示されます。

- [サマリー\* (Summary \*) ]領域で、イベントの[プロパティ (原因) ]フィールドを確認します。 The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.
- サマリ\*領域の下に推奨される対処方法が表示されます。



Suggested Corrective Actions は一部のイベントについてのみ表示されるため、すべてのタイプのイベントについてこの領域が表示されるわけではありません。

「ボリュームスペースがフル」 イベントを解決するために実施する推奨対処策をクリックしていきます。

- このボリュームで自動拡張を有効にします。
- ボリュームのサイズを変更する。
- このボリュームで重複排除を有効にして実行する。
- このボリュームで圧縮を有効にして実行する。

13. ボリュームの自動拡張を有効にすることにしましたが、これを行うには、親アグリゲート上の使用可能な空きスペースと現在のボリューム増加率を確認する必要があります。

a. 親アグリゲートを確認します。`cluster2\_src\_aggr1`をクリックします。



アグリゲートの名前をクリックすると、アグリゲートに関する詳細を確認できます。

ボリュームに自動拡張を有効にするための十分なスペースがあることを確認します。

b. ページの上部で、重要なインシデントを示すアイコンを確認し、アイコンの下テキストを確認します。

「フルまでの日数： 1 日未満 | 日次増加率： 5.4%」と指定します。

14. System ManagerまたはONTAP CLIにアクセスしてを有効にします volume autogrow オプション



ボリュームとアグリゲートの名前をメモしておいて、自動拡張を有効にするときに参照できるようにします。

15. 容量問題 を解決したら、Unified Managerのイベントの詳細ページに戻って、イベントを解決済みとマークします。

## 遅延の問題を解決する

このワークフローでは、遅延問題を解決する方法の例を示します。このシナリオでは、管理者またはオペレータがUnified Managerの[ダッシュボード/概要]ページにアクセスして、保護関係に問題がないかどうかを確認し、問題がある場合は解決策を探します。

### 作業を開始する前に

OnCommand 管理者またはストレージ管理者のロールが必要です。

### このタスクについて

[ダッシュボード/概要]ページで、[未解決のインシデントとリスク]領域を確認し、[保護のリスク]の下の[保護]ペインでSnapMirrorの遅延エラーを確認します。

## 手順

1. [ダッシュボード/概要]ページの[保護]ペインで、SnapMirror関係の遅延エラーを探してクリックします。

遅延エラーイベントのイベントの詳細ページが表示されます。

2. イベント \* の詳細ページでは、次のタスクを 1 つ以上実行できます。
  - 概要領域の原因フィールドのエラーメッセージを確認して、推奨される対処方法があるかどうかを判断します。
  - ボリュームの詳細を確認するには、サマリー領域のソースフィールドでオブジェクト名（この場合はボリューム）をクリックします。
  - このイベントに関して追加されたメモを探します。
  - イベントにメモを追加します。
  - イベントを特定のユーザに割り当てます。
  - イベントに応答するか、またはイベントを解決します。
3. このシナリオでは、サマリー \* 領域のソースフィールドでオブジェクト名（この場合はボリューム）をクリックすると、ボリュームの詳細が表示されます。

健全性/ボリュームの詳細ページの保護タブが表示されます。

4. [\* 保護 \*] タブでは、トポロジ図を確認します。

3 つのボリュームで構成される SnapMirror カスケードの最後のボリュームで遅延エラーが発生していることがわかりました。選択したボリュームがダークグレーの線で囲われます。ソースボリュームから延びるオレンジ色の二重線は、SnapMirror 関係のエラーを示しています。



5. SnapMirror カスケード内の各ボリュームをクリックします。

各ボリュームを選択すると、サマリ、トポロジ、履歴、イベント、関連デバイス、 および関連するアラート領域が変更され、選択したボリュームに関連する詳細が表示されます。

6. サマリ \* 領域を表示し、各ボリュームの \* スケジュールの更新 \* フィールドの情報アイコンにカーソルを合わせます。

このシナリオでは、SnapMirror ポリシーが DPDefault であり、SnapMirror スケジュールが毎時 5 分に更新されます。関係内のすべてのボリュームが同時に SnapMirror 転送を試行することがわかりました。

7. 遅延問題を解決するには、カスケードされたボリュームのうちの 2 つのスケジュールを変更して、ソース

が転送を完了したあとにデスティネーションが SnapMirror 転送を開始するようにします。

## 著作権に関する情報

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。