保護関係の作成とトラブルシューティング

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-910/data-protection/concept_types_of_snapmirror_protection.html on December 18, 2023. Always check docs.netapp.com for the latest.

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 3
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 5
保護ジョブの失敗を解決する 9
遅延の問題を解決する 13

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）。9.1 ソースから 9.0 デスティネーションへのレプリケーションはサポートされていません。これは、デスティネーションで古いメジャーバージョンが実行されているためです。

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の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 8.3.1 、 8.3 から 9.1 、 9.2 から 9.2.2 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。

SnapMirror ユニファイドレプリケーション（ミラーバックアップ）

SnapMirror ユニファイドレプリケーションを使用すると、同じデスティネーションボリュームでディザスタリカバリとアーカイブを設定できます。SnapMirror と同様に、一元化されたデータ保護機能の初回起動時に、ベースライン転送が実行されます。デフォルトの一元化されたデータ保護ポリシー「 MirrorAllSnapshots 」に基づくベースライン転送では、ソースボリュームの Snapshot コピーが作成され、そのコピーおよびコピーが参照するデータブロックがデスティネーションボリュームに転送されます。SnapVault と同様に、一元化されたデータ保護にはベースラインの古い Snapshot コピーは含まれません。

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 Health ： All Volumes ビューまたは Volume/Health Details ページから監視する場合、 Restore ボタンと Relationship 操作ボタンは使用できません。

SnapMirror Synchronous によるビジネス継続性

ONTAP 9.8 以降では、 SnapMirror のビジネス継続性（ SM-BC ）機能を使用できます。また、この機能を使用して LUN でアプリケーションを保護できるため、アプリケーションのフェイルオーバーを透過的に実行し、災害発生時のビジネス継続性を確保できます。

クラスタおよび Storage Virtual Machine で使用される Consistency Groups （ CG ；整合グループ）の同期 SnapMirror 関係を Unified Manager から検出して監視できます。SM-BC は、 AFF クラスタまたは All SAN Array （ ASA ）クラスタでサポートされます。プライマリクラスタとセカンダリクラスタは、 AFF または ASA のどちらかになります。SM-BC は、 iSCSI LUN または FCP LUN を使用してアプリケーションを保護します。

SM-BC 関係で保護されているボリュームと LUN を表示すると、保護関係の一元化されたビュー、ボリューム

インベントリ内の整合グループ、整合グループ関係の保護トポロジの表示、 1 年以内の整合グループ関係の履歴データの表示が可能になります。レポートをダウンロードすることもできます。また、整合グループ関係の概要の表示、整合グループ関係のサポートの検索、整合グループで保護されているボリュームに関する情報の取得も可能です。

[関係] ページでは ' ソースストレージオブジェクトとデスティネーションストレージオブジェクト ' およびコンシステンシグループによって保護されているそれらの関係の保護をソート ' フィルタ ' および拡張することもできます

SnapMirror Synchronous のビジネス継続性の詳細については、を参照してください "SM-BC に関する ONTAP 9 のマニュアル"。

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。

- 必要なもの *
- アプリケーション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。

- 必要なもの *

- Workflow Automation のバージョン 5.1 以降がインストールされている必要があります。

> WFA 5.1 には「 WFA pack for managing Clustered Data ONTAP 」が含まれています。したがって、以前のようにこのパックを NetAppStorage Automation Store からダウンロードして、 WFA サーバに個別にインストールする必要はありません。 "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。
- アプリケーション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. 左側のナビゲーションペインで、 * 一般 * > * Workflow Automation * をクリックします。
2. Workflow Automation ページ * の * データベースユーザ * 領域で、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. ページの * Workflow Automation Credentials * 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。

   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。
   - 関連情報 *

"ネットアップのマニュアル： OnCommand Workflow Automation （現在のリリース）"

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。

- 必要なもの *

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。

OnCommand Workflow Automation を再インストールまたはアップグレードするとどうなりますか

OnCommand Workflow Automation を再インストールまたはアップグレードする前に、 OnCommand Workflow Automation と Unified Manager の間の接続を削除し、実行中のすべての OnCommand Workflow Automation またはスケジュールされたジョブが停止されていることを確認する必要があります。

また、 OnCommand Workflow Automation から Unified Manager を手動で削除する必要があります。

OnCommand Workflow Automation を再インストールまたはアップグレードしたら、 Unified Manager との接続を再度セットアップする必要があります。

OnCommand Workflow Automation セットアップを **Unified Manager** から削除しています

Workflow Automation が不要となった場合は、 Unified Manager から OnCommand Workflow Automation のセットアップを削除できます。

- 必要なもの *

アプリケーション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. 左側のナビゲーションペインで、左の [セットアップ] メニューの [一般 **>** Workflow Automation *] をクリックします。
2. [* Workflow Automation*] ページで、 [セットアップの削除] をクリックします。

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。

- 必要なもの *

- アプリケーション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

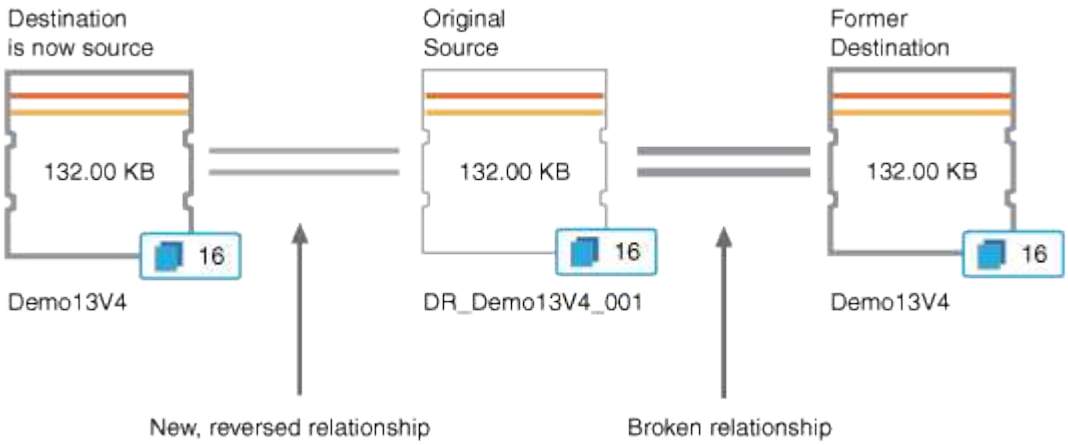
1. "SnapMirror 関係を解除"。

   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。

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

保護関係をボリューム / 健全性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。

- 必要なもの *
- アプリケーション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. ボリューム / 健全性 * 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。

ボリューム / 健全性の詳細ページで保護関係を反転しています

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。

- 必要なもの *
- アプリケーション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. ボリューム / 健常性 * の詳細ページの * 保護 * タブで、トポロジからソースとデスティネーションを反転する SnapMirror 関係を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、ボリューム / 健全性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. * オプション： * Volume/Health * details ページで * View Jobs * をクリックして、各逆再同期ジョブのステータスを追跡します。

   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. * オプション：ブラウザの * 戻る * 矢印をクリックして、 * 音量 / ヘルス * 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。

ボリューム / 健全性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。

- 必要なもの *
- アプリケーション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. ボリューム / 健全性 * 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。

   関係がボリューム / 健全性の詳細ページから削除されます。

ボリューム / 健全性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

があります。

- 必要なもの *
- アプリケーション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. ボリューム / 健全性 * の詳細ページの * 保護 * 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、ボリューム / 健全性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. * オプション： * Volume/Health details * ページで * View Jobs * をクリックして、各再同期ジョブのステータスを追跡します。

   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. * オプション：ブラウザの * 戻る * 矢印をクリックして、 * 音量 / ヘルス * 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。

- 必要なもの *

このワークフローの一部のタスクは管理者ロールでログインする必要があるため、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。

このシナリオでは、ダッシュボード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. [未解決のインシデントとリスクのダッシュボード] 領域の [保護インシデント] パネルで、 [保護ジョブの失敗 *] 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は 'object_name:/ object_name -Error Name' の形式で書き込まれますたとえば 'cluster2_src_SVM:/cluster2_src_vol2 -Protection Job Failed' のようになります

   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。次に、ボリューム / 健全性の詳細ページに移動して詳細情報を収集します。

- 必要なもの *

アプリケーション管理者のロールが必要です。

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。

このジョブには、仮想サーバ cluster3_src_svm のソースボリューム cluster2_src_vol2 とデスティネーションボリューム 'managed_svc2_vol3' と、 cluster3_dst_svm という名前の仮想サーバのデスティネーションボリューム 'cluster2_src_vol3' との間の保護関係が含まれていました。

- ソース・ボリューム 'cluster2_src_SVM:/cluster2_src_vol2’で '0426cluster2_src_vol2snap' の Snapshot コピー・ジョブが失敗しました

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。

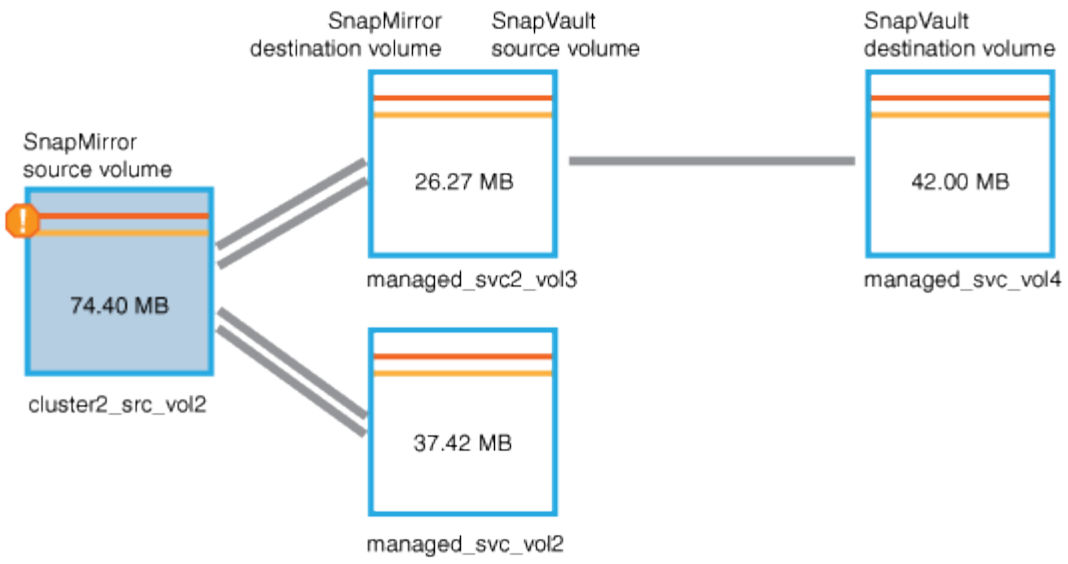
3. [Summary] * ペインで [Source] * フィールドをクリックして、ソース・ボリュームの詳細を表示します。

   「 * 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。

   Volume/Health の詳細ページには 'cluster2_src_vol2 の [Protection] タブの内容が表示されます

4. 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示されます。



5. 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。
6. [容量 *] タブをクリックします。

   ボリューム 'cluster2_src_vol2 に関する容量情報が表示されます

7. 容量 * パネルの棒グラフに、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。
8. 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。

9. 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。
10. 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。

11. **[Summary]** 領域で、イベントの原因フィールドを読みます。「 90% に設定されたフルしきい値に違反しています。47.50 MB の 45.38 MB （ 95.54% ）が使用されます
12. 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. 親アグリゲートである「 cluster2_src_aggr1 」を「 Related Devices 」ペインで確認します。

    > 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、アイコンの下の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 にアクセスするか、 ONTAP CLI にアクセスして「 volume autogrow 」オプションを有効にします。

    > 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 * 詳細ページに戻り、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。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ダッシュボードページで、未解決のインシデントとリスク領域を確認し、保護ペインの保護リスクの下に SnapMirror 遅延エラーが表示されます。

手順

1. ダッシュボード * 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。

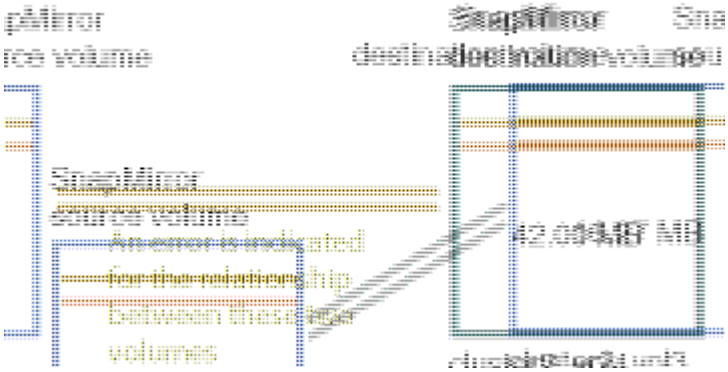
- このイベントに関して追加されたメモを探します。
- イベントにメモを追加します。
- イベントを特定のユーザに割り当てます。
- イベントに応答するか、またはイベントを解決します。

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。

   ボリューム / 健全性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まれます。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権を有し、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権については、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。