Créer et dépanner les relations de protection

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/data-protection/concept_types_of_snapmirror_protection.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Créer et dépanner les relations de protection . . . 1
Types de protection SnapMirror dans Active IQ Unified Manager . . . 1
Traditionnelles SnapMirror relations de protection asynchrones . . . 1
SnapMirror Protection asynchrone avec réplication flexible selon la version . . . 1
SnapMirror protection asynchrone avec option de réplication flexible selon les versions et de sauvegarde . . . 1
SnapMirror Réplication unifiée (miroir et archivage) . . . 2
SnapMirror Protection synchrone avec synchronisation stricte . . . 2
SnapMirror protection synchrone avec synchronisation régulière . . . 2
SnapMirror active sync . . . 2
Configurez les relations de protection dans Unified Manager . . . 3
Configurez les relations de protection dans Active IQ Unified Manager . . . 3
Configurez une connexion entre Workflow Automation et Active IQ Unified Manager . . . 3
Vérifiez la mise en cache de la source de données Active IQ Unified Manager dans Workflow Automation . . . 4
Comment la réinstallation ou la mise à niveau de OnCommand Workflow Automation affecte Active IQ Unified Manager . . . 5
Supprimez la configuration OnCommand Workflow Automation d'Active IQ Unified Manager . . . 5
Effectuer un basculement et un rétablissement de la relation de protection . . . 5
Effectuez un basculement et un retour en arrière d'une relation de protection dans Active IQ Unified Manager . . . 5
Interrompre une relation de protection SnapMirror depuis la page Volume/Santé d'Active IQ Unified Manager . . . 7
Inverser les relations de protection à partir de la page Détails du volume/de la santé dans Active IQ Unified Manager . . . 7
Supprimez une relation de protection depuis la page Détails du volume/de l'état dans Active IQ Unified Manager . . . 8
Resynchronisez les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager . . . 9
Résoudre l'échec d'une tâche de protection . . . 10
Résoudre un échec de tâche de protection dans Active IQ Unified Manager . . . 10
Identifiez le problème et effectuez les actions correctives pour un travail de protection ayant échoué dans Active IQ Unified Manager . . . 10
Résoudre les problèmes de latence dans Active IQ Unified Manager . . . 13

Créer et dépanner les relations de protection

Types de protection SnapMirror dans Active IQ Unified Manager

Selon le déploiement de votre topologie de stockage des données, Unified Manager vous permet de configurer plusieurs types de relations de protection SnapMirror. Toutes les variantes de protection SnapMirror offrent une protection de reprise après sinistre avec basculement, mais proposent des capacités différentes en matière de performances, de flexibilité des versions et de protection par copie de sauvegarde multiple.

Traditionnelles SnapMirror relations de protection asynchrones

La protection asynchrone traditionnelle SnapMirror assure une protection miroir par réplication de blocs entre les volumes source et de destination.

Dans les relations SnapMirror traditionnelles, les opérations de mise en miroir s'exécutent plus rapidement que dans d'autres relations SnapMirror, car l'opération de mise en miroir repose sur la réplication par blocs. Cependant, la protection SnapMirror traditionnelle exige que le volume de destination exécute la même version mineure ou une version mineure ultérieure du logiciel ONTAP que le volume source, au sein de la même version majeure (par exemple, version 8.x vers 8.x ou version 9.x vers 9.x). La réplication d'une source 9.1 vers une destination 9.0 n'est pas prise en charge, car la destination exécute une version majeure antérieure.

SnapMirror Protection asynchrone avec réplication flexible selon la version

SnapMirror La protection asynchrone avec réplication flexible par version fournit une protection miroir de réplication logique entre les volumes source et de destination, même si ces volumes exécutent différentes versions du logiciel ONTAP 8.3 ou version ultérieure (par exemple, de la version 8.3 à 8.3.1, ou de 8.3 à 9.1, ou de 9.2.2 à 9.2).

Dans les relations SnapMirror avec réplication flexible en termes de version, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

En raison de son exécution plus lente, SnapMirror avec protection de réplication flexible par version ne convient pas à une mise en œuvre dans l'une ou l'autre des circonstances suivantes :

- L'objet source contient plus de 10 millions de fichiers à protéger.
- L'objectif de point de récupération pour les données protégées est de deux heures ou moins. (Autrement dit, la destination doit toujours contenir des données répliquées et récupérables qui ne sont pas plus anciennes de deux heures que les données de la source.)

Dans l'un ou l'autre des cas énumérés, l'exécution plus rapide de la protection SnapMirror par défaut, basée sur la réplication de blocs, est requise.

SnapMirror protection asynchrone avec option de réplication flexible selon les versions et de sauvegarde

SnapMirror La protection asynchrone avec réplication flexible des versions et option de sauvegarde assure une protection miroir entre les volumes source et de destination et la possibilité de stocker plusieurs copies

des données mises en miroir à destination.

L'administrateur du stockage peut spécifier quelles copies Snapshot sont répliquées de la source vers la destination et peut également spécifier combien de temps conserver ces copies à la destination, même si elles sont supprimées à la source.

Dans les relations SnapMirror avec une option de réplication flexible en termes de version et de sauvegarde, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

SnapMirror Réplication unifiée (miroir et archivage)

SnapMirror unified replication vous permet de configurer la reprise après sinistre et l'archivage sur le même volume de destination. Comme avec SnapMirror, la protection unifiée des données effectue un transfert de base la première fois que vous l'utilisez. Un transfert de base dans le cadre de la stratégie de protection unifiée des données par défaut "MirrorAndVault" crée une copie Snapshot du volume source, puis transfère cette copie et les blocs de données auxquels elle fait référence vers le volume de destination. Comme SnapVault, la protection unifiée des données n'inclut pas les anciennes copies Snapshot dans le transfert de base.

SnapMirror Protection synchrone avec synchronisation stricte

SnapMirror La protection synchrone avec la synchronisation « `strict` » garantit que les volumes primaire et secondaire sont toujours une copie conforme l'un de l'autre. En cas d'échec de réplication lors d'une tentative d'écriture de données sur le volume secondaire, les E/S client vers le volume primaire sont interrompues.

SnapMirror protection synchrone avec synchronisation régulière

SnapMirror La protection synchrone avec la synchronisation "regular" n'exige pas que les volumes primaire et secondaire soient toujours des copies conformes l'un de l'autre, garantissant ainsi la disponibilité du volume primaire. En cas d'échec de réplication lors d'une tentative d'écriture de données sur le volume secondaire, les volumes primaire et secondaire se désynchronisent et les E/S client continuent sur le volume primaire.



Le bouton Restaurer et les boutons d'opération de relation ne sont pas disponibles lors de la surveillance des relations de protection synchrones à partir de la vue Santé : tous les volumes ou de la page de détails Volume / Santé.

SnapMirror active sync

La fonction de synchronisation active SnapMirror est disponible avec ONTAP 9.8 et les versions ultérieures, et vous pouvez l'utiliser pour protéger les applications avec des LUN, ce qui permet aux applications de basculer de manière transparente et assure la continuité des activités en cas de sinistre.

Il vous permet de découvrir et de surveiller les relations synchrones SnapMirror pour les groupes de cohérence (CG) disponibles sur les clusters et les machines virtuelles de stockage depuis Unified Manager. SnapMirror active sync est pris en charge sur les clusters AFF ou les clusters All SAN Array (ASA), où les clusters principal et secondaire peuvent être AFF ou ASA. SnapMirror active sync protège les applications avec des LUN iSCSI ou FCP.

Lorsque vous consultez les volumes et les LUN protégés par la relation de synchronisation active SnapMirror, vous obtenez une vue unifiée des relations de protection, des groupes de cohérence dans l'inventaire des volumes, de la topologie de protection des relations de groupes de cohérence, ainsi que des données historiques de ces relations sur une période pouvant aller jusqu'à un an. Vous pouvez également télécharger

le rapport. Vous pouvez également consulter le résumé des relations de groupes de cohérence, rechercher la prise en charge de ces relations et obtenir des informations sur les volumes protégés par le groupe de cohérence.

Sur la page Relations, vous pouvez également trier, filtrer et étendre la protection des objets de stockage source et de destination ainsi que de la relation qui les unit, protégés par le groupe de cohérence.

Pour en savoir plus sur SnapMirror active sync, consultez "Documentation ONTAP 9 pour Snapmirror active sync (anciennement SM-BC)".

Configurez les relations de protection dans Unified Manager

Configurez les relations de protection dans Active IQ Unified Manager

Vous devez effectuer plusieurs étapes pour utiliser Unified Manager et OnCommand Workflow Automation afin de configurer des relations SnapMirror et SnapVault pour protéger vos données.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir établi des relations d'égal à égal entre deux clusters ou deux machines virtuelles de stockage (SVM).
- OnCommand Workflow Automation doit être intégré à Unified Manager :
  - "Configurer OnCommand Workflow Automation".
  - "Vérification de la mise en cache de la source de données Unified Manager dans Workflow Automation".

Étapes

1. Selon le type de relation de protection que vous souhaitez créer, procédez comme suit :
   - "Créer une relation de protection SnapMirror".
   - "Créer une relation de protection SnapVault".
2. Si vous souhaitez créer une politique pour la relation, en fonction du type de relation que vous créez, procédez comme suit :
   - "Créer une stratégie SnapVault".
   - "Créer une stratégie SnapMirror".
3. "Créez une planification SnapMirror ou SnapVault".

Configurez une connexion entre Workflow Automation et Active IQ Unified Manager

Vous pouvez configurer une connexion sécurisée entre OnCommand Workflow Automation (WFA) et Unified Manager. La connexion à Workflow Automation vous permet d'utiliser des fonctionnalités de protection telles que les workflows de configuration SnapMirror et SnapVault, ainsi que des commandes pour gérer les relations SnapMirror.

Avant de commencer

- La version installée de Workflow Automation doit être la version 5.1.1P6 ou une version ultérieure.

> Le « pack WFA pour la gestion de Clustered Data ONTAP » est inclus dans WFA 5.1.1P6, il n'est donc plus nécessaire de télécharger ce pack depuis le NetAppStorage Automation Store et de l'installer séparément sur votre serveur WFA comme c'était le cas auparavant. "Téléchargement WFA"

- Vous devez disposer du nom de l'utilisateur de la base de données que vous avez créé dans Unified Manager pour prendre en charge les connexions WFA et Unified Manager.

  Cet utilisateur de base de données doit s'être vu attribuer le rôle d'utilisateur « Integration Schema ».

- Le rôle d'administrateur ou d'architecte doit vous être attribué dans Workflow Automation.
- Vous devez disposer de l'adresse de l'hôte, du numéro de port 443, du nom d'utilisateur et du mot de passe pour la configuration de Workflow Automation.
- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **General** > **Workflow Automation**.
2. Dans la zone **Utilisateur de la base de données** de la **page Workflow Automation**, sélectionnez le nom et saisissez le mot de passe de l'utilisateur de la base de données que vous avez créé pour prendre en charge les connexions à Unified Manager et à Workflow Automation.
3. Dans la zone **Workflow Automation Credentials** de la page, saisissez le nom de l'hôte ou l'adresse IP (IPv4 ou IPv6), ainsi que le nom d'utilisateur et le mot de passe de la configuration Workflow Automation.

   Vous devez utiliser le port du serveur Unified Manager (port 443).

4. Cliquez sur **Enregistrer**.
5. Si vous utilisez un certificat auto-signé, cliquez sur **Oui** pour autoriser le certificat de sécurité.

   La page Workflow Automation s'affiche.

6. Cliquez sur **Oui** pour recharger la web UI et ajouter les fonctionnalités de Workflow Automation.

Informations connexes

"NetApp Documentation : OnCommand Workflow Automation (versions actuelles)"

Vérifiez la mise en cache de la source de données Active IQ Unified Manager dans Workflow Automation

Vous pouvez déterminer si la mise en cache des sources de données de Unified Manager fonctionne correctement en vérifiant si l'acquisition de la source de données réussit dans Workflow Automation. Vous pouvez effectuer cette vérification lorsque vous intégrez Workflow Automation à Unified Manager afin de vous assurer que les fonctionnalités de Workflow Automation sont disponibles après l'intégration.

Avant de commencer

Vous devez disposer du rôle Administrator ou du rôle Architect dans Workflow Automation pour effectuer cette tâche.

Étapes

1. Dans l'interface utilisateur de Workflow Automation, sélectionnez **Execution** > **Data Sources**.
2. Cliquez avec le bouton droit sur le nom de la source de données Unified Manager, puis sélectionnez **Acquire Now**.
3. Vérifiez que l'acquisition se déroule sans erreurs.

   Les erreurs d'acquisition doivent être résolues pour que l'intégration de Workflow Automation avec Unified Manager réussisse.

Comment la réinstallation ou la mise à niveau de OnCommand Workflow Automation affecte Active IQ Unified Manager

Avant de réinstaller ou de mettre à niveau OnCommand Workflow Automation, vous devez d'abord supprimer la connexion entre OnCommand Workflow Automation et Unified Manager, et vous assurer que toutes les tâches OnCommand Workflow Automation en cours d'exécution ou planifiées sont arrêtées.

Vous devez également supprimer manuellement Unified Manager de OnCommand Workflow Automation.

Après avoir réinstallé ou mis à niveau OnCommand Workflow Automation, vous devez configurer de nouveau la connexion avec Unified Manager.

Supprimez la configuration OnCommand Workflow Automation d'Active IQ Unified Manager

Vous pouvez supprimer la configuration de OnCommand Workflow Automation de Unified Manager lorsque vous ne souhaitez plus utiliser Workflow Automation.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **General** > **Workflow Automation** dans le menu Setup de gauche.
2. Sur la page **Workflow Automation**, cliquez sur **Remove Setup**.

Effectuer un basculement et un rétablissement de la relation de protection

Effectuez un basculement et un retour en arrière d'une relation de protection dans Active IQ Unified Manager

Lorsqu'un volume source de votre relation de protection est désactivé en raison d'une défaillance matérielle ou d'une catastrophe, vous pouvez utiliser les fonctionnalités de relation de protection d'Unified Manager pour rendre la destination de protection accessible en lecture/écriture et basculer vers ce volume jusqu'à ce que la source soit de nouveau en ligne ; vous pouvez ensuite revenir à la source d'origine lorsqu'elle est

disponible pour fournir des données.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré OnCommand Workflow Automation pour effectuer cette opération.

Étapes

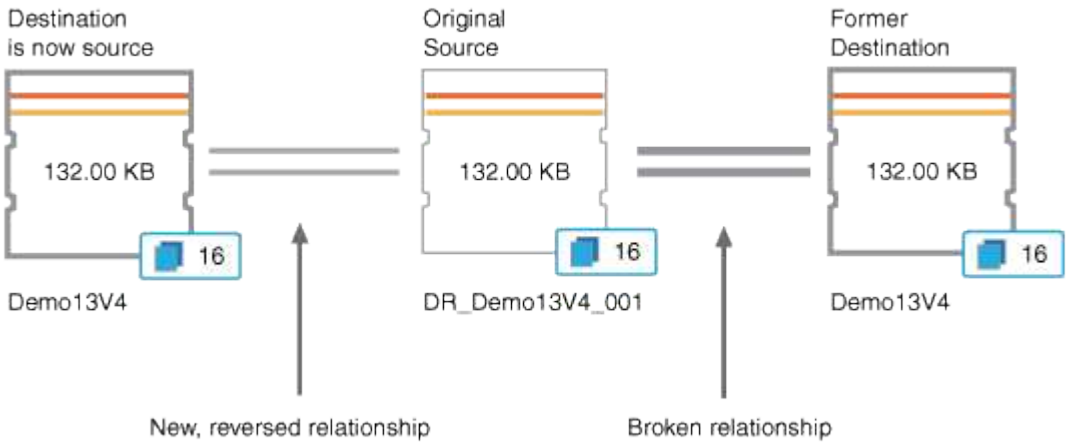
1. "Rompre la SnapMirror relation".

   Vous devez rompre la relation avant de pouvoir convertir le volume de destination d'un volume de protection des données en un volume de lecture/écriture, et avant de pouvoir inverser la relation.

2. "Inverser la relation de protection".

   Lorsque le volume source d'origine est de nouveau disponible, vous pouvez rétablir la relation de protection initiale en restaurant le volume source. Avant de pouvoir restaurer la source, vous devez la synchroniser avec les données écrites sur l'ancienne destination. Vous utilisez l'opération de resynchronisation inverse pour créer une nouvelle relation de protection en inversant les rôles de la relation initiale et en synchronisant le volume source avec l'ancienne destination. Une nouvelle copie Snapshot de référence est créée pour la nouvelle relation.

   La relation inversée ressemble à une relation en cascade :



3. "Rompre la relation SnapMirror inversée".

   Lorsque le volume source d'origine est resynchronisé et peut à nouveau fournir des données, utilisez l'opération de rupture pour rompre la relation inversée.

4. "Supprimer la relation".

   Lorsque la relation inversée n'est plus nécessaire, vous devez la supprimer avant de rétablir la relation d'origine.

5. "Resynchroniser la relation".

   Utilisez l'opération de resynchronisation pour synchroniser les données de la source vers la destination et rétablir la relation d'origine.

Interrompre une relation de protection SnapMirror depuis la page Volume/Santé d'Active IQ Unified Manager

Vous pouvez rompre une relation de protection depuis la page Détails du volume / de l'état et arrêter les transferts de données entre un volume source et un volume de destination dans une relation SnapMirror. Vous pouvez rompre une relation lorsque vous souhaitez migrer des données, pour la reprise après sinistre ou pour tester des applications. Le volume de destination devient un volume en lecture-écriture. Vous ne pouvez pas rompre une relation SnapVault.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez rompre.
2. Faites un clic droit sur la destination et sélectionnez **Interrompre** dans le menu.

   La boîte de dialogue « Rompre la relation » s'affiche.

3. Cliquez sur **Continuer** pour rompre la relation.
4. Dans la topologie, vérifiez que la relation est rompue.

Inverser les relations de protection à partir de la page Détails du volume/de la santé dans Active IQ Unified Manager

Lorsqu'un sinistre rend inutilisable le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour fournir les données en le convertissant en lecture/écriture pendant que vous réparez ou remplacez la source. Lorsque la source est de nouveau disponible pour recevoir des données, vous pouvez utiliser l'opération de resynchronisation inverse pour rétablir la relation dans le sens inverse, en synchronisant les données de la source avec celles du volume de destination en lecture/écriture.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- La relation ne doit pas être une relation SnapVault.
- Une relation de protection doit déjà exister.
- Il faut rompre la relation de protection.
- La source et la destination doivent toutes deux être en ligne.
- La source ne doit pas être la destination d'un autre volume de protection des données.
- Lorsque vous effectuez cette tâche, les données de la source plus récentes que celles de la copie Snapshot commune sont supprimées.
- Les politiques et les planifications créées sur la relation de resynchronisation inverse sont les mêmes que celles de la relation de protection d'origine.

Si les politiques et les planifications n'existent pas, elles sont créées.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, repérez dans la topologie la relation SnapMirror dont vous souhaitez inverser la source et la destination, puis cliquez dessus avec le bouton droit.
2. Sélectionnez **Resynchronisation inversée** dans le menu.

   La boîte de dialogue de resynchronisation inverse s'affiche.

3. Vérifiez que la relation affichée dans la boîte de dialogue **Resynchronisation inverse** est bien celle pour laquelle vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Soumettre**.

   La boîte de dialogue Reverse Resync se ferme et un lien vers une tâche s'affiche en haut de la page de détails Volume / Health.

4. **Facultatif :** Cliquez sur **Afficher les tâches** dans la page de détails **Volume / Health** pour suivre l'état de chaque tâche de resynchronisation inverse.

   Une liste filtrée des tâches s'affiche.

5. **Facultatif :** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

   L'opération de resynchronisation inverse est terminée lorsque toutes les tâches du travail ont été exécutées avec succès.

Supprimez une relation de protection depuis la page Détails du volume/de l'état dans Active IQ Unified Manager

Vous pouvez supprimer une relation de protection pour supprimer définitivement une relation existante entre la source et la destination sélectionnées : par exemple, lorsque vous souhaitez créer une relation avec une destination différente. Cette opération supprime toutes les métadonnées et est irréversible.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez supprimer.
2. Faites un clic droit sur le nom de la destination et sélectionnez **Supprimer** dans le menu.

   La boîte de dialogue Supprimer la relation s'affiche.

3. Cliquez sur **Continuer** pour supprimer la relation.

   La relation est supprimée de la page des détails Volume / Santé.

Resynchronisez les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager

Vous pouvez resynchroniser les données d'une relation SnapMirror ou SnapVault qui a été interrompue, puis rendre la destination accessible en lecture/écriture afin que les données de la source correspondent à celles de la destination. Vous pouvez également effectuer une resynchronisation lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, entraînant l'échec des mises à jour SnapMirror ou SnapVault.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, repérez dans la topologie la relation de protection que vous souhaitez resynchroniser et cliquez dessus avec le bouton droit.
2. Sélectionnez **Resynchronize** dans le menu.

   Vous pouvez également, dans le menu **Actions**, sélectionner **Relation** > **Resynchroniser** pour resynchroniser la relation dont vous consultez actuellement les détails.

   La boîte de dialogue Resynchroniser s'affiche.
3. Dans l'onglet **Options de resynchronisation**, sélectionnez une priorité de transfert et le débit de transfert maximal.
4. Cliquez sur **Copies d'instantané source**; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

   La boîte de dialogue « Sélectionner la copie d'instantané source » s'affiche.
5. Si vous souhaitez spécifier une copie Snapshot existante plutôt que de transférer la copie Snapshot par défaut, cliquez sur **Copie Snapshot existante** et sélectionnez une copie Snapshot dans la liste.
6. Cliquez sur **Submit**.

   Vous revenez à la boîte de dialogue Resynchronize.
7. Si vous avez sélectionné plusieurs sources à resynchroniser, cliquez sur **Default** pour la source suivante pour laquelle vous souhaitez spécifier une copie Snapshot existante.
8. Cliquez sur **Submit** pour lancer la tâche de resynchronisation.

   La tâche de resynchronisation démarre, vous revenez à la page Détails du volume / de l'état et un lien vers les tâches s'affiche en haut de la page.
9. **Facultatif:** Cliquez sur **Afficher les tâches** dans la page **Détails du volume / de l'état** pour suivre l'état de chaque tâche de resynchronisation.

   Une liste filtrée des tâches s'affiche.
10. **Facultatif :** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

Le travail de resynchronisation est terminé lorsque toutes les tâches du travail se terminent avec succès.

Résoudre l'échec d'une tâche de protection

Résoudre un échec de tâche de protection dans Active IQ Unified Manager

Ce flux de travail illustre comment identifier et résoudre un échec de tâche de protection à partir du tableau de bord Unified Manager.

Avant de commencer

Étant donné que certaines tâches de ce flux de travail nécessitent que vous vous connectiez avec le rôle Administrator, vous devez vous familiariser avec les rôles requis pour utiliser les différentes fonctionnalités.

Dans ce scénario, vous accédez à la page Dashboard pour vérifier si vos tâches de protection présentent des problèmes. Dans la zone Incident de protection, vous remarquez qu'il existe un incident Job Terminated, indiquant une erreur Protection Job Failed sur un volume. Vous examinez cette erreur afin d'en déterminer la cause possible et la solution potentielle.

Étapes

1. Dans le panneau Protection Incidents de la zone Dashboard Unresolved Incidents and Risks, cliquez sur l'événement **Protection job failed**.

   Le texte lié à l'événement est écrit sous la forme `object_name:/object_name - Error Name`, par exemple `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   La page de détails de l'événement relatif à la tâche de protection ayant échoué s'affiche.

2. Consultez le message d'erreur dans le champ Cause de la zone **Summary** pour déterminer le problème et évaluer les actions correctives potentielles.

   Voir "Identifier le problème et effectuer des actions correctives pour une tâche de protection ayant échoué".

Identifiez le problème et effectuez les actions correctives pour un travail de protection ayant échoué dans Active IQ Unified Manager

Vous examinez le message d'erreur d'échec de la tâche dans le champ Cause de la page Event details et déterminez que la tâche a échoué en raison d'une erreur de copie Snapshot. Vous accédez ensuite à la page Volume / Health details pour recueillir davantage d'informations.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Le message d'erreur indiqué dans le champ Cause de la page Détails de l'événement contient le texte suivant concernant la tâche ayant échoué :

```
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
```

Ce message fournit les informations suivantes :

- La tâche de sauvegarde ou de mise en miroir n'a pas abouti.

  Le travail impliquait une relation de protection entre le volume source `cluster2_src_vol2` sur le serveur virtuel `cluster2_src_svm` et le volume de destination `managed_svc2_vol3` sur le serveur virtuel nommé `cluster3_dst_svm`.

- Une tâche de copie Snapshot a échoué pour `0426cluster2_src_vol2snap` sur le volume source `cluster2_src_svm:/cluster2_src_vol2`.

Dans ce cas, vous pouvez identifier la cause de l'échec de la tâche et les actions correctives potentielles. Cependant, la résolution de cet échec nécessite d'accéder à l'interface web de System Manager ou aux commandes de l'interface de ligne de commande ONTAP.

Étapes

1. Vous examinez le message d'erreur et déterminez qu'une tâche de copie Snapshot a échoué sur le volume source, ce qui indique qu'il y a probablement un problème avec votre volume source.

   Si vous le souhaitez, vous pouvez cliquer sur le lien **Job Details** à la fin du message d'erreur, mais pour les besoins de ce scénario, vous choisissez de ne pas le faire.

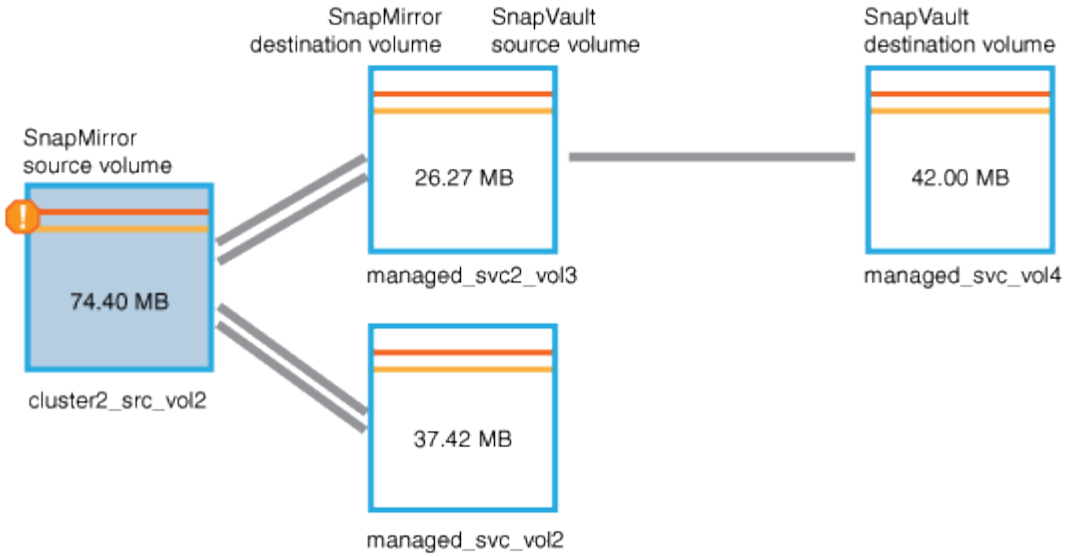
2. Vous décidez d'essayer de résoudre l'événement, vous procédez donc comme suit :
   a. Cliquez sur le bouton **Assign To** et sélectionnez **Me** dans le menu.
   b. Cliquez sur le bouton **Acknowledge** pour ne plus recevoir de notifications d'alerte répétées, si des alertes ont été configurées pour cet événement.
   c. Vous pouvez également ajouter des notes sur l'événement si vous le souhaitez.
3. Cliquez sur le champ **Source** dans le volet **Résumé** pour afficher les détails concernant le volume source.

   Le champ **Source** contient le nom de l'objet source : dans ce cas, le volume sur lequel la tâche de copie Snapshot a été planifiée.

   La page des détails Volume / Santé s'affiche pour `cluster2_src_vol2`, affichant le contenu de l'onglet Protection.

4. En consultant le graphique de topologie de protection, vous voyez une icône d'erreur associée au premier volume de la topologie, qui est le volume source de la relation SnapMirror.

   Vous pouvez également observer les barres horizontales dans l'icône du volume source, indiquant les seuils d'avertissement et d'erreur définis pour ce volume.



5. Vous placez votre curseur sur l'icône d'erreur pour afficher la boîte de dialogue contextuelle indiquant les paramètres de seuil et constater que le volume a dépassé le seuil d'erreur, ce qui indique un problème de capacité.
6. Cliquez sur l'onglet **Capacité**.

   Informations sur la capacité des affichages `cluster2_src_vol2` de volume.

7. Dans le panneau **Capacité**, vous pouvez constater la présence d'une icône d'erreur dans le graphique à barres, indiquant à nouveau que la capacité du volume a dépassé le seuil défini pour ce volume.
8. Sous le graphique de capacité, vous constatez que la croissance automatique du volume a été désactivée et qu'une garantie d'espace du volume a été définie.

   Vous pourriez décider d'activer l'extension automatique, mais dans le cadre de ce scénario, vous décidez d'approfondir la question avant de prendre une décision sur la manière de résoudre le problème de capacité.

9. Vous faites défiler l'écran jusqu'à la liste **Événements** et vous voyez que les événements « Protection Job Failed », « Volume Days Until Full » et « Volume Space Full » ont été générés.
10. Dans la liste **Événements**, vous cliquez sur l'événement **Volume Space Full** pour obtenir plus d'informations, après avoir déterminé que cet événement semble le plus pertinent pour votre problème de capacité.

    La page de détails de l'événement affiche l'événement Volume Space Full pour le volume source.

11. Dans la zone **Résumé**, vous lisez le champ Cause de l'événement : `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Sous la zone Résumé, vous voyez les actions correctives suggérées.

    Les actions correctives suggérées ne s'affichent que pour certains événements, vous ne verrez donc pas cette zone pour tous les types d'événements.

    Vous parcourez la liste des actions suggérées que vous pouvez effectuer pour résoudre l'événement « Volume Space Full » :

    - Activer l'extension automatique sur ce volume.

- Redimensionnez le volume.
- Activez et exécutez la déduplication sur ce volume.
- Activez et exécutez la compression sur ce volume.

13. Vous décidez d'activer la croissance automatique du volume, mais pour ce faire, vous devez déterminer l'espace libre disponible sur l'agrégat parent et le taux de croissance actuel du volume :
    a. Consultez l'agrégat parent, `cluster2_src_aggr1`, dans le volet **Appareils associés**.

       Vous pouvez cliquer sur le nom de l'agrégat pour obtenir plus de détails à son sujet.

       Vous déterminez que l'agrégat dispose d'un espace suffisant pour permettre l'augmentation automatique du volume.

    b. En haut de la page, repérez l'icône indiquant un incident critique et consultez le texte situé en dessous.

       Vous déterminez que "Jours avant remplissage complet : moins d'un jour | Taux de croissance quotidien : 5,4 %".

14. Accédez à System Manager ou à l'interface de ligne de commande ONTAP pour activer l' `volume autogrow`option.

    Notez les noms du volume et de l'agrégat afin de les avoir à disposition lors de l'activation d'autogrow.

15. Une fois le problème de capacité résolu, retournez à la page de détails **Event** dans Unified Manager et marquez l'événement comme résolu.

Résoudre les problèmes de latence dans Active IQ Unified Manager

Ce flux de travail fournit un exemple de la façon dont vous pouvez résoudre un problème de retard. Dans ce scénario, vous êtes un administrateur ou un opérateur qui accède à la page Unified ManagerDashboard pour vérifier s'il existe des problèmes dans vos relations de protection et, le cas échéant, trouver des solutions.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Sur la page Tableau de bord, vous consultez la zone Incidents et risques non résolus et vous constatez une erreur de décalage SnapMirror dans le volet Protection, sous Risques de protection.

Étapes

1. Dans le volet **Protection** de la page **Tableau de bord**, repérez l'erreur de décalage de la relation SnapMirror et cliquez dessus.

   La page de détails de l'événement correspondant à l'événement d'erreur de décalage s'affiche.

2. Depuis la page de détails de l'**événement**, vous pouvez effectuer une ou plusieurs des tâches suivantes:
   - Consultez le message d'erreur dans le champ Cause de la zone Summary pour déterminer s'il existe une action corrective suggérée.

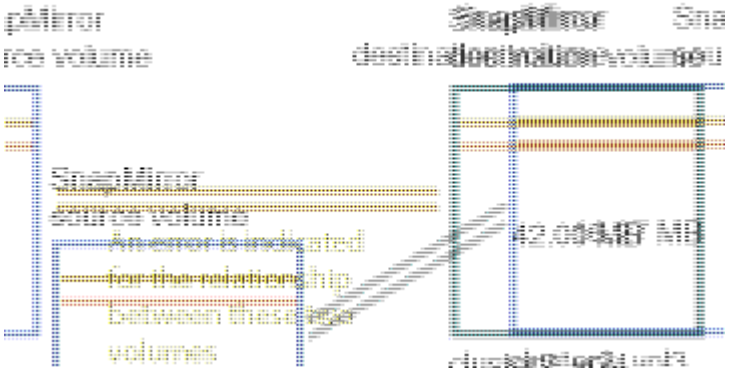
- Cliquez sur le nom de l'objet, dans ce cas un volume, dans le champ Source de la zone Summary pour obtenir des détails sur le volume.
- Recherchez les notes qui auraient pu être ajoutées concernant cet événement.
- Ajouter une note à l'événement.
- Attribuer l'événement à un utilisateur spécifique.
- Accusez réception de l'événement ou résolvez-le.

3. Dans ce scénario, vous cliquez sur le nom de l'objet (dans ce cas, un volume) dans le champ Source de la zone **Summary** pour obtenir des détails sur le volume.

   La page Détails Volume / Santé s'affiche sur l'onglet Protection.

4. Dans l'onglet **Protection**, vous pouvez consulter le diagramme de topologie.

   Vous constatez que le volume présentant l'erreur de décalage est le dernier volume d'une cascade SnapMirror de trois volumes. Le volume que vous avez sélectionné est entouré de gris foncé, et une double ligne orange partant du volume source indique une erreur de relation SnapMirror.



5. Cliquez sur chacun des volumes de la cascade SnapMirror.

   Lorsque vous sélectionnez chaque volume, les informations de protection dans les sections Résumé, Topologie, Historique, Événements, Appareils associés et Alertes associées changent pour afficher les détails relatifs au volume sélectionné.

6. Vous consultez la zone **Résumé** et placez votre curseur sur l'icône d'information dans le champ **Calendrier des mises à jour** pour chaque volume.

   Dans ce scénario, vous constatez que la stratégie SnapMirror est DPDefault et que la planification SnapMirror se met à jour toutes les heures, cinq minutes après l'heure. Vous vous rendez compte que tous les volumes de la relation tentent d'effectuer un transfert SnapMirror en même temps.

7. Pour résoudre le problème de décalage, vous modifiez les planifications de deux des volumes en cascade afin que chaque destination commence un transfert SnapMirror une fois que sa source a terminé un transfert.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.