



Créer et dépanner les relations de protection

Active IQ Unified Manager

NetApp

October 15, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-916/data-protection/concept_types_of_snapmirror_protection.html on October 15, 2025. Always check docs.netapp.com for the latest.

Sommaire

Créer, surveiller et dépanner les relations de protection	1
Types de protection SnapMirror	1
Relations de protection asynchrones SnapMirror traditionnelles	1
Protection asynchrone SnapMirror avec réplication flexible en fonction des versions	1
Protection asynchrone SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions	2
Réplication unifiée SnapMirror (miroir et coffre-fort)	2
SnapMirror Protection synchrone avec synchronisation stricte	2
SnapMirror Protection synchrone avec synchronisation régulière	2
Synchronisation active de SnapMirror	2
Configurer les relations de protection dans Unified Manager	3
Configurer une connexion entre Workflow Automation et Unified Manager	3
Vérifier la mise en cache des sources de données d'Unified Manager dans Workflow Automation	4
Que se passe-t-il lorsque OnCommand Workflow Automation est réinstallé ou mis à niveau	5
Supprimer la configuration OnCommand Workflow Automation d'Unified Manager	5
Effectuer un basculement et une restauration de la relation de protection	5
Rompre une relation SnapMirror à partir de la page de détails Volume/Santé	7
Relations de protection inverse à partir de la page Détails Volume/Santé	7
Supprimer une relation de protection de la page Détails du volume/de la santé	8
Resynchroniser les relations de protection à partir de la page Détails du volume/de la santé	9
Résoudre un échec de tâche de protection	10
Identifier le problème et effectuer des actions correctives pour une tâche de protection ayant échoué ..	10
Résoudre les problèmes de décalage	13

Créer, surveiller et dépanner les relations de protection

Unified Manager vous permet de créer des relations de protection, de surveiller et de dépanner la protection miroir et la protection du coffre de sauvegarde des données stockées sur des clusters gérés, et de restaurer les données lorsqu'elles sont écrasées ou perdues.

Types de protection SnapMirror

Selon le déploiement de votre topologie de stockage de données, Unified Manager vous permet de configurer plusieurs types de relations de protection SnapMirror. Toutes les variantes de la protection SnapMirror offrent une protection de reprise après sinistre en cas de basculement, mais offrent des capacités différentes en termes de performances, de flexibilité de version et de protection contre les copies de sauvegarde multiples.

Relations de protection asynchrones SnapMirror traditionnelles

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

Dans les relations SnapMirror traditionnelles, les opérations de miroir s'exécutent plus rapidement que dans les relations SnapMirror alternatives, car l'opération de miroir est basée sur la réplication de blocs. Cependant, la protection SnapMirror traditionnelle nécessite que le volume de destination s'exécute sous la même version mineure ou une version ultérieure du logiciel ONTAP que le volume source dans la même version majeure (par exemple, version 8.x à 8.x ou 9.x à 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.

Protection asynchrone SnapMirror avec réplication flexible en fonction des versions

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

Dans les relations SnapMirror avec réplication flexible en fonction des versions, les opérations de mise en miroir ne s'exécutent pas aussi rapidement qu'elles le feraient dans les relations SnapMirror traditionnelles.

En raison d'une exécution plus lente, SnapMirror avec protection de réplication flexible en fonction des versions n'est pas adapté à la 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 du point de récupération pour les données protégées est de deux heures ou moins. (C'est-à-dire que la destination doit toujours contenir des données en miroir récupérables qui ne sont pas plus anciennes de deux heures que les données de la source.)

Dans l'une ou l'autre des circonstances répertoriées, l'exécution plus rapide basée sur la réplication de blocs de la protection SnapMirror par défaut est requise.

Protection asynchrone SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions

La protection asynchrone SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions offre une protection miroir entre les volumes source et de destination et la possibilité de stocker plusieurs copies des données en miroir à la destination.

L'administrateur de stockage peut spécifier quelles copies Snapshot sont mises en miroir de la source vers la destination et peut également spécifier la durée de conservation de ces copies à la destination, même si elles sont supprimées à la source.

Dans les relations SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions, les opérations de mise en miroir ne s'exécutent pas aussi rapidement qu'elles le feraient dans les relations SnapMirror traditionnelles.

Réplication unifiée SnapMirror (miroir et coffre-fort)

La réplication unifiée SnapMirror 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'appellez. Un transfert de base sous la politique de protection des données unifiée par défaut « MirrorAndVault » effectue une copie instantanée 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 la ligne de base.

SnapMirror Protection synchrone avec synchronisation stricte

La protection synchrone SnapMirror avec synchronisation « stricte » garantit que les volumes principal et secondaire sont toujours une copie conforme l'un de l'autre. Si une erreur de réplication se produit lors de la tentative d'écriture de données sur le volume secondaire, les E/S client sur le volume principal sont interrompues.

SnapMirror Protection synchrone avec synchronisation régulière

La protection synchrone SnapMirror avec synchronisation « régulière » ne nécessite pas que le volume principal et le volume secondaire soient toujours une copie conforme l'un de l'autre, garantissant ainsi la disponibilité du volume principal. Si une erreur de réplication se produit lors de la tentative d'écriture de données sur le volume secondaire, les volumes principal et secondaire ne sont plus synchronisés et les E/S client continuent vers le volume principal.



Le bouton Restaurer et les boutons d'opération 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 Détails Volume/Santé.

Synchronisation active de SnapMirror

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

Il vous permet de découvrir et de surveiller les relations SnapMirror synchrones pour les groupes de cohérence (CG) disponibles sur les clusters et les machines virtuelles de stockage à partir d'Unified Manager. La synchronisation active SnapMirror est prise en charge sur les clusters AFF ou 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 affichez les volumes et les LUN protégés par la relation de synchronisation active SnapMirror, vous pouvez obtenir une vue unifiée des relations de protection, des groupes de cohérence dans l'inventaire des volumes, afficher la topologie de protection pour les relations de groupe de cohérence, afficher les données historiques pour les relations de groupe de cohérence jusqu'à un an. Vous pouvez également télécharger le rapport. Vous pouvez également afficher le résumé des relations du groupe de cohérence, rechercher de l'aide pour les relations du groupe de cohérence 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 et de leur relation qui sont protégés par le groupe de cohérence.

Pour en savoir plus sur la synchronisation active de SnapMirror, reportez-vous à ["Documentation ONTAP 9 pour Snapmirror Active Sync \(anciennement SM-BC\)"](#).

Configurer les relations de protection dans Unified Manager

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

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir établi des relations homologues 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 des sources de données d'Unified Manager dans Workflow Automation"](#).

Étapes

1. Selon le type de relation de protection que vous souhaitez créer, effectuez l'une des opérations suivantes :
 - ["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, effectuez l'une des opérations suivantes :
 - ["Créer une politique SnapVault"](#).
 - ["Créer une politique SnapMirror"](#).
3. ["Créer une planification SnapMirror ou SnapVault"](#).

Configurer une connexion entre Workflow Automation et 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 de gestion des relations SnapMirror

Avant de commencer

- La version installée de Workflow Automation doit être 5.1.1P6 ou supérieure.



Le « pack WFA pour la gestion des Data ONTAP » est inclus dans WFA 5.1.1P6. Il n'est donc pas nécessaire de télécharger ce pack depuis NetAppStorage Automation Store et de l'installer séparément sur votre serveur WFA comme cela était requis par le passé. "[Pack WFA pour la gestion ONTAP](#)"

- Vous devez disposer du nom de l'utilisateur de 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 avoir reçu le rôle d'utilisateur de schéma d'intégration.

- Vous devez disposer du rôle d'administrateur ou du rôle d'architecte 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 d'administrateur d'application ou d'administrateur de stockage.

Étapes

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

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 Automatisation du flux de travail s'affiche.

6. Cliquez sur **Oui** pour recharger l'interface utilisateur Web et ajouter les fonctionnalités d'automatisation du flux de travail.

Informations connexes

["Documentation NetApp : OnCommand Workflow Automation \(versions actuelles\)"](#)

Vérifier la mise en cache des sources de données d'Unified Manager dans Workflow Automation

Vous pouvez déterminer si la mise en cache de la source de données Unified Manager fonctionne correctement en vérifiant si l'acquisition de la source de données réussit dans Workflow Automation. Vous pouvez le faire lorsque vous intégrez Workflow Automation à Unified Manager pour garantir que la fonctionnalité Workflow Automation est disponible

après l'intégration.

Avant de commencer

Vous devez disposer du rôle d'administrateur ou du rôle d'architecte dans Workflow Automation pour effectuer cette tâche.

Étapes

1. Depuis l'interface utilisateur d'automatisation du flux de travail, sélectionnez **Exécution > Sources de données**.
2. Cliquez avec le bouton droit sur le nom de la source de données Unified Manager, puis sélectionnez **Acquérir maintenant**.
3. Vérifiez que l'acquisition réussit sans erreur.

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

Que se passe-t-il lorsque OnCommand Workflow Automation est réinstallé ou mis à niveau

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 tous les travaux OnCommand Workflow Automation en cours d'exécution ou planifiés sont arrêtés.

Vous devez également supprimer manuellement Unified Manager d' OnCommand Workflow Automation.

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

Supprimer la configuration OnCommand Workflow Automation d'Unified Manager

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

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Automatisation du flux de travail** dans le menu Configuration de gauche.
2. Sur la page **Automatisation du flux de travail**, cliquez sur **Supprimer la configuration**.

Effectuer un basculement et une restauration de la relation de protection

Lorsqu'un volume source de votre relation de protection est désactivé en raison d'une panne matérielle ou d'un sinistre, vous pouvez utiliser les fonctionnalités de relation de protection dans Unified Manager pour rendre la destination de protection accessible en

lecture/écriture et basculer vers ce volume jusqu'à ce que la source soit à nouveau en ligne ; vous pouvez ensuite revenir à la source d'origine lorsqu'elle est disponible pour diffuser des données.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation pour effectuer cette opération.

Étapes

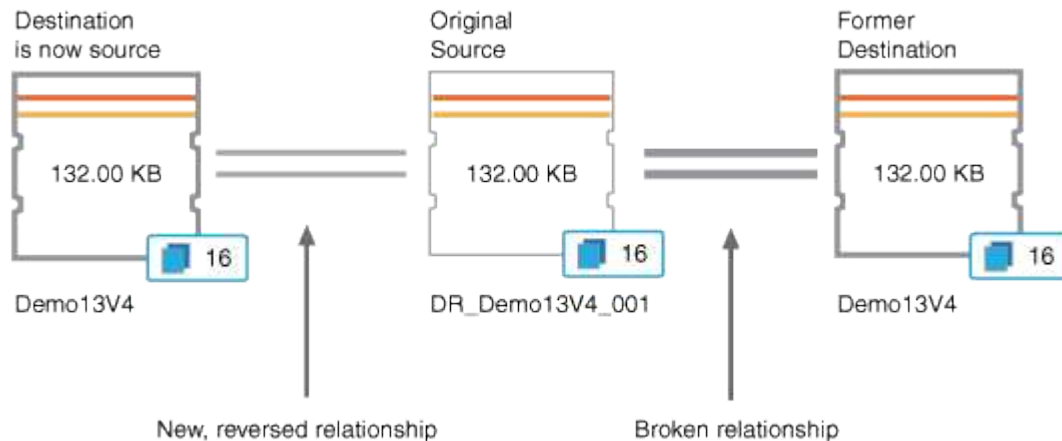
1. "Rompre la relation SnapMirror".

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

2. "Inverser la relation de protection".

Lorsque le volume source d'origine est à nouveau disponible, vous pouvez décider de rétablir la relation de protection d'origine 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 d'origine et en synchronisant le volume source avec l'ancienne destination. Une nouvelle copie d'instantané de base est créée pour la nouvelle relation.

La relation inversée ressemble à une relation en cascade :



3. "Rompre la relation inversée SnapMirror".

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

4. "Supprimer la relation".

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

Rompre une relation SnapMirror à partir de la page de détails Volume/Santé

Vous pouvez rompre une relation de protection à partir de la page Détails Volume/Santé 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 une reprise après sinistre ou pour des tests d'application. Le volume de destination est modifié en volume de lecture-écriture. Vous ne pouvez pas rompre une relation SnapVault .

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

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. Cliquez avec le bouton droit sur la destination et sélectionnez **Pause** 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.

Relations de protection inverse à partir de la page Détails Volume/Santé

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

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- La relation ne doit pas être une relation SnapVault .
- Une relation de protection doit déjà exister.
- La relation de protection doit être rompue.
- La source et la destination doivent 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 qui sont plus récentes que les données 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 calendriers n'existent pas, ils sont créés.

Étapes

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

La boîte de dialogue Resynchronisation inversée s'affiche.

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

La boîte de dialogue Resynchronisation inversée est fermée et un lien de tâche s'affiche en haut de la page Détails du volume/de l'état de santé.

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

Une liste filtrée de 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 sont terminées avec succès.

Supprimer une relation de protection de la page Détails du volume/de la santé

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 à l'aide d'une destination différente. Cette opération supprime toutes les métadonnées et ne peut pas être annulée.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

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. Cliquez avec le bouton 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 Détails Volume / Santé.

Resynchroniser les relations de protection à partir de la page Détails du volume/de la santé

Vous pouvez resynchroniser les données sur une relation SnapMirror ou SnapVault qui a été rompue, puis la destination a été rendue en lecture/écriture afin que les données de la source correspondent aux données de la destination. Vous pouvez également resynchroniser lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, ce qui entraîne l'échec des mises à jour de SnapMirror ou de SnapVault .

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

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

Alternativement, dans le menu **Actions**, sélectionnez **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'instantanés 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 d'instantané existante plutôt que de transférer la copie d'instantané par défaut, cliquez sur **Copie d'instantané existante** et sélectionnez une copie d'instantané dans la liste.
6. Cliquez sur **Soumettre**.

Vous revenez à la boîte de dialogue Resynchroniser.

7. Si vous avez sélectionné plusieurs sources à resynchroniser, cliquez sur **Par défaut** pour la source suivante pour laquelle vous souhaitez spécifier une copie instantanée existante.
8. Cliquez sur **Soumettre** pour commencer le travail de resynchronisation.

La tâche de resynchronisation est démarrée, vous revenez à la page des détails Volume / Santé et un lien vers les tâches s'affiche en haut de la page.

9. **Facultatif** : cliquez sur **Afficher les tâches** sur la page **Détails du volume/de l'état** pour suivre l'état de chaque tâche de resynchronisation.

Une liste filtrée de 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 sont terminées avec succès.

Résoudre un échec de tâche de protection

Ce workflow fournit un exemple de la manière dont vous pouvez 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 à l'aide du rôle Administrateur, vous devez être familiarisé avec les rôles requis pour utiliser diverses fonctionnalités.

Dans ce scénario, vous accédez à la page Tableau de bord pour voir s'il existe des problèmes avec vos tâches de protection. Dans la zone Incident de protection, vous remarquez qu'il existe un incident de tâche terminée, indiquant une erreur d'échec de tâche de protection sur un volume. Vous examinez cette erreur pour déterminer la cause possible et la résolution potentielle.

Étapes

1. Dans le panneau Incidents de protection de la zone Incidents et risques non résolus du tableau de bord, cliquez sur l'événement **Échec de la tâche de protection**.



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

La page Détails de l'événement pour la tâche de protection ayant échoué s'affiche.

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

Voir "[Identifier le problème et effectuer des actions correctives en cas d'échec d'une tâche de protection](#)".

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

Vous examinez le message d'erreur d'échec de la tâche dans le champ Cause de la page Détails de l'événement et déterminez que la tâche a échoué en raison d'une erreur de copie d'instantané. Vous accédez ensuite à la page Détails Volume / Santé pour recueillir plus d'informations.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Le message d'erreur fourni 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 :

- Une tâche de sauvegarde ou de mise en miroir n'a pas été effectuée avec succès.

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 d'instantané a échoué pour `0426cluster2_src_vol2snap` sur le volume source `cluster2_src_svm:/cluster2_src_vol2`.

Dans ce scénario, vous pouvez identifier la cause et les actions correctives potentielles de l'échec du travail. Cependant, la résolution de l'échec nécessite que vous accédiez à l'interface utilisateur Web du gestionnaire de système ou aux commandes CLI ONTAP.

Étapes

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

Vous pouvez également cliquer sur le lien **Détails du travail** à la fin du message d'erreur, mais dans le cadre de ce scénario, vous choisissez de ne pas le faire.

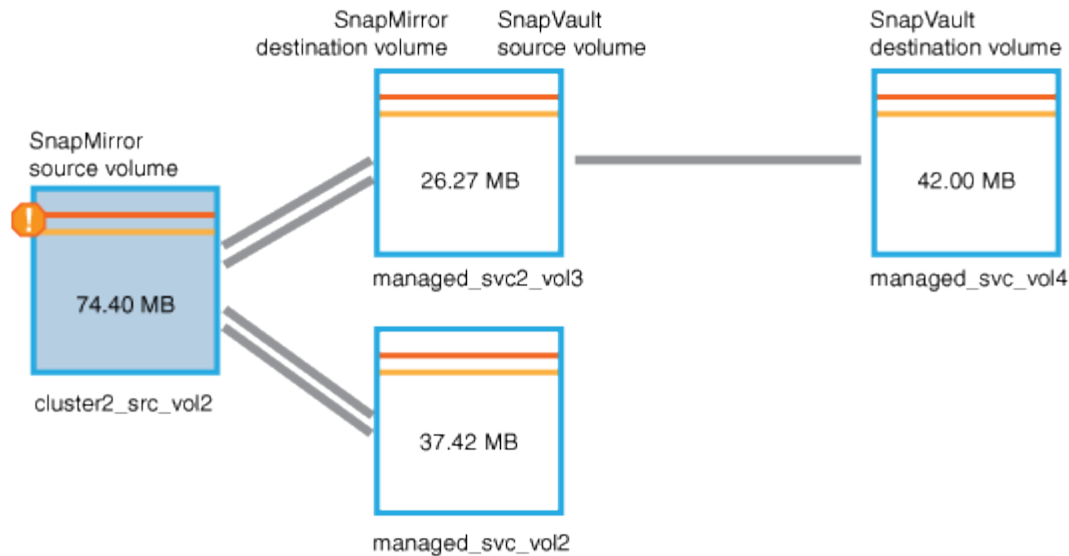
2. Vous décidez que vous souhaitez essayer de résoudre l'événement, vous procédez donc comme suit :
 - a. Cliquez sur le bouton **Attribuer à** et sélectionnez **Moi** dans le menu.
 - b. Cliquez sur le bouton **Accuser réception** pour ne plus recevoir de notifications d'alerte répétées, si des alertes ont été définies pour l'événement.
 - c. En option, vous pouvez également ajouter des notes sur l'événement.
3. Cliquez sur le champ **Source** dans le volet **Résumé** pour voir les détails sur le volume source.

Le champ **Source** contient le nom de l'objet source : dans ce cas, le volume sur lequel le travail de copie de snapshot a été planifié.

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

4. En regardant 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 voyez également 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 voir la boîte de dialogue contextuelle qui affiche les paramètres de seuil et constatez que le volume a dépassé le seuil d'erreur, indiquant un problème de capacité.

6. Cliquez sur l'onglet **Capacité**.

Informations sur la capacité concernant le volume `cluster2_src_vol2` affiche.

7. Dans le panneau **Capacité**, vous voyez qu'il y a une icône d'erreur dans le graphique à barres, indiquant à nouveau que la capacité du volume a dépassé le niveau de seuil défini pour le volume.

8. Sous le graphique de capacité, vous voyez que la croissance automatique du volume a été désactivée et qu'une garantie d'espace de volume a été définie.

Vous pouvez décider d'activer la croissance automatique, mais dans le cadre de ce scénario, vous décidez d'enquêter davantage avant de prendre une décision sur la manière de résoudre le problème de capacité.

9. Faites défiler la liste jusqu'à la liste **Événements** et constatez que les événements Échec du travail de protection, Jours du volume jusqu'à saturation et Espace du volume plein ont été générés.

10. Dans la liste **Événements**, cliquez sur l'événement **Espace volume plein** pour obtenir plus d'informations, après avoir décidé que cet événement semble le plus pertinent pour votre problème de capacité.

La page Détails de l'événement affiche l'événement Espace volume plein 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 s'affichent uniquement pour certains événements. Vous ne voyez donc pas cette zone pour tous les types d'événements.

Vous cliquez sur la liste des actions suggérées que vous pouvez effectuer pour résoudre l'événement d'espace de volume plein :

- Activer la croissance automatique sur ce volume.
- Redimensionner le volume.

- Activez et exécutez la déduplication sur ce volume.
 - Activer et exécuter la compression sur ce volume.
13. Vous décidez d'activer la croissance automatique sur le 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. Regardez l'agrégat parent, `cluster2_src_aggr1` , dans le volet **Périphériques associés**.



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

Vous déterminez que l'agrégat dispose de suffisamment d'espace pour permettre la croissance automatique du volume.

- b. En haut de la page, regardez l'icône indiquant un incident critique et examinez le texte sous l'icône.

Vous déterminez que « Jours jusqu'à épuisement : moins d'un jour | Taux de croissance quotidien : 5,4 % ».

14. Accédez au Gestionnaire de système ou à l'interface de ligne de commande ONTAP pour activer le `volume autogrow option`.



Notez les noms du volume et de l'agrégat afin de les avoir à disposition lors de l'activation de la croissance automatique.

15. Après avoir résolu le problème de capacité, revenez à la page des détails de l'événement Unified Manager **Événement** et marquez l'événement comme résolu.

Résoudre les problèmes de décalage

Ce flux de travail fournit un exemple de la manière dont vous pouvez résoudre un problème de décalage. Dans ce scénario, vous êtes un administrateur ou un opérateur accédant à la page Tableau de bord d'Unified Manager pour voir s'il existe des problèmes avec vos relations de protection et, s'ils existent, pour trouver des solutions.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Dans la page Tableau de bord, vous examinez la zone Incidents et risques non résolus et voyez 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**, recherchez l'erreur de décalage de relation SnapMirror et cliquez dessus.

La page Détails de l'événement pour l'événement d'erreur de décalage s'affiche.

2. À partir de 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 Résumé 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 Résumé pour

obtenir des détails sur le volume.

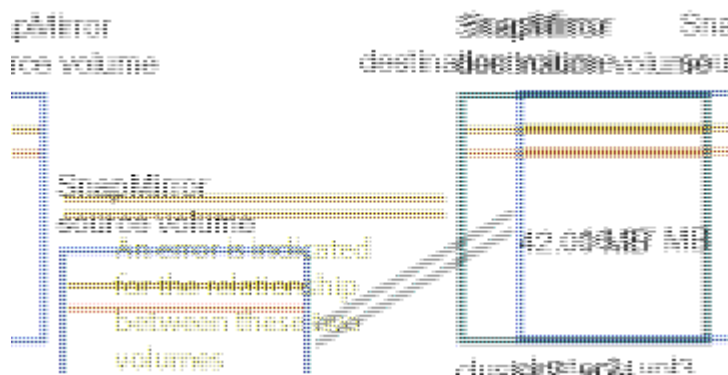
- Recherchez des notes qui pourraient avoir été ajoutées à propos de cet événement.
- Ajoutez une note à l'événement.
- Affecter l'événement à un utilisateur spécifique.
- Reconnaître ou résoudre l'événement.

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

L'onglet Protection de la page Détails Volume / Santé s'affiche.

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

Vous constatez que le volume avec l'erreur de décalage est le dernier volume d'une cascade SnapMirror à trois volumes. Le volume que vous avez sélectionné est entouré en gris foncé et une double ligne orange provenant 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 zones Résumé, Topologie, Historique, Événements, Périphériques associés et Alertes associées changent pour afficher les détails relatifs au volume sélectionné.

6. Vous regardez la zone **Résumé** et positionnez votre curseur sur l'icône d'informations dans le champ **Calendrier de mise à jour** pour chaque volume.

Dans ce scénario, vous remarquez que la stratégie SnapMirror est DPDefault et que la planification SnapMirror est mise à jour toutes les heures, cinq minutes après l'heure. Vous réalisez 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 © 2025 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 DÉLICTELLE (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.