Création et résolution des problèmes de relations de protection

Active IQ Unified Manager 9.12

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-912/data-protection/concept_types_of_snapmirror_protection.html on October 16, 2025. Always check docs.netapp.com for the latest.

Sommaire

Création, surveillance et résolution des problèmes de relations de protection . . . 1
Types de protection SnapMirror . . . 1
Relations de protection asynchrones SnapMirror classiques . . . 1
Protection asynchrone de SnapMirror avec réplication flexible de la version . . . 1
Protection asynchrone de SnapMirror avec l'option de réplication et de sauvegarde flexibles de la version . . . 2
Réplication unifiée SnapMirror (mise en miroir et archivage sécurisé) . . . 2
Protection SnapMirror synchrone avec synchronisation stricte . . . 2
Protection SnapMirror synchrone avec synchronisation régulière . . . 2
Continuité de l'activité SnapMirror synchrone . . . 2
Configuration des relations de protection dans Unified Manager . . . 3
Configuration d'une connexion entre Workflow Automation et Unified Manager . . . 3
Vérification de la mise en cache des sources de données Unified Manager dans Workflow Automation . . . 4
Que se passe-t-il lorsque OnCommand Workflow Automation est réinstallé ou mis à niveau . . . 5
Suppression de la configuration OnCommand Workflow Automation depuis Unified Manager . . . 5
Effectuer un basculement et un retour arrière de la relation de protection . . . 5
Briser une relation SnapMirror depuis la page des détails du volume / intégrité . . . 7
Inversion des relations de protection à partir de la page Détails du volume/intégrité . . . 7
Suppression d'une relation de protection de la page Détails du volume/intégrité . . . 8
Resynchronisation des relations de protection à partir de la page Détails du volume/intégrité . . . 9
Résolution de l'échec d'une tâche de protection . . . 10
Identification du problème et exécution d'actions correctives pour une tâche de protection ayant échoué . . . 10
Résolution des problèmes de décalage . . . 13

Création, surveillance et résolution des problèmes de relations de protection

Unified Manager vous permet de créer des relations de protection, de surveiller et de résoudre les problèmes de protection en miroir et de sauvegarde des données stockées sur les clusters gérés, et de restaurer les données lorsqu'elles sont remplacées ou perdues.

Types de protection SnapMirror

Selon le déploiement de la 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 contre les basculements après incident, mais elles proposent plusieurs fonctionnalités en performances, une flexibilité de version et une protection contre les copies de sauvegarde différentes.

Relations de protection asynchrones SnapMirror classiques

La protection asynchrone traditionnelle de SnapMirror protège les miroirs de 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 est basée sur la réplication de blocs. La protection traditionnelle par SnapMirror implique cependant que le volume de destination s'exécute sous la même version mineure du logiciel ONTAP ou une version ultérieure, que le volume source soit au sein de la même version principale (par exemple, version 8.x vers 8.x ou 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.

Protection asynchrone de SnapMirror avec réplication flexible de la version

La protection asynchrone de SnapMirror avec la réplication flexible de la version protège les miroirs de réplication logique entre les volumes source et de destination, même si ces volumes sont exécutés sous différentes versions du logiciel ONTAP 8.3 ou version ultérieure (par exemple, la 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 la réplication flexible de la version, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

Compte tenu du ralentissement d'exécution, SnapMirror avec protection de réplication flexible de la version ne convient pas à implémenter dans l'un ou l'autre des cas suivants :

- L'objet source contient plus de 10 millions de fichiers à protéger.
- L'objectif de point de restauration des données protégées est de deux heures maximum. (La destination doit donc toujours contenir des données mises en miroir et récupérables datant d'au plus deux heures que les données de la source.)

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

Protection asynchrone de SnapMirror avec l'option de réplication et de sauvegarde flexibles de la version

La protection asynchrone de SnapMirror avec l'option de réplication et de sauvegarde flexible de la version protège les données en miroir entre les volumes source et de destination, et permet de stocker plusieurs copies des données en miroir sur la destination.

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

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

Réplication unifiée SnapMirror (mise en miroir et archivage sécurisé)

La réplication unifiée SnapMirror vous permet de configurer la reprise après incident et l'archivage sur le même volume de destination. Comme pour SnapMirror, la protection unifiée des données effectue un transfert de base dès le premier appel que vous l'appelez. Un transfert de base placé sous la règle de protection unifiée des données par défaut « irriorAndVault » effectue une copie Snapshot du volume source, puis transfère cette copie et les données qu'elle renvoie au volume de destination. Comme SnapVault, la protection unifiée des données n'inclut pas d'anciennes copies Snapshot de la configuration de base.

Protection SnapMirror synchrone avec synchronisation stricte

La protection SnapMirror synchrone avec synchronisation « par suppression » garantit que les volumes primaires et secondaires sont toujours une copie authentique les uns des autres. En cas de défaillance de réplication lors d'une tentative d'écriture de données sur le volume secondaire, les E/S du client vers le volume primaire sont interrompues.

Protection SnapMirror synchrone avec synchronisation régulière

La protection synchrone de SnapMirror avec la synchronisation « granulaire » n'exige pas que les volumes primaire et secondaire soient toujours une copie authentique des uns des autres, ce qui assure la disponibilité du volume primaire. Si une défaillance de réplication se produit lors d'une tentative d'écriture de données sur le volume secondaire, les volumes primaire et secondaire sont désynchronisés 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 synchrone à partir de la vue Santé : tous les volumes ou de la page Détails du volume / intégrité.

Continuité de l'activité SnapMirror synchrone

La fonction de continuité de l'activité SnapMirror est disponible avec ONTAP 9.8 et versions ultérieures. Vous pouvez l'utiliser pour protéger les applications avec des LUN, ce qui permet aux applications de basculer en toute transparence, assurant ainsi la continuité de l'activité en cas d'incident.

Elle vous permet de détecter et de surveiller les relations SnapMirror synchrones pour les groupes de cohérence disponibles sur les clusters et les machines virtuelles de stockage de Unified Manager. SM-BC est pris en charge sur les clusters AFF ou sur tous les clusters SAN Array (ASA), dans lesquels les clusters principaux et secondaires peuvent être AFF ou ASA. SM-BC protège les applications avec des LUN iSCSI ou

FCP.

Lorsque vous affichez les volumes et les LUN protégés par la relation SM-BC, vous pouvez obtenir une vue unifiée des relations de protection, des groupes de cohérence dans l'inventaire des volumes, afficher la topologie de protection des relations de groupe de cohérence, afficher les données historiques des relations de groupe de cohérence jusqu'à un an. Vous pouvez également télécharger le rapport. Vous pouvez également afficher le récapitulatif des relations de groupe de cohérence, rechercher le support des relations de 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 protégée par le groupe de cohérence.

Pour en savoir plus sur la continuité de l'activité SnapMirror synchrone, reportez-vous à "Documentation ONTAP 9 pour SM-BC".

Configuration des relations de protection dans Unified Manager

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

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir établi des relations entre deux clusters ou deux SVM (Storage Virtual machine).
- OnCommand Workflow Automation doit être intégré avec Unified Manager :
  - "Configurer OnCommand Workflow Automation".
  - "Vérification de la mise en cache des sources de données 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 stratégie pour la relation, en fonction du type de relation que vous créez, effectuez l'une des opérations suivantes :
   - "Création d'une règle SnapVault".
   - "Créer une règle SnapMirror".
3. "Créer une planification SnapMirror ou SnapVault".

Configuration d'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 flux de travail de configuration SnapMirror et SnapVault, ainsi que des commandes pour gérer les relations SnapMirror.

Ce dont vous aurez besoin

- La version installée de Workflow Automation doit être égale ou supérieure à 5.1.

  WFA 5.1 inclut le pack WFA de gestion de clustered Data ONTAP. Il n'est donc pas nécessaire de télécharger ce pack sur le site NetApp Storage Automation Store et de l'installer séparément sur votre serveur WFA, comme cela était requis par le passé. "WFA pack pour la gestion de 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 utilisateur du schéma d'intégration.

- Vous devez être affecté soit au rôle Administrateur, soit au rôle architecte dans Workflow Automation.
- L'adresse de l'hôte, le numéro de port 443, le nom d'utilisateur et le mot de passe doivent être définis pour Workflow Automation.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Workflow Automation**.
2. Dans la zone **Database User** de la page **Workflow Automation**, 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 **Workflow Automation Credentials** de la page, entrez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6), ainsi que le nom d'utilisateur et le mot de passe de la configuration de Workflow Automation.

   Vous devez utiliser le port de 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 l'interface utilisateur Web et ajouter les fonctions Workflow Automation.

Informations connexes

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

Vérification de la mise en cache des sources de données Unified Manager dans Workflow Automation

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

Ce dont vous aurez besoin

Pour effectuer cette tâche, vous devez être affecté soit au rôle Administrateur, soit au rôle architecte dans Workflow Automation.

Étapes

1. Dans l'interface utilisateur Workflow Automation, sélectionnez **exécution** > **sources de données**.
2. Cliquez avec le bouton droit de la souris sur le nom de la source de données Unified Manager, puis sélectionnez **acquérir maintenant**.
3. Vérifiez que l'acquisition réussit sans erreur.

   Pour que l'intégration de Workflow Automation à Unified Manager réussisse, les erreurs d'acquisition doivent être résolues.

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 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 de nouveau configurer la connexion avec Unified Manager.

Suppression de la configuration OnCommand Workflow Automation depuis Unified Manager

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

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Workflow Automation** dans le menu de configuration de gauche.
2. Dans la page **Workflow Automation**, cliquez sur **Supprimer la configuration**.

Effectuer un basculement et un retour arrière 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 incident, vous pouvez utiliser les fonctions de relation de protection de Unified Manager pour rendre les données de destination de protection accessibles en lecture/écriture et basculer vers le volume jusqu'à ce que la source soit à nouveau en ligne. vous pouvez ensuite revenir à la source d'origine lorsqu'il est

disponible pour transmettre les données.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation pour effectuer cette opération.

Étapes

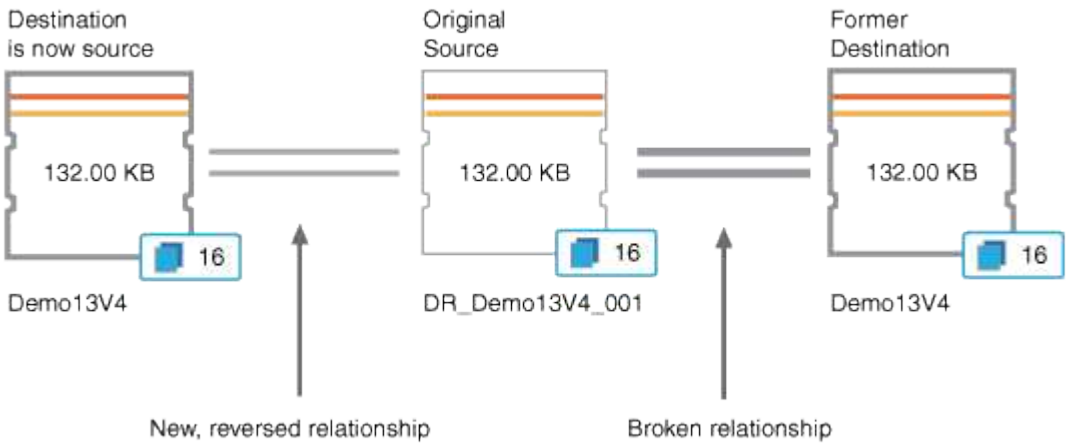
1. "Interrompre la relation SnapMirror".

   Vous devez interrompre la relation avant de pouvoir convertir la destination d'un volume de protection des données en volume de lecture/écriture, et avant d'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. 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 Snapshot de base est créée pour la nouvelle relation.

   La relation inversée ressemble à une relation en cascade :



3. "Interrompre la relation SnapMirror inversée".

   Lorsque le volume source d'origine est resynchronisé et peut à nouveau transmettre les données, utilisez l'opération de coupure pour interrompre 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.

Briser une relation SnapMirror depuis la page des détails du volume / intégrité

Vous pouvez interrompre une relation de protection à partir de la page des détails de volume/intégrité et arrêter les transferts de données entre un volume source et un volume cible dans une relation SnapMirror. Vous pouvez briser une relation lorsque vous souhaitez migrer des données, pour la reprise d'activité ou pour le test d'application. Le volume de destination est modifié en volume de lecture-écriture. Vous ne pouvez pas interrompre une relation SnapVault.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez interrompre.
2. Cliquez avec le bouton droit de la souris 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.

Inversion des relations de protection à partir de la page Détails du volume/intégrité

Lorsqu'un incident désactive le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour transmettre des données en les 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 établir la relation dans le sens inverse, en synchronisant les données de la source avec celles de la destination de lecture/écriture.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.
- 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 règles et les planifications créées sur la relation de resynchronisation inverse sont identiques à celles

de la relation de protection d'origine.

Si des stratégies et des plannings n'existent pas, ils sont créés.

Étapes

1. Dans l'onglet **protection** de la page de détails **Volume/Santé**, localisez dans la topologie la relation SnapMirror sur laquelle vous souhaitez inverser la source et la destination, et cliquez avec le bouton droit de la souris.
2. Sélectionnez **Reverse Resync** dans le menu.

   La boîte de dialogue Reverse Resync s'affiche.

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

   La boîte de dialogue Reverse Resync est fermée et un lien de tâche s'affiche en haut de la page Volume / Health details.

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

   Une liste filtrée des travaux 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 de travail sont terminées avec succès.

Suppression d'une relation de protection de la page Détails du volume/intégrité

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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page d'informations **Volume/Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez supprimer.
2. Cliquez avec le bouton droit de la souris 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 Volume / Health details.

Resynchronisation des relations de protection à partir de la page Détails du volume/intégrité

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

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page de détails **Volume / Santé**, localisez 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.

   Vous pouvez également sélectionner **relations** > **Resynchroniser** dans le menu **actions** pour resynchroniser la relation pour laquelle vous consultez actuellement les détails.

   La boîte de dialogue Resynchroniser s'affiche.

3. Dans l'onglet **Resynchronisation Options**, sélectionnez une priorité de transfert et le taux de transfert maximal.
4. Cliquez sur **copies snapshot source**, puis, dans la colonne **copie snapshot**, cliquez sur **par défaut**.

   La boîte de dialogue Sélectionner une copie Snapshot source s'affiche.

5. Pour 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 **soumettre**.

   Vous revenez à la boîte de dialogue Resynchroniser.

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 le travail de resynchronisation.

   Le travail de resynchronisation est lancé, vous êtes renvoyé à la page Détails du volume / intégrité et un lien tâches s'affiche en haut de la page.

9. **Facultatif:** cliquez sur **Afficher les travaux** dans la page **Détails du volume / de l'état de santé** pour suivre l'état de chaque travail de resynchronisation.

   Une liste filtrée des travaux s'affiche.

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

    La tâche de resynchronisation est terminée lorsque toutes les tâches de travail sont terminées avec

succès.

Résolution de l’échec d’une tâche de protection

Ce flux de travail fournit un exemple d’identification et de résolution d’une défaillance de tâche de protection à partir du tableau de bord Unified Manager.

Ce dont vous aurez besoin

Comme certaines tâches de ce flux de travail nécessitent de vous connecter à l’aide du rôle Administrateur, vous devez connaître les rôles requis pour utiliser diverses fonctionnalités.

Dans ce scénario, vous accédez à la page Tableau de bord pour voir s’il y a des problèmes avec vos tâches de protection. Dans la zone incident de protection, vous remarquez qu’un incident de fin de tâche est survenu, indiquant une erreur d’échec de tâche de protection sur un volume. Vous étudiez cette erreur afin de déterminer la cause possible et la résolution potentielle.

Étapes

1. Dans le panneau protection incidents de la zone Tableau de bord incidents et risques non résolus, cliquez sur l’événement **protection job failed**.

   Le texte lié de l’événement est écrit dans le formulaire `object_name:/object_name - Error Name`, comme `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 mesures correctives possibles.

   Voir "Identification du problème et exécution d’actions correctives pour une tâche de protection ayant échoué".

Identification du problème et exécution d’actions correctives pour une tâche de protection ayant échoué

Vous examinez le message d’erreur d’échec du travail dans le champ cause de la page Détails de l’événement et déterminez que le travail a échoué en raison d’une erreur de copie Snapshot. Vous allez ensuite à la page Volume / Health details pour recueillir plus d’informations.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d’applications.

Le message d’erreur fourni dans le champ cause de la page Détails de l’événement contient le texte suivant concernant le travail en échec :

```
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 miroir ne s'est pas terminée 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`.

- Échec d'une tâche de copie Snapshot 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. Toutefois, pour résoudre ce problème, vous devez accéder à l'interface utilisateur Web de System Manager ou aux commandes de l'interface de ligne de commande de ONTAP.

Étapes

1. Vous passez en revue 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 le volume source.

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

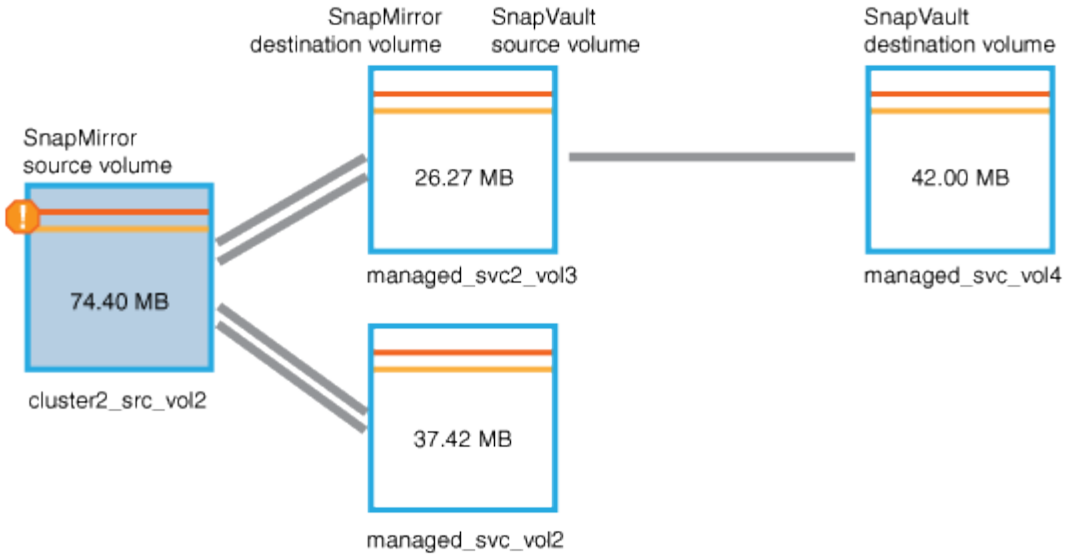
2. Vous décidez que vous voulez essayer de résoudre l'événement, vous devez donc procéder comme suit :
   a. Cliquez sur le bouton **affecter à** et sélectionnez **Me** dans le menu.
   b. Cliquez sur le bouton **Acknowledge** pour ne pas continuer à recevoir de notifications d'alerte répétées si des alertes ont été définies pour l'événement.
   c. Vous pouvez également ajouter des remarques à propos de l'événement.
3. Cliquez sur le champ **Source** dans le volet **Résumé** pour afficher les détails du volume source.

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

   La page Volume / Détails de l'intégrité s'affiche pour `cluster2_src_vol2`, Montrant le contenu de l'onglet protection.

4. Sur le graphique de topologie de protection, une icône d'erreur s'affiche, associée au premier volume de la topologie, qui correspond au 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. Placez le curseur sur l'icône d'erreur pour afficher la boîte de dialogue contextuelle qui affiche les paramètres de seuil et voir que le volume a dépassé le seuil d'erreur, ce qui indique un problème de capacité.
6. Cliquez sur l'onglet **capacité**.

   Informations de capacité relatives au volume `cluster2_src_vol2` s'affiche.

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

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

9. Vous faites défiler la liste **Events** et voyez que les événements protection Job failed, Volume Days jusqu'à Full et Volume Space Full ont été générés.
10. Dans la liste **Evénements**, vous cliquez sur l'événement **Volume Space Full** pour obtenir plus d'informations, ayant décidé que cet événement semble le plus pertinent pour votre problème de capacité.

    La page 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 suggestions d'actions correctives.

    Les actions correctives suggérées s'affichent uniquement pour certains événements. Vous ne voyez donc pas cette zone pour tous les types d'événements.

    Vous pouvez cliquer sur la liste des actions suggérées pour résoudre l'événement Volume Space Full :

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

- Activer et exécuter la déduplication sur ce volume.
- Activer et exécuter la compression sur ce volume.

13. Vous décidez d'activer la croissance automatique sur le volume. Pour ce faire, vous devez déterminer l'espace libre disponible sur l'agrégat parent et le taux de croissance actuel du volume :
    a. Examiner l'agrégat parent, `cluster2_src_aggr1`, Dans le volet périphériques connexes*.

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

       Vous avez établi que l'agrégat dispose d'un espace suffisant pour activer la croissance automatique de volumes.

    b. En haut de la page, regardez l'icône indiquant un incident critique et passez en revue le texte au-dessous de l'icône.

       Vous déterminez que « jours complets : moins d'une journée | taux de croissance quotidien : 5.4 % ».

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

    Notez les noms du volume et de l'agrégat pour qu'ils soient disponibles en cas d'activation de la croissance automatique.

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

Résolution des problèmes de décalage

Ce flux de travail fournit un exemple de résolution d'un problème de décalage. Dans ce scénario, vous êtes un administrateur ou un opérateur qui accède à la page Tableau de bord Unified ManagerLe cas échéant, pour voir s'il y a des problèmes avec vos relations de protection et, le cas échéant, pour trouver des solutions.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Sur 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 protection risques.

Étapes

1. Dans le volet **protection** de la page **Dashboard**, localisez l'erreur de décalage de la 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 **Event**, vous pouvez effectuer une ou plusieurs des tâches suivantes :
   - Passez en revue le message d'erreur dans le champ cause de la zone Résumé pour déterminer s'il y a 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.

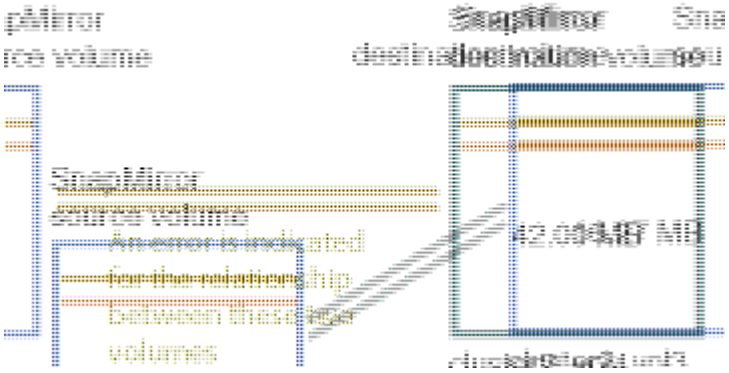
- Recherchez les notes qui ont peut-être été ajoutées à ce sujet.
- Ajoutez une note à l'événement.
- Attribuez l'événement à un utilisateur spécifique.
- Accuser réception ou résoudre l'événement.

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 du volume/intégrité s'affiche.

4. Dans l'onglet **protection**, vous examinez le diagramme de topologie.

   Vous remarquerez que le volume avec l'erreur de décalage est le dernier volume d'une cascade SnapMirror à trois volumes. Le volume sélectionné est en gris foncé et une ligne double orange du volume source indique une erreur de relation SnapMirror.



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

   Lorsque vous sélectionnez chaque volume, les informations de protection dans le récapitulatif, topologie, Historique, événements, périphériques associés, Les zones alertes associées changent pour afficher les détails relatifs au volume sélectionné.

6. Vous regardez la zone **Résumé** et placez votre curseur sur l'icône d'information dans le champ **mettre à jour le programme** pour chaque volume.

   Dans ce scénario, vous remarquerez que la règle SnapMirror est DPDefault et que la planification SnapMirror est mise à jour toutes les heures à cinq minutes après l'heure. Vous avez conscience que tous les volumes de la relation tentent de réaliser 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 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.