Configuration des relations de protection dans Unified Manager

OnCommand Unified Manager 9.5

NetApp
August 02, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/oncommand-unified-manager-95/health-checker/task-configuring-a-connection-between-workflow-automation-and-unified-manager.html on August 02, 2024. Always check docs.netapp.com for the latest.

Sommaire

Configuration des relations de protection dans Unified Manager . . . 1
Avant de commencer . . . 1
Étapes . . . 1
Configuration d'une connexion entre Workflow Automation et Unified Manager . . . 1
Vérification de la mise en cache des sources de données Unified Manager dans Workflow Automation . . . 2
Création d'une relation de protection SnapMirror à partir de la page de détails Health/Volume . . . 3
Création d'une relation de protection SnapVault à partir de la page des détails intégrité/volume . . . 4
Création d'une règle SnapVault pour optimiser l'efficacité du transfert . . . 5
Création d'une règle SnapMirror pour optimiser l'efficacité du transfert . . . 6
Création de planifications SnapMirror et SnapVault . . . 6

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.

Avant de commencer

- Vous devez avoir le rôle d'administrateur OnCommand ou d'administrateur du 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.

Avant de commencer

- La version installée de Workflow Automation doit être égale ou supérieure à 4.2.
- Vous devez avoir installé la version 9.5.0 (ou ultérieure) de WFA (pack pour la gestion de clustered Data ONTAP) sur le serveur WFA. Vous pouvez télécharger le pack requis sur le site NetApp Storage Automation Store.

  "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 d'administrateur OnCommand ou d'administrateur du stockage.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **Workflow Automation** dans le menu de configuration de gauche.
2. Dans la zone utilisateur de base de données **OnCommand Unified Manager** de la page **Setup/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 **OnCommand Workflow Automation Credentials** de la page **Setup/Workflow Automation**, 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 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 Configuration/Workflow Automation s'affiche.

6. Cliquez sur **Oui** pour recharger l'interface utilisateur Web et ajouter les fonctions Workflow Automation.

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.

Avant de commencer

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.

Création d'une relation de protection SnapMirror à partir de la page de détails Health/Volume

Vous pouvez utiliser la page de détails Health/Volume pour créer une relation SnapMirror de sorte que la réplication des données soit activée à des fins de protection. La réplication SnapMirror vous permet de restaurer les données à partir du volume de destination en cas de perte de données sur la source.

Avant de commencer

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

Description de la tâche

Le menu **Protect** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Si le volume est un volume FlexGroup
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert

Vous pouvez effectuer jusqu'à 10 tâches de protection en même temps, sans affecter les performances. Vous pouvez avoir un impact certain sur les performances lorsque vous exécutez simultanément entre 11 et 30 tâches. Il n'est pas recommandé d'exécuter plus de 30 tâches simultanément.

Étapes

1. Dans l'onglet **protection** de la page de détails **Santé/Volume**, cliquez avec le bouton droit de la souris dans la vue topologique sur le nom d'un volume que vous souhaitez protéger.
2. Sélectionnez **Protect** > **SnapMirror** dans le menu.

   La boîte de dialogue configurer la protection s'affiche.

3. Cliquez sur **SnapMirror** pour afficher l'onglet **SnapMirror** et configurer les informations de destination.
4. Cliquez sur **Avancé** pour définir la garantie d'espace, selon les besoins, puis cliquez sur **appliquer**.
5. Renseignez la zone **destination information** et la zone **Relationship Settings** de la boîte de dialogue **Configure protection**.
6. Cliquez sur **appliquer**.

   Vous revenez à la page Détails de l'état/volume.

7. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page **Santé/Volume**.

   Les tâches et les détails de la tâche s'affichent dans la page protection/Détails de la tâche.

8. Dans la page **protection/travail** details, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails de la tâche associée à la tâche de configuration de la protection et déterminer quand la tâche est terminée.
9. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails **Santé/Volume**.

   La nouvelle relation s'affiche dans la vue topologique de la page détaillée de l'état de santé/volume.

Résultats

En fonction du SVM de destination que vous avez spécifié lors de la configuration ou des options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut être l'une des variantes suivantes :

- Si vous avez spécifié un SVM de destination qui s'exécute sous la même version ou plus récente de ONTAP que celui du volume source, une relation SnapMirror basée sur la réplication de bloc est le résultat par défaut.
- Si vous avez spécifié un SVM de destination qui s'exécute sous la même version ou plus récente de ONTAP (version 8.3 ou supérieure) par rapport au volume source, mais que vous avez activé la réplication flexible de la version dans les paramètres avancés, une relation SnapMirror avec la réplication flexible de la version est résultat.
- Si vous avez spécifié un SVM de destination qui s'exécute sous une version antérieure de ONTAP 8.3 ou une version supérieure à celle du volume source et que la version précédente prend en charge la réplication flexible de la version, il s'agit du résultat automatique d'une relation SnapMirror avec la réplication flexible de la version.

Création d'une relation de protection SnapVault à partir de la page des détails intégrité/volume

Vous pouvez créer une relation SnapVault à l'aide de la page d'informations sur l'intégrité/le volume afin que les sauvegardes de données soient activées à des fins de protection sur des volumes.

Avant de commencer

- Vous devez avoir le rôle d'administrateur OnCommand ou d'administrateur du stockage.
- Vous devez avoir configuré Workflow Automation pour effectuer cette tâche.

Description de la tâche

Le menu **Protect** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le

cluster destination n’a pas encore été découvert

Étapes

1. Dans l’onglet **protection** de la page de détails **Santé/Volume**, cliquez avec le bouton droit de la souris sur un volume dans la vue topologique que vous souhaitez protéger.
2. Sélectionnez **protéger** > **SnapVault** dans le menu.

   La boîte de dialogue configurer la protection s’ouvre.

3. Cliquez sur **SnapVault** pour afficher l’onglet **SnapVault** et configurer les informations de ressource secondaire.
4. Cliquez sur **Advanced** pour définir la déduplication, la compression, la croissance automatique et la garantie d’espace selon les besoins, puis cliquez sur **Apply**.
5. Renseignez la zone **destination information** et la zone **Relationship Settings** de la boîte de dialogue **Configure protection**.
6. Cliquez sur **appliquer**.

   Vous revenez à la page Détails de l’état/volume.

7. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page **Santé/Volume**.

   La page protection/informations sur le travail s’affiche.

8. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de protection et déterminer quand la tâche est terminée.

   Une fois les tâches terminées, les nouvelles relations s’affichent dans la vue topologique de la page Détails de l’état/volume.

Création d’une règle SnapVault pour optimiser l’efficacité du transfert

Vous pouvez créer une nouvelle règle SnapVault afin de définir la priorité d’un transfert SnapVault. Vous utilisez des règles pour optimiser l’efficacité des transferts du stockage primaire au stockage secondaire dans une relation de protection.

Avant de commencer

- Vous devez avoir le rôle d’administrateur OnCommand ou d’administrateur du stockage.
- Vous devez avoir configuré Workflow Automation.
- Vous devez avoir déjà terminé la zone informations sur la destination dans la boîte de dialogue configurer la protection.

Étapes

1. Dans l’onglet **SnapVault** de la boîte de dialogue **configurer la protection**, cliquez sur le lien **Créer une stratégie** dans la zone **Paramètres de relation**.

L'onglet SnapVault s'affiche.

2. Dans le champ **Policy Name**, saisissez le nom que vous souhaitez attribuer à la stratégie.
3. Dans le champ **priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la stratégie.
4. Dans le champ **Commentaire**, entrez un commentaire pour la stratégie.
5. Dans la zone **Replication Label**, ajoutez ou modifiez une étiquette de réplication, selon les besoins.
6. Cliquez sur **Créer**.

   La nouvelle stratégie s'affiche dans la liste déroulante Créer une stratégie.

Création d'une règle SnapMirror pour optimiser l'efficacité du transfert

Vous pouvez créer une règle SnapMirror pour spécifier la priorité de transfert SnapMirror pour les relations de protection. Les règles SnapMirror vous permettent d'optimiser l'efficacité du transfert entre la source et la destination en définissant des priorités. De cette manière, les transferts avec priorité inférieure doivent être programmés pour s'exécuter après les transferts prioritaires.

Avant de commencer

- Vous devez avoir le rôle d'administrateur OnCommand ou d'administrateur du stockage.
- Vous devez avoir configuré Workflow Automation.
- Cette tâche suppose que vous avez déjà terminé la zone informations de destination dans la boîte de dialogue configurer la protection.

Étapes

1. Dans l'onglet **SnapMirror** de la boîte de dialogue **Configure protection**, cliquez sur le lien **Create Policy** dans la zone **Relationship Settings**.

   La boîte de dialogue Créer une règle SnapMirror s'affiche.

2. Dans le champ **Policy Name**, saisissez le nom que vous souhaitez attribuer à la stratégie.
3. Dans le champ **priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la stratégie.
4. Dans le champ **Commentaire**, entrez un commentaire facultatif pour la stratégie.
5. Cliquez sur **Créer**.

   La nouvelle règle s'affiche dans la liste déroulante SnapMirror Policy.

Création de planifications SnapMirror et SnapVault

Vous pouvez créer des planifications SnapMirror et SnapVault de base ou avancées pour activer les transferts automatiques sur un volume source ou primaire. Les transferts ont

ainsi lieu plus ou moins fréquemment, selon la fréquence à laquelle les données sont modifiées sur vos volumes.

Avant de commencer

- Vous devez avoir le rôle Administrateur OnCommand ou Administrateur stockage.
- Vous devez avoir déjà terminé la zone informations sur la destination dans la boîte de dialogue configurer la protection.
- Vous devez avoir configuré Workflow Automation pour effectuer cette tâche.

Étapes

1. Dans l'onglet **SnapMirror** ou **SnapVault** de la boîte de dialogue **configurer la protection**, cliquez sur le lien **Créer un programme** dans la zone **Paramètres de relation**.

   La boîte de dialogue Créer un programme s'affiche.

2. Dans le champ **Nom de l'horaire**, saisissez le nom que vous souhaitez donner à l'horaire.
3. Sélectionnez l'une des options suivantes :
   - **De base**

     Sélectionnez cette option si vous souhaitez créer une planification de base de style d'intervalle.

   - **Avancé**

     Sélectionnez cette option pour créer une planification de style cron.

4. Cliquez sur **Créer**.

   La nouvelle planification est affichée dans la liste déroulante planification SnapMirror ou planification SnapVault.

Informations sur le copyright

Copyright © 2024 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.