



# **Configuration et activation de la protection des données pilotée par des règles**

SnapManager Oracle

NetApp  
October 04, 2023

This PDF was generated from [https://docs.netapp.com/fr-fr/snapmanager-oracle/unix-administration/task\\_configuring\\_snapdrive\\_when\\_rbac\\_is\\_enabled.html](https://docs.netapp.com/fr-fr/snapmanager-oracle/unix-administration/task_configuring_snapdrive_when_rbac_is_enabled.html) on October 04, 2023. Always check docs.netapp.com for the latest.

# Sommaire

- Configuration et activation de la protection des données pilotée par des règles ..... 1
  - Configuration du serveur et de SnapDrive de DataFabric Manager lorsque le RBAC est activé ..... 1
  - Configuration d'SnapDrive lorsque le RBAC n'est pas activé ..... 2
  - Présentation de l'activation ou de la désactivation de la protection des données dans le profil ..... 2

# Configuration et activation de la protection des données pilotée par des règles

Vous devez configurer SnapDrive et le serveur DataFabric Manager pour activer la protection des données sur le profil afin de protéger les sauvegardes sur les systèmes de stockage secondaires. Vous pouvez sélectionner les règles de protection dans la console protection Manager pour spécifier comment les sauvegardes de bases de données seront protégées.



Vous devez vous assurer que OnCommand Unified Manager est installé sur un serveur distinct pour permettre la protection des données.

## Configuration du serveur et de SnapDrive de DataFabric Manager lorsque le RBAC est activé

Lorsque le contrôle d'accès basé sur des rôles (RBAC) est activé, vous devez configurer le serveur DataFabric Manager pour inclure les fonctionnalités RBAC. Vous devez également enregistrer l'utilisateur SnapDrive créé sur le serveur DataFabric Manager et l'utilisateur root du système de stockage dans SnapDrive.

1. Configurez le serveur DataFabric Manager.
  - a. Pour actualiser le serveur DataFabric Manager afin de mettre à jour les modifications effectuées directement sur le système de stockage par la base de données cible, entrez la commande suivante :`dfm host Discover Storage_system`
  - b. Créez un nouvel utilisateur sur le serveur DataFabric Manager et définissez le mot de passe.
  - c. Pour ajouter l'utilisateur du système d'exploitation à la liste d'administration du serveur DataFabric Manager, entrez la commande suivante :`dfm user add sd-admin`
  - d. Pour créer un nouveau rôle sur le serveur DataFabric Manager, entrez la commande suivante :`dfm role create sd-admin-role`
  - e. Pour ajouter la fonctionnalité DFM.Core.AccessCheck Global au rôle, entrez la commande suivante :`dfm role add sd-admin-role DFM.Core.AccessCheck Global`
  - f. Pour ajouter sd-admin-role à l'utilisateur du système d'exploitation, entrez la commande suivante :`dfm user role set sd-adminsd-admin-role`
  - g. Pour créer un autre rôle sur le serveur DataFabric Manager pour l'utilisateur root SnapDrive, entrez la commande suivante :`dfm role create SD-Protect`
  - h. Pour ajouter des fonctionnalités RBAC au rôle créé pour l'utilisateur root ou l'administrateur SnapDrive, entrez les commandes suivantes :`dfm role add sd-Protect SD.Config.Read Global``dfm role add sd-Protect SD.Config.Write Global``dfm role add sd-Protect SD.Config.Delete Global``dfm role add sd-Protect SD-Protect.DFM rôle.add-Protect`
  - i. Pour ajouter l'utilisateur oracle de la base de données cible à la liste des administrateurs du serveur DataFabric Manager et affecter le rôle sd-Protect, entrez la commande suivante :`dfm user add -r sd-protecttardb_host1\oracle`
  - j. Pour ajouter le système de stockage utilisé par la base de données cible dans le serveur DataFabric Manager, entrez la commande suivante :`dfm host set Storage_system hostLogin=oracle`

hostPassword=password

- k. Pour créer un nouveau rôle dans le système de stockage utilisé par la base de données cible sur le serveur DataFabric Manager, entrez la commande suivante : `dfm host role create -h Storage_system-c « api-,login- » Storage-rbac-role`
- l. Pour créer un nouveau groupe dans le système de stockage et attribuer le nouveau rôle créé sur le serveur DataFabric Manager, entrez la commande suivante : `dfm host usergroup create -h Storage_system-r Storage-rbac-roleStorage-rbac-group-rbac-group`
- m. Pour créer un nouvel utilisateur dans le système de stockage et affecter le nouveau rôle et le groupe créé sur le serveur DataFabric Manager, entrez la commande suivante : `dfm host utilisateur create -h Storage_system-r Storage-rbac-role -p password -g Storage-rbac-groupardb_host1`

## 2. Configurez SnapDrive.

- a. Pour enregistrer les identifiants de l'utilisateur sd-admin avec SnapDrive, entrez la commande suivante : `snapdrive config set -dfm sd-admin dfm_host`
- b. Pour enregistrer l'utilisateur root ou l'administrateur du système de stockage avec SnapDrive, entrez la commande suivante : `snapdrive config set tadb_host_modifier_System`

## Configuration d'SnapDrive lorsque le RBAC n'est pas activé

Pour assurer la protection des données, vous devez enregistrer l'utilisateur root ou l'administrateur du serveur DataFabric Manager et l'utilisateur root du système de stockage avec SnapDrive.

1. Pour actualiser le serveur DataFabric Manager afin de mettre à jour les modifications effectuées directement sur le système de stockage par la base de données cible, entrez la commande suivante :

l'hôte dfm détecte storage\_system

2. Pour enregistrer l'utilisateur root ou l'administrateur du serveur DataFabric Manager avec SnapDrive, entrez la commande suivante :

SnapDrive config set -dfm Administratidfm\_host

3. Pour enregistrer l'utilisateur root ou l'administrateur du système de stockage avec SnapDrive, entrez la commande suivante :

config SnapDrive set root storage\_system

## Présentation de l'activation ou de la désactivation de la protection des données dans le profil

Vous pouvez activer ou désactiver la protection des données lors de la création ou de la mise à jour d'un profil de base de données.

Pour créer une sauvegarde protégée d'une base de données sur les ressources de stockage secondaires, les administrateurs de base de données et les administrateurs du stockage effectuent les actions suivantes.

Les fonctions que vous recherchez...	Alors...
<p>Créez ou modifiez un profil</p>	<p>Pour créer ou modifier un profil, procédez comme suit :</p> <ul style="list-style-type: none"> <li>• Protection des sauvegardes sur le système de stockage secondaire</li> <li>• Si vous utilisez Data ONTAP sous 7-mode et que vous avez installé protection Manager, vous pouvez sélectionner les règles créées par l'administrateur du stockage ou des sauvegardes dans protection Manager.</li> </ul> <p>Si vous utilisez Data ONTAP sous 7-mode et que la protection est activée, SnapManager crée un jeu de données pour la base de données. Un jeu de données se compose d'un ensemble de jeux de données de stockage, ainsi que d'informations de configuration associées à leurs données. Les jeux de données associés à un jeu de données incluent un jeu de stockage principal utilisé pour exporter les données vers les clients, ainsi que l'ensemble des répliques et des archives qui existent sur d'autres jeux de stockage. Les jeux de données représentent des données utilisateur exportables. Si l'administrateur désactive la protection d'une base de données, SnapManager supprime le jeu de données.</p> <ul style="list-style-type: none"> <li>• Si vous utilisez ONTAP, vous devez sélectionner la stratégie <i>SnapManager_cdot_Mirror</i> ou <i>SnapManager_cdot_Vault</i> en fonction de la relation SnapMirror ou SnapVault créée.</li> </ul> <p>Lorsque vous désactivez la protection de sauvegarde, un message d'avertissement s'affiche indiquant que le jeu de données sera supprimé et que la restauration ou le clonage des sauvegardes de ce profil ne sera pas possible.</p>
<p>Afficher le profil</p>	<p>Comme l'administrateur du stockage n'a pas encore affecté de ressources de stockage pour mettre en œuvre la règle de protection, le profil apparaît comme un non-confortant dans l'interface graphique de SnapManager que dans la sortie de la commande <code>profile show</code>.</p>

Les fonctions que vous recherchez...	Alors...
Attribuez des ressources de stockage dans la console de gestion de protection Manager	Dans la console de gestion de protection Manager, l'administrateur du stockage affiche le jeu de données non protégé et attribue un pool de ressources à chaque nœud du jeu de données associé au profil. L'administrateur du stockage s'assure ensuite que les volumes secondaires sont provisionnés et que les relations de protection sont initialisées.
Consultez le profil du répondant dans SnapManager	Dans SnapManager, l'administrateur de base de données constate que le profil a été modifié en état de conformité à la fois dans l'interface utilisateur graphique et dans la sortie de la commande profile show, ce qui indique que des ressources ont été affectées.
Créez la sauvegarde	<ul style="list-style-type: none"> <li>• Sélectionnez sauvegarde complète.</li> <li>• Indiquez également si la sauvegarde doit être protégée et sélectionnez la classe de rétention principale (par exemple, horaire ou quotidien).</li> <li>• Si vous utilisez Data ONTAP sous 7-mode et que vous souhaitez protéger immédiatement la sauvegarde sur un stockage secondaire, en ignorant la planification de protection de protection Manager, spécifiez l'option -protectnow.</li> <li>• Si vous utilisez ONTAP et que vous souhaitez protéger immédiatement la sauvegarde sur le stockage secondaire, spécifiez l'option protéger.</li> </ul> <div>  <p>L'option de protection n'est pas applicable dans clustered Data ONTAP.</p> </div>
Afficher la sauvegarde	La nouvelle sauvegarde est indiquée comme programmée pour la protection, mais pas encore protégée (dans l'interface SnapManager et dans la sortie de la commande backup show). L'État de protection est indiqué comme « non protégé ».
Afficher la liste des sauvegardes	Une fois que l'administrateur du stockage a vérifié que la sauvegarde a été copiée sur le stockage secondaire, SnapManager modifie l'état de protection de sauvegarde de « non protégé » à « protégé ».

## Informations sur le copyright

Copyright © 2023 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.