Contrôle d'accès basé sur des rôles dans SnapDrive pour UNIX

Snapdrive for Unix

NetApp
August 08, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/snapdrive-unix/aix/concept_what_rbac_in_snapdrive_for_unix_is.html on August 08, 2024. Always check docs.netapp.com for the latest.

Sommaire

Contrôle d’accès basé sur des rôles dans SnapDrive pour UNIX 1
À quoi correspond le contrôle d’accès basé sur des rôles (RBAC) dans SnapDrive for UNIX 1
Interaction de console avec SnapDrive pour UNIX et Operations Manager 2
Configuration du contrôle d’accès basé sur des rôles dans SnapDrive for UNIX 3
Fonctionnalités et commandes SnapDrive 8
Rôles préconfigurés pour faciliter la configuration des rôles utilisateur 11
Mise à jour automatique du système de stockage sur la console Operations Manager 12
Plusieurs serveurs console Operations Manager 12
Console Operations Manager indisponible 13
RBAC et exemples d’opérations de stockage 14

Contrôle d’accès basé sur des rôles dans SnapDrive pour UNIX

Le contrôle d’accès basé sur des rôles (RBAC) est utilisé pour la connexion des utilisateurs et les autorisations liées aux rôles. Le RBAC permet aux administrateurs de gérer des groupes d’utilisateurs en définissant des rôles. Si vous devez restreindre l’accès à la base de données à des administrateurs spécifiques, vous devez configurer des comptes d’administrateur pour eux. En outre, si vous souhaitez restreindre les informations, ces administrateurs peuvent les afficher et les opérations qu’ils peuvent effectuer, vous devez appliquer des rôles aux comptes d’administrateur que vous créez.

Le RBAC est utilisé dans SnapDrive for UNIX avec l’aide de la console Operations Manager. La console Operations Manager fournit un accès granulaire aux objets de stockage tels que les LUN, les qtrees, les volumes, les agrégats et les unités vFiler.

Informations connexes

Vérifications obligatoires du SnapRestore basé sur les volumes

Restauration de copies Snapshot sur un système de stockage de destination

Procédure de déconnexion par enclenchement

À quoi correspond le contrôle d’accès basé sur des rôles (RBAC) dans SnapDrive for UNIX

Les RBAC permettent aux administrateurs SnapDrive de restreindre l’accès à un système de stockage pendant différentes opérations SnapDrive. Ce niveau d’accès limité ou complet pour les opérations de stockage dépend du rôle attribué à l’utilisateur.

SnapDrive 4.0 pour UNIX et les versions ultérieures nécessitent une vérification d’accès RBAC pour toutes les opérations SnapDrive pour UNIX. Ce comportement permet aux administrateurs du stockage de limiter les opérations que les utilisateurs de SnapDrive peuvent effectuer en fonction de leurs rôles attribués. La fonction RBAC est implémentée à l’aide de l’infrastructure Operations Manager. Dans les versions antérieures à SnapDrive 4.0 pour UNIX, le contrôle d’accès était limité et seul l’utilisateur root pouvait exécuter des opérations SnapDrive pour UNIX. SnapDrive 4.0 pour UNIX et les versions ultérieures prennent en charge les utilisateurs locaux non racines et les utilisateurs de systèmes d’information réseau (NIS) via l’infrastructure RBAC de la console Operations Manager. SnapDrive pour UNIX ne nécessite pas le mot de passe root du système de stockage ; il communique avec le système de stockage en utilisant sd-<hostname> user.

Par défaut, la fonctionnalité RBAC de la console Operations Manager n’est pas utilisée. Vous devez activer la fonctionnalité RBAC en définissant la variable *`rbac-method=dfm`* dans le `snapdrive.conf` Et redémarrez le démon SnapDrive pour UNIX.

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser cette fonction :

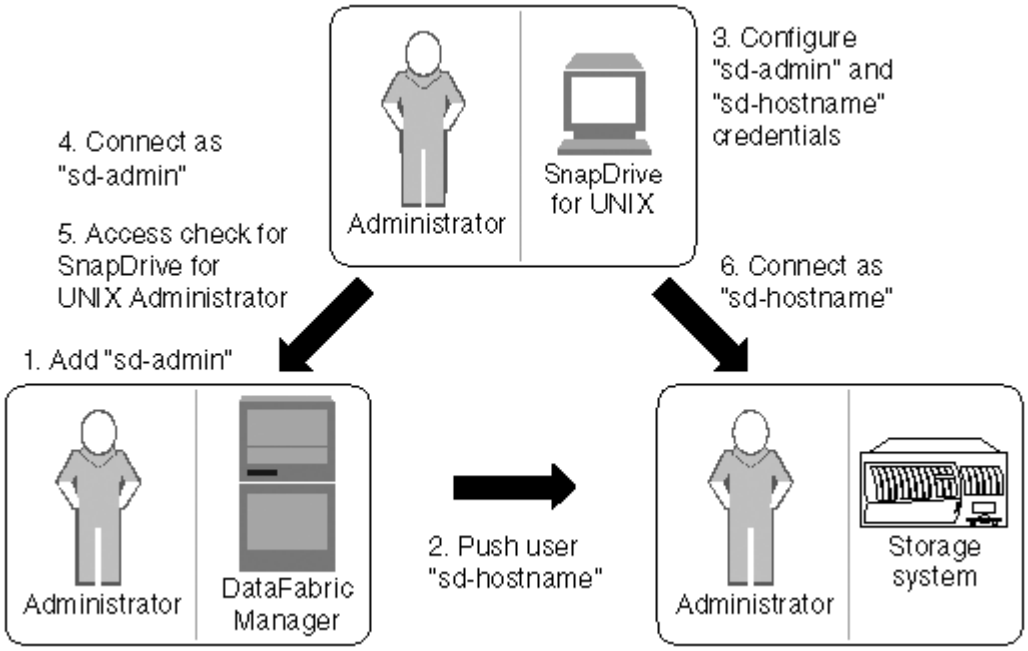
- Console Operations Manager 3.7 ou version ultérieure.
- Le serveur de console Operations Manager doit être présent et configuré sur le réseau IP qui contient les hôtes SnapDrive et les systèmes de stockage.

- Les paramètres de communication de la console Operations Manager doivent être configurés lors de l'installation de SnapDrive.
- Le démon SnapDrive pour UNIX doit être en cours d'exécution.

Interaction de console avec SnapDrive pour UNIX et Operations Manager

L'utilisation du contrôle d'accès basé sur des rôles (RBAC) dépend de l'infrastructure de la console Operations Manager. L'administrateur de la console Operations Manager doit créer des noms d'utilisateur pour SnapDrive à utiliser sous UNIX. Toutes les demandes d'opérations de stockage sont d'abord envoyées à la console Operations Manager pour un contrôle d'accès. Une fois que la console Operations Manager a vérifié une opération de stockage auprès d'un utilisateur SnapDrive spécifique, l'opération est terminée.

Le diagramme suivant illustre le RBAC complet pour les opérations de stockage.



1. L'administrateur de la console Operations Manager ajoute un utilisateur sd-admin sur la console Operations Manager.
2. L'administrateur de la console Operations Manager crée un utilisateur sd-hostname sur le système de stockage.
3. L'administrateur de la console Operations Manager envoie les informations d'identification sd-admin et sd-hostname à l'administrateur SnapDrive for UNIX.
4. L'administrateur SnapDrive configure SnapDrive avec les informations d'identification de l'utilisateur reçues.
5. La console Operations Manager effectue une vérification d'accès pour une utilisation sous SnapDrive UNIX avec les informations d'identification utilisateur ajoutées par l'administrateur SnapDrive.
6. Une fois l'utilisateur SnapDrive authentifié, l'utilisateur peut se connecter au système de stockage.

Lorsqu'un utilisateur SnapDrive souhaite effectuer une certaine opération de stockage, l'utilisateur émet la

commande correspondante sur la ligne de commande. La demande est envoyée à la console Operations Manager pour une vérification d'accès. La console Operations Manager vérifie si l'utilisateur requis dispose des autorisations appropriées pour effectuer l'opération SnapDrive. Le résultat du contrôle d'accès est renvoyé à SnapDrive. Selon le résultat, l'utilisateur est autorisé ou non à effectuer les opérations de stockage sur le système de stockage.

Si l'utilisateur est vérifié après la vérification d'accès, il se connecte au système de stockage en tant que nom d'hôte sd.

> sd-hostname et sd-admin sont les noms d'utilisateur recommandés. Vous pouvez configurer SnapDrive pour UNIX avec d'autres noms d'utilisateur.

Configuration du contrôle d'accès basé sur des rôles dans SnapDrive for UNIX

Vous devez effectuer diverses tâches afin de configurer le contrôle d'accès basé sur des rôles (RBAC) pour SnapDrive pour UNIX. Vous pouvez utiliser la console Operations Manager ou l'interface de ligne de commandes pour effectuer les tâches.

Configuration de sd-admin dans la console Operations Manager

L'administrateur de la console Operations Manager peut créer l'utilisateur sd-admin.

L'administrateur de la console Operations Manager crée un utilisateur nommé sd-admin, avec la possibilité d'effectuer un contrôle d'accès de base sur le groupe global (global) `DFM.Core.AccessCheck`). Une fois que l'administrateur de la console Operations Manager a configuré l'utilisateur sd-admin, vous devez envoyer manuellement les informations d'identification à l'administrateur SnapDrive for UNIX. Pour plus d'informations sur l'utilisation de la console Operations Manager pour configurer les utilisateurs et les rôles, reportez-vous au guide d'administration de la console *Operations Manager* et à l'aide en ligne.

> Vous pouvez utiliser n'importe quel nom à la place de sd-admin ; cependant, il est préférable d'utiliser sd-admin.

Pour créer un rôle dans la console Operations Manager, sélectionnez **Configuration** > **rôles**. Dans la page de configuration sd-admin, l'administrateur de la console Operations Manager doit affecter `DFM.Database.Write` Fonctionnalité du groupe global sur sd-admin-role, de sorte que SnapDrive for UNIX puisse actualiser les entités de stockage dans la console Operations Manager.

Configuration de sd-admin à l'aide de l'interface de ligne de commande

L'administrateur du système de stockage peut configurer l'utilisateur sd-admin à l'aide de l'interface de ligne de commande.

Étapes

1. Ajoutez un utilisateur nommé sd-admin.

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. Ajoutez un administrateur nommé sd-admin.

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. Créez un rôle nommé sd-admin-role.

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. Ajoutez une fonctionnalité au rôle créé à l'étape 3.

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. L'administrateur Operations Manager peut également accorder `DFM.Database.Write` capacité du groupe global à `<sd-admin>` Pour permettre à SnapDrive for UNIX de mettre à jour les entités du système de stockage dans Operations Manager.

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. Ajoutez un rôle sd-admin à l'utilisateur sd-admin.

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

Ajout du nom d'hôte sd au système de stockage

L'administrateur de la console Operations Manager peut créer l'utilisateur sd-hostname sur le système de stockage à l'aide de la console Operations Manager. Une fois les étapes terminées, l'administrateur de la console Operations Manager doit envoyer manuellement les informations d'identification à l'administrateur SnapDrive for UNIX. Vous pouvez utiliser n'importe quel nom à la place de sd-hostname ; cependant, il est

préférable d'utiliser sd-hostname.

Étapes

1. Obtenir le mot de passe root du système de stockage et stocker le mot de passe.

   Pour ajouter le mot de passe du système de stockage, sélectionnez **Management** > **Storage System**.

2. Créez un utilisateur sd-hostname pour chaque système UNIX.
3. Attribuer des fonctionnalités `api- et login-` à un rôle, tel que sd-role.
4. Inclure ce rôle (sd-role) dans un nouveau groupe d'utilisateurs, tel que sd-usergroup.
5. Associez ce groupe d'utilisateurs (sd-usergroup) à l'utilisateur sd-hostname sur le système de stockage.

Ajout du nom d'hôte sd au système de stockage à l'aide de l'interface de ligne de commande

L'administrateur du système de stockage peut créer et configurer l'utilisateur sd-hostname à l'aide de la commande useradmin.

Étapes

1. Ajouter du stockage.

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. Définissez le mot de passe de l'hôte.

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

3. Créer un rôle sur l'hôte.

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. Créez un groupe d'utilisateurs.

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. Créez un utilisateur local.

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

Configuration des informations d'identification utilisateur sous SnapDrive for UNIX

L'administrateur SnapDrive pour UNIX reçoit les informations d'identification de l'utilisateur de l'administrateur de la console Operations Manager. Ces identifiants utilisateur doivent être configurés sur SnapDrive pour UNIX afin que les opérations de stockage soient correctes.

Étapes

1. Configurez sd-admin sur le système de stockage.

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. Configurez sd-hostname sur le système de stockage.

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. Vérifier les étapes 1 et 2 à l'aide du `snapdrive config list` commande.

```
user name       appliance name          appliance type
-------------------------------------------------------
sd-admin        ops_mngr_server         DFM
sd-unix_host    storage_array1          StorageSystem
```

4. Configurer SnapDrive pour UNIX afin d'utiliser le contrôle d'accès basé sur des rôles (RBAC) sur la console Operations Manager en définissant la variable de configuration `rbac-method="dfm"` dans le `snapdrive.conf` fichier.

> Les informations d'identification de l'utilisateur sont cryptées et enregistrées dans l'existant `.sdupw` fichier. L'emplacement par défaut du fichier précédent est `/opt/NetApp/snapdrive/.sdupw`.

Formats de noms d'utilisateur pour effectuer des contrôles d'accès avec la console Operations Manager

SnapDrive for UNIX utilise les formats de noms d'utilisateur pour effectuer des contrôles d'accès via la console Operations Manager. Ces formats varient selon que vous êtes un système d'information réseau (NIS) ou un utilisateur local.

SnapDrive pour UNIX utilise les formats suivants pour vérifier si un utilisateur est autorisé à effectuer certaines tâches :

- Si vous êtes un utilisateur NIS exécutant le `snapdrive` SnapDrive for UNIX utilise le format de la commande `<nisdomain>\<username>` (par exemple, `netapp.com\marc`)
- Si vous êtes un utilisateur local d'un hôte UNIX tel que lnx197-141, SnapDrive for UNIX utilise le format `<hostname>\<username>` format (par exemple, `lnx197-141\john`)
- Si vous êtes administrateur (root) d'un hôte UNIX, SnapDrive pour UNIX traite toujours l'administrateur comme un utilisateur local et utilise le format `lnx197-141\root`.

Les variables de configuration pour le contrôle d'accès basé sur des rôles

Vous devez définir les différentes variables de configuration associées au contrôle d'accès basé sur les rôles dans le `snapdrive.conf` fichier.

Variable	Description
`contact-http-dfm-port = 8088`	Spécifie le port HTTP à utiliser pour communiquer avec un serveur de console Operations Manager. La valeur par défaut est 8088.
`contact-ssl-dfm-port = 8488`	Spécifie le port SSL à utiliser pour communiquer avec un serveur de console Operations Manager. La valeur par défaut est 8488.
`rbac-method=dfm`	Spécifie les méthodes de contrôle d'accès. Les valeurs possibles sont `native` et `dfm`. Si la valeur est de `native`, le fichier de contrôle d'accès stocké dans `/vol/vol0/sdprbac/sdhost-name.prbac` est utilisé pour les vérifications d'accès. Si la valeur est définie sur `dfm`, La console Operations Manager est un prérequis. Dans ce cas, SnapDrive for UNIX envoie des vérifications d'accès à la console Operations Manager.

Variable	Description
rbac-cache=on	SnapDrive pour UNIX conserve un cache de requêtes de vérification d'accès et les résultats correspondants. SnapDrive for UNIX utilise ce cache uniquement lorsque tous les serveurs de console Operations Manager configurés sont en panne. Vous pouvez définir cette valeur sur l'une ou l'autre `on` pour activer le cache, ou à `off` pour le désactiver. La valeur par défaut est désactivée pour que vous puissiez configurer SnapDrive pour UNIX afin qu'il utilise la console Operations Manager et définir le `rbac-method` variable de configuration à `dfm`.
rbac-cache-timeout	Spécifie la période d'expiration du cache rbac et ne s'applique que lorsque *`rbac-cache`* est activé. La valeur par défaut est `24` heures SnapDrive for UNIX utilise ce cache uniquement lorsque tous les serveurs de console Operations Manager configurés sont en panne.
use-https-to-dfm=on	Cette variable vous permet de configurer SnapDrive pour UNIX afin qu'il utilise le cryptage SSL (HTTPS) lorsqu'il communique avec la console Operations Manager. La valeur par défaut est `on`.

Fonctionnalités et commandes SnapDrive

Le contrôle d'accès basé sur des rôles (RBAC) requiert une fonctionnalité spécifique pour réussir chaque opération. Les capacités affectées à l'exécution des opérations de stockage doivent être correctes.

Le tableau suivant répertorie les commandes et les fonctionnalités requises :

Commande	Fonctionnalité
`storage show`	SD.Storage.Lire sur le volume
`storage list`	SD.Storage.Lire sur le volume
`storage create`	• Pour les LUN dans les volumes : `SD.Storage.Write` Sur le volume • Pour les LUN dans les qtrees : `SD.Storage.Write` sur qtree
`storage resize`	`SD.Storage.Write` Sur la LUN

Commande	Fonctionnalité
`storage delete`	`SD.Storage.Delete` Sur la LUN
`snap show`	`SD.SnapShot.Read` sur le volume
`snap list`	`SD.SnapShot.Read` sur le volume
`snap delete`	`SD.Storage.Delete` sur le volume
`snap rename`	`SD.Storage.Write` sur le volume
`snap connect`	• Pour les clones de LUN dans le volume : `SD.SnapShot.Clone` sur le volume • Pour les clones LUN dans qtree : `SD.SnapShot.Clone` sur qtree • Pour les clones de volumes traditionnels : `SD.SnapShot.Clone` sur le système de stockage • Pour un volume FlexClone : `SD.SnapShot.Clone` sur le volume parent • Pour les volumes FlexClone sans restriction : `SD.SnapShot.UnrestrictedClone` sur le volume parent
`snap connect-split`	• Pour les clones de LUN (LUN clonée et répartition dans le volume) : `SD.SnapShot.Clone` sur le volume et `SD.Storage.Write` sur le volume • Pour les clones de LUN (LUN clonée et Split dans qtree) : `SD.SnapShot.Clone` sur les qtrees et `SD.Storage.Write` sur qtree • Pour les clones de volumes traditionnels qui sont répartis : `SD.SnapShot.Clone` sur le système de stockage et `SD.Storage.Write` sur le système de stockage • Pour les clones de volume Flex qui sont répartis : `SD.SnapShot.Clone` sur le volume parent.
`clone split start`	• Pour les clones LUN où réside la LUN dans le volume ou qtree : `SD.SnapShot.Clone` contenant un volume ou un qtree • Pour les clones de volumes : `SD.SnapShot.Clone` sur le volume parent

Commande	Fonctionnalité
`snap disconnect`	• Pour les clones LUN où réside la LUN dans le volume ou qtree : `SD.SnapShot.Clone` contenant un volume ou un qtree • Pour les clones de volumes : `SD.SnapShot.Clone` sur le volume parent • Pour la suppression de clones de volumes sans restriction : `SD.SnapShot.DestroyUnrestrictedClone` sur le volume
`snap disconnect-split`	• Pour les clones LUN où réside la LUN dans le volume ou qtree : `SD.SnapShot.Clone` sur le volume ou qtree contenant • Pour les clones de volumes : `SD.Storage.Delete` sur le volume parent • Pour la suppression de clones de volumes sans restriction : `SD.SnapShot.DestroyUnrestrictedClone` sur le volume
`snap restore`	• Pour les LUN qui existent dans un volume : `SD.SnapShot.Restore` sur le volume et `SD.Storage.Write` Sur la LUN • Pour les LUN qui existent dans un qtree : `SD.SnapShot.Restore` sur les qtrees et `SD.Storage.Write` Sur la LUN • Pour les LUN qui ne figurent pas dans les volumes : `SD.SnapShot.Restore` sur le volume et `SD.Storage.Write` sur le volume • Pour les LUN qui ne sont pas dans le qtree : `SD.SnapShot.Restore` sur les qtrees et `SD.Storage.Write` sur qtree • Pour les volumes : `SD.SnapShot.Restore` sur un système de stockage pour les volumes traditionnels, ou `SD.SnapShot.Restore` cet agrégat permet de traiter des volumes flexibles • Pour la restauration Snapshot de fichiers uniques dans les volumes : `SD.SnapShot.Restore` sur le volume • Pour la restauration Snapshot d'un seul fichier dans qtree : `SD.SnapShot.Restore` qtree • Pour ignorer les copies Snapshot de base : `SD.SnapShot.DisruptBaseline` sur le volume

Commande	Fonctionnalité
`host connect`, `host disconnect`	`SD.Config.Write` Sur la LUN
`config access`	`SD.Config.Read` sur le système de stockage
`config prepare`	`SD.Config.Write` sur au moins un système de stockage
`config check`	`SD.Config.Read` sur au moins un système de stockage
`config show`	`SD.Config.Read` sur au moins un système de stockage
`config set`	`SD.Config.Write` sur le système de stockage
`config set -dfm`, `config set -mgmtpath`,	`SD.Config.Write` sur au moins un système de stockage
`config delete`	`SD.Config.Delete` sur le système de stockage
`config delete dfm_appliance`, `config delete -mgmtpath`	`SD.Config.Delete` sur au moins un système de stockage
`config list`	`SD.Config.Read` sur au moins un système de stockage
`config migrate set`	`SD.Config.Write` sur au moins un système de stockage
`config migrate delete`	`SD.Config.Delete` sur au moins un système de stockage
`config migrate list`	`SD.Config.Read` sur au moins un système de stockage

SnapDrive pour UNIX ne vérifie aucune capacité pour l'administrateur (root).

Rôles préconfigurés pour faciliter la configuration des rôles utilisateur

Les rôles préconfigurés simplifient l'attribution de rôles aux utilisateurs.

Le tableau suivant répertorie les rôles prédéfinis :

Nom du rôle	Description
GlobalSDStorage	Gestion du stockage avec SnapDrive pour UNIX
GlobalSDConfig	Gérez les configurations avec SnapDrive pour UNIX
GlobalSDSnapshot	Gestion des copies Snapshot avec SnapDrive pour UNIX
GlobalSDFullControl	Utilisation complète de SnapDrive pour UNIX

Dans le tableau précédent, Global fait référence à tous les systèmes de stockage gérés par une console Operations Manager.

Mise à jour automatique du système de stockage sur la console Operations Manager

La console Operations Manager détecte les systèmes de stockage pris en charge sur votre réseau. Il surveille régulièrement les données collectées à partir des systèmes de stockage découverts. Les données sont actualisées à un intervalle défini. L'administrateur de la console Operations Manager peut configurer l'intervalle d'actualisation.

Intervalle de surveillance des LUN, intervalle de surveillance des qtrees et intervalle de surveillance vFiler sont des champs importants qui déterminent la fréquence des mises à jour de LUN, qtree et vFiler. Par exemple, si une nouvelle LUN est créée sur un système de stockage, la nouvelle LUN n'est pas immédiatement mise à jour sur la console Operations Manager. C'est pour cette raison que la vérification d'accès émise à la console d'Operations Manager pour cette LUN vers la console d'Operations Manager échoue. Pour éviter cette situation, vous pouvez modifier l'intervalle de surveillance des LUN en fonction de vos besoins.

1. Sélectionnez **Setup** > **Options** dans la console Operations Manager pour modifier l'intervalle de surveillance.
2. L'administrateur de la console Operations Manager peut également actualiser la console Operations Manager avec force `dfm host discovery filername` dans l'interface de ligne de commande.
3. L'administrateur de la console Operations Manager peut également accorder des droits `DFM.Database.Write` Fonctionnalité du groupe global sur sd-admin pour permettre à SnapDrive for UNIX d'actualiser les entités du système de stockage sur la console Operations Manager.

   ```
   # dfm role add sd-admin-role DFM.Database.Write Global
   Added 1 capability to role sd-admin-role.
   ```

Plusieurs serveurs console Operations Manager

SnapDrive pour UNIX prend en charge plusieurs serveurs console Operations Manager. Cette fonctionnalité est requise lorsqu'un groupe de systèmes de stockage est géré par

plusieurs serveurs de console Operations Manager. SnapDrive for UNIX contacte les serveurs de console Operations Manager dans le même ordre que les serveurs de console Operations Manager sont configurés dans SnapDrive for UNIX. Vous pouvez exécuter le `snapdrive config list` pour obtenir l'ordre de configuration.

L'exemple suivant montre les valeurs de sortie de plusieurs serveurs console Operations Manager :

```
# snapdrive config list
username    appliance name     appliance type
----------------------------------------------
root        storage_array1     StorageSystem
root        storage_array2     StorageSystem
sd-admin    ops_mngr_server1   DFM
sd-admin    ops_mngr_server2   DFM
```

Dans l'exemple précédent, Storage_array1 est géré par OPS_mngr_server1 et Storage_array2 est géré par OPS_mngr_server2. Dans cet exemple, SnapDrive pour UNIX contacte en premier lieu OPS_mngr_server1. Si OPS_mngr_server1 ne peut pas déterminer l'accès, SnapDrive pour UNIX contacte OPS_mngr_server2.

SnapDrive pour UNIX ne contacte la deuxième console Operations Manager que dans les conditions suivantes :

- Lorsque la première console Operations Manager ne parvient pas à déterminer l'accès. Ce cas de figure peut survenir, car la première console Operations Manager ne gère pas le système de stockage.
- Lorsque la première console Operations Manager est inactive.

Console Operations Manager indisponible

SnapDrive pour UNIX a besoin d'une console Operations Manager pour effectuer des vérifications d'accès. Parfois, il est possible que le serveur de console Operations Manager ne soit pas disponible pour différentes raisons.

Lorsque la méthode RBAC *`rbac-method = dfm`* Est défini et la console Operations Manager n'est pas disponible, SnapDrive pour UNIX affiche le message d'erreur suivant :

```
[root]# snapdrive storage delete -lun storage_array1:/vol/vol2/qtree1/lun1
0002-333 Admin error: Unable to connect to the DFM ops_mngr_server
```

SnapDrive pour UNIX peut également gérer un cache des résultats du contrôle d'accès utilisateur renvoyés par la console Operations Manager. Ce cache est valide pendant 24 heures et n'est pas configurable. Si la console Operations Manager n'est pas disponible, SnapDrive for UNIX utilise le cache pour déterminer l'accès. Ce cache est utilisé uniquement lorsque tous les serveurs de console Operations Manager configurés ne répondent pas.

Pour que SnapDrive pour UNIX puisse utiliser le cache pour une vérification d'accès, vous devez activer le *`rbac-cache`* la variable de configuration doit être activée pour conserver le cache des résultats d'accès. Le *`rbac-cache`* la variable de configuration est désactivée par défaut.

Pour utiliser SnapDrive pour UNIX même lorsque la console Operations Manager n'est pas disponible, l'administrateur du serveur doit réinitialiser la méthode de contrôle d'accès basé sur des rôles (RBAC) sur *`rbac-method = native`* dans le `snapdrive.conf` fichier. Après avoir modifié le `snapdrive.conf` File, vous devez redémarrer le démon SnapDrive pour UNIX. Quand *`rbac-method = native`* Est défini, seul l'utilisateur root peut utiliser SnapDrive pour UNIX.

RBAC et exemples d'opérations de stockage

Le contrôle d'accès basé sur des rôles permet les opérations de stockage en fonction des capacités qui vous sont attribuées. Vous recevez un message d'erreur si vous ne disposez pas des capacités nécessaires pour effectuer l'opération de stockage.

Opération avec une seule spécification de fichier sur un seul objet de stockage

SnapDrive pour UNIX affiche un message d'erreur lorsque vous n'êtes pas un utilisateur autorisé à créer une spécification de fichier sur un volume spécifié.

Filespec : filespec peut être un système de fichiers, un volume hôte, un groupe de disques ou une LUN.

```
[john]$ snapdrive storage create -fs /mnt/testfs -filervol
storage_array1:/vol/vol1 -dgsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

Dans cet exemple, John est un utilisateur non root et n'est pas autorisé à créer une spécification de fichier sur le volume spécifié. John doit demander à l'administrateur de la console Operations Manager d'accorder une subvention `SD.Storage.Write` accès sur le volume `storage_array1:/vol/vol1`.

Opération avec une seule spécification de fichier sur plusieurs objets de stockage

SnapDrive pour UNIX affiche un message d'erreur lorsque l'administrateur ne dispose pas de l'autorisation requise sur plusieurs objets de stockage pour effectuer les opérations de stockage.

Filespec : spécif de fichier peut être n'importe quel système de fichiers, volume hôte, groupe de disques ou LUN

```
[root]# snapdrive storage create -fs /mnt/testfs -lun
storage_array1:/vol/vol1/lun2 -lun storage_array1:/vol/vol2/lun2  -lunsize
100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
unix_host\root on Operations Manager server ops_mngr_server
```

Dans cet exemple, les données de fichier s'étendent sur deux volumes du système de stockage, vol1 et vol2. L'administrateur (root) d'unix_host n'a pas `SD.Storage.Write` accès aux deux volumes. Par conséquent, SnapDrive pour UNIX affiche un message d'erreur pour chaque volume. Pour poursuivre `storage create`, L'administrateur (root) doit demander à l'administrateur de la console Operations Manager d'accorder une subvention `SD.Storage.Write` accès aux deux volumes.

Fonctionnement avec plusieurs objets de spécification de fichier et de stockage

L'exemple suivant montre le message d'erreur que vous recevrez lorsque vous n'êtes pas un utilisateur autorisé à effectuer l'opération spécifique.

```
[marc]$ snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array1:/vol/vol2/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user nis_domain\marc on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
nis_domain\marc on Operations Manager server ops_mngr_server
```

Dans cet exemple, trois LUN résident sur deux volumes du système de stockage, vol1 et vol2. L'utilisateur Marc appartient à nis_domain et n'est pas autorisé à créer des spécif de fichier sur vol1 et vol2. SnapDrive pour UNIX affiche les deux messages d'erreur dans l'exemple précédent. Les messages d'erreur indiquent que l'utilisateur doit avoir `SD.Storage.Write` accès sur vol1 et vol2.

Fonctionnement avec plusieurs objets de stockage

L'exemple suivant montre le message d'erreur que vous recevrez lorsque vous n'êtes pas un utilisateur autorisé à effectuer l'opération spécifique.

```
[john]$ snapdrive storage show -all

Connected LUNs and devices:

device filename   adapter  path  size  proto  state  clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----  -----  --------
---------------
/dev/sdao            -     -     200m  iscsi  online  No
storage_array1:/vol/vol2/passlun1           -
/dev/sda1            -     -     200m  fcp    online  No
storage_array1:/vol/vol2/passlun2           -

Host devices and file systems:

dg: testfs1_SdDg                dgtype lvm
hostvol: /dev/mapper/testfs1_SdDg-testfs1_SdHv  state: AVAIL
fs: /dev/mapper/testfs1_SdDg-testfs1_SdHv       mount point: /mnt/testfs1
(persistent) fstype jfs2

device filename   adapter  path  size  proto  state   clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----   -----  --------
---------
/dev/sdn             -      P    108m  iscsi  online   No
storage_array1:/vol/vol2/testfs1_SdLun         -
/dev/sdn1             -      P    108m  fcp  online   No
storage_array1:/vol/vol2/testfs1_SdLun1         -

0002-719 Warning: SD.Storage.Read access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

John est autorisé à répertorier les entités de stockage sur vol2, mais pas sur vol1. SnapDrive pour UNIX affiche les entités de vol1 et affiche un message d'avertissement pour vol2.

> Pour `storage list`, `storage show`, `snap list`, et `snap show` Commandes SnapDrive pour UNIX affiche un avertissement au lieu de l'erreur.

Utilisation de plusieurs serveurs console Operations Manager gérant les systèmes de stockage

Le résultat suivant affiche un message d'erreur que vous recevrez lorsque les systèmes de stockage sont gérés par plusieurs console Operations Manager.

```
[root]# snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array2:/vol/vol1/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server1
SD.Storage.Write access denied on volume storage_array2:/vol/vol1 for user
unix_host\root on Operations Manager server ops_mngr_server2
```

storage_array1 est géré par ops_mngr_server1 et storage_array2 est géré par ops_mngr_server2. L'administrateur d'unix_host n'est pas autorisé à créer des fichiers pour Storage_array1 et Storage_array2. Dans l'exemple précédent, SnapDrive for UNIX affiche la console Operations Manager utilisée pour déterminer les accès.

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.