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

Snapdrive for Unix

NetApp
August 08, 2024

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

Sommaire

Configuration du contrôle d’accès basé sur des rôles dans SnapDrive for UNIX 1
Configuration de sd-admin dans la console Operations Manager 1
Ajout du nom d’hôte sd au système de stockage 2
Configuration des informations d’identification utilisateur sous SnapDrive for UNIX 4
Formats de noms d’utilisateur pour effectuer des contrôles d’accès avec la console Operations Manager . . 4
Les variables de configuration pour le contrôle d’accès basé sur des rôles 5

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`.

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.