



Contrôle d'accès dans SnapDrive pour UNIX

Snapdrive for Unix

NetApp

October 04, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/snapdrive-unix/aix/concept_what_access_control_settings_are.html on October 04, 2023. Always check docs.netapp.com for the latest.

Sommaire

- Contrôle d'accès dans SnapDrive pour UNIX 1
 - Quels sont les paramètres du contrôle d'accès 1
 - Niveaux de contrôle d'accès disponibles 2
 - Configuration de l'autorisation de contrôle d'accès 2
 - Affichage de l'autorisation de contrôle d'accès 3

Contrôle d'accès dans SnapDrive pour UNIX

SnapDrive pour UNIX vous permet de contrôler le niveau d'accès de chaque hôte à chaque système de stockage auquel l'hôte est connecté.

Le niveau d'accès dans SnapDrive pour UNIX indique quelles opérations l'hôte est autorisé à effectuer lorsqu'il cible un système de stockage donné. À l'exception des opérations d'affichage et de liste, les autorisations de contrôle d'accès peuvent affecter toutes les opérations de snapshot et de stockage.

Quels sont les paramètres du contrôle d'accès

Pour déterminer l'accès utilisateur, SnapDrive for UNIX vérifie l'un des deux fichiers d'autorisation dans le volume racine du système de stockage. Vous devez vérifier les règles définies dans ces fichiers pour évaluer le contrôle d'accès.

- `sdhost-name.prbac` le fichier se trouve dans le répertoire `/vol/vol0/sdprbac` (Contrôle d'accès basé sur des rôles avec autorisations SnapDrive).

Le nom de fichier est `sdhost-name.prbac`, où *host-name* est le nom de l'hôte auquel s'appliquent les autorisations. Vous pouvez avoir un fichier d'autorisations pour chaque hôte connecté au système de stockage. Vous pouvez utiliser le `snapdrive config access` commande permettant d'afficher des informations sur les autorisations disponibles pour un hôte sur un système de stockage spécifique.

Si le `sdhost-name.prbac` n'existe pas, utilisez ensuite le `sdgeneric.prbac` fichier pour vérifier les autorisations d'accès.

- `sdgeneric.prbac` le fichier se trouve également dans le répertoire `/vol/vol0/sdprbac`.

Nom du fichier `sdgeneric.prbac` est utilisé comme paramètres d'accès par défaut pour plusieurs hôtes qui n'ont pas accès à `sdhost-name.prbac` fichier sur le système de stockage.

Si vous avez les deux `sdhost-name.prbac` et `sdgeneric.prbac` fichiers disponibles dans le `/vol/vol0/sdprbac` chemin d'accès, puis utilisez le `sdhost-name.prbac` pour vérifier les autorisations d'accès, cette opération écrase les valeurs indiquées pour `sdgeneric.prbac` fichier.

Si vous n'avez pas les deux `sdhost-name.prbac` et `sdgeneric.prbac` les fichiers, puis vérifiez la variable de configuration `all-access-if-rbac-unspecified` qui est défini dans le `snapdrive.conf` fichier.

La configuration manuelle du contrôle d'accès entre un hôte donné et une unité vFiler donnée est une opération. L'accès à partir d'un hôte donné est contrôlé par un fichier résidant dans le volume racine de l'unité vFiler affectée. Le fichier contient `/vol/<vfiler root volume>/sdprbac/sdhost-name.prbac`, où *host-name* est le nom de l'hôte affecté, tel que renvoyé par `gethostname(3)`. Vous devez vous assurer que ce fichier est lisible, mais pas inscriptible, à partir de l'hôte qui peut y accéder.



Pour déterminer le nom de l'hôte, exécutez le `hostname` commande.

Si le fichier est vide, illisible ou dans un format non valide, SnapDrive pour UNIX ne permet pas à l'hôte d'accéder à l'une des opérations.

Si le fichier est manquant, SnapDrive for UNIX vérifie la variable de configuration `all-access-if-rbac-`

unspecified dans le `snapdrive.conf` fichier. Si la variable est définie sur `on` (valeur par défaut), il permet aux hôtes d'accéder pleinement à toutes ces opérations sur ce système de stockage. Si la variable est définie sur `off`, SnapDrive pour UNIX refuse l'autorisation de l'hôte d'effectuer toutes les opérations régies par le contrôle d'accès sur ce système de stockage.

Niveaux de contrôle d'accès disponibles

SnapDrive pour UNIX fournit différents niveaux de contrôle d'accès aux utilisateurs. Ces niveaux d'accès sont liés aux copies Snapshot et aux opérations du système de stockage.

Vous pouvez définir les niveaux d'accès suivants :

- AUCUN - l'hôte n'a pas accès au système de stockage.
- SNAP CREATE—l'hôte peut créer des copies Snapshot.
- SNAP USE—l'hôte peut supprimer et renommer les copies Snapshot.
- SNAP ALL - l'hôte peut créer, restaurer, supprimer et renommer des copies Snapshot.
- SUPPRESSION DE LA FONCTION DE CRÉATION DE STOCKAGE - l'hôte peut créer, redimensionner et supprimer du stockage.
- UTILISATION DU STOCKAGE : l'hôte peut connecter et déconnecter le stockage, ainsi que réaliser une estimation de la répartition des clones et le démarrage par clone sur le stockage.
- TOUT LE STOCKAGE- l'hôte peut créer, supprimer, connecter et déconnecter le stockage, mais aussi réaliser une estimation du fractionnement du clone et le démarrage du fractionnement du clone sur le stockage.
- TOUS LES ACCÈS—l'hôte a accès à toutes les opérations SnapDrive pour UNIX ci-dessus.

Chaque niveau est distinct. Si vous spécifiez une autorisation pour certaines opérations uniquement, SnapDrive pour UNIX ne peut exécuter que ces opérations. Par exemple, si vous spécifiez L'UTILISATION DU STOCKAGE, l'hôte peut utiliser SnapDrive pour UNIX pour connecter et déconnecter le stockage, mais il ne peut pas effectuer d'autres opérations régies par les autorisations de contrôle d'accès.

Configuration de l'autorisation de contrôle d'accès

Vous pouvez configurer l'autorisation de contrôle d'accès dans SnapDrive for UNIX en créant un répertoire et un fichier spéciaux dans le volume racine du système de stockage.

Assurez-vous d'être connecté en tant qu'utilisateur racine.

Étapes

1. Créez le répertoire `sdprbac` dans le volume racine du système de stockage cible.

Pour rendre le volume racine accessible, vous pouvez monter le volume via NFS.

2. Créez le fichier d'autorisations dans le `sdprbac` répertoire. Assurez-vous que les affirmations suivantes sont vraies :
 - Le fichier doit être nommé `sdhost-name.prbac` où `nom-hôte` est le nom de l'hôte pour lequel vous spécifiez des autorisations d'accès.

- Le fichier doit être en lecture seule pour que SnapDrive pour UNIX puisse le lire, mais qu'il ne peut pas être modifié.

Pour donner l'autorisation d'accès dev-sun1 à un hôte, créez le fichier suivant sur le système de stockage : `/vol/vol1/sdprbac/sddev-sun1.prbac`

3. Définissez les autorisations dans le fichier pour cet hôte.

Vous devez utiliser le format suivant pour le fichier :

- Vous ne pouvez spécifier qu'un seul niveau d'autorisation. Pour donner à l'hôte un accès complet à toutes les opérations, entrez la chaîne TOUT ACCÈS.
- La chaîne d'autorisation doit être la première chose dans le fichier. Le format de fichier n'est pas valide si la chaîne d'autorisation n'est pas dans la première ligne.
- Les chaînes de permission ne sont pas sensibles à la casse.
- Aucun espace blanc ne peut précéder la chaîne d'autorisation.
- Aucun commentaire n'est autorisé.

Ces chaînes d'autorisation valides autorisent les niveaux d'accès suivants :

- AUCUN - l'hôte n'a pas accès au système de stockage.
- SNAP CREATE—l'hôte peut créer des copies Snapshot.
- SNAP USE—l'hôte peut supprimer et renommer les copies Snapshot.
- SNAP ALL - l'hôte peut créer, restaurer, supprimer et renommer des copies Snapshot.
- SUPPRESSION DE LA FONCTION DE CRÉATION DE STOCKAGE - l'hôte peut créer, redimensionner et supprimer du stockage.
- UTILISATION DU STOCKAGE : l'hôte peut connecter et déconnecter le stockage, ainsi que réaliser une estimation de la répartition des clones et le démarrage par clone sur le stockage.
- TOUT LE STOCKAGE- l'hôte peut créer, supprimer, connecter et déconnecter le stockage, mais aussi réaliser une estimation du fractionnement du clone et le démarrage du fractionnement du clone sur le stockage.
- TOUS LES ACCÈS—l'hôte a accès à toutes les opérations SnapDrive pour UNIX ci-dessus. Chacune de ces chaînes d'autorisation est discrète. Si vous spécifiez SNAP USE, l'hôte peut supprimer ou renommer les copies Snapshot, mais il ne peut pas créer de copies Snapshot, ni restaurer, ni effectuer d'opérations de provisionnement du stockage.

Quelles que soient les autorisations que vous avez définies, l'hôte peut effectuer des opérations d'affichage et de liste.

4. Vérifiez les autorisations d'accès en entrant la commande suivante :

```
snapdrive config access show filer_name
```

Affichage de l'autorisation de contrôle d'accès

Vous pouvez afficher les autorisations de contrôle d'accès en exécutant le `snapdrive config access show` commande.

Étapes

1. Exécutez le `snapdrive config access show` commande.

Cette commande a le format suivant : `snapdrive config access {show | list} filename`

Vous pouvez utiliser les mêmes paramètres, que vous saisissez ou non le `show` ou `list` version de la commande.

Cette ligne de commande vérifie le grille-pain du système de stockage pour déterminer les autorisations dont dispose l'hôte. En fonction de la sortie, les autorisations de l'hôte sur ce système de stockage SONT TOUTES SNAP.

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

Dans cet exemple, le fichier d'autorisations n'est pas sur le système de stockage, donc SnapDrive for UNIX vérifie la variable `all-access-if-rbac-unspecified` dans le `snapdrive.conf` fichier pour déterminer les autorisations dont dispose l'hôte. Cette variable est définie sur `activé`, ce qui équivaut à créer un fichier d'autorisations avec le niveau d'accès défini sur TOUS LES ACCÈS.

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

Cet exemple montre le type de message que vous recevez si aucun fichier d'autorisation n'est sur le gril-pain du système de stockage et la variable *all-access-if-rbac-unspecified* dans le `snapdrive.conf` le fichier est défini sur `off`.

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

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.