Fonctions de sécurité d'SnapDrive for UNIX

Snapdrive for Unix

NetApp
October 04, 2023

Sommaire

Fonctions de sécurité d’SnapDrive for UNIX

Avant d’utiliser SnapDrive pour UNIX, vous devez comprendre ses fonctions de sécurité et apprendre à y accéder.

Définition des fonctions de sécurité

SnapDrive pour UNIX offre certaines fonctionnalités qui vous permettent de travailler avec vous en toute sécurité. Ces fonctionnalités vous permettent de mieux contrôler l’hôte et l’hôte auxquels les utilisateurs peuvent effectuer des opérations sur un système de stockage.

Les fonctions de sécurité vous permettent d’effectuer les tâches suivantes :

- Configurez les autorisations de contrôle d’accès
- Spécifiez les informations de connexion pour les systèmes de stockage
- Préciser que SnapDrive pour UNIX utilise HTTPS

La fonction de contrôle d’accès vous permet de spécifier les opérations qu’un hôte exécutant SnapDrive pour UNIX peut effectuer sur un système de stockage. Vous définissez ces autorisations individuellement pour chaque hôte. En outre, pour permettre à SnapDrive for UNIX d’accéder à un système de stockage, vous devez fournir le nom de connexion et le mot de passe correspondant à ce système de stockage.

La fonction HTTPS vous permet de spécifier le cryptage SSL pour toutes les interactions avec le système de stockage via l’interface Manage ONTAP, y compris l’envoi des mots de passe. Ce comportement est le comportement par défaut dans SnapDrive 4.1 pour UNIX et versions ultérieures pour les hôtes AIX ; cependant, vous pouvez désactiver le cryptage SSL en modifiant la valeur de l' `use-https-to-filer` variable de configuration à `off`.

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 saisiez 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 grille-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 de connexion des systèmes de stockage

Un nom d'utilisateur ou un mot de passe permet à SnapDrive for UNIX d'accéder à chaque système de stockage. En plus d'être connecté en tant que root, la personne exécutant SnapDrive pour UNIX doit fournir le nom d'utilisateur ou le mot de passe approprié lorsque vous y êtes invité. Si une connexion est compromise, vous pouvez la supprimer et définir une nouvelle connexion utilisateur.

Vous avez créé le login utilisateur pour chaque système de stockage lors de sa configuration. Pour que SnapDrive pour UNIX puisse fonctionner avec le système de stockage, vous devez lui fournir ces informations de connexion. En fonction de ce que vous avez spécifié lors de la configuration des systèmes de stockage, chaque système de stockage peut utiliser le même identifiant ou une seule connexion.

SnapDrive pour UNIX stocke ces connexions et mots de passe sous une forme chiffrée sur chaque hôte. Vous pouvez spécifier que SnapDrive pour UNIX chiffre ces informations lorsqu'il communique avec le système de stockage en configurant le *`snapdrive.conf`* variable de configuration *`use-https-to-filer=on`*.

Spécification des informations de connexion

Vous devez spécifier les informations de connexion de l'utilisateur pour un système de stockage. En fonction de ce que vous avez spécifié lors de la configuration du système de stockage, chaque système de stockage peut utiliser le même nom d'utilisateur ou mot de passe, ou un nom d'utilisateur ou un mot de passe unique. Si tous les systèmes de stockage utilisent les mêmes informations de nom d'utilisateur ou de mot de passe, vous devez effectuer les opérations suivantes une fois. Si les systèmes de stockage utilisent des noms d'utilisateur ou des mots de passe uniques, vous devez répéter les étapes suivantes pour chaque système de stockage.

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

Étapes

1. Saisissez la commande suivante :

   `snapdrive config set` ***`user_name filename`*** **`[`**`filename…`**`]`**

   `user_name` correspond au nom d'utilisateur spécifié pour ce système de stockage lors de sa première configuration.

   `filename` est le nom du système de stockage.

   `[filename…]` définit que vous pouvez entrer plusieurs noms de système de stockage sur une ligne de commande s'ils ont tous le même nom d'utilisateur ou mot de passe. Vous devez entrer le nom d'au moins un système de stockage.

2. À l'invite, entrez le mot de passe, s'il y en a un.

   > Si aucun mot de passe n'a été défini, appuyez sur entrée (valeur nulle) lorsque vous êtes invité à saisir un mot de passe.

   Cet exemple définit un utilisateur appelé `root` pour un système de stockage appelé grille-pain :

```
# snapdrive config set `root` toaster
Password for root:
Retype Password:
```

Cet exemple définit un utilisateur appelé `root` pour trois systèmes de stockage :

```
# snapdrive config set root toaster oven broiler
Password for root:
Retype Password:
```

3. Si vous possédez un autre système de stockage avec un nom d'utilisateur ou un mot de passe différent, répétez ces étapes.

Vérification des noms d'utilisateur du système de stockage associés à SnapDrive pour UNIX

Vous pouvez vérifier le nom d'utilisateur SnapDrive pour UNIX associé à un système de stockage en exécutant le `snapdrive config list` commande.

Vous devez vous connecter en tant qu'utilisateur root.

Étapes

1. Saisissez la commande suivante :

   `snapdrive config list`

   Cette commande affiche les paires de nom d'utilisateur ou de système de stockage pour tous les systèmes ayant des utilisateurs spécifiés dans SnapDrive pour UNIX. Elle n'affiche pas les mots de passe des systèmes de stockage.

   Cet exemple présente les utilisateurs associés aux systèmes de stockage appelés raiponce et le système de stockage moyen format :

```
# snapdrive config list
user name           storage system name
-----------------------------
rumplestiltskins    rapunzel
longuser            mediumstoragesystem
```

Suppression d'une connexion utilisateur pour un système de stockage

Vous pouvez supprimer une connexion utilisateur pour un ou plusieurs systèmes de stockage en exécutant le `snapdrive config delete` commande.

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

Étapes

1. Saisissez la commande suivante :

   ```
   snapdrive config delete appliance_name [appliance_name]
   ```

   appliance_name est le nom du système de stockage pour lequel vous souhaitez supprimer les informations de connexion de l'utilisateur.

   SnapDrive pour UNIX supprime les informations de connexion au nom d'utilisateur ou au mot de passe des systèmes de stockage que vous avez spécifiés.

   > Pour permettre à SnapDrive pour UNIX d'accéder au système de stockage, vous devez spécifier un nouveau login utilisateur.

Configuration de HTTP

Vous pouvez configurer SnapDrive pour UNIX afin qu'il utilise HTTP pour votre plate-forme hôte.

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

Étapes

1. Faire une sauvegarde du `snapdrive.conf` fichier.
2. Ouvrez le `snapdrive.conf` fichier dans un éditeur de texte.
3. Modifiez la valeur de *use-https-to-filer* variable à `off`.

   Une bonne pratique à chaque fois que vous modifiez le `snapdrive.conf` le fichier doit effectuer les opérations suivantes :

   a. Faites un commentaire sur la ligne que vous souhaitez modifier.
   b. Copiez la ligne de commentaires.
   c. Annulez le commentaire du texte copié en supprimant le signe dièse (#).
   d. Modifier la valeur.
4. Enregistrez le fichier après avoir effectué vos modifications.

   SnapDrive for UNIX vérifie automatiquement ce fichier à chaque démarrage. Vous devez redémarrer le démon SnapDrive pour UNIX pour que les modifications prennent effet.