Sécurité et gestion des identifiants

SnapManager for SAP

NetApp
April 19, 2024

Sommaire

Sécurité et gestion des identifiants

Vous pouvez gérer la sécurité dans SnapManager en appliquant l'authentification des utilisateurs. La méthode d'authentification utilisateur vous permet d'accéder à des ressources telles que des référentiels, des hôtes et des profils.

Lorsque vous effectuez une opération à l'aide de l'interface de ligne de commande ou de l'interface utilisateur graphique, SnapManager récupère les informations d'identification des référentiels et profils. SnapManager enregistre les informations d'identification des installations précédentes.

Le référentiel et les profils peuvent être sécurisés par un mot de passe. Un identifiant est le mot de passe configuré pour l'utilisateur pour un objet et le mot de passe n'est pas configuré sur l'objet lui-même.

Vous pouvez gérer l'authentification et les informations d'identification en effectuant les tâches suivantes :

- Gérez l'authentification des utilisateurs à l'aide d'invites de mot de passe lors des opérations ou à l'aide de `smsap credential set` commande.

  Définissez les informations d'identification d'un référentiel, d'un hôte ou d'un profil.

- Affichez les informations d'identification qui régissent les ressources auxquelles vous avez accès.
- Effacez les informations d'identification d'un utilisateur pour toutes les ressources (hôtes, référentiels et profils).
- Supprimer les informations d'identification d'un utilisateur pour des ressources individuelles (hôtes, référentiels et profils).

> Si la base de données du référentiel se trouve sur un hôte Windows, l'utilisateur local ou administrateur et l'utilisateur du domaine doivent disposer des mêmes informations d'identification.

Qu'est-ce que l'authentification utilisateur

SnapManager authentifie l'utilisateur à l'aide d'une connexion du système d'exploitation sur l'hôte sur lequel le serveur SnapManager est exécuté. Vous pouvez activer l'authentification utilisateur via des invites de mot de passe sur les opérations ou en utilisant les informations d'identification smo pour activer l'authentification utilisateur via des invites de mot de passe sur les opérations ou à l'aide de `smsap credential set`.

Les exigences d'authentification de l'utilisateur dépendent de l'endroit où l'opération est effectuée.

- Si le client SnapManager se trouve sur le même serveur que l'hôte SnapManager, vous êtes authentifié par les informations d'identification du système d'exploitation.

  Vous n'êtes pas invité à saisir un mot de passe car vous êtes déjà connecté à l'hôte sur lequel le serveur SnapManager est exécuté.

- Si le client SnapManager et le serveur SnapManager se trouvent sur des hôtes différents, SnapManager doit vous authentifier auprès des deux identifiants du système d'exploitation.

  SnapManager vous invite à saisir des mots de passe pour toute opération, si vous n'avez pas enregistré

vos identifiants de système d'exploitation dans le cache des informations d'identification utilisateur SnapManager. Si vous saisissez le `smsap credential set -host` Commande, vous enregistrez les informations d'identification du système d'exploitation dans le fichier de cache des informations d'identification SnapManager. SnapManager ne demande donc pas le mot de passe pour une opération.

Si vous êtes authentifié avec le serveur SnapManager, vous êtes considéré comme l'utilisateur efficace. L'utilisateur effectif pour toute opération doit être un compte utilisateur valide sur l'hôte sur lequel l'opération est exécutée. Par exemple, si vous exécutez une opération de clonage, vous devez pouvoir vous connecter à l'hôte de destination du clone.

> SnapManager pour SAP peut ne pas autoriser les utilisateurs créés dans les services Active Directory centraux, tels que LDAP et ADS. Pour vous assurer que l'authentification ne échoue pas, vous devez définir configurable `auth.disableServerAuthorization` à **vrai**.

En tant qu'utilisateur efficace, vous pouvez gérer les informations d'identification de la manière suivante :

- Vous pouvez également configurer SnapManager pour stocker les informations d'identification de l'utilisateur dans le fichier des informations d'identification de l'utilisateur SnapManager.

  Par défaut, SnapManager ne stocke pas les informations d'identification de l'hôte. Vous pouvez modifier ce type de script, par exemple si vous avez des scripts personnalisés qui nécessitent un accès sur un hôte distant. L'opération de clonage à distance est un exemple d'opération SnapManager qui nécessite les identifiants de connexion d'un utilisateur pour un hôte distant. Pour que SnapManager se souvienne des informations d'identification de l'hôte utilisateur dans le cache des informations d'identification de l'utilisateur SnapManager, définissez le `host.credentials.persist` propriété à **true** dans le `smsap.config` fichier.

- Vous pouvez autoriser l'accès des utilisateurs au référentiel.
- Vous pouvez autoriser l'accès des utilisateurs aux profils.
- Vous pouvez afficher toutes les informations d'identification utilisateur.
- Vous pouvez effacer les informations d'identification d'un utilisateur pour toutes les ressources (hôtes, référentiels et profils).
- Vous pouvez supprimer des informations d'identification pour des ressources individuelles (hôtes, référentiels et profils).

Stocker des mots de passe cryptés pour les scripts personnalisés

Par défaut, SnapManager ne stocke pas les informations d'identification de l'hôte dans le cache des informations d'identification de l'utilisateur. Cependant, vous pouvez modifier cela. Vous pouvez modifier le `smsap.config` fichier permettant le stockage des informations d'identification de l'hôte.

Description de la tâche

Le `smsap.config` le fichier est situé à `<default installation location>\properties\smsap.config`

Étapes

1. Modifiez le `smsap.config` fichier.
2. Réglez *`host.credentials.persist`* à **vrai**.

Autoriser l'accès au référentiel

SnapManager vous permet de définir les informations d'identification des utilisateurs de base de données pour accéder au référentiel. À l'aide des informations d'identification, vous pouvez restreindre ou empêcher l'accès aux hôtes, référentiels, profils et bases de données SnapManager.

Description de la tâche

Si vous définissez des informations d'identification à l'aide de l' `credential set` SnapManager ne vous invite pas à saisir un mot de passe.

Vous pouvez définir les informations d'identification de l'utilisateur lors de l'installation de SnapManager ou d'une version ultérieure.

Étape

1. Saisissez la commande suivante :

```
smsap credential set -repository -dbname repo_service_name -host repo_host
-login -username repo_username [-password repo_password] -port repo_port
```

Autoriser l'accès aux profils

SnapManager vous permet de définir un mot de passe pour un profil afin d'empêcher tout accès non autorisé.

Étape

1. Saisissez la commande suivante :

```
smsap credential set -profile -name profile_name [-password password]
```

Afficher les informations d'identification de l'utilisateur

Vous pouvez afficher la liste des hôtes, des profils et des référentiels auxquels vous avez accès.

Étape

1. Pour lister les ressources auxquelles vous avez accès, entrez la commande suivante :

```
smsap credential list
```

Exemple d'affichage des informations d'identification des utilisateurs

Cet exemple affiche les ressources auxquelles vous avez accès.

```
smsap credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMSAPREPO/hotspur:1521
Host2_test_user@SMSAPREPO/hotspur:1521
user1_1@SMSAPREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMSAPREPO/hotspur:1521) [PASSWORD NOT
SET]
Hosts:
Host2
Host5
```

Effacer les informations d'identification utilisateur pour tous les hôtes, référentiels et profils

Vous pouvez effacer la mémoire cache de vos informations d'identification pour les ressources (hôtes, référentiels et profils). Ceci supprime toutes les informations d'identification de ressource pour l'utilisateur exécutant la commande. Après avoir effacé le cache, vous devez à nouveau authentifier vos identifiants pour accéder à ces ressources sécurisées.

Étapes

1. Pour effacer vos informations d'identification, entrez le `smsap credential clear` Dans l'interface de ligne de commande SnapManager ou sélectionnez **Admin** > **Credentials** > **Clear cache** dans l'interface graphique de SnapManager.
2. Quittez l'interface graphique de SnapManager.

   - Si vous avez effacé le cache des informations d'identification de l'interface graphique SnapManager, il n'est pas nécessaire de quitter l'interface graphique SnapManager.
   - Si vous avez effacé le cache des informations d'identification de l'interface de ligne de commande SnapManager, vous devez redémarrer l'interface graphique de SnapManager.
   - Si vous avez supprimé manuellement le fichier d'informations d'identification cryptées, vous devez redémarrer l'interface graphique de SnapManager.

3. Pour définir à nouveau les informations d'identification, répétez le processus pour définir les informations

d'identification du référentiel, de l'hôte du profil et du profil. Pour plus d'informations sur la configuration des informations d'identification de l'utilisateur, reportez-vous à la section « Définition des informations d'identification après effacement du cache des informations d'identification ».

Définissez les informations d'identification après avoir effacé le cache des informations d'identification

Après avoir effacé le cache pour supprimer les informations d'identification de l'utilisateur stocké, vous pouvez définir les informations d'identification des hôtes, des référentiels et des profils.

Description de la tâche

Vous devez vous assurer que vous définissez les mêmes informations d'identification utilisateur pour le référentiel, l'hôte de profil et le profil que vous avez donnés précédemment. Un fichier d'informations d'identification chiffré est créé lors de la configuration des informations d'identification de l'utilisateur.

Le fichier d'informations d'identification se trouve à `C:\Documents and Settings\Administrator\Application Data\NetApp\smsap\3.3.0`.

À partir de l'interface utilisateur graphique SnapManager, si aucun référentiel n'est placé sous des référentiels, effectuez les opérations suivantes :

Étapes

1. Cliquez sur **tâches** > **Ajouter un référentiel existant** pour ajouter un référentiel existant.
2. Procédez comme suit pour définir les informations d'identification du référentiel :
   a. Cliquez avec le bouton droit de la souris sur le référentiel et sélectionnez **Ouvrir**.
   b. Dans le `Repository Credentials Authentication` entrez les informations d'identification de l'utilisateur.
3. Procédez comme suit pour définir les informations d'identification de l'hôte :
   a. Cliquez avec le bouton droit de la souris sur l'hôte sous le référentiel et sélectionnez **Ouvrir**.
   b. Dans le `Host Credentials Authentication` entrez les informations d'identification de l'utilisateur.
4. Procédez comme suit pour définir les informations d'identification du profil :
   a. Cliquez avec le bouton droit de la souris sur le profil sous l'hôte et sélectionnez **Ouvrir**.
   b. Dans le `Profile Credentials Authentication` entrez les informations d'identification de l'utilisateur.

Supprimer les informations d'identification des ressources individuelles

Vous pouvez supprimer les informations d'identification de l'une des ressources sécurisées, telles qu'un profil, un référentiel ou un hôte. Cela vous permet de supprimer les informations d'identification pour une seule ressource, au lieu de supprimer les informations d'identification de l'utilisateur pour toutes les ressources.

Supprimer les informations d'identification des utilisateurs pour les référentiels

Vous pouvez supprimer les informations d'identification pour qu'un utilisateur ne puisse plus accéder à un référentiel particulier. Cette commande vous permet de supprimer les informations d'identification d'une seule ressource au lieu de supprimer les informations d'identification de l'utilisateur pour toutes les ressources.

Étape

1. Pour supprimer les informations d'identification du référentiel pour un utilisateur, entrez la commande suivante :

   smsap credential delete -repository -dbname *repo_service_name* -host *repo_host* -login -username *repo_username* -port *repo_port*

Supprimer les informations d'identification utilisateur pour les hôtes

Vous pouvez supprimer les informations d'identification d'un hôte pour qu'un utilisateur ne puisse plus y accéder. Cette commande vous permet de supprimer les informations d'identification d'une seule ressource, au lieu de supprimer toutes les informations d'identification de l'utilisateur pour toutes les ressources.

Étape

1. Pour supprimer les informations d'identification d'hôte d'un utilisateur, entrez la commande suivante :

   ```
   smsap credential delete -host -name_host_name_-username_-username_
   ```

Supprimer les informations d'identification des profils

Vous pouvez supprimer les informations d'identification d'un profil pour qu'un utilisateur ne puisse plus y accéder.

Étape

1. Pour supprimer les informations d'identification du profil d'un utilisateur, entrez la commande suivante :

   smsap credential delete -profile -name *profile_name*