# Sicherheits- und Anmeldeinformationsmanagement

SnapManager for SAP

NetApp
April 19, 2024

# Inhalt

Sicherheits- und Anmeldeinformationsmanagement . . . 1
Was ist die Benutzerauthentifizierung . . . 1
Verschlüsselte Passwörter für benutzerdefinierte Skripts speichern . . . 2
Zugriff auf das Repository autorisieren . . . 3
Zugriff auf Profile autorisieren . . . 3
Benutzeranmeldeinformationen anzeigen . . . 3
Löschen Sie die Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile . . . 4
Löschen von Anmeldeinformationen für einzelne Ressourcen . . . 5

# Sicherheits- und Anmeldeinformationsmanagement

Sie können die Sicherheit in SnapManager durch Benutzerauthentifizierung verwalten. Die Benutzerauthentifizierungsmethode ermöglicht den Zugriff auf Ressourcen wie Repositorys, Hosts und Profile.

Wenn Sie einen Vorgang über die Befehlszeilenschnittstelle (CLI) oder die grafische Benutzeroberfläche (GUI) ausführen, ruft SnapManager die für Repositorys und Profile festgelegten Anmeldeinformationen ab. SnapManager speichert Anmeldeinformationen früherer Installationen.

Das Repository und die Profile können mit einem Passwort gesichert werden. Eine Anmeldeinformationen ist das für den Benutzer für ein Objekt konfigurierte Passwort, und das Passwort ist nicht für das Objekt selbst konfiguriert.

Sie können die Authentifizierung und Anmeldeinformationen verwalten, indem Sie die folgenden Aufgaben ausführen:

- Verwalten Sie die Benutzerauthentifizierung entweder durch Eingabeaufforderungen für Passwörter für Vorgänge oder mithilfe des `smsap credential set` Befehl.

  Legen Sie Anmeldedaten für ein Repository, einen Host oder ein Profil fest.

- Zeigen Sie die Anmeldeinformationen an, die die Ressourcen regeln, auf die Sie Zugriff haben.
- Löschen Sie die Anmeldeinformationen eines Benutzers für alle Ressourcen (Hosts, Repositorys und Profile).
- Löschen Sie die Anmeldeinformationen eines Benutzers für einzelne Ressourcen (Hosts, Repositorys und Profile).

> Wenn sich die Repository-Datenbank auf einem Windows-Host befindet, müssen sowohl der lokale Benutzer als auch der Domänenbenutzer über dieselben Anmeldeinformationen verfügen.

## Was ist die Benutzerauthentifizierung

SnapManager authentifiziert den Benutzer mithilfe einer Betriebssystemanmeldung auf dem Host, auf dem der SnapManager-Server ausgeführt wird. Sie können die Benutzerauthentifizierung entweder durch Eingabeaufforderungen zum Passwort oder durch Verwendung der Smo-Anmeldeinformationen aktivieren, die die Benutzerauthentifizierung entweder durch Eingabeaufforderungen zum Passwort oder über die aktivieren `smsap credential set`.

Die Anforderungen an die Benutzerauthentifizierung hängen davon ab, wo der Vorgang ausgeführt wird.

- Wenn sich der SnapManager-Client auf demselben Server wie der SnapManager-Host befindet, werden Sie durch die BS-Anmeldedaten authentifiziert.

  Sie werden nicht zur Eingabe eines Passworts aufgefordert, da Sie bereits beim Host angemeldet sind, auf dem der SnapManager-Server ausgeführt wird.

- Wenn der SnapManager-Client und der SnapManager-Server auf verschiedenen Hosts sind, muss SnapManager Sie mit beiden OS-Anmeldedaten authentifizieren.

  SnapManager fordert Sie zur Eingabe von Passwörtern für jeden Vorgang auf, wenn Sie Ihre BS-Anmeldeinformationen nicht im SnapManager-Benutzereinweiscache gespeichert haben. Wenn Sie das eingeben `smsap credential set -host` Befehl, Sie speichern die OS-Anmeldeinformationen in Ihrer SnapManager-Cachedatei für Zugangsdaten, sodass SnapManager nicht zur Eingabe des Passworts für einen Vorgang aufgefordert wird.

Wenn Sie mit dem SnapManager-Server authentifiziert sind, gelten Sie als effektiver Benutzer. Der effektive Benutzer für einen Vorgang muss ein gültiges Benutzerkonto auf dem Host sein, auf dem der Vorgang ausgeführt wird. Wenn Sie beispielsweise einen Klonvorgang ausführen, sollten Sie sich beim Ziel-Host für den Klon einloggen können.

> SnapManager für SAP kann die Autorisierung von Benutzern, die in zentralen Active Directory-Diensten erstellt wurden, z. B. LDAP und ADS, möglicherweise nicht unterstützen. Um sicherzustellen, dass die Authentifizierung nicht fehlschlägt, müssen Sie die Konfiguration festlegen `auth.disableServerAuthorization` Für **wahr**.

Als effektiver Benutzer können Sie die Anmeldeinformationen folgendermaßen verwalten:

- Optional können Sie SnapManager so konfigurieren, dass Benutzeranmeldeinformationen in der SnapManager-Benutzeranmeldedatei gespeichert werden.

  Standardmäßig werden in SnapManager keine Host-Anmeldedaten gespeichert. Sie können dies ändern, beispielsweise, wenn Sie benutzerdefinierte Skripte haben, die Zugriff auf einen Remote-Host benötigen. Der Remote-Klonvorgang ist ein Beispiel für eine SnapManager-Operation, die die Anmeldedaten eines Benutzers für einen Remote-Host benötigt. Um die Anmeldedaten des SnapManager-Benutzerhosts im SnapManager-Benutzeranmeldungs-Cache zu speichern, legen Sie den fest `host.credentials.persist` Hotel für **wahr** im `smsap.config` Datei:

- Sie können den Benutzerzugriff auf das Repository autorisieren.
- Sie können den Benutzerzugriff auf Profile autorisieren.
- Sie können alle Benutzeranmeldeinformationen anzeigen.
- Sie können die Anmeldeinformationen eines Benutzers für alle Ressourcen (Hosts, Repositorys und Profile) löschen.
- Anmeldedaten für einzelne Ressourcen (Hosts, Repositorys und Profile) können gelöscht werden.

# Verschlüsselte Passwörter für benutzerdefinierte Skripts speichern

Standardmäßig speichert SnapManager keine Hostanmeldeinformationen im Cache für Benutzeranmeldeinformationen. Sie können dies jedoch ändern. Sie können die bearbeiten `smsap.config` Datei zum Speichern von Host-Anmeldeinformationen.

## Über diese Aufgabe

Der `smsap.config` Datei befindet sich unter `<default installation location>\properties\smsap.config`

**Schritte**

1. Bearbeiten Sie das `smsap.config` Datei:
2. Einstellen *`host.credentials.persist`* Für **wahr**.

# Zugriff auf das Repository autorisieren

Mit SnapManager können Sie Anmeldedaten für Datenbankbenutzer für den Zugriff auf das Repository festlegen. Mithilfe von Zugangsdaten können Sie den Zugriff auf die SnapManager-Hosts, Repositorys, Profile und Datenbanken einschränken oder verhindern.

## Über diese Aufgabe

Wenn Sie die Anmeldeinformationen mithilfe des festlegen `credential set` Befehl, SnapManager fordert Sie nicht zur Eingabe eines Passworts auf.

Sie können Benutzeranmeldeinformationen festlegen, wenn Sie SnapManager oder höher installieren.

**Schritt**

1. Geben Sie den folgenden Befehl ein:

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

# Zugriff auf Profile autorisieren

Mit SnapManager können Sie ein Kennwort für ein Profil festlegen, um unbefugten Zugriff zu verhindern.

**Schritt**

1. Geben Sie den folgenden Befehl ein:

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

# Benutzeranmeldeinformationen anzeigen

Sie können die Hosts, Profile und Repositorys auflisten, auf die Sie Zugriff haben.

**Schritt**

1. Geben Sie den folgenden Befehl ein, um die Ressourcen anzuzeigen, auf die Sie Zugriff haben:

```
smsap credential list
```

## Beispiel für die Anzeige von Benutzeranmeldeinformationen

In diesem Beispiel werden die Ressourcen angezeigt, auf die Sie Zugriff haben.

```
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
```

## Löschen Sie die Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile

Sie können den Cache Ihrer Anmeldeinformationen für Ressourcen (Hosts, Repositorys und Profile) löschen. Dadurch werden alle Ressourcen-Anmeldeinformationen für den Benutzer gelöscht, der den Befehl ausführt. Nach dem Löschen des Cache müssen Sie Ihre Anmeldeinformationen erneut authentifizieren, um auf diese gesicherten Ressourcen zugreifen zu können.

**Schritte**

1. Um Ihre Anmeldeinformationen zu löschen, geben Sie das ein `smsap credential clear` Befehl aus der SnapManager CLI oder wählen Sie **Admin** > **Anmeldeinformationen** > **Cache löschen** aus der SnapManager-Benutzeroberfläche.
2. Schließen Sie die SnapManager-Benutzeroberfläche.

   - Wenn Sie den Anmeldeinformationscache von der SnapManager-GUI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche nicht beenden.
   - Wenn Sie den Anmeldeinformationscache von der SnapManager-CLI gelöscht haben, müssen Sie die SnapManager-GUI neu starten.
   - Wenn Sie die verschlüsselte Anmeldedatei manuell gelöscht haben, müssen Sie die SnapManager-GUI erneut starten.

3. Um die Anmeldeinformationen erneut festzulegen, wiederholen Sie den Vorgang, um die Anmeldeinformationen für das Repository, den Profilhost und das Profil festzulegen. Weitere Informationen zum erneuten Einstellen der Benutzeranmeldeinformationen finden Sie unter „Anmeldeinformationen nach dem Löschen des Anmeldeinformationscache festlegen“.

### Legen Sie die Anmeldeinformationen fest, nachdem Sie den Anmeldeinformationscache gelöscht haben

Nachdem Sie den Cache gelöscht haben, um die gespeicherten Benutzeranmeldeinformationen zu entfernen, können Sie die Anmeldeinformationen für die Hosts, Repositorys und Profile festlegen.

#### Über diese Aufgabe

Sie müssen sicherstellen, dass Sie die gleichen Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil festlegen, das Sie zuvor angegeben haben. Beim Festlegen der Benutzeranmeldeinformationen wird eine verschlüsselte Anmeldedatei erstellt.

Die Anmeldedatei befindet sich unter `C:\Documents and Settings\Administrator\Application Data\NetApp\smsap\3.3.0`.

Führen Sie in der grafischen Benutzeroberfläche von SnapManager (GUI) die folgenden Schritte aus, wenn unter „Repositories“ kein Repository vorhanden ist:

#### Schritte

1. Klicken Sie auf **Tasks** > **vorhandenes Repository hinzufügen**, um ein vorhandenes Repository hinzuzufügen.
2. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für das Repository festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf das Repository und wählen Sie **Öffnen**.
   b. Im `Repository Credentials Authentication` Geben Sie die Benutzeranmeldeinformationen ein.
3. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für den Host festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf den Host unter dem Repository und wählen Sie **Öffnen**.
   b. Im `Host Credentials Authentication` Geben Sie die Benutzeranmeldeinformationen ein.
4. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für das Profil festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf das Profil unter dem Host und wählen Sie **Öffnen**.
   b. Im `Profile Credentials Authentication` Geben Sie die Benutzeranmeldeinformationen ein.

## Löschen von Anmeldeinformationen für einzelne Ressourcen

Sie können die Anmeldeinformationen für eine der gesicherten Ressourcen löschen, z. B. ein Profil, ein Repository oder einen Host. Auf diese Weise können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt die Anmeldeinformationen des Benutzers für alle Ressourcen zu löschen.

### Benutzeranmeldeinformationen für Repositories löschen

Sie können die Anmeldeinformationen löschen, damit ein Benutzer nicht mehr auf ein bestimmtes Repository zugreifen kann. Mit diesem Befehl können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt die

Anmeldeinformationen des Benutzers für alle Ressourcen zu löschen.

**Schritt**

1. Um Repository-Anmeldedaten für einen Benutzer zu löschen, geben Sie folgenden Befehl ein:

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

## Löschen Sie die Benutzeranmeldeinformationen für Hosts

Sie können die Anmeldeinformationen für einen Host löschen, sodass ein Benutzer nicht mehr darauf zugreifen kann. Mit diesem Befehl können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt alle Benutzeranmeldeinformationen für alle Ressourcen zu löschen.

**Schritt**

1. Geben Sie den folgenden Befehl ein, um die Hostanmeldeinformationen für einen Benutzer zu löschen:

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

## Benutzeranmeldeinformationen für Profile löschen

Sie können die Benutzeranmeldeinformationen für ein Profil löschen, damit ein Benutzer nicht mehr darauf zugreifen kann.

**Schritt**

1. Geben Sie den folgenden Befehl ein, um die Profilanmeldeinformationen für einen Benutzer zu löschen:

   **smsap credential delete -profile -name *profile_name***