セキュリティと資格情報の管理

SnapManager for SAP

NetApp
April 19, 2024

目次

セキュリティと資格情報の管理

SnapManager では、ユーザ認証を適用してセキュリティを管理できます。ユーザ認証方式を使用すると、リポジトリ、ホスト、プロファイルなどのリソースにアクセスできます。

コマンドラインインターフェイス（ CLI ）またはグラフィカルユーザインターフェイス（ GUI ）を使用して処理を実行すると、 SnapManager はリポジトリおよびプロファイルに設定されているクレデンシャルを取得します。SnapManager は以前のインストールのクレデンシャルを保存します。

リポジトリとプロファイルは、パスワードで保護できます。クレデンシャルとは、ユーザがオブジェクト用に設定したパスワードであり、パスワードはオブジェクト自体には設定されません。

認証とクレデンシャルを管理するには、次のタスクを実行します。

- ユーザ認証は、操作時にパスワードプロンプトを使用するか、または「smsapscredential set」コマンドを使用して管理します。

  リポジトリ、ホスト、またはプロファイルのクレデンシャルを設定する

- アクセスできるリソースを制御するクレデンシャルを表示します。
- すべてのリソース（ホスト、リポジトリ、およびプロファイル）について、ユーザのクレデンシャルをクリアします。
- 個々のリソース（ホスト、リポジトリ、およびプロファイル）に対するユーザのクレデンシャルを削除する。

> リポジトリ・データベースが Windows ホスト上にある場合、ローカル・ユーザまたは管理者ユーザとドメイン・ユーザの両方に同じクレデンシャルが必要です。

ユーザ認証とは

SnapManager は、 SnapManager サーバが実行されているホストでオペレーティングシステム（ OS ）ログインを使用してユーザを認証します。ユーザ認証は、操作時にパスワードプロンプトを使用するか、smoクレデンシャルを使用して有効にできます。ユーザ認証は、操作時にパスワード・プロンプトを使用するか、または「SMSAPのクレデンシャル・セット」を使用して有効にできます。

ユーザ認証の要件は、処理を実行する場所によって異なります。

- SnapManager クライアントが SnapManager ホストと同じサーバ上にある場合は、 OS のクレデンシャルによって認証されます。

  SnapManager サーバが実行されているホストにすでにログインしているため、パスワードの入力は求められません。

- SnapManager クライアントと SnapManager サーバが異なるホスト上にある場合、 SnapManager は両方の OS クレデンシャルを使用してユーザを認証する必要があります。

SnapManager ユーザクレデンシャルキャッシュに OS クレデンシャルを保存していない場合、SnapManager は処理のためのパスワードの入力を求めます。「SMSAP credential set -host」コマンドを入力する場合は、SnapManager クレデンシャルキャッシュファイルにOSクレデンシャルを保存します。このため、SnapManager は処理のためにパスワードの入力を求めません。

SnapManager サーバで認証されている場合は、有効なユーザとみなされます。すべての処理の実効ユーザは、処理が実行されるホストの有効なユーザアカウントである必要があります。たとえば、クローニング処理を実行する場合は、クローンのデスティネーションホストにログインできる必要があります。

SnapManager for SAPで、LDAPやADSなどの中央Active Directoryサービスで作成されたユーザの許可が失敗することがあります。認証が失敗しないようにするには、構成可能な「auth.disableServerAuthorization」を「* true *」に設定する必要があります。

実効ユーザとして、次の方法でクレデンシャルを管理できます。

- 必要に応じて、 SnapManager ユーザクレデンシャルファイルにユーザクレデンシャルを格納するように SnapManager を設定することができます。

  デフォルトでは、 SnapManager にはホストクレデンシャルは格納されません。たとえば、リモートホストへのアクセスを必要とするカスタムスクリプトがある場合などに、この変更が必要になることがあります。リモートクローニング処理は、リモートホストのユーザのログインクレデンシャルが必要な SnapManager 処理の例です。SnapManager がSnapManager ユーザのクレデンシャルキャッシュにユーザのホストのログインクレデンシャルを保存するようにするには、「SMSAP_CONFIG」ファイルで「host.credentials.Persist`」プロパティを「* true」に設定します。

- リポジトリへのユーザ・アクセスを許可できます。
- プロファイルへのユーザアクセスを許可できます。
- すべてのユーザクレデンシャルを表示できます。
- すべてのリソース（ホスト、リポジトリ、およびプロファイル）について、ユーザのクレデンシャルを消去できます。
- 個々のリソース（ホスト、リポジトリ、およびプロファイル）のクレデンシャルを削除できます。

カスタムスクリプトの暗号化されたパスワードを保存します

デフォルトでは、 SnapManager はホストクレデンシャルをユーザクレデンシャルキャッシュに格納しません。ただし、これは変更できます。「SMSAP_CONFIG」ファイルを編集して、ホストクレデンシャルを格納できるようにすることができます。

このタスクについて

「smsap.config」ファイルは「<default installation location>\properties\smsap.config`」にあります

手順

1. 「smsap.config」ファイルを編集します。
2. 「*host.credentials_persist*」を「* true」に設定します。

リポジトリへのアクセスを許可します

SnapManager を使用すると、データベースユーザがリポジトリにアクセスするためのクレデンシャルを設定できます。クレデンシャルを使用すると、 SnapManager ホスト、リポジトリ、プロファイル、およびデータベースへのアクセスを制限したり、禁止したりできます。

このタスクについて

credential setコマンドを使用してクレデンシャルを設定する場合、SnapManager はパスワードの入力を求めません。

ユーザクレデンシャルは、 SnapManager 以降のインストール時に設定できます。

ステップ

1. 次のコマンドを入力します。

   * SMSAPクレデンシャルセット-repository-dbname_repo_repo_service_name_-login -username repo_repo_username *[-password_repo_password]*-port_repo_port_*

プロファイルへのアクセスを許可します

SnapManager では、プロファイルのパスワードを設定して、不正なアクセスを防止できます。

ステップ

1. 次のコマンドを入力します。

   * SMSAPのクレデンシャルセット-profile-name_profile_[-password_password_]*

ユーザクレデンシャルを表示する

アクセス可能なホスト、プロファイル、およびリポジトリをリスト表示できます。

ステップ

1. アクセス可能なリソースを一覧表示するには、次のコマンドを入力します。

   '**SMSAP**クレデンシャル・リスト

ユーザクレデンシャルの表示例

次の例は、アクセス可能なリソースを表示します。

```
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
```

すべてのホスト、リポジトリ、およびプロファイルのユーザクレデンシャルを消去します

リソース（ホスト、リポジトリ、およびプロファイル）のクレデンシャルのキャッシュをクリアできます。これにより、コマンドを実行しているユーザのリソースクレデンシャルがすべて削除されます。キャッシュをクリアしたら、クレデンシャルを再度認証して、これらのセキュアなリソースにアクセスできるようにする必要があります。

手順

1. クレデンシャルをクリアするには、SnapManager のCLIで「SMSAP credential clear」コマンドを入力するか、SnapManager のGUIで「* Admin 」>「 Credentials 」>「 Clear Cache *」を選択します。
2. SnapManager GUI を終了します。

   - SnapManager GUI からクレデンシャルキャッシュをクリアした場合は、 SnapManager GUI を終了する必要はありません。
   - SnapManager CLI からクレデンシャルキャッシュをクリアした場合は、 SnapManager GUI を再起動する必要があります。
   - 暗号化されたクレデンシャルファイルを手動で削除した場合は、 SnapManager GUI を再起動する必要があります。

3. クレデンシャルを再度設定するには、同じプロセスを繰り返して、リポジトリ、プロファイルホスト、およびプロファイルのクレデンシャルを設定します。ユーザクレデンシャルを再度設定する追加情報の場合は、「クレデンシャルキャッシュをクリアしたあとのクレデンシャルの設定」を参照してください。

クレデンシャルキャッシュを消去したあとにクレデンシャルを設定

キャッシュをクリアして格納されているユーザクレデンシャルを削除したら、ホスト、リポジトリ、およびプロファイルのクレデンシャルを設定できます。

このタスクについて

リポジトリ、プロファイルホスト、およびプロファイルには、以前に指定したのと同じユーザクレデンシャルを設定する必要があります。ユーザクレデンシャルの設定時に暗号化されたクレデンシャルファイルが作成されます。

クレデンシャルファイルは「C：\Documents and Settings\ Administrator \Application Data\NetApp\SMS\3.3.0」にあります。

SnapManager GUI （グラフィカルユーザーインタフェース）で、リポジトリにリポジトリがない場合は、次の手順を実行します。

手順

1. 既存のリポジトリを追加するには '[タスク *>] → [既存のリポジトリの追加] をクリックします
2. リポジトリのクレデンシャルを設定するには、次の手順を実行します。
   a. リポジトリを右クリックし '[* 開く *] を選択します
   b. [Repository Credentials Authentication]ウィンドウで、ユーザクレデンシャルを入力します。
3. ホストのクレデンシャルを設定するには、次の手順を実行します。
   a. リポジトリの下のホストを右クリックし '[**Open**] を選択します
   b. ［ホストの認証情報］ウィンドウで’ユーザーの認証情報を入力します
4. プロファイルのクレデンシャルを設定するには、次の手順を実行します。
   a. ホストの下のプロファイルを右クリックし、 * 開く * を選択します。
   b. [Profile Credentials Authentication]ウィンドウで、ユーザクレデンシャルを入力します。

個々のリソースのクレデンシャルを削除する

プロファイル、リポジトリ、ホストなど、いずれかのセキュアなリソースのクレデンシャルを削除できます。これにより、すべてのリソースについてユーザのクレデンシャルを消去するのではなく、 1 つのリソースについてのみクレデンシャルを削除することができます。

リポジトリのユーザクレデンシャルを削除します

クレデンシャルを削除して、ユーザが特定のリポジトリにアクセスできないようにすることができます。このコマンドでは、すべてのリソースについてユーザのクレデンシャルを消去するのではなく、 1 つのリソースについてのみクレデンシャルを削除できます。

ステップ

1. ユーザのリポジトリクレデンシャルを削除するには、次のコマンドを入力します。

   「* SMSAP credential delete -repository -dbdbname_repo_service_name」-host_repo_host__ login -username repo_username -*port_repo_port*'

ホストのユーザクレデンシャルを削除します

ホストのクレデンシャルを削除して、ユーザがアクセスできないようにすることができます。このコマンドでは、すべてのリソースについてユーザのクレデンシャルをすべて消去するのではなく、１つのリソースについてのみクレデンシャルを削除できます。

ステップ

1. ユーザのホストクレデンシャルを削除するには、次のコマンドを入力します。

   'SMSAP credential delete -host-name *host_name -username-username*`

プロファイルのユーザクレデンシャルを削除する

プロファイルのユーザクレデンシャルを削除して、ユーザがアクセスできないようにすることができます。

ステップ

1. ユーザのプロファイルクレデンシャルを削除するには、次のコマンドを入力します。

   SMSAP credential delete -profile name *profile_name*