Security and credential management

SnapManager for SAP

NetApp
February 20, 2023

Table of Contents

Security and credential management

You can manage security in SnapManager by applying user authentication. The user authentication method allows you to access resources such as repositories, hosts, and profiles.

When you perform an operation using either the command-line interface (CLI) or graphical user interface (GUI), SnapManager retrieves the credentials set for repositories and profiles. SnapManager saves credentials from previous installations.

The repository and profiles can be secured with a password. A credential is the password configured for the user for an object, and the password is not configured on the object itself.

You can manage authentication and credentials by performing the following tasks:

- Manage user authentication either through password prompts on operations or by using the `smsap credential set` command.

  Set credentials for a repository, host, or profile.

- View the credentials that govern the resources to which you have access.
- Clear a user's credentials for all resources (hosts, repositories, and profiles).
- Delete a user's credentials for individual resources (hosts, repositories, and profiles).

If the repository database is on a Windows host, then both local or administrator user and the domain user must have the same credentials.

What user authentication is

SnapManager authenticates the user by using an operating system (OS) login on the host where the SnapManager server is running. You can enable user authentication either through password prompts on operations or by using the smo credential You can enable user authentication either through password prompts on operations or by using the `smsap credential set`.

User authentication requirements depend on where the operation is performed.

- If the SnapManager client is on the same server as the SnapManager host, you are authenticated by the OS credentials.

  You are not prompted for a password because you are already logged in to the host where the SnapManager server is running.

- If the SnapManager client and the SnapManager server are on different hosts, SnapManager needs to authenticate you with both OS credentials.

  SnapManager prompts you for passwords for any operation, if you have not saved your OS credentials in your SnapManager user credential cache. If you enter the `smsap credential set -host` command, you save the OS credentials in your SnapManager credential cache file and so SnapManager does not prompt for the password for any operation.

If you are authenticated with the SnapManager server, you are considered the effective user. The effective user for any operation must be a valid user account on the host on which the operation is executed. For example, if you execute a clone operation, you should be able to log in to the destination host for the clone.

SnapManager for SAP might fail in authorizing users created in Central Active Directory Services, such as LDAP and ADS. To ensure the authentication does not fail, you must set configurable `auth.disableServerAuthorization` to **true**.

As an effective user you can manage credentials in the following ways:

- Optionally, you can configure SnapManager to store user credentials in the SnapManager user credentials file.

  By default, SnapManager does not store host credentials. You might want to change this, for example, if you have custom scripts that require access on a remote host. The remote clone operation is an example of a SnapManager operation that needs the login credentials of a user for a remote host. To have SnapManager remember user host login credentials in the SnapManager user credentials cache, set the `host.credentials.persist` property to **true** in the `smsap.config` file.

- You can authorize user access to the repository.
- You can authorize user access to profiles.
- You can view all user credentials.
- You can clear a user's credentials for all resources (hosts, repositories, and profiles).
- You can delete credentials for individual resources (hosts, repositories, and profiles).

Store encrypted passwords for custom scripts

By default, SnapManager does not store host credentials in the user credentials cache. However, you can change this. You can edit the `smsap.config` file to allow storing of host credentials.

About this task

The `smsap.config` file is located at `<default installation location>\properties\smsap.config`

Steps

1. Edit the `smsap.config` file.
2. Set *`host.credentials.persist`* to **true**.

Authorize access to the repository

SnapManager enables you to set credentials for database users to access the repository. Using credentials, you can restrict or prevent access to the SnapManager hosts, repositories, profiles, and databases.

About this task

If you set credentials by using the `credential set` command, SnapManager does not prompt you for a password.

You can set user credentials when you install SnapManager or later.

Step

1. Enter the following command:

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

Authorize access to profiles

SnapManager enables you to set a password for a profile to prevent unauthorized access.

Step

1. Enter the following command:

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

View user credentials

You can list the hosts, profiles, and repositories to which you have access.

Step

1. To list the resources to which you have access, enter this command:

   smsap credential list

Example of viewing user credentials

This example displays the resources to which you have access.

```
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
```

Clear user credentials for all hosts, repositories, and profiles

You can clear the cache of your credentials for resources (hosts, repositories, and profiles). This deletes all of the resource credentials for the user running the command. After clearing the cache, you must authenticate your credentials again to gain access to these secured resources.

Steps

1. To clear your credentials, enter the `smsap credential clear` command from the SnapManager CLI or select **Admin** > **Credentials** > **Clear Cache** from the SnapManager GUI.
2. Exit the SnapManager GUI.

   - If you have cleared the credential cache from the SnapManager GUI, you do not need to exit the SnapManager GUI.
   - If you have cleared the credential cache from the SnapManager CLI, you must restart SnapManager GUI.
   - If you have deleted the encrypted credential file manually, you must restart the SnapManager GUI again.

3. To set the credentials again, repeat the process to set credentials for the repository, profile host, and profile. For additional information on setting the user credentials again, refer to "Setting credentials after clearing credential cache."

Set credentials after clearing the credential cache

After clearing the cache to remove the stored user credentials, you can set the credentials for the hosts, repositories, and profiles.

About this task

You must ensure that you set the same user credentials for the repository, profile host, and profile that you had given earlier. An encrypted credentials file is created while setting the user credentials.

The credentials file is located at `C:\Documents and Settings\Administrator\Application Data\NetApp\smsap\3.3.0`.

From the SnapManager graphical user interface (GUI), if there is no repository under Repositories, perform the following steps:

Steps

1. Click **Tasks** > **Add Existing Repository** to add an existing repository.
2. Perform the following steps to set the credentials for repository:
   a. Right-click the repository and select **Open**.
   b. In the `Repository Credentials Authentication` window, enter the user credentials.
3. Perform the following steps to set the credentials for host:
   a. Right-click the host under the repository and select **Open**.
   b. In the `Host Credentials Authentication` window, enter the user credentials.
4. Perform the following steps to set the credentials for profile:
   a. Right-click the profile under the host and select **Open**.
   b. In the `Profile Credentials Authentication` window, enter the user credentials.

Delete credentials for individual resources

You can delete the credentials for any one of the secured resources, such as a profile, repository, or host. This enables you to remove the credentials for just one resource, rather than clearing the user's credentials for all resources.

Delete user credentials for repositories

You can delete the credentials so a user can no longer access a particular repository. This command enables you to remove the credentials for just one resource, rather than clearing the user's credentials for all resources.

Step

1. To delete repository credentials for a user, enter this command:

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

Delete user credentials for hosts

You can delete the credentials for a host so a user can no longer access it. This command enables you to remove the credentials for just one resource, rather than clearing all the user's credentials for all resources.

Step

1. To delete host credentials for a user, enter this command:

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

Delete user credentials for profiles

You can delete the user credentials for a profile so a user can no longer access it.

Step

1. To delete profile credentials for a user, enter this command:

smsap credential delete -profile -name *profile_name*

Copyright information

Trademark information