



安全性和凭据管理 SnapManager for SAP

NetApp
April 19, 2024

目录

- 安全性和凭据管理..... 1
 - 什么是用户身份验证..... 1
 - 存储自定义脚本的加密密码 2
 - 授权访问存储库 2
 - 授权对配置文件的访问..... 3
 - 查看用户凭据 3
 - 清除所有主机、存储库和配置文件的用户凭据..... 3
 - 删除单个资源的凭据..... 5

安全性和凭据管理

您可以通过应用用户身份验证来管理 SnapManager 中的安全性。通过用户身份验证方法，您可以访问存储库，主机和配置文件等资源。

使用命令行界面（CLI）或图形用户界面（GUI）执行操作时，SnapManager 会检索为存储库和配置文件设置的凭据。SnapManager 会保存先前安装的凭据。

可以使用密码保护存储库和配置文件。凭据是为用户配置的对象密码，而不是在对象本身上配置密码。

您可以通过执行以下任务来管理身份验证和凭据：

- 通过操作时的密码提示或使用 `smsap credential set` 命令来管理用户身份验证。

设置存储库，主机或配置文件的凭据。

- 查看用于管理您有权访问的资源的凭据。
- 清除所有资源（主机，存储库和配置文件）的用户凭据。
- 删除单个资源（主机，存储库和配置文件）的用户凭据。



如果存储库数据库位于 Windows 主机上，则本地或管理员用户和域用户都必须具有相同的凭据。

什么是用户身份验证

SnapManager 通过在运行 SnapManager 服务器的主机上使用操作系统（OS）登录来对用户进行身份验证。您可以通过操作时的密码提示或使用 SMO 凭据来启用用户身份验证、您可以通过操作时的密码提示或使用 `smsap 凭据集` 来启用用户身份验证。

用户身份验证要求取决于操作的执行位置。

- 如果 SnapManager 客户端与 SnapManager 主机位于同一服务器上，您将通过操作系统凭据进行身份验证。

系统不会提示您输入密码，因为您已登录到运行 SnapManager 服务器的主机。

- 如果 SnapManager 客户端和 SnapManager 服务器位于不同的主机上，则 SnapManager 需要使用这两个操作系统凭据对您进行身份验证。

如果您尚未将操作系统凭据保存在 SnapManager 用户凭据缓存中，则 SnapManager 会提示您输入任何操作的密码。如果输入 `smsap credential set -host` 命令、则会将操作系统凭据保存在 SnapManager 凭据缓存文件中、因此 SnapManager 不会提示输入任何操作的密码。

如果您通过 SnapManager 服务器的身份验证，则视为有效用户。执行任何操作的有效用户都必须是执行操作的主机上的有效用户帐户。例如，如果您执行克隆操作，则应能够登录到克隆的目标主机。



SnapManager for SAP 可能无法授权在中央 Active Directory 服务中创建的用户、例如 LDAP 和 ADS。要确保身份验证不会失败、您必须将可配置的 `auth.disableServerAuthorization` 设置为 `true`。

作为有效用户，您可以通过以下方式管理凭据：

- 您也可以将 SnapManager 配置为将用户凭据存储在 SnapManager 用户凭据文件中。

默认情况下， SnapManager 不存储主机凭据。例如，如果您的自定义脚本需要访问远程主机，则可能需要更改此设置。远程克隆操作是一个需要远程主机用户登录凭据的 SnapManager 操作示例。要使 SnapManager 在 SnapManager 用户凭据缓存中记住用户主机登录凭据、请在 `smsap.config` 文件中将 `host.credentials.persist` 属性设置为 `* true *`。

- 您可以授权用户访问存储库。
- 您可以授权用户访问配置文件。
- 您可以查看所有用户凭据。
- 您可以清除所有资源（主机，存储库和配置文件）的用户凭据。
- 您可以删除各个资源（主机，存储库和配置文件）的凭据。

存储自定义脚本的加密密码

默认情况下， SnapManager 不会将主机凭据存储在用户凭据缓存中。但是，您可以更改此设置。您可以编辑 `smsap.config` 文件以允许存储主机凭据。

关于此任务

`smsap.config` 文件位于 `<default installation location>\properties\smsap.config`

步骤

1. 编辑 `smsap.config` 文件。
2. 将 `host.credentials.persistent` 设置为 `* true *`。

授权访问存储库

通过 SnapManager ，您可以为数据库用户设置访问存储库的凭据。您可以使用凭据限制或阻止对 SnapManager 主机，存储库，配置文件和数据库的访问。

关于此任务

如果使用 `credential set` 命令设置凭据、则 SnapManager 不会提示您输入密码。

您可以在安装 SnapManager 或更高版本时设置用户凭据。

步骤

1. 输入以下命令：

```
* smsap凭据集-repository -dbname repo_service_name-host repo_host-login  
-username repo_username[-password repo_password]-port repo_port*
```

授权对配置文件的访问

使用 SnapManager 可以为配置文件设置密码，以防止未经授权的访问。

步骤

1. 输入以下命令：

```
* smsap凭据集-profile -name profile_name[-password password]*
```

查看用户凭据

您可以列出有权访问的主机，配置文件和存储库。

步骤

1. 要列出您有权访问的资源、请输入以下命令：

```
* smsap凭据列表*
```

查看用户凭据的示例

此示例显示您有权访问的资源。

```
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
```

清除所有主机、存储库和配置文件的用户凭据

您可以清除资源（主机，存储库和配置文件）的凭据缓存。此操作将删除运行命令的用户的所有资源凭据。清除缓存后，您必须重新对凭据进行身份验证，才能访问这些受保护的

资源。

步骤

1. 要清除凭据、请在SnapManager 命令行界面中输入`smsap credential clear`命令、或者从SnapManager 图形用户界面中选择*管理*>*凭据*>*清除缓存*。
2. 退出 SnapManager 图形用户界面。



- 如果已从 SnapManager 图形用户界面中清除凭据缓存，则无需退出 SnapManager 图形用户界面。
- 如果已从 SnapManager 命令行界面清除凭据缓存，则必须重新启动 SnapManager 图形用户界面。
- 如果您手动删除了加密的凭据文件，则必须重新启动 SnapManager 图形用户界面。

3. 要再次设置凭据，请重复此过程为存储库，配置文件主机和配置文件设置凭据。有关重新设置用户凭据的追加信息信息，请参阅 "清除凭据缓存后设置凭据"。

清除凭据缓存后设置凭据

清除缓存以删除存储的用户凭据后，您可以设置主机，存储库和配置文件的凭据。

关于此任务

您必须确保为存储库，配置文件主机和配置文件设置与先前相同的用户凭据。在设置用户凭据时，系统会创建加密的凭据文件。

凭据文件位于`C:\Documents and Settings\Administrator\Application Data\NetApp\smsap\3.3.0`。

在 SnapManager 图形用户界面（GUI）中，如果存储库下没有存储库，请执行以下步骤：

步骤

1. 单击 * 任务 * > * 添加现有存储库 * 以添加现有存储库。
2. 执行以下步骤为存储库设置凭据：
 - a. 右键单击存储库并选择 * 打开 *。
 - b. 在`Repository Credentials Authentication`窗口中、输入用户凭据。
3. 执行以下步骤为主机设置凭据：
 - a. 右键单击存储库下的主机，然后选择 * 打开 *。
 - b. 在`Host Credentials Authentication`窗口中、输入用户凭据。
4. 执行以下步骤为配置文件设置凭据：
 - a. 右键单击主机下的配置文件并选择 * 打开 *。
 - b. 在`Profile Credentials Authentication`窗口中、输入用户凭据。

删除单个资源的凭据

您可以删除任何一个受保护资源的凭据，例如配置文件，存储库或主机。这样，您就可以仅删除一个资源的凭据，而不是清除所有资源的用户凭据。

删除存储库的用户凭据

您可以删除凭据，以使用户无法再访问特定存储库。使用此命令，您可以仅删除一个资源的凭据，而不是清除所有资源的用户凭据。

步骤

1. 要删除用户的存储库凭据、请输入以下命令：

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

删除主机的用户凭据

您可以删除主机的凭据，使用户无法再访问它。使用此命令，您可以仅删除一个资源的凭据，而不是清除所有资源的所有用户凭据。

步骤

1. 要删除用户的主机凭据、请输入以下命令：

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

删除配置文件的用户凭据

您可以删除配置文件的用户凭据，以使用户无法再访问它。

步骤

1. 要删除用户的配置文件凭据、请输入以下命令：

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

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。