



## 보안 및 자격 증명 관리 SnapManager for SAP

NetApp  
April 19, 2024

# 목차

보안 및 자격 증명 관리 .....	1
사용자 인증이란 무엇입니까 .....	1
사용자 지정 스크립트에 대해 암호화된 암호를 저장합니다 .....	2
리포지토리에 대한 액세스 권한을 부여합니다 .....	2
프로파일에 대한 액세스를 승인합니다 .....	3
사용자 자격 증명을 봅니다 .....	3
모든 호스트, 저장소 및 프로필에 대한 사용자 자격 증명을 지웁니다 .....	4
개별 리소스에 대한 자격 증명을 삭제합니다 .....	5

# 보안 및 자격 증명 관리

사용자 인증을 적용하여 SnapManager에서 보안을 관리할 수 있습니다. 사용자 인증 방법을 사용하면 저장소, 호스트 및 프로필과 같은 리소스에 액세스할 수 있습니다.

CLI(Command-Line Interface) 또는 GUI(그래픽 사용자 인터페이스)를 사용하여 작업을 수행할 때 SnapManager는 리포지토리 및 프로파일에 대해 설정된 자격 증명을 검색합니다. SnapManager는 이전 설치의 자격 증명을 저장합니다.

리포지토리와 프로필은 암호로 보호할 수 있습니다. 자격 증명은 개체에 대해 사용자에게 대해 구성된 암호이며 암호는 개체 자체에 구성되어 있지 않습니다.

다음 작업을 수행하여 인증 및 자격 증명을 관리할 수 있습니다.

- 운용에 대한 비밀번호 프롬프트나 'msap credential set' 명령어를 이용하여 사용자 인증을 관리한다.

리포지토리, 호스트 또는 프로파일에 대한 자격 증명을 설정합니다.

- 액세스 권한이 있는 리소스를 제어하는 자격 증명을 봅니다.
- 모든 리소스(호스트, 리포지토리 및 프로필)에 대한 사용자 자격 증명을 지웁니다.
- 개별 리소스(호스트, 리포지토리 및 프로필)에 대한 사용자의 자격 증명을 삭제합니다.



리포지토리 데이터베이스가 Windows 호스트에 있는 경우 로컬 또는 관리자 사용자와 도메인 사용자 모두 동일한 자격 증명을 가져야 합니다.

## 사용자 인증이란 무엇입니까

SnapManager는 SnapManager 서버가 실행 중인 호스트에서 운영 체제(OS) 로그인을 사용하여 사용자를 인증합니다. 작업 시 암호 프롬프트를 통해 또는 SMO 자격 증명을 사용하여 사용자 인증을 활성화할 수 있습니다. 작업 시 암호 프롬프트를 통해 또는 'msap 자격 증명 세트'를 사용하여 사용자 인증을 활성화할 수 있습니다.

사용자 인증 요구 사항은 작업이 수행되는 위치에 따라 다릅니다.

- SnapManager 클라이언트가 SnapManager 호스트와 동일한 서버에 있는 경우 OS 자격 증명을 통해 인증됩니다.

SnapManager 서버가 실행 중인 호스트에 이미 로그인했으므로 암호를 묻는 메시지가 표시되지 않습니다.

- SnapManager 클라이언트와 SnapManager 서버가 서로 다른 호스트에 있는 경우 SnapManager는 두 OS 자격 증명을 모두 사용하여 사용자를 인증해야 합니다.

SnapManager 사용자 자격 증명 캐시에 OS 자격 증명을 저장하지 않은 경우 SnapManager에서 작업에 대한 암호를 묻는 메시지를 표시합니다. 'msap credentials set-host' 명령을 입력하면 OS 자격 증명을 SnapManager 자격 증명 캐시 파일에 저장하므로 SnapManager에서 작업에 대한 암호를 묻지 않습니다.

SnapManager 서버로 인증된 사용자는 유효한 사용자로 간주됩니다. 모든 작업에 대한 유효 사용자는 작업이 실행되는 호스트의 유효한 사용자 계정이어야 합니다. 예를 들어 클론 작업을 실행하는 경우 클론의 대상 호스트에 로그인할 수 있어야 합니다.



SnapManager for SAP는 LDAP 및 ADS와 같은 중앙 Active Directory 서비스에서 생성된 사용자에게 권한을 부여하는 데 실패할 수 있습니다. 인증이 실패하지 않도록 하려면 구성 가능한 "auth.disableServerAuthorization"을 \* true \* 로 설정해야 합니다.

효과적인 사용자는 다음과 같은 방법으로 자격 증명을 관리할 수 있습니다.

- 필요에 따라 SnapManager 사용자 자격 증명 파일에 사용자 자격 증명을 저장하도록 SnapManager를 구성할 수 있습니다.

기본적으로 SnapManager는 호스트 자격 증명을 저장하지 않습니다. 예를 들어 원격 호스트에서 액세스해야 하는 사용자 지정 스크립트가 있는 경우 이 옵션을 변경할 수 있습니다. 원격 클론 작업은 원격 호스트에 대한 사용자의 로그인 자격 증명이 필요한 SnapManager 작업의 예입니다. SnapManager가 SnapManager 사용자 자격 증명 캐시에서 사용자 호스트 로그인 자격 증명을 기억하도록 하려면 'smsap.config' 파일에서 'host.credentials.persist' 속성을 \* true \* 로 설정합니다.

- 리포지토리에 대한 사용자 액세스를 승인할 수 있습니다.
- 프로파일에 대한 사용자 액세스 권한을 부여할 수 있습니다.
- 모든 사용자 자격 증명을 볼 수 있습니다.
- 모든 리소스(호스트, 리포지토리 및 프로필)에 대한 사용자 자격 증명을 지울 수 있습니다.
- 개별 리소스(호스트, 리포지토리 및 프로필)에 대한 자격 증명을 삭제할 수 있습니다.

## 사용자 지정 스크립트에 대해 암호화된 암호를 저장합니다

기본적으로 SnapManager는 호스트 자격 증명을 사용자 자격 증명 캐시에 저장하지 않습니다. 그러나 변경할 수 있습니다. 'msap.config' 파일을 편집하여 호스트 자격 증명을 저장할 수 있습니다.

### 이 작업에 대해

'msap.config' 파일은 '<기본 설치 위치>\properties\smsap.config'에 있습니다

단계

1. 'msap.config' 파일을 편집합니다.
2. 'host.credentials.persist'를 \* TRUE \* 로 설정합니다.

## 리포지토리에 대한 액세스 권한을 부여합니다

SnapManager를 사용하면 데이터베이스 사용자가 리포지토리에 액세스할 수 있도록 자격 증명을 설정할 수 있습니다. 자격 증명을 사용하여 SnapManager 호스트, 저장소, 프로필 및 데이터베이스에 대한 액세스를 제한하거나 제한할 수 있습니다.

### 이 작업에 대해

'credentials set' 명령어를 사용해 credentials를 설정하는 경우 SnapManager에서 암호를 묻는 메시지를 표시하지 않습니다.

SnapManager 이상을 설치할 때 사용자 자격 증명을 설정할 수 있습니다.

단계

1. 다음 명령을 입력합니다.

```
"* smssap 자격 증명 세트 -repository -dbname_repo_service_name_-host_repo_host_-login  
-username_repo_username_-password_repo_password_-port_repo_port_*
```

## 프로파일에 대한 액세스를 승인합니다

SnapManager를 사용하면 무단 액세스를 방지하기 위해 프로필에 대한 암호를 설정할 수 있습니다.

단계

1. 다음 명령을 입력합니다.

```
"* smssap 자격 증명 세트 -profile-name_profile_name_-password_password_*
```

## 사용자 자격 증명을 봅니다

액세스 권한이 있는 호스트, 프로필 및 리포지토리를 나열할 수 있습니다.

단계

1. 액세스 권한이 있는 리소스를 나열하려면 다음 명령을 입력합니다.

```
'* smsap 자격 증명 목록 *'
```

### 사용자 자격 증명 보기 예

이 예제에서는 액세스 권한이 있는 리소스를 표시합니다.

```
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
```

## 모든 호스트, 저장소 및 프로필에 대한 사용자 자격 증명을 지웁니다

리소스(호스트, 리포지토리 및 프로필)에 대한 자격 증명의 캐시를 지울 수 있습니다. 이렇게 하면 명령을 실행하는 사용자의 모든 리소스 자격 증명에 삭제가 됩니다. 캐시를 지운 후 이러한 보안 리소스에 액세스하려면 자격 증명을 다시 인증해야 합니다.

단계

1. 자격 증명을 지우려면 SnapManager CLI에서 'msap 자격 증명 지우기' 명령을 입력하거나 SnapManager GUI에서 \* 관리자 \* > \* 자격 증명 \* > \* 캐시 지우기 \* 를 선택합니다.
2. SnapManager GUI를 종료합니다.



- SnapManager GUI에서 자격 증명 캐시를 지운 경우에는 SnapManager GUI를 종료할 필요가 없습니다.
- SnapManager CLI에서 자격 증명 캐시를 지운 경우 SnapManager GUI를 다시 시작해야 합니다.
- 암호화된 자격 증명 파일을 수동으로 삭제한 경우 SnapManager GUI를 다시 시작해야 합니다.

3. 자격 증명을 다시 설정하려면 프로세스를 반복하여 리포지토리, 프로필 호스트 및 프로필에 대한 자격 증명을 설정합니다. 사용자 자격 증명 다시 설정에 대한 자세한 내용은 "자격 증명 캐시 지우기 후 자격 증명 설정"을 참조하십시오.

## 자격 증명 캐시를 지운 후 자격 증명을 설정합니다

캐시를 지워 저장된 사용자 자격 증명을 제거한 후 호스트, 저장소 및 프로필에 대한 자격 증명을 설정할 수 있습니다.

이 작업에 대해

이전에 제공한 리포지토리, 프로필 호스트 및 프로필에 대해 동일한 사용자 자격 증명을 설정해야 합니다. 사용자 자격 증명을 설정하는 동안 암호화된 자격 증명 파일이 생성됩니다.

자격 증명 파일은 'C:\Documents and Settings\Administrator\Application Data\NetApp\smssap\3.3.0'에 있습니다.

SnapManager 그래픽 사용자 인터페이스(GUI)에서 리포지토리에 리포지토리가 없는 경우 다음 단계를 수행합니다.

단계

1. 기존 리포지토리를 추가하려면 \* 작업 \* > \* 기존 리포지토리 추가 \* 를 클릭합니다.
2. 리포지토리에 대한 자격 증명을 설정하려면 다음 단계를 수행하십시오.
  - a. 리포지토리를 마우스 오른쪽 단추로 클릭하고 \* 열기 \* 를 선택합니다.
  - b. 리포지터리 자격 증명 인증 창에 사용자 자격 증명을 입력합니다.
3. 호스트에 대한 자격 증명을 설정하려면 다음 단계를 수행하십시오.
  - a. 리포지토리 아래에서 호스트를 마우스 오른쪽 버튼으로 클릭하고 \* Open \* 을 선택합니다.
  - b. Host Credentials Authentication 창에 사용자 자격 증명을 입력합니다.
4. 프로파일에 대한 자격 증명을 설정하려면 다음 단계를 수행하십시오.
  - a. 호스트 아래에서 프로파일을 마우스 오른쪽 단추로 클릭하고 \* 열기 \* 를 선택합니다.
  - b. Profile Credentials Authentication 창에서 사용자 자격 증명을 입력합니다.

## 개별 리소스에 대한 자격 증명을 삭제합니다

프로필, 리포지토리 또는 호스트와 같은 보안 리소스 중 하나에 대한 자격 증명을 삭제할 수 있습니다. 이렇게 하면 모든 리소스에 대한 사용자 자격 증명을 지우지 않고 한 리소스에 대한 자격 증명만 제거할 수 있습니다.

### 리포지토리에 대한 사용자 자격 증명을 삭제합니다

사용자가 더 이상 특정 리포지토리에 액세스할 수 없도록 자격 증명을 삭제할 수 있습니다. 이 명령을 사용하면 모든 리소스에 대한 사용자 자격 증명을 지우지 않고 한 리소스에 대한 자격 증명만 제거할 수 있습니다.

단계

1. 사용자의 저장소 자격 증명을 삭제하려면 다음 명령을 입력합니다.

```
* smssap 자격 증명 삭제 - repository-dbname_repo_service_name_-host_repo_host_-login-username_repo_username_-port_repo_port_ *
```

### 호스트에 대한 사용자 자격 증명을 삭제합니다

사용자가 더 이상 액세스할 수 없도록 호스트의 자격 증명을 삭제할 수 있습니다. 이 명령을 사용하면 모든 리소스에 대한 사용자 자격 증명을 지우지 않고 한 리소스에 대한 자격 증명만 제거할 수 있습니다.

단계

1. 사용자의 호스트 자격 증명을 삭제하려면 다음 명령을 입력합니다.

```
'msap credential delete-host-name_host_name_-username_-username_'
```

프로파일에 대한 사용자 자격 증명을 삭제합니다

사용자가 더 이상 프로파일에 액세스할 수 없도록 프로파일의 사용자 자격 증명을 삭제할 수 있습니다.

단계

1. 사용자의 프로필 자격 증명을 삭제하려면 다음 명령을 입력합니다.

```
* smssap 자격 증명 삭제 - profile-name_profile_name_*
```



## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.