



## 인증서 기반 인증을 구성합니다

### SnapCenter Software 5.0

NetApp  
April 30, 2024

# 목차

인증서 기반 인증을 구성합니다 .....	1
SnapCenter 서버에서 CA(인증 기관) 인증서를 내보냅니다 .....	1
CA(인증 기관) 인증서를 Windows 플러그인 호스트로 가져옵니다 .....	1
CA 인증서를 UNIX 호스트 플러그인으로 가져오고 SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다 .....	2
인증서 기반 인증을 사용합니다 .....	3

# 인증서 기반 인증을 구성합니다

## SnapCenter 서버에서 CA(인증 기관) 인증서를 내보냅니다

MMC(Microsoft Management Console)를 사용하여 SnapCenter 서버에서 플러그인 호스트로 CA 인증서를 내보내야 합니다.

시작하기 전에

양방향 SSL을 구성해야 합니다.

• 단계 \*

1. MMC(Microsoft Management Console)로 이동한 다음 \* 파일 \* > \* Snapin 추가/제거 \* 를 클릭합니다.
2. 스냅인 추가/제거 창에서 \* 인증서 \* 를 선택한 다음 \* 추가 \* 를 클릭합니다.
3. 인증서 스냅인 창에서 \* 컴퓨터 계정 \* 옵션을 선택한 다음 \* 마침 \* 을 클릭합니다.
4. 콘솔 루트 \* > \* 인증서 - 로컬 컴퓨터 \* > \* 개인 \* > \* 인증서 \* 를 클릭합니다.
5. SnapCenter 서버에 사용되는 조달된 CA 인증서를 마우스 오른쪽 단추로 클릭한 다음 \* 모든 작업 \* > \* 내보내기 \* 를 선택하여 내보내기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행합니다.
개인 키를 내보냅니다	아니오, 개인 키를 내보내지 않습니다 * 를 선택한 후 * 다음 * 을 클릭합니다.
파일 형식 내보내기	다음 * 을 클릭합니다.
파일 이름	찾아보기 * 를 클릭하고 인증서를 저장할 파일 경로를 지정한 후 * 다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 내보내기를 시작합니다.



SnapCenter HA 구성 및 VMware vSphere용 SnapCenter 플러그인에는 인증서 기반 인증이 지원되지 않습니다.

## CA(인증 기관) 인증서를 Windows 플러그인 호스트로 가져옵니다

내보낸 SnapCenter 서버 CA 인증서를 사용하려면 Microsoft 관리 콘솔(MMC)을 사용하여 관련 인증서를 SnapCenter Windows 플러그인 호스트로 가져와야 합니다.

• 단계 \*

1. MMC(Microsoft Management Console)로 이동한 다음 \* 파일 \* > \* Snapin 추가/제거 \* 를 클릭합니다.

2. 스냅인 추가/제거 창에서 \* 인증서 \* 를 선택한 다음 \* 추가 \* 를 클릭합니다.
3. 인증서 스냅인 창에서 \* 컴퓨터 계정 \* 옵션을 선택한 다음 \* 마침 \* 을 클릭합니다.
4. 콘솔 루트 \* > \* 인증서 - 로컬 컴퓨터 \* > \* 개인 \* > \* 인증서 \* 를 클릭합니다.
5. "개인" 폴더를 마우스 오른쪽 단추로 클릭한 다음 \* 모든 작업 \* > \* 가져오기 \* 를 선택하여 가져오기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행합니다.
매장 위치	다음 * 을 클릭합니다.
가져올 파일	cer 확장자로 끝나는 SnapCenter 서버 인증서를 선택합니다.
인증서 저장소	다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

## CA 인증서를 UNIX 호스트 플러그인으로 가져오고 SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

### CA 인증서를 UNIX 플러그인 호스트로 가져옵니다

CA 인증서를 UNIX 플러그인 호스트로 가져와야 합니다.

- 이 작업에 대한 정보 \*
- SPL 키 저장소의 암호 및 사용 중인 CA 서명 키 쌍의 별칭을 관리할 수 있습니다.
- SPL 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.
- 단계 \*
  1. SPL 속성 파일에서 SPL 키 저장소 기본 암호를 검색할 수 있습니다. 키에 해당하는 값입니다 `SPL_KEYSTORE_PASS`.
  2. 키 저장소 암호를 변경합니다. `$ keytool -storepasswd -keystore keystore.jks`
  3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다. `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. `SPL_keystore_pass` in 키에 대해서도 동일하게 업데이트하십시오 `spl.properties`` 파일.
  5. 암호를 변경한 후 서비스를 다시 시작합니다.

### SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

루트 또는 중간 인증서를 SPL 신뢰 저장소에 구성해야 합니다. 루트 CA 인증서와 중간 CA

인증서를 추가해야 합니다.

• 단계 \*

1. SPL 키 저장소가 포함된 폴더로 이동합니다. `/var/opt/snapcenter/spl/etc.`
2. 파일을 찾습니다 `keystore.jks`.
3. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
4. 루트 또는 중간 인증서 추가: `$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.

**CA 서명 키 쌍을 SPL 신뢰 저장소에 구성합니다**

CA 서명된 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

• 단계 \*

1. SPL의 키 저장소가 포함된 폴더로 이동합니다 `/var/opt/snapcenter/spl/etc.`
2. 파일을 찾습니다 `keystore.jks`.`
3. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
4. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

기본 SPL 키 저장소 암호는 `SPL_keystore_pass` in 키의 값입니다 `spl.properties` 파일.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. CA 인증서의 별칭 이름이 길고 공백 또는 특수 문자(" ", ",")가 포함된 경우 별칭 이름을 단순 이름으로 변경합니다. `$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks``
2. 에 있는 키 저장소에서 별칭 이름을 구성합니다 `spl.properties` 파일. 이 값을 `SPL_CERTIFICATE_ALIAS` 키에 대해 업데이트합니다.
3. CA 서명 키 쌍을 SPL 신뢰 저장소에 구성한 후 서비스를 다시 시작합니다.

## 인증서 기반 인증을 사용합니다

SnapCenter 서버 및 Windows 플러그인 호스트에 대한 인증서 기반 인증을 활성화하려면 다음 PowerShell cmdlet을 실행합니다. Linux 플러그인 호스트의 경우 양방향 SSL을 활성화하면

## 인증서 기반 인증이 활성화됩니다.

- 클라이언트 인증서 기반 인증을 사용하려면 다음을 따르십시오.

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 클라이언트 인증서 기반 인증을 사용하지 않도록 설정하려면 다음을 따르십시오.

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

## 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.