



CA 인증서 구성

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/snapcenter-61/protect-nsp/generate_CA_certificate_CSR_file.html on November 06, 2025. Always check docs.netapp.com for the latest.

목차

CA 인증서 구성	1
CA 인증서 CSR 파일 생성	1
CA 인증서 가져오기	1
CA 인증서 지문을 받으세요	2
Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성	2
Linux 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성	3
사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리	3
플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성	4
플러그인 신뢰 저장소에 CA 서명 키 쌍 구성	4
플러그인에 대한 인증서 해지 목록(CRL) 구성	5
Windows 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성	5
사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리	6
플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성	6
플러그인 신뢰 저장소에 CA 서명 키 쌍 구성	7
SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성	7
플러그인에 대한 CA 인증서 활성화	8

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

-  CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".

-  도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 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 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.

이 마법사 창에서...	다음을 수행하세요...
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
 - a. 인증서를 두 번 클릭합니다.
 - b. 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
 - c. 필드 목록을 스크롤하여 *지문*을 클릭하세요.
 - d. 상자에서 16진수 문자를 복사하세요.
 - e. 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
 - a. 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.
 - b. 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에  
바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::.NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0:_<SMCore Port>_ certhash=$cert  
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::.NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0:_<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Linux 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `/opt/NetApp/snapcenter/scc/etc`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
```

- . 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

- . 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks  
. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자 ("*, ", ") 가 포함된 경우 별칭 이름을  
간단한 이름으로 변경합니다.
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks  
. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.
```

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 KEYSTORE_PASS 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

```
C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키툴 -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. `keystore.jks` 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

`keytool -list -v -keystore keystore.jks`

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

키툴 `-importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -`
대상키스토어 `keystore.jks` -대상키스토어 유형 JKS

5. 키스토어에 추가된 인증서를 나열합니다.

`keytool -list -v -keystore keystore.jks`

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 `agent.properties` 파일의 `KEYSTORE_PASS` 키 값입니다.

키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks

8. `agent.properties` 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 `SCC_CERTIFICATE_ALIAS` 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)" .
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 `_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl_`입니다.

단계

1. `agent.properties` 파일에서 기본 디렉토리를 `CRL_PATH` 키에 맞춰 수정하고 업데이트할 수 있습니다.

2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- *Set-SmCertificateSettings* cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- *_Get-SmCertificateSettings_* 를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 *_Get-Help command_name_* 을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- * *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- * *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- * *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- * *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그레픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 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 라이센스도 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 있으며 재사용이 불가능하며 취소 불가능한 라이센스를 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 라이센스는 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.