인증서 기반 인증을 구성합니다

SnapCenter Software 5.0

NetApp
July 18, 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 `SPL_KEYSTORE_PASS`값입니다.
  2. 키 저장소 암호 변경: `$ keytool -storepasswd -keystore keystore.jks`
  3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용된 것과 동일한 암호로 변경합니다.
     `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. 파일에서 SPL_keystore_pass 키에 대해 동일하게 `spl.properties` 업데이트합니다.
  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 있는 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 <AliasNameForCerticateToBeImported> -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 있는 폴더로 `/var/opt/snapcenter/spl/etc`이동합니다.
2. 파일을 찾습니다 `keystore.jks`.
3. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
4. 개인 키와 공개 키가 모두 있는 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 파일의 키 SPL_keystore_pass `spl.properties` 값입니다.

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

1. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*",",")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다. `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. 파일에 있는 키 저장소에서 별칭 이름을 `spl.properties` 구성합니다. 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

상표 정보