CA 인증서를 구성합니다

SnapCenter Software 4.9

NetApp
March 20, 2024

목차

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

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

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 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 * > * 신뢰할 수 있는 루트 인증 기관 * > * 인증서 * 를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.

이 마법사 창에서...	다음을 수행합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

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

단계

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

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

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와
   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 들면 다음과 같습니다.

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

Linux 호스트에서 SnapCenter 사용자 지정 플러그인 서비스에 대한 CA 인증서를 구성합니다

사용자 지정 플러그인 키 저장소 및 인증서의 암호를 관리하고, CA 인증서를 구성하고, 사용자 지정 플러그인 트러스트 저장소에 대한 루트 또는 중간 인증서를 구성하고, SnapCenter 사용자 지정 플러그인 서비스를 사용하여 사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

사용자 지정 플러그인은 _/opt/netapp/snapcenter/SCC/etc_에 있는 'keystore.jks' 파일을 신뢰 저장소 및 키 저장소로 사용합니다.

사용자 지정 플러그인 키 저장소 및 사용 중인 CA 서명 키 쌍의 별칭에 대한 암호를 관리합니다

단계

1. 사용자 지정 플러그인 에이전트 속성 파일에서 사용자 지정 플러그인 키 저장소 기본 암호를 검색할 수 있습니다.

   'keystore_pass' 키에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

```
 keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.
```

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

agent.properties 파일의 keystore_pass 키에 대해서도 동일한 업데이트를 하십시오.

3. 암호를 변경한 후 서비스를 다시 시작합니다.

사용자 지정 플러그인 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 루트 또는 중간 인증서를 구성합니다

사용자 지정 플러그인 트러스트 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 사용자 지정 플러그인 키 저장소가 포함된 폴더로 이동합니다. /opt/netapp/snapcenter/SCC 등
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

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

4. 루트 또는 중간 인증서 추가:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. 루트 또는 중간 인증서를 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.
```

루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 **CA** 서명 키 쌍을 구성합니다

CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성해야 합니다.

단계

1. 사용자 지정 플러그인 키 저장소/opt/NetApp/snapcenter/SCC 등이 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
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 /root/snapcenter.ssl.test.netapp.com.pfx
-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 사용자 지정 플러그인 키 저장소 암호는 agent.properties 파일의 keystore_pass 키 값입니다.

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

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

   이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

SnapCenter 사용자 지정 플러그인에 대한 CRL(인증서 해지 목록)을 구성합니다

이 작업에 대해

- SnapCenter 사용자 지정 플러그인은 사전 구성된 디렉터리에서 CRL 파일을 검색합니다.
- SnapCenter 사용자 지정 플러그인에 대한 CRL 파일의 기본 디렉토리는 'opt/netapp/snapcenter/SCC/etc/CRL'입니다.

단계

1. agent.properties 파일의 기본 디렉터리를 수정하여 CRL_path 키에 맞게 업데이트할 수 있습니다.

   이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

Windows 호스트에서 SnapCenter 사용자 지정 플러그인 서비스에 대한 CA 인증서를 구성합니다

사용자 지정 플러그인 키 저장소 및 인증서의 암호를 관리하고, CA 인증서를 구성하고, 사용자 지정 플러그인 트러스트 저장소에 대한 루트 또는 중간 인증서를 구성하고, SnapCenter 사용자

지정 플러그인 서비스를 사용하여 사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

사용자 지정 플러그인은 _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 file_keystore.jks_를 신뢰 저장소 및 키 저장소로 사용합니다.

사용자 지정 플러그인 키 저장소 및 사용 중인 **CA** 서명 키 쌍의 별칭에 대한 암호를 관리합니다

단계

1. 사용자 지정 플러그인 에이전트 속성 파일에서 사용자 지정 플러그인 키 저장소 기본 암호를 검색할 수 있습니다.

   key_keystore_pass_에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

   _keytool - storepasswd - keystore keystore.jks _

   Windows 명령 프롬프트에서 "keytool" 명령을 인식할 수 없는 경우 keytool 명령을 전체 경로로 바꿉니다.

   _C:\Program Files\Java\<JDK_VERSION>\bin\keytool.exe" - 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_in_cert" -keystore keystore.jks _

   agent.properties 파일의 keystore_pass 키에 대해서도 동일한 업데이트를 하십시오.

4. 암호를 변경한 후 서비스를 다시 시작합니다.

   사용자 지정 플러그인 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 루트 또는 중간 인증서를 구성합니다

사용자 지정 플러그인 트러스트 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 사용자 지정 플러그인 keystore_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_가 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

4. 루트 또는 중간 인증서 추가:

   _keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks _

5. 루트 또는 중간 인증서를 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성합니다

CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성해야 합니다.

단계

1. 사용자 지정 플러그인 keystore_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_가 포함된 폴더로 이동합니다
2. *keystore.jks* 파일을 찾습니다.
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 /root/snapcenter.ssl.test.netapp.com.pfx -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 사용자 지정 플러그인 키 저장소 암호는 agent.properties 파일의 keystore_pass 키 값입니다.

   _keytool -keykeyasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks _

8. *agent.properties* 파일의 CA 인증서에서 별칭 이름을 구성합니다.

   이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

SnapCenter 사용자 지정 플러그인에 대한 CRL(인증서 해지 목록)을 구성합니다

이 작업에 대해

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 를 참조하십시오 "SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법".
- SnapCenter 사용자 지정 플러그인은 사전 구성된 디렉터리에서 CRL 파일을 검색합니다.
- SnapCenter 사용자 지정 플러그인에 대한 CRL 파일의 기본 디렉토리는 _'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\CRL'_입니다.

단계

1. *agent.properties* 파일의 기본 디렉터리를 수정하여 CRL_path 키에 맞게 업데이트할 수 있습니다.
2. 이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다.

들어오는 인증서는 각 CRL에 대해 확인됩니다.

플러그인에 대해 CA 인증서를 활성화합니다

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

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

> 상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.