Linux 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다

SnapCenter Software 6.0

NetApp
July 23, 2024

목차

Linux 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다

Linux 호스트에서 양방향 SSL 통신을 구성합니다

Linux 호스트의 SnapCenter 서버와 플러그인 간의 상호 통신을 보호하기 위해 양방향 SSL 통신을 구성해야 합니다.

시작하기 전에

- Linux 호스트용 CA 인증서를 구성해야 합니다.
- 모든 플러그인 호스트와 SnapCenter 서버에서 양방향 SSL 통신을 활성화해야 합니다.

단계

1. certificate.pem * 을 */etc/pki/ca-trust/source/anchors/* 에 복사합니다.
2. Linux 호스트의 신뢰 목록에 인증서를 추가합니다.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. 인증서가 신뢰 목록에 추가되었는지 확인합니다. `trust list | grep "<CN of your certificate>"`
4. SnapCenter * nginx * 파일에서 * ssl_certificate * 및 * ssl_certificate_key * 를 업데이트하고 다시 시작합니다.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. SnapCenter 서버 GUI 링크를 새로 고칩니다.
6. /<installation path>/NetApp/snapcenter/snapmanagerWeb_및 _/<installation path>/netapp/snapcenter/smcore_에 있는 * snapcoeServiceHost.dll.config * 에서 다음 키의 값을 업데이트합니다.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
   - <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>
7. 다음 서비스를 다시 시작합니다.
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. 인증서가 SnapManager 웹 포트에 연결되어 있는지 확인합니다. `openssl s_client -connect localhost:8146 -brief`
9. 인증서가 smcore 포트에 연결되어 있는지 확인합니다. `openssl s_client -connect localhost:8145 -brief`
10. SPL 키 저장소 및 별칭에 대한 암호를 관리합니다.
    a. SPL 속성 파일에서 * SPL_keystore_pass * 키에 할당된 SPL 키 저장소 기본 암호를 검색합니다.
    b. 키 저장소 암호를 변경합니다. `keytool -storepasswd -keystore keystore.jks`

c. 개인 키 항목의 모든 별칭에 대한 암호를 변경합니다. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`

d. *spl.properties* 에서 키 * spl_keystore_pass * 에 대해 동일한 암호를 업데이트합니다.

e. 서비스를 다시 시작합니다.

11. 플러그인 Linux 호스트에서 SPL 플러그인의 키 저장소에 루트 및 중간 인증서를 추가합니다.

- `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
- `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
  i. keystore.jks에서 항목을 확인합니다. `keytool -list -v -keystore <path to keystore.jks>`
  ii. 필요한 경우 별칭 이름을 바꿉니다. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`

12. *spl.properties* 파일의 * spl_certificate_alias * 값을 _keystore.jks_에 저장된 * certificate.pfx * 별칭으로 업데이트하고 SPL 서비스를 다시 시작합니다. `systemctl restart spl`

13. 인증서가 smcore 포트에 연결되어 있는지 확인합니다. `openssl s_client -connect localhost:8145 -brief`

Linux 호스트에서 SSL 통신을 활성화합니다

PowerShell 명령을 사용하여 Linux 호스트의 SnapCenter 서버와 플러그인 간의 상호 통신을 보호하기 위해 양방향 SSL 통신을 설정할 수 있습니다.

단계

1. 단방향 SSL 통신을 활성화하려면 다음을 수행하십시오.

a. SnapCenter GUI에 로그인합니다.

b. 설정 * > * 글로벌 설정 * 을 클릭하고 * SnapCenter Server에서 인증서 검증 활성화 * 를 선택합니다.

c. Hosts * > * Managed Hosts * 를 클릭하고 단방향 SSL을 활성화할 플러그인 호스트를 선택합니다.

d. 아이콘을 클릭한  다음 * 인증서 유효성 검사 활성화 * 를 클릭합니다.

2. SnapCenter 서버 Linux 호스트에서 양방향 SSL 통신을 활성화합니다.

- `Open-SmConnection`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
- `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

저작권 정보

상표 정보