



Linux 호스트에서 양방향 **SSL** 통신을 구성하고 활성화합니다

SnapCenter Software 6.0

NetApp
July 23, 2024

목차

Linux 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다	1
Linux 호스트에서 양방향 SSL 통신을 구성합니다	1
Linux 호스트에서 SSL 통신을 활성화합니다	2

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.jks`에서 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

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.