



Windows 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다

SnapCenter Software 6.0

NetApp
July 23, 2024

목차

Windows 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다	1
Windows 호스트에서 양방향 SSL 통신을 구성합니다	1
Windows 호스트에서 양방향 SSL 통신을 활성화합니다.....	3

Windows 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다

Windows 호스트에서 양방향 SSL 통신을 구성합니다

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

시작하기 전에

- 지원되는 최소 키 길이가 3072인 CA 인증서 CSR 파일을 생성해야 합니다.
- CA 인증서는 서버 인증 및 클라이언트 인증을 지원해야 합니다.
- 개인 키와 지문 세부 정보가 포함된 CA 인증서가 있어야 합니다.
- 단방향 SSL 구성을 활성화해야 합니다.

자세한 내용은 을 참조하십시오 "[CA 인증서 구성 섹션을 참조하십시오.](#)"

- 모든 플러그인 호스트와 SnapCenter 서버에서 양방향 SSL 통신을 활성화해야 합니다.

일부 호스트 또는 서버가 양방향 SSL 통신에 사용되지 않는 환경은 지원되지 않습니다.

단계

1. 포트를 바인딩하려면 SnapCenter IIS 웹 서버 포트 8146(기본값)용 SnapCenter 서버 호스트에서 다음 단계를 수행하고 PowerShell 명령을 사용하여 SMCORE 포트 8145(기본값)에 대해 다시 한 번 수행합니다.

- a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명된 인증서 포트 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

예를 들면, 다음과 같습니다.

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. 새로 조달한 CA 인증서를 SnapCenter 서버 및 SMCORE 포트와 바인딩합니다.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

예를 들면, 다음과 같습니다.

```

> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145

```

2. CA 인증서에 대한 권한에 액세스하려면 다음 단계를 수행하여 새로 조달된 CA 인증서에 액세스하여 인증서 권한 목록에 SnapCenter의 기본 IIS 웹 서버 사용자 "**IIS AppPool\SnapCenter**"를 추가합니다.
 - a. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * SnapIn 추가/제거 * 를 클릭합니다.
 - b. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
 - c. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
 - d. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 개인 * > * 인증서 * 를 클릭합니다.
 - e. SnapCenter 인증서를 선택합니다.
 - f. 사용자 추가권한 마법사를 시작하려면 CA 인증서를 마우스 오른쪽 버튼으로 클릭하고 * 모든 작업 * > * 개인 키 관리 * 를 선택합니다.
 - g. 추가 * 를 클릭하고 사용자 및 그룹 선택 마법사에서 위치를 로컬 컴퓨터 이름으로 변경합니다(계층 구조에서 맨 위).
 - h. IIS AppPool\SnapCenter 사용자를 추가하고 모든 제어 권한을 제공합니다.

3. CA 인증서 IIS 권한*의 경우 다음 경로에서 SnapCenter 서버의 새 DWORD 레지스트리 키 항목을 추가합니다.

Windows 레지스트리 편집기에서 아래 경로로 이동합니다.

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. SChannel 레지스트리 구성의 컨텍스트에서 새 DWORD 레지스트리 키 항목을 만듭니다.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

양방향 SSL 통신을 위해 SnapCenter Windows 플러그인을 구성합니다

PowerShell 명령을 사용하여 양방향 SSL 통신을 위해 SnapCenter Windows 플러그인을 구성해야 합니다.

시작하기 전에

CA 인증서 지문을 사용할 수 있는지 확인합니다.

단계

1. 포트를 바인딩하려면 Windows 플러그인 호스트에서 SMCore 포트 8145(기본값)에 대해 다음 작업을 수행합니다.

a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명된 인증서 포트 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
```

b. 새로 조달한 CA 인증서를 SMCore 포트와 바인딩합니다.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

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

예를 들면, 다음과 같습니다.

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

Windows 호스트에서 양방향 SSL 통신을 활성화합니다

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

• 시작하기 전에 *

모든 플러그인 및 SMCore 에이전트에 대한 명령을 먼저 실행한 다음 서버에 대해 명령을 실행합니다.

• 단계 *

1. 양방향 SSL 통신을 활성화하려면 플러그인, 서버 및 양방향 SSL 통신이 필요한 각 에이전트에 대해 SnapCenter 서버에서 다음 명령을 실행합니다.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

1. 다음 명령을 사용하여 IIS SnapCenter 응용 프로그램 풀 재활용 작업을 수행합니다. > Restart-WebAppPool -Name "SnapCenter"

2. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

양방향 SSL 통신을 비활성화합니다

PowerShell 명령을 사용하여 양방향 SSL 통신을 사용하지 않도록 설정할 수 있습니다.

- 이 작업에 대한 정보 *
- 모든 플러그인 및 SMCore 에이전트에 대한 명령을 먼저 실행한 다음 서버에 대해 명령을 실행합니다.
- 양방향 SSL 통신을 비활성화하면 CA 인증서와 해당 구성이 제거되지 않습니다.
- SnapCenter 서버에 새 호스트를 추가하려면 모든 플러그인 호스트에 대해 양방향 SSL을 비활성화해야 합니다.
- NLB 및 F5는 지원되지 않습니다.
- 단계 *

1. 양방향 SSL 통신을 비활성화하려면 모든 플러그인 호스트 및 SnapCenter 호스트에 대해 SnapCenter 서버에서 다음 명령을 실행합니다.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

1. 다음 명령을 사용하여 IIS SnapCenter 응용 프로그램 풀 재활용 작업을 수행합니다. > Restart-WebAppPool -Name "SnapCenter"

2. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

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.