



## **NetApp** 지원 플러그인 설치를 준비하세요 SnapCenter software

NetApp  
November 06, 2025

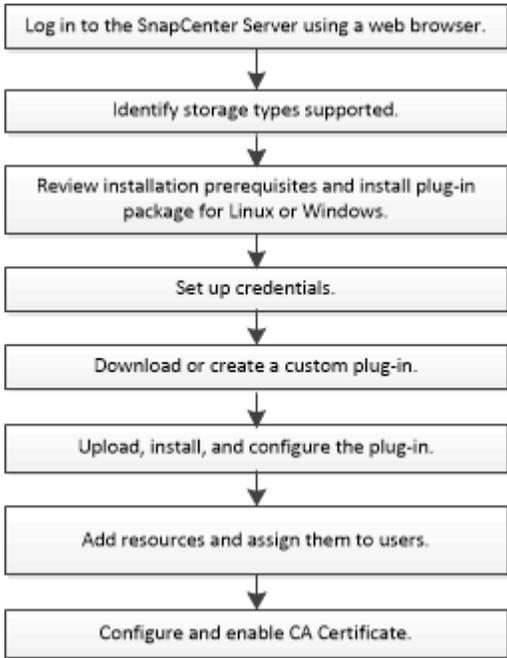
# 목차

NetApp 지원 플러그인 설치를 준비하세요	1
SnapCenter NetApp 지원 플러그인 설치 워크플로	1
Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건	1
일반적인	1
Windows 호스트	2
Linux 및 AIX 호스트	2
AIX 호스트 요구 사항	3
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	6
Linux 및 AIX용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	7
NetApp 지원 플러그인에 대한 자격 증명 설정	8
Windows Server 2016 이상에서 gMSA 구성	9
NetApp 지원 플러그인을 설치하세요	11
원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.	11
cmdlet을 사용하여 여러 원격 호스트에 Linux, Windows 또는 AIX용 SnapCenter 플러그인 패키지 설치	15
명령줄 인터페이스를 사용하여 Linux 호스트에 NetApp 지원 플러그인을 설치합니다.	15
NetApp 지원 플러그인 설치 상태 모니터링	16
CA 인증서 구성	17
CA 인증서 CSR 파일 생성	17
CA 인증서 가져오기	17
CA 인증서 지문을 받으세요	18
Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성	19
Linux 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성	19
Windows 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성	22
플러그인에 대한 CA 인증서 활성화	24

# NetApp 지원 플러그인 설치를 준비하세요

## SnapCenter NetApp 지원 플러그인 설치 워크플로

NetApp 지원 플러그인 리소스를 보호하려면 SnapCenter NetApp 지원 플러그인을 설치하고 설정해야 합니다.



## Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다. NetApp 지원 플러그인은 Windows, Linux 및 AIX 환경에서 지원됩니다.

**i** AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

- Linux, Windows 또는 AIX 호스트에 Java 11을 설치했어야 합니다.

**i** IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB 및 Storage 플러그인과 같은 NetApp 지원 플러그인은 호스트 추가 작업이 수행되는 클라이언트 호스트에서 사용할 수 있어야 합니다.

### 일반적인

iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.

## Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- SnapCenter 에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Microsoft Windows용 SnapCenter 플러그인을 수동으로 선택해야 합니다.

["Windows용 JAVA 다운로드"](#)

## Linux 및 AIX 호스트



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

SnapCenter 서버 호스트로 Windows Server 2019 또는 Windows Server 2016을 사용하는 경우 Java 11을 설치해야 합니다. 상호 운용성 매트릭스 도구(IMT)에는 요구 사항에 대한 최신 정보가 포함되어 있습니다.

["Linux용 JAVA 다운로드"](#)

["AIX용 JAVA 다운로드"](#)

["NetApp 상호 운용성 매트릭스 도구"](#)

- 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.



Sudo 버전 1.8.7 이상을 사용하고 있는지 확인하세요.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

`_LINUX_USER_`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value_`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

## AIX 호스트 요구 사항

AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.



AIX용 SnapCenter 플러그인 패키지의 일부인 UNIX용 SnapCenter 플러그인은 동시 볼륨 그룹을 지원하지 않습니다.

목	요구 사항
운영 체제	AIX 7.1 이상

목	요구 사항
호스트의 SnapCenter 플러그인을 위한 최소 RAM	4GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  <p>충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.</p> </div>
필수 소프트웨어 패키지	자바 11 IBM 자바  JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 도구](#)".

#### AIX 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 4.4 이상에서는 루트가 아닌 사용자도 AIX용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

#### 필요한 것

- Sudo 버전 1.8.7 이상.
- /etc/ssh/sshd\_config 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256

```

## 이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- /home/AIX\_USER/.sc\_netapp/snapcenter\_aix\_host\_plugin.bsx
- /custom\_location/ NetApp/snapcenter/spl/설치/플러그인/제거
- /custom\_location/ NetApp/snapcenter/spl/bin/spl

## 단계

1. AIX용 SnapCenter 플러그인 패키지를 설치하려는 AIX 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. '`<crs_home>/bin/olsnodes`'

`crs_home`의 값은 `_/etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_AIX_USER`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

## Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우  지원되는 버전에 대한 최신 정보는 다음을 참조하세요. " <a href="#">NetApp 상호 운용성 매트릭스 도구</a> ".
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB   충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.

목	요구 사항
필수 소프트웨어 패키지	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들</li> <li>• 파워셸 코어 7.4.2</li> <li>• Java 11 Oracle Java 및 OpenJDK</li> </ul> <p>Java 11 Oracle Java 및 OpenJDK는 SAP HANA, IBM Db2, PostgreSQL, MySQL, NetApp 지원 플러그인 및 Windows 호스트에 설치할 수 있는 기타 사용자 정의 애플리케이션에만 필요합니다.</p> <p>지원되는 버전에 대한 최신 정보는 다음을 참조하세요.  <a href="#">"NetApp 상호 운용성 매트릭스 도구"</a> .</p>

## Linux 및 AIX용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

목	요구 사항
운영 체제	<ul style="list-style-type: none"> <li>• 레드햇 엔터프라이즈 리눅스</li> <li>• 오라클 리눅스</li> <li>• SUSE Linux Enterprise Server(SLES)</li> </ul>
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.</p> </div>

목	요구 사항
필수 소프트웨어 패키지	Java 11 Oracle Java 또는 OpenJDK  JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 도구](#)"

## NetApp 지원 플러그인에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

시작하기 전에

- Linux 또는 AIX 호스트

Linux 또는 AIX 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

- NetApp 지원 플러그인 애플리케이션

플러그인은 리소스를 추가하는 동안 선택하거나 생성된 자격 증명을 사용합니다. 데이터 보호 작업 중에 리소스에 자격 증명이 필요하지 않은 경우 자격 증명을 \*없음\*으로 설정할 수 있습니다.

이 작업에 관하여

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 \*설정\*을 클릭합니다.
2. 설정 페이지에서 \*자격 증명\*을 클릭합니다.
3. \*새로 만들기\*를 클릭합니다.

4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름	<p>인증에 사용할 사용자 이름과 비밀번호를 입력하세요.</p> <ul style="list-style-type: none"> <li>도메인 관리자 또는 관리자 그룹의 모든 구성원</li> </ul> <p>SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS</i> 사용자 이름</li> <li>◦ 도메인 <i>FQDN</i> 사용자 이름</li> </ul> <ul style="list-style-type: none"> <li>로컬 관리자(작업 그룹에만 해당)</li> </ul> <p>작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i></p>
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 유형	사용할 인증 유형을 선택하세요.
sudo 권한을 사용하세요	<p>루트가 아닌 사용자에게 자격 증명을 생성하는 경우 <b>sudo</b> 권한 사용 확인란을 선택합니다.</p> <p> Linux 및 AIX 사용자에게만 적용됩니다.</p>

5. \*확인\*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

## Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

## 시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

## 단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
  - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
  - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.  
이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 호스트를 다시 시작합니다.
  - b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`
  - c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`
5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.
  6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

## NetApp 지원 플러그인을 설치하세요

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"사용자 지정 애플리케이션을 위해 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

- Windows 호스트의 경우 Windows용 SnapCenter 플러그인을 선택해야 합니다.

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- 클러스터(WSFC)에 플러그인을 설치하면 플러그인이 클러스터의 모든 노드에 설치됩니다.

단계

1. 왼쪽 탐색 창에서 \*호스트\*를 선택합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. \*추가\*를 선택하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
<p>호스트 유형</p>	<p>호스트 유형을 선택하세요:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• 리눅스</li> <li>• 에이엑스</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> NetApp 지원 플러그인은 Windows, Linux, AIX 환경에서 사용할 수 있습니다.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.</p> </div>
<p>호스트 이름</p>	<p>호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요.</p> <p>SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.</p> <p>Windows 환경의 경우 IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다.</p> <p>독립형 호스트의 IP 주소나 FQDN을 입력할 수 있습니다.</p> <p>SnapCenter 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.</p>

이 분야에서는...	이렇게 하세요...
신임장	<p>생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요.</p> <p>자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요.</p> <p>지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.</p> </div>

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

목록에서 다음 플러그인을 설치할 수 있습니다.

- 몽고디비
- ORASCPM(Oracle Applications로 표시됨)
- SAP ASE
- SAP 맥스DB
- 스토리지

6. (선택 사항) 다른 플러그인을 설치하려면 \*추가 옵션\*을 선택하세요.

이 분야에서는...	이렇게 하세요...
포트	<p>기본 포트 번호를 유지하거나 포트 번호를 지정하세요.</p> <p>기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.</p> </div>

이 분야에서는...	이렇게 하세요...
설치 경로	<p>NetApp 지원 플러그인은 Windows 시스템이나 Linux 시스템에 설치할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter 입니다.</li> </ul> <p>선택적으로 경로를 사용자 정의할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• Linux용 SnapCenter 플러그인 패키지 및 AIX용 SnapCenter 플러그인 패키지의 경우 기본 경로는 다음과 같습니다. /opt/NetApp/snapcenter .</li> </ul> <p>선택적으로 경로를 사용자 정의할 수 있습니다.</p>
사전 설치 확인 건너뛰기	<p>플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.</p>
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	<p>Windows 호스트의 경우 플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택합니다.</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div data-bbox="873 1045 928 1096">  <p>다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.</p> </div> <div data-bbox="873 1213 928 1264">  <p>gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.</p> </div> </div>

7. \*제출\*을 선택하세요.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 버전(Linux 플러그인의 경우)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 다음 위치에 있는 web.config 파일을 업데이트할 수 있습니다. C:\Program Files\NetApp\SnapCenter WebApp 기본값을 수정합니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 SnapManager.Web.UI.dll.config를 업데이트하는 경우 두 노드에서 파일을 업데이트하고 SnapCenter 앱 풀을 다시 시작해야 합니다.

Windows 기본 경로는 다음과 같습니다. C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

Linux 기본 경로는 다음과 같습니다.

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 \*확인 및 제출\*을 선택합니다.



동일한 호스트가 이전에 SnapCenter에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

설치별 로그 파일은 다음 위치에 있습니다. /custom\_location/snapcenter/ 로그.

## cmdlet을 사용하여 여러 원격 호스트에 Linux, Windows 또는 AIX용 SnapCenter 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux, Windows 또는 AIX용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

호스트를 추가하는 사용자는 해당 호스트에 대한 관리 권한이 있어야 합니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 Linux 호스트에 NetApp 지원 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 NetApp 지원 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 NetApp 지원 플러그인을 설치할 수 있습니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter\_linux\_host\_plugin.bin)을 C:\ProgramData\NetApp\SnapCenter\Package Repository에서 NetApp 지원 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin`  
`-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address`  
`-DSERVER_HTTPS_PORT=port_number_for_server`
  - -DPORT는 SMCORE HTTPS 통신 포트를 지정합니다.
  - -DSERVER\_IP는 SnapCenter 서버 IP 주소를 지정합니다.
  - -DSERVER\_HTTPS\_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.
  - -DUSER\_INSTALL\_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
  - \_DINSTALL\_LOG\_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_` 을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

5. SnapCenter 에 로그인하고 UI 또는 PowerShell cmdlet을 사용하여 NetApp 지원 플러그인을 업로드합니다.

UI에서 NetApp 지원 플러그인을 업로드하려면 다음을 참조하세요. "[원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.](#)" 부분.

SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

"[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

## NetApp 지원 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다

- ❌ 실패한
- ⚠️ 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
- ⌛ 대기 중

단계

1. 왼쪽 탐색 창에서 \*모니터\*를 클릭합니다.
2. 모니터 페이지에서 \*작업\*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
  - a. \*필터\*를 클릭하세요.
  - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
  - c. 유형 드롭다운 메뉴에서 \*플러그인 설치\*를 선택합니다.
  - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
  - e. \*적용\*을 클릭하세요.
4. 설치 작업을 선택하고 \*세부정보\*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 \*로그 보기\*를 클릭합니다.

## CA 인증서 구성

### CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

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



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. ["CA 인증서 CSR 파일을 생성하는 방법"](#).



도메인(\*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(\*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

### CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

## 단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > \*스냅인 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 버튼으로 클릭한 다음, 모든 작업 > \*가져오기\*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: \*.pfx, \*.p12, \*.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

## CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

## 단계

1. GUI에서 다음을 수행합니다.
  - a. 인증서를 두 번 클릭합니다.
  - b. 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
  - c. 필드 목록을 스크롤하여 \*지문\*을 클릭하세요.
  - d. 상자에서 16진수 문자를 복사하세요.
  - e. 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- a. 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-ChildItem -경로 인증서:\LocalMachine\My
```

- b. 지문을 복사하세요.

## Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

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

단계

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

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

예를 들어:

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

. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 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 들어:

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

## Linux 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `_opt/NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

## 사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

### 단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE\_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
```

. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

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

*agent.properties* 파일의 KEYSTORE\_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

### 플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

### 단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

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

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

### 플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

## 단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

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

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

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

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE\_PASS 키 값입니다.

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

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("\*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC\_CERTIFICATE\_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

## 플러그인에 대한 인증서 해지 목록(CRL) 구성

### 이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

## 단계

1. agent.properties 파일에서 기본 디렉토리를 CRL\_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

## Windows 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*에 있는 *\_keystore.jks* 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 *KEYSTORE\_PASS* 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키tool -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

```
C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키tool -키패스워드 -별칭 "인증서의 별칭\_이름" -키스토어 키스토어.jks

*agent.properties* 파일의 *KEYSTORE\_PASS* 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

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

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 **CA** 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*

2. *keystore.jks* 파일을 찾으세요.

3. 키 저장소에 추가된 인증서를 나열합니다.

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

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
키툴 -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -대상키스토어 keystore.jks -대상키스토어 유형 JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

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

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 *agent.properties* 파일의 *KEYSTORE\_PASS* 키 값입니다.

```
키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks
```

8. *agent.properties* 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 *SCC\_CERTIFICATE\_ALIAS* 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

## SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 *\_C:\Program Files\NetApp\*

SnapCenter\Snapcenter Plug-in Creator\ etc\crl' \_입니다.

단계

1. *agent.properties* 파일에서 기본 디렉토리를 CRL\_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

## 플러그인에 대한 CA 인증서 활성화

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

시작하기 전에

- *Set-SmCertificateSettings* cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- *\_Get-SmCertificateSettings\_*를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 *\_Get-Help command\_name\_*을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 \*호스트\*를 클릭합니다.
2. 호스트 페이지에서 \*관리되는 호스트\*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. \*추가 옵션\*을 클릭하세요.
5. \*인증서 검증 사용\*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- \*  \*는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- \*  \*는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- \*  \*는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- \*  \*는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

## 저작권 정보

Copyright © 2025 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.