IBM DB2용 SnapCenter 플러그인 설치를 준비합니다

SnapCenter Software 6.0

NetApp
July 23, 2024

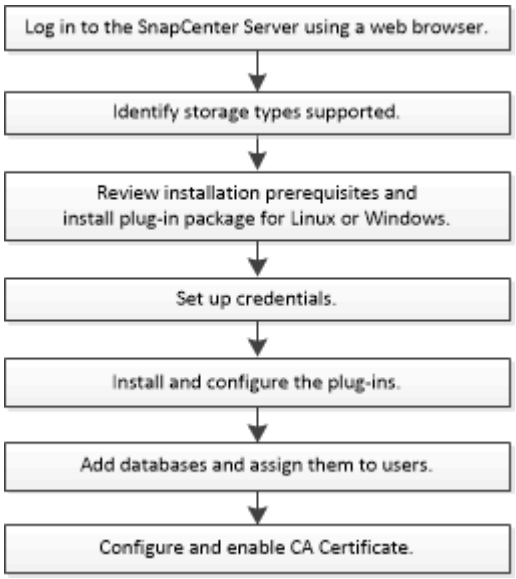
목차

IBM DB2용 SnapCenter 플러그인 설치를 준비합니다 . . . 1
- IBM DB2용 SnapCenter 플러그인 설치 워크플로우 . . . 1
- 호스트를 추가하고 IBM DB2용 SnapCenter 플러그인을 설치하기 위한 사전 요구 사항 . . . 1
- Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항 . . . 5
- Linux용 SnapCenter 플러그인 패키지 설치를 위한 호스트 요구 사항 . . . 5
- IBM DB2용 SnapCenter 플러그인에 대한 자격 증명을 설정합니다 . . . 6
- Windows Server 2016 이상에서 GMSA를 구성합니다 . . . 8
- IBM DB2용 SnapCenter 플러그인을 설치합니다 . . . 9
- CA 인증서를 구성합니다 . . . 15

IBM DB2용 SnapCenter 플러그인 설치를 준비합니다

IBM DB2용 SnapCenter 플러그인 설치 워크플로우

IBM DB2 데이터베이스를 보호하려면 IBM DB2용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 IBM DB2용 SnapCenter 플러그인을 설치하기 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다. IBM DB2용 SnapCenter 플러그인은 Windows 및 Linux 환경 모두에서 사용할 수 있습니다.

- 호스트에 Java 11을 설치해야 합니다.

  IBM Java는 지원되지 않습니다.

- Windows의 경우 IBM DB2용 플러그인이 도메인 관리자로 설치된 경우 기본 동작인 ""LocalSystem"" Windows 사용자를 사용하여 플러그인 Creator Service를 실행해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 Windows 호스트에 IBM DB2 플러그인과 함께 기본적으로 배포됩니다.
- SnapCenter 서버는 IBM DB2 호스트용 플러그인의 8145 또는 사용자 지정 포트에 액세스할 수 있어야 합니다.

Windows 호스트

- 원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- Windows 호스트에 IBM DB2용 플러그인을 설치하는 동안 Microsoft Windows용 SnapCenter 플러그인이 자동으로 설치됩니다.

- 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 11을 설치해야 합니다.

  "모든 운영 체제에 대한 Java 다운로드"

  "NetApp 상호 운용성 매트릭스 툴"

Linux 호스트

- 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 * mksh * 라이브러리를 설치해야 합니다.
- Linux 호스트에 Java 11을 설치해야 합니다.

  "모든 운영 체제에 대한 Java 다운로드"

  "NetApp 상호 운용성 매트릭스 툴"

- Linux 호스트에서 실행되는 IBM DB2 데이터베이스의 경우 IBM DB2용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 플러그인 설치를 위한 기본 셸은 * bash * 이어야 합니다.

보조 명령

IBM DB2용 SnapCenter 플러그인에서 추가 명령을 실행하려면 해당 명령을 파일에 포함해야 `allowed_commands.config` 합니다.

`allowed_commands.config` 파일은 IBM DB2용 SnapCenter 플러그인 디렉토리의 "etc" 하위 디렉토리에 있습니다.

Windows 호스트

기본값: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

사용자 지정 경로: `<Custom_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Linux 호스트

기본값: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

사용자 지정 경로: `<custom_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config`

플러그인 호스트에서 추가 명령을 허용하려면 을 엽니다 `allowed_commands.config` 편집기의 파일. 각 명령을 별도의 줄에 입력합니다. 이름은 대소문자를 구분하지 않습니다. 예를 들면, 다음과 같습니다.

명령: mount

명령: 마운트 해제

정규화된 경로 이름을 지정해야 합니다. 공백이 포함된 경우, 경로 이름은 따옴표(")로 묶어야 합니다. 예를 들면, 다음과 같습니다.

명령: "C:\Program Files\NetApp\SnapCreator Commands\sdcli.exe"

명령: myscript.bat

를 누릅니다 `allowed_commands.config` 파일이 없거나 명령 또는 스크립트 실행이 차단되고 워크플로가 실패하고 다음 오류가 발생합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여하십시오."

명령 또는 스크립트가 에 없는 경우 `allowed_commands.config`, 명령 또는 스크립트 실행이 차단되고 워크플로가 실패하고 다음 오류가 발생합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여하십시오."

와일드카드 항목(*)을 사용하여 모든 명령을 허용해서는 안 됩니다.

Linux 호스트에 대해 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다

SnapCenter 2.0 이상 버전에서는 루트가 아닌 사용자가 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 효과적인 비루트 사용자로 실행됩니다. 여러 경로에 대한 액세스를 제공하려면 루트가 아닌 사용자에 대해 sudo 권한을 구성해야 합니다.

- 필요한 것 *
- sudo 버전 1.8.7 이상
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자 및 사용자 그룹의 이름이 동일해야 합니다.
- MAC HMAC-SHA2-256 및 MAC HMAC-SHA2-512의 메시지 인증 코드 알고리즘을 구성하려면 _/etc/ssh/sshd_config_file을 편집합니다.

  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 대한 정보 *

루트가 아닌 사용자에 대해 sudo 권한을 구성하여 다음 경로에 대한 액세스를 제공해야 합니다.

- /home/*linux_user*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/netapp/snapcenter/SPL/설치/플러그인/제거
- /custom_location/NetApp/snapcenter/SPL/bin/SPL입니다
- 단계 *
  1. Linux용 SnapCenter 플러그인 패키지를 설치할 Linux 호스트에 로그인합니다.
  2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 행을 추가합니다.

```
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/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

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

*/etc/oracle/OLR.loc_file*에서 *_CRS_HOME* 값을 가져올 수 있습니다.

_linux_user_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

다음 위치에 있는 * SC_UNIX_plugins_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

- _C:\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt_SnapCenter 서버가 Windows 호스트에 설치된 경우
- _/opt/netapp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt_if SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우.

이 예제는 고유한 데이터를 만들기 위한 참조로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• .. 순수 코어 8.0.5 • PowerShell 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Linux용 SnapCenter 플러그인 패키지 설치를 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server(SLES) 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK Java를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties 에 있는 java_home 옵션이 올바른 Java 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

IBM DB2용 SnapCenter 플러그인에 대한 자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 데이터베이스 또는 Windows 파일 시스템에서 데이터 보호 작업을 수행하려면 SnapCenter 플러그인 설치를 위한 자격 증명과 추가 자격 증명을 만들어야 합니다.

이 작업에 대해

- Linux 호스트

  Linux 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다.

  플러그인 프로세스를 설치 및 시작할 수 있는 sudo 권한이 있는 루트 사용자 또는 루트 이외의 사용자에 대한 자격 증명을 설정해야 합니다.

  * 모범 사례: * 호스트를 구축하고 플러그인을 설치한 후 Linux에 대한 자격 증명을 생성할 수 있지만, 모범 사례는 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정했고 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 증명 구성에 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름입니다	인증에 사용할 사용자 이름과 암호를 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다. ◦ _NetBIOS\사용자 이름 _ ◦ _도메인 FQDN\사용자 이름 _ • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우 SnapCenter 플러그인을 설치할 시스템에 기본 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 _ 사용자 이름 _ 입니다 암호에 큰따옴표(") 또는 백틱(')을 사용하지 마십시오. 보다 작음(<) 및 느낌표(!)를 사용해서는 안 됩니다. 암호를 사용한 기호. 예를 들어 LessThan <!10, Lessthan10 <!, backtick'12.
암호	인증에 사용되는 암호를 입력합니다.
인증 모드	사용할 인증 모드를 선택합니다.

이 필드의 내용...	수행할 작업...
sudo 권한을 사용합니다	루트가 아닌 사용자에 대한 자격 증명을 생성하는 경우 * sudo 권한 사용 * 확인란을 선택합니다. Linux 사용자에게만 적용됩니다.

5. 확인 * 을 클릭합니다.

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

Windows Server 2016 이상에서 GMSA를 구성합니다

Windows Server 2016 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

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

단계

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Get-ADServiceAccount 명령을 실행하여 서비스 계정을 확인한다.
```

4. 호스트에서 GMSA를 구성합니다.
   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

      이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
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 'Install-AdServiceAccount<GMSA>'를 실행하여 호스트에 GMSA를 설치합니다

c. 'Test-AdServiceAccount <GMSA>' 명령을 실행하여 GMSA 계정을 확인합니다

5. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.
6. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

   SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

IBM DB2용 SnapCenter 플러그인을 설치합니다

호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다

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

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
  - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드합니다
  - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하십시오
- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹

사용자에 속한 경우 호스트에서 UAC를 비활성화해야 합니다.

- 메시지 큐 서비스가 실행 중인지 확인해야 합니다.
- 관리 설명서에는 호스트 관리에 대한 정보가 포함되어 있습니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다.

  "IBM DB2용 Windows Server 2016 이상에서 그룹 관리 서비스 계정을 구성합니다"

이 작업에 대해

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 탭이 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형을 선택합니다. • Windows • 리눅스 IBM DB2용 플러그인은 IBM DB2 클라이언트 호스트에 설치되며 이 호스트는 Windows 시스템 또는 Linux 시스템에 있을 수 있습니다.
호스트 이름입니다	통신 호스트 이름을 입력합니다. FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하십시오. 입력한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다. 자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

   REST API를 사용하여 DB2용 플러그인을 설치하는 동안 버전을 3.0으로 전달해야 합니다. 예: DB2:3.0

6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	IBM DB2용 플러그인은 IBM DB2 클라이언트 호스트에 설치되며 이 호스트는 Windows 시스템 또는 Linux 시스템에 있을 수 있습니다. • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. 선택적으로 경로를 사용자 지정할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/netapp/snapcenter입니다. 선택적으로 경로를 사용자 지정할 수 있습니다.
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	Windows 호스트의 경우 그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다.  GMSA 이름을 domainName\accountName$ 형식으로 제공합니다.  GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 클릭합니다.

   Skip prechecks 확인란을 선택하지 않은 경우 호스트는 호스트가 플러그인 설치 요구 사항을 충족하는지

확인합니다. 디스크 공간, RAM, PowerShell 버전, NET 버전, 위치(Windows 플러그인의 경우) 및 Java 11(Windows 및 Linux 플러그인의 경우)은 최소 요구 사항에 따라 검증됩니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간 또는 RAM과 관련된 경우 C:\Program Files\NetApp\SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.

ⓘ HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 파일을 업데이트해야 합니다.

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

   클러스터 설정에서 클러스터의 각 노드에 대한 지문을 확인해야 합니다.

   ⓘ 동일한 호스트가 SnapCenter에 이전에 추가되었고 지문이 확인되었더라도 지문 확인은 필수입니다.

9. 설치 과정을 모니터링합니다.
   - Windows 플러그인의 경우 설치 및 업그레이드 로그는 *C:\Windows\SnapCenter plugin\Install*<JOBID>\에 있습니다
   - Linux 플러그인의 경우 설치 로그는 */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log에 있으며 업그레이드 로그는 */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log에 있습니다

작업을 마친 후

SnapCenter 6.0 버전으로 업그레이드하려는 경우 원격 플러그인 서버에서 기존 DB2용 PERL 기반 플러그인이 제거됩니다.

cmdlet을 사용하여 여러 원격 호스트에 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 설치합니다

설치-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치할 각 호스트에 대한 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet 및 필수 매개 변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

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

   플러그인을 수동으로 설치했으며 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 확인하지

않으려는 경우 -skipprecheck 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력합니다.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **IBM DB2**용 **SnapCenter** 플러그인을 설치합니다

SnapCenter UI(사용자 인터페이스)를 사용하여 IBM DB2 데이터베이스용 SnapCenter 플러그인을 설치해야 합니다. 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 CLI(명령줄 인터페이스)를 사용하여 콘솔 모드 또는 자동 모드로 IBM DB2 데이터베이스용 플러그인을 설치할 수 있습니다.

시작하기 전에

- IBM DB2 클라이언트가 있는 각 Linux 호스트에 IBM DB2 데이터베이스용 플러그인을 설치해야 합니다.
- IBM DB2 데이터베이스용 SnapCenter 플러그인을 설치하는 Linux 호스트는 종속 소프트웨어, 데이터베이스 및 운영 체제 요구 사항을 충족해야 합니다.

  상호 운용성 매트릭스 툴(IMT): 지원되는 구성에 대한 최신 정보를 제공합니다.

  "NetApp 상호 운용성 매트릭스 툴"

- IBM DB2 데이터베이스용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter가 이미 설치되어 있어야 합니다.

이 작업에 대해

매개 변수가 언급되지 않으면 SnapCenter가 기본값으로 설치됩니다.

단계

1. C:\ProgramData\NetApp\SnapCenter\Package Repository에서 IBM DB2용 플러그인을 설치하려는 호스트로 Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)을 복사합니다.

   SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그 인 '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'를 설치합니다

   - -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. /<installation directory>/netapp/snapcenter/scc/etc/SC_SMS_Services.properties 파일을 편집한 다음 plugins_enabled=DB2:3.0 매개 변수를 추가합니다.
5. Add-Smhost cmdlet 및 필수 매개 변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

   명령에 사용할 수 있는 매개 변수와 해당 설명에 대한 정보는 _get-Help command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 "SnapCenter 소프트웨어 cmdlet 참조 가이드"있습니다.

IBM DB2용 플러그인 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

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.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.

이 마법사 창에서...	다음을 수행합니다.
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>"를 선택합니다

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 IBM DB2 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.

   키툴-리스트-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.

   키툴-리스트-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.

   키툴-리스트-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 IBM DB2** 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 "SnapCenter 소프트웨어 cmdlet 참조 가이드"있습니다.

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.