Oracle Database용 SnapCenter 플러그인 설치

SnapCenter software

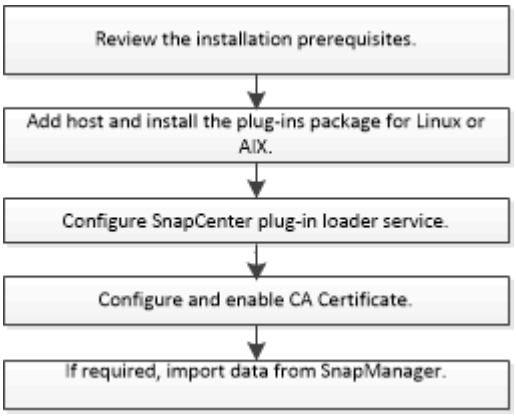
NetApp
November 06, 2025

목차

Oracle Database용 SnapCenter 플러그인 설치

Oracle Database용 SnapCenter 플러그인 설치 워크플로

Oracle 데이터베이스를 보호하려면 Oracle 데이터베이스용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



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

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 루트 또는 루트가 아닌 사용자에 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.

  Oracle Database용 SnapCenter 플러그인은 루트가 아닌 사용자도 설치할 수 있습니다. 하지만 루트가 아닌 사용자가 플러그인 프로세스를 설치하고 시작하려면 sudo 권한을 구성해야 합니다. 플러그인을 설치한 후에는 프로세스가 루트가 아닌 사용자 권한으로 실행됩니다.

- AIX 호스트에 AIX용 SnapCenter 플러그인 패키지를 설치하는 경우 디렉토리 수준 심볼릭 링크를 수동으로 해결했어야 합니다.

  AIX용 SnapCenter 플러그인 패키지는 JAVA_HOME 절대 경로를 얻기 위해 파일 수준 심볼릭 링크는 자동으로 확인하지만 디렉토리 수준 심볼릭 링크는 확인하지 않습니다.

- 설치 사용자에 대해 Linux 또는 AIX 인증 모드로 자격 증명을 생성합니다.
- Linux 또는 AIX 호스트에 Java 11을 설치했어야 합니다.
  - Linux에서는 Oracle 및 OpenJDK의 Java가 지원됩니다.
  - AIX용 IBM Java. 에서 다운로드할 수 있습니다 "IBM Semeru 런타임 다운로드"

    Linux 호스트에 JAVA 11 인증 버전만 설치했는지 확인하세요.

- Linux 또는 AIX 호스트에서 실행되는 Oracle 데이터베이스의 경우 Oracle Database용 SnapCenter 플러그인과 UNIX용 SnapCenter 플러그인을 모두 설치해야 합니다.

Oracle Database용 플러그인을 사용하면 SAP용 Oracle 데이터베이스도 관리할 수 있습니다. 하지만 SAP BR*Tools 통합은 지원되지 않습니다.

- Oracle 데이터베이스 11.2.0.3 이상을 사용하는 경우 13366202 Oracle 패치를 설치해야 합니다.

SnapCenter 는 /etc/fstab 파일의 UUID 매핑을 지원하지 않습니다.

- 플러그인 설치를 위해 기본 셸로 *bash*를 사용해야 합니다.

Linux 호스트 요구 사항

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

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • 오라클 리눅스 Oracle Linux 또는 Red Hat Enterprise Linux 6.6 또는 7.0 운영 체제에서 LVM에서 Oracle 데이터베이스를 사용하는 경우 최신 버전의 Logical Volume Manager(LVM)를 설치해야 합니다. • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인을 위한 최소 RAM	2GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 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	Java 11 Oracle 및 OpenJDK Linux 호스트에 JAVA 11 인증 버전만 설치했는지 확인하세요. 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" .

Linux 호스트에 대한 루트가 아닌 사용자에 대한 **sudo** 권한 구성

SnapCenter 2.0 및 이후 릴리스에서는 루트가 아닌 사용자도 Linux용 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.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- */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/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거
- /custom_location/ NetApp/snapcenter/spl/bin/spl

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 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/Config
_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 env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_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.

_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.

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

목	요구 사항
운영 체제	AIX 7.1 이상
호스트의 SnapCenter 플러그인을 위한 최소 RAM	4GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 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.
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 사용자에 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.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- */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.

자격 증명 설정

SnapCenter 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. Linux 또는 AIX 호스트에 플러그인 패키지를 설치하려면 자격 증명을 만들어야 합니다.

이 작업에 관하여

자격 증명은 루트 사용자 또는 플러그인 프로세스를 설치하고 시작할 수 있는 sudo 권한이 있는 루트가 아닌 사용자를 위해 생성됩니다.

자세한 내용은 다음을 참조하세요.Linux 호스트에 대한 루트가 아닌 사용자에 대한 sudo 권한 구성 또는AIX 호스트에

대한 루트가 아닌 사용자에 대한 sudo 권한 구성

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

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 정보를 입력하세요.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름/비밀번호	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자를 지정하세요. 사용자 이름 필드에 사용할 수 있는 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 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. *UserName*
인증 모드	사용할 인증 모드를 선택하세요. 플러그인 호스트의 운영 체제에 따라 Linux 또는 AIX를 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에 대한 자격 증명을 생성하는 경우 **sudo** 권한 사용 확인란을 선택합니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후에는 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할

수 있습니다.

Oracle 데이터베이스에 대한 자격 증명 구성

Oracle 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용되는 자격 증명을 구성해야 합니다.

이 작업에 관하여

Oracle 데이터베이스에서 지원되는 다양한 인증 방법을 검토해야 합니다. 자세한 내용은 다음을 참조하세요."자격 증명에 대한 인증 방법" .

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

Oracle 데이터베이스 인증을 활성화한 경우 리소스 보기에 빨간색 자물쇠 아이콘이 표시됩니다. 데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 데이터베이스 자격 증명을 구성해야 합니다.

자격 증명을 생성하는 동안 잘못된 세부 정보를 지정하면 오류 메시지가 표시됩니다. *취소*를 클릭한 후 다시 시도하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.
3. 딸깍 하는 소리 그런 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

   그런 다음 클릭할 수 있습니다 필터 창을 닫으려면.
4. 데이터베이스를 선택한 다음 데이터베이스 설정 > *데이터베이스 구성*을 클릭합니다.
5. 데이터베이스 설정 구성 섹션의 기존 자격 증명 사용 드롭다운 목록에서 Oracle 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   Oracle 사용자는 sysdba 권한이 있어야 합니다.

   또한 다음을 클릭하여 자격 증명을 만들 수도 있습니다. .
6. ASM 설정 구성 섹션의 기존 자격 증명 사용 드롭다운 목록에서 ASM 인스턴스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   ASM 사용자는 sysasm 권한이 있어야 합니다.

   또한 다음을 클릭하여 자격 증명을 만들 수도 있습니다. .
7. RMAN 카탈로그 설정 구성 섹션의 기존 자격 증명 사용 드롭다운 목록에서 Oracle Recovery Manager(RMAN) 카탈로그 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   또한 다음을 클릭하여 자격 증명을 만들 수도 있습니다. .

   TNSName 필드에 SnapCenter 서버가 데이터베이스와 통신하는 데 사용할 TNS(Transparent Network

Substrate) 파일 이름을 입력합니다.

8. 선호하는 **RAC** 노드 필드에서 백업에 선호하는 RAC(Real Application Cluster) 노드를 지정합니다.

   선호되는 노드는 RAC 데이터베이스 인스턴스가 있는 하나 또는 모든 클러스터 노드일 수 있습니다. 백업 작업은 선호도 순서대로 이러한 선호 노드에서만 실행됩니다.

   RAC One Node에서는 기본 노드에 노드가 하나만 나열되어 있으며, 이 기본 노드는 현재 데이터베이스가 호스팅되는 노드입니다.

   RAC One Node 데이터베이스를 장애 조치하거나 이전한 후 SnapCenter 리소스 페이지에서 리소스를 새로 고치면 이전에 데이터베이스가 호스팅되었던 선호 **RAC** 노드 목록에서 호스트가 제거됩니다. 데이터베이스가 이전된 RAC 노드는 *RAC 노드*에 나열되며, 기본 RAC 노드로 수동으로 구성해야 합니다.

   자세한 내용은 다음을 참조하세요. "RAC 설정에서 선호하는 노드" .

9. *확인*을 클릭합니다.

GUI를 사용하여 Linux 또는 AIX용 호스트를 추가하고 플러그인 패키지를 설치합니다.

호스트 추가 페이지를 사용하여 호스트를 추가한 다음 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치할 수 있습니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

이 작업에 관하여

개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다. 클러스터(Oracle RAC)에 플러그인을 설치하는 경우 플러그인은 클러스터의 모든 노드에 설치됩니다. Oracle RAC One Node의 경우 액티브 노드와 패시브 노드 모두에 플러그인을 설치해야 합니다.

Oracle RAC에 플러그인을 설치하는 경우 암호 기반 인증만 지원됩니다. SSH 키 기반 인증은 지원되지 않습니다.

SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할이 할당되어야 합니다.

SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

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

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형으로 **Linux** 또는 *AIX*를 선택하세요. SnapCenter 서버는 호스트를 추가한 다음, 호스트에 플러그인이 아직 설치되어 있지 않으면 Oracle Database용 플러그인과 UNIX용 플러그인을 설치합니다.
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 다음 중 하나의 IP 주소나 FQDN을 입력할 수 있습니다. • 독립형 호스트 • Oracle Real Application Clusters(RAC) 환경의 모든 노드 노드 VIP 또는 스캔 IP가 지원되지 않습니다. SnapCenter 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다. 자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 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	기본 경로는 _/opt/ NetApp/snapcenter_입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.
Oracle RAC에 모든 호스트 추가	Oracle RAC의 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다. Flex ASM 설정에서는 허브 노드나 리프 노드인지에 관계없이 모든 노드가 추가됩니다.
선택적 사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.

7. *제출*을 클릭하세요.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트가 검증됩니다.

   사전 확인 스크립트는 방화벽 거부 규칙에 지정된 경우 플러그인 포트 방화벽 상태를 검증하지 않습니다.

   최소 요구 사항을 충족하지 못하면 적절한 오류 또는 경고 메시지가 표시됩니다. 오류가 디스크 공간이나 RAM과 관련된 경우 _C:\Program Files\ NetApp\ SnapCenter WebApp_에 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 모두 파일을 업데이트해야 합니다.

8. 지문을 확인한 후 *확인 및 제출*을 클릭하세요.

   클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.

   SnapCenter ECDSA 알고리즘을 지원하지 않습니다.

동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

   설치 관련 로그 파일은 _/custom_location/snapcenter/logs_에 있습니다.

결과

호스트의 모든 데이터베이스는 자동으로 검색되어 리소스 페이지에 표시됩니다. 아무것도 표시되지 않으면 *리소스 새로 고침*을 클릭하세요.

모니터 설치 상태

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.

Linux 또는 AIX용 플러그인 패키지를 설치하는 대체 방법

cmdlet이나 CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 수동으로 설치할 수도

있습니다.

플러그인을 수동으로 설치하기 전에 _C:\ProgramData\ NetApp\ SnapCenter\Package Repository_에 있는 키 **snapcenter_public_key.pub** 및 *snapcenter_linux_host_plugin.bin.sig*를 사용하여 바이너리 패키지의 서명을 확인해야 합니다.

플러그인을 설치하려는 호스트에 *OpenSSL 1.0.2g*가 설치되어 있는지 확인하세요.

다음 명령을 실행하여 바이너리 패키지의 서명을 검증합니다.

- Linux 호스트의 경우: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- AIX 호스트의 경우: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

cmdlet을 사용하여 여러 원격 호스트에 설치

Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 여러 호스트에 설치하려면 *Install-SmHostPackage* PowerShell cmdlet을 사용해야 합니다.

필요한 것

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

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 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다.

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

   사전 확인 스크립트는 방화벽 거부 규칙에 지정된 경우 플러그인 포트 방화벽 상태를 검증하지 않습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

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" .

클러스터 호스트에 설치

클러스터 호스트의 두 노드 모두에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치해야 합니다.

클러스터 호스트의 각 노드에는 두 개의 IP가 있습니다. IP 중 하나는 해당 노드의 공용 IP가 되고, 두 번째 IP는 두 노드 간에 공유되는 클러스터 IP가 됩니다.

단계

1. 클러스터 호스트의 두 노드에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다.
2. _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일에 SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT 및 SPL_ENABLED_PLUGINS 매개변수에 대한 올바른 값이 지정되었는지 확인합니다.

   spl.properties에 SPL_ENABLED_PLUGINS가 지정되어 있지 않으면 이를 추가하고 SCO,SCU 값을 할당할 수 있습니다.

3. SnapCenter 서버 호스트에서 *Open-SmConnection* cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
4. 각 노드에서 *Set-PreferredHostIPsInStorageExportPolicy* sccli 명령과 필요한 매개변수를 사용하여 노드의 기본 IP를 설정합니다.
5. SnapCenter 서버 호스트에서 _C:\Windows\System32\drivers\etc\hosts_에 클러스터 IP와 해당 DNS 이름에 대한 항목을 추가합니다.
6. *Add-SmHost* cmdlet을 사용하여 호스트 이름에 클러스터 IP를 지정하여 SnapCenter 서버에 노드를 추가합니다.

노드 1에서 Oracle 데이터베이스를 검색하고(클러스터 IP가 노드 1에 호스팅된다고 가정) 데이터베이스 백업을 만듭니다. 장애 조치가 발생하면 노드 1에서 생성된 백업을 사용하여 노드 2의 데이터베이스를 복원할 수 있습니다. 노드 1에서 생성된 백업을 사용하여 노드 2에 복제본을 생성할 수도 있습니다.

> 다른 SnapCenter 작업이 실행되는 동안 장애 조치가 발생하면 오래된 볼륨, 디렉토리 및 잠금 파일이 생성됩니다.

Linux용 플러그인 패키지를 자동 모드로 설치합니다.

명령줄 인터페이스(CLI)를 사용하여 Linux용 SnapCenter 플러그인 패키지를 자동 모드로 설치할 수 있습니다.

필요한 것

- 플러그인 패키지를 설치하기 위한 필수 구성 요소를 검토해야 합니다.
- DISPLAY 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

  DISPLAY 환경 변수가 설정되어 있는 경우 unset DISPLAY를 실행한 다음 플러그인을 수동으로 설치해보세요.

이 작업에 관하여

콘솔 모드로 설치하는 경우 필요한 설치 정보를 제공해야 하지만, 사일런트 모드로 설치하는 경우에는 설치 정보를 제공할 필요가 없습니다.

단계

1. SnapCenter 서버 설치 위치에서 Linux용 SnapCenter 플러그인 패키지를 다운로드합니다.

기본 설치 경로는 _C:\ProgramData\ NetApp\ SnapCenter\PackageRepository_입니다. 이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.
3. 달리다

```
./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path
```

4. _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일을 편집하여 SPL_ENABLED_PLUGINS=SCO,SCU를 추가한 다음 SnapCenter 플러그인 Loader 서비스를 다시 시작합니다.

> 플러그인 패키지를 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록해야 합니다. 호스트를 추가하는 동안 자격 증명으로 "없음"을 선택하세요. 호스트가 추가되면 설치된 플러그인이 자동으로 검색됩니다.

AIX용 플러그인 패키지를 자동 모드로 설치합니다.

명령줄 인터페이스(CLI)를 사용하여 AIX용 SnapCenter 플러그인 패키지를 자동 모드로 설치할 수 있습니다.

필요한 것

- 플러그인 패키지를 설치하기 위한 필수 구성 요소를 검토해야 합니다.
- DISPLAY 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

  DISPLAY 환경 변수가 설정되어 있는 경우 unset DISPLAY를 실행한 다음 플러그인을 수동으로 설치해보세요.

단계

1. SnapCenter 서버 설치 위치에서 AIX용 SnapCenter 플러그인 패키지를 다운로드합니다.

   기본 설치 경로는 _C:\ProgramData\ NetApp\ SnapCenter\PackageRepository_입니다. 이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.
3. 달리다

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path-
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일을 편집하여 SPL_ENABLED_PLUGINS=SCO,SCU를 추가한 다음 SnapCenter 플러그인 Loader 서비스를 다시 시작합니다.

플러그인 패키지를 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록해야 합니다. 호스트를 추가하는 동안 자격 증명으로 "없음"을 선택하세요. 호스트가 추가되면 설치된 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 Loader 서비스 구성

SnapCenter 플러그인 Loader 서비스는 Linux 또는 AIX용 플러그인 패키지를 로드하여 SnapCenter 서버와 상호 작용합니다. SnapCenter 플러그인 Loader 서비스는 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치할 때 설치됩니다.

이 작업에 관하여

Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치하면 SnapCenter 플러그인 Loader 서비스가 자동으로 시작됩니다. SnapCenter 플러그인 Loader 서비스가 자동으로 시작되지 않으면 다음을 수행해야 합니다.

- 플러그인이 작동 중인 디렉토리가 삭제되지 않았는지 확인하세요.
- Java Virtual Machine에 할당된 메모리 공간을 늘리세요

_/custom_location/ NetApp/snapcenter/spl/etc/_에 있는 spl.properties 파일에는 다음 매개변수가 포함되어 있습니다. 이러한 매개변수에는 기본값이 할당됩니다.

매개변수 이름	설명
로그 레벨	지원되는 로그 수준을 표시합니다. 가능한 값은 TRACE, DEBUG, INFO, WARN, ERROR, FATAL입니다.
SPL_프로토콜	SnapCenter 플러그인 Loader 가 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
SNAPCENTER_SERVER_프로토콜	SnapCenter Server에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.

매개변수 이름	설명
자바 홈 업데이트 건너뛰기	기본적으로 SPL 서비스는 Java 경로를 감지하고 JAVA_HOME 매개변수를 업데이트합니다. 따라서 기본값은 FALSE로 설정됩니다. 기본 동작을 비활성화하고 Java 경로를 수동으로 수정하려면 TRUE로 설정하면 됩니다.
SPL_키스토어_패스	키스토어 파일의 비밀번호를 표시합니다. 비밀번호를 변경하거나 새로운 키스토어 파일을 만드는 경우에만 이 값을 변경할 수 있습니다.
SPL_PORT	SnapCenter 플러그인 Loader 서비스가 실행 중인 포트 번호를 표시합니다. 기본값이 없는 경우 값을 추가할 수 있습니다. 플러그인을 설치한 후에는 값을 변경하지 마세요.
SNAPCENTER_SERVER_HOST	SnapCenter 서버의 IP 주소 또는 호스트 이름을 표시합니다.
SPL_키스토어_경로	키스토어 파일의 절대 경로를 표시합니다.
SNAPCENTER_SERVER_PORT	SnapCenter 서버가 실행 중인 포트 번호를 표시합니다.
LOGS_MAX_COUNT	*/custom_location/snapcenter/spl/logs* 폴더에 보관된 SnapCenter 플러그인 Loader 로그 파일의 수를 표시합니다. 기본값은 5000으로 설정되어 있습니다. 개수가 지정된 값보다 많으면 마지막으로 수정된 5000개의 파일이 보존됩니다. SnapCenter 플러그인 Loader 서비스가 시작된 후 24시간마다 파일 개수 확인이 자동으로 수행됩니다. spl.properties 파일을 수동으로 삭제하면 보존되는 파일 수가 9999로 설정됩니다.
자바 홈	SPL 서비스를 시작하는 데 사용되는 JAVA_HOME의 절대 디렉토리 경로를 표시합니다. 이 경로는 설치 중 및 SPL 시작의 일부로 결정됩니다.

매개변수 이름	설명
로그 최대 크기	작업 로그 파일의 최대 크기를 표시합니다. 최대 크기에 도달하면 로그 파일이 압축되고 로그는 해당 작업의 새 파일에 기록됩니다.
지난 며칠 동안의 로그 보관	로그가 보관되는 일수를 표시합니다.
인증서 검증 활성화	호스트에 대해 CA 인증서 검증이 활성화된 경우 true로 표시됩니다. spl.properties를 편집하거나 SnapCenter GUI 또는 cmdlet을 사용하여 이 매개변수를 활성화하거나 비활성화할 수 있습니다.

이러한 매개변수 중 하나라도 기본값에 할당되지 않았거나 값을 할당하거나 변경하려는 경우 spl.properties 파일을 수정할 수 있습니다. spl.properties 파일을 확인하고 파일을 편집하여 매개변수에 할당된 값과 관련된 문제를 해결할 수도 있습니다. spl.properties 파일을 수정한 후에는 SnapCenter 플러그인 Loader 서비스를 다시 시작해야 합니다.

단계

1. 필요에 따라 다음 작업 중 하나를 수행합니다.
   - SnapCenter 플러그인 Loader 서비스를 시작합니다.
     - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - SnapCenter 플러그인 Loader 서비스를 중지합니다.
     - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

       stop 명령과 함께 -force 옵션을 사용하면 SnapCenter 플러그인 Loader 서비스를 강제로 중지할 수 있습니다. 하지만 그렇게 하면 기존 작업도 종료되므로 주의해서 작업해야 합니다.

   - SnapCenter 플러그인 Loader 서비스를 다시 시작합니다.
     - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - SnapCenter 플러그인 Loader 서비스의 상태를 확인하세요.
     - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl`

status

- 루트 사용자가 아닌 경우 다음을 실행합니다. sudo /custom_location/NetApp/snapcenter/spl/bin/spl status

◦ SnapCenter 플러그인 Loader 서비스에서 변경 사항을 찾으세요.

- 루트 사용자로 다음을 실행합니다. /custom_location/NetApp/snapcenter/spl/bin/spl change
- 루트가 아닌 사용자로 다음을 실행합니다. sudo /custom_location/NetApp/snapcenter/spl/bin/spl change

Linux 호스트에서 SnapCenter 플러그인 Loader (SPL) 서비스를 사용하여 CA 인증서 구성

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

SPL은 '/var/opt/snapcenter/spl/etc'에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

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

단계

1. SPL 속성 파일에서 SPL 키 저장소 기본 비밀번호를 검색할 수 있습니다.

   이는 'SPL_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>" -keystore keystore.jks
```

   spl.properties 파일에서 SPL_KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.

SPL 키 저장소의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서 구성

SPL 신뢰 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. SPL 키 저장소가 포함된 폴더로 이동합니다: */var/opt/snapcenter/spl/etc*.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
 keytool -list -v -keystore keystore.jks
. 루트 또는 중간 인증서를 추가합니다.
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. 루트 또는 중간 인증서를 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.
```

루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

SPL 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

단계

1. SPL 키 저장소 /var/opt/snapcenter/spl/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
 keytool -list -v -keystore keystore.jks
. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. 키스토어에 추가된 인증서를 나열합니다.
```

```
 keytool -list -v -keystore keystore.jks
```
. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 SPL 키 저장소 비밀번호는 spl.properties 파일의 SPL_KEYSTORE_PASS 키 값입니다.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
```
. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*",",")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
```
. spl.properties 파일에 있는 키스토어에서 별칭 이름을 구성합니다.

이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

4. CA 서명 키 쌍을 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SPL에 대한 인증서 해지 목록(CRL) 구성

SPL에 대한 CRL을 구성해야 합니다.

이 작업에 관하여

- SPL은 미리 구성된 디렉토리에서 CRL 파일을 찾습니다.
- SPL의 CRL 파일에 대한 기본 디렉토리는 _/var/opt/snapcenter/spl/etc/crl_입니다.

단계

1. spl.properties 파일에서 기본 디렉토리를 SPL_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.

Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터 가져오기

Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터를 가져오면 이전 버전의 데이터를 계속 사용할 수 있습니다.

명령줄 인터페이스(Linux 호스트 CLI)에서 가져오기 도구를 실행하여 Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터를 가져올 수 있습니다.

가져오기 도구는 SnapCenter 에서 정책과 리소스 그룹을 생성합니다. SnapCenter 에서 생성된 정책과 리소스 그룹은 SnapManager for Oracle 및 SnapManager for SAP에서 해당 프로필을 사용하여 수행되는 프로필과 작업에 해당합니다. SnapCenter 가져오기 도구는 Oracle용 SnapManager 및 SAP용 SnapManager 저장소 데이터베이스와 가져오려는 데이터베이스와 상호 작용합니다.

- 프로필을 사용하여 수행된 모든 프로필, 일정 및 작업을 검색합니다.
- 프로필에 첨부된 각 고유한 작업과 각 일정에 대해 SnapCenter 백업 정책을 만듭니다.
- 각 대상 데이터베이스에 대한 리소스 그룹을 만듭니다.

_/opt/ NetApp/snapcenter/spl/bin_에 있는 sc-migrate 스크립트를 실행하여 가져오기 도구를 실행할 수 있습니다. 가져오려는 데이터베이스 호스트에 Linux용 SnapCenter 플러그인 패키지를 설치하면 sc-migrate 스크립트가 _/opt/ NetApp/snapcenter/spl/bin_에 복사됩니다.

SnapCenter 그래픽 사용자 인터페이스(GUI)에서는 데이터 가져오기가 지원되지 않습니다.

SnapCenter 7-Mode에서 작동하는 Data ONTAP 지원하지 않습니다. 7-Mode Transition Tool을 사용하면 7-Mode로 운영되는 Data ONTAP 시스템에 저장된 데이터와 구성을 ONTAP 시스템으로 마이그레이션할 수 있습니다.

데이터 가져오기에 지원되는 구성

Oracle용 SnapManager 3.4.x 및 SAP용 SnapManager 3.4.x에서 SnapCenter 로 데이터를 가져오기 전에 Oracle 데이터베이스용 SnapCenter 플러그인에서 지원되는 구성을 알아야 합니다.

Oracle Database용 SnapCenter 플러그인에서 지원되는 구성은 다음에 나열되어 있습니다. "NetApp 상호 운용성 매트릭스 도구" .

SnapCenter 로 가져오는 내용

프로필을 사용하여 수행된 프로필, 일정 및 작업을 가져올 수 있습니다.

Oracle용 **SnapManager** 및 **SAP**용 **SnapManager** 에서	**SnapCenter** 로
어떠한 작업이나 일정도 없는 프로필	정책은 기본 백업 유형을 온라인으로, 백업 범위를 전체로 설정하여 생성됩니다.
하나 이상의 작업이 포함된 프로필	프로필과 해당 프로필을 사용하여 수행되는 작업의 고유한 조합을 기반으로 여러 정책이 생성됩니다. SnapCenter 에서 생성된 정책에는 프로필과 해당 작업에서 검색된 보관 로그 정리 및 보존 세부 정보가 포함되어 있습니다.
Oracle Recovery Manager(RMAN) 구성을 사용한 프로필	정책은 **Oracle Recovery Manager**를 사용한 카탈로그 백업 옵션을 활성화하여 생성됩니다. SnapManager 에서 외부 RMAN 카탈로그를 사용한 경우 SnapCenter 에서 RMAN 카탈로그 설정을 구성해야 합니다. 기존 자격증명을 선택하거나 새 자격증명을 만들 수 있습니다. SnapManager 의 제어 파일을 통해 RMAN이 구성된 경우 SnapCenter 에서 RMAN을 구성할 필요가 없습니다.
프로필에 첨부된 일정	일정에 대한 정책이 생성됩니다.

Oracle용 **SnapManager** 및 **SAP**용 **SnapManager**에서	**SnapCenter** 로
데이터 베이스	가져온 각 데이터베이스에 대해 리소스 그룹이 생성됩니다. RAC(Real Application Clusters) 설정에서 가져오기 도구를 실행하는 노드는 가져오기가 완료된 후 기본 노드가 되고 해당 노드에 대한 리소스 그룹이 생성됩니다.

프로필을 가져오면 백업 정책과 함께 검증 정책이 생성됩니다.

Oracle용 SnapManager 및 SAP용 SnapManager 프로필, 일정 및 프로필을 사용하여 수행되는 모든 작업을 SnapCenter 로 가져오면 다양한 매개변수 값도 함께 가져옵니다.

Oracle용 **SnapManager** 및 **SAP**용 **SnapManager** 매개변수 및 값	**SnapCenter** 매개변수 및 값	노트
백업 범위 • 가득한 • 데이터 • 통나무	백업 범위 • 가득한 • 데이터 • 통나무	
백업 모드 • 자동 • 온라인 • 오프라인	백업 유형 • 온라인 • 오프라인 종료	백업 모드가 자동인 경우 가져오기 도구는 작업이 수행될 당시의 데이터베이스 상태를 확인하고 백업 유형을 온라인 또는 오프라인 종료로 적절히 설정합니다.
보유 • 날 • 카운트	보유 • 날 • 카운트	Oracle용 SnapManager 와 SAP용 SnapManager 일수와 횟수를 모두 사용하여 보존 기간을 설정합니다. SnapCenter 에는 일 또는 카운트가 있습니다. 따라서 SnapManager for Oracle과 SnapManager for SAP에서는 일수가 개수보다 우선하므로 보존 기간은 일수로 설정됩니다.

Oracle용 **SnapManager** 및 **SAP**용 **SnapManager** 매개변수 및 값	**SnapCenter** 매개변수 및 값	노트
일정에 대한 가지치기 • 모두 • 시스템 변경 번호(SCN) • 날짜 • 지정된 시간, 일, 주, 월 이전에 생성된 로그	일정에 대한 가지치기 • 모두 • 지정된 시간 및 요일 이전에 생성된 로그	SnapCenter SCN, 날짜, 주, 월을 기준으로 한 정리를 지원하지 않습니다.
공고 • 성공적인 작업에 대해서만 이메일이 전송됩니다. • 실패한 작업에 대해서만 이메일이 전송됩니다. • 성공 및 실패한 작업에 대한 이메일이 전송되었습니다.	공고 • 언제나 • 실패 시 • 경고 • 오류	이메일 알림을 가져왔습니다. 하지만 SnapCenter GUI를 사용하여 SMTP 서버를 수동으로 업데이트해야 합니다. 이메일 제목은 비워두어 직접 구성하실 수 있습니다.

SnapCenter 로 가져오지 못하는 것

가져오기 도구는 모든 것을 SnapCenter 로 가져오지 않습니다.

SnapCenter 로 다음을 가져올 수 없습니다.

- 백업 메타데이터
- 부분 백업
- 원시 장치 매핑(RDM) 및 가상 스토리지 콘솔(VSC) 관련 백업
- Oracle용 SnapManager 및 SAP용 SnapManager 저장소에서 사용 가능한 역할 또는 자격 증명
- 검증, 복원 및 복제 작업과 관련된 데이터
- 운영을 위한 가지치기
- Oracle용 SnapManager 및 SAP용 SnapManager 프로필에 지정된 복제 세부 정보

  가져온 후에는 SnapCenter 에서 생성된 해당 정책을 수동으로 편집하여 복제 세부 정보를 포함해야 합니다.

- 카탈로그화된 백업 정보

데이터 가져오기 준비

SnapCenter 로 데이터를 가져오기 전에 특정 작업을 수행하여 가져오기 작업을 성공적으로 실행해야 합니다.

단계

1. 가져오려는 데이터베이스를 식별합니다.

2. SnapCenter 사용하여 데이터베이스 호스트를 추가하고 Linux용 SnapCenter 플러그인 패키지를 설치합니다.
3. SnapCenter 사용하여 호스트의 데이터베이스에서 사용하는 스토리지 가상 머신(SVM)에 대한 연결을 설정합니다.
4. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
5. 리소스 페이지에서 가져올 데이터베이스가 검색되어 표시되는지 확인하세요.

   가져오기 도구를 실행하려면 데이터베이스에 액세스할 수 있어야 하며, 그렇지 않으면 리소스 그룹 생성이 실패합니다.

   데이터베이스에 자격 증명이 구성되어 있는 경우 SnapCenter 에서 해당 자격 증명을 만들고, 자격 증명을 데이터베이스에 할당한 다음 데이터베이스 검색을 다시 실행해야 합니다. 데이터베이스가 ASM(Automatic Storage Management)에 있는 경우 ASM 인스턴스에 대한 자격 증명을 만들고 해당 자격 증명을 데이터베이스에 할당해야 합니다.

6. 가져오기 도구를 실행하는 사용자에게 SnapManager for Oracle 또는 SnapManager for SAP 호스트에서 SnapManager for Oracle 또는 SnapManager for SAP CLI 명령(예: 일정을 일시 중단하는 명령)을 실행할 수 있는 충분한 권한이 있는지 확인하세요.
7. Oracle용 SnapManager 또는 SAP용 SnapManager 호스트에서 다음 명령을 실행하여 일정을 일시 중단합니다.
   a. Oracle 호스트용 SnapManager 에서 일정을 일시 중단하려면 다음을 실행하세요.
      - `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smo credential set -profile -name profile_name`

        호스트의 각 프로필에 대해 smo credential set 명령을 실행해야 합니다.

   b. SAP 호스트용 SnapManager 에서 일정을 일시 중단하려면 다음을 실행하세요.
      - `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smsap credential set -profile -name profile_name`

        호스트의 각 프로필에 대해 smsap 자격 증명 설정 명령을 실행해야 합니다.

8. hostname -f를 실행할 때 데이터베이스 호스트의 정규화된 도메인 이름(FQDN)이 표시되는지 확인하세요.

   FQDN이 표시되지 않으면 /etc/hosts를 수정하여 호스트의 FQDN을 지정해야 합니다.

데이터 가져오기

데이터베이스 호스트에서 가져오기 도구를 실행하여 데이터를 가져올 수 있습니다.

이 작업에 관하여

가져온 후 생성된 SnapCenter 백업 정책은 서로 다른 명명 형식을 갖습니다.

- 어떠한 작업이나 일정도 없는 프로필에 대해 생성된 정책은 SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED 형식을 갖습니다.

  프로필을 사용하여 아무 작업도 수행하지 않으면 기본 백업 유형이 온라인으로, 백업 범위가 전체로 설정된 해당 정책이 생성됩니다.

- 하나 이상의 작업이 포함된 프로필에 대해 생성된 정책은 SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED 형식을 갖습니다.
- 프로필에 첨부된 일정에 대해 생성된 정책은 SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED 형식을 갖습니다.

단계

1. 가져오려는 데이터베이스 호스트에 로그인합니다.
2. _/opt/ NetApp/snapcenter/spl/bin_에 있는 sc-migrate 스크립트를 실행하여 가져오기 도구를 실행합니다.
3. SnapCenter 서버 사용자 이름과 비밀번호를 입력하세요.

   자격 증명을 검증한 후 SnapCenter 와 연결이 설정됩니다.

4. Oracle용 SnapManager 또는 SAP용 SnapManager 저장소 데이터베이스 세부 정보를 입력하세요.

   저장소 데이터베이스는 호스트에서 사용 가능한 데이터베이스를 나열합니다.

5. 대상 데이터베이스 세부 정보를 입력하세요.

   호스트의 모든 데이터베이스를 가져오려면 all을 입력하세요.

6. 실패한 작업에 대한 시스템 로그를 생성하거나 ASUP 메시지를 보내려면 *Add-SmStorageConnection* 또는 *Set-SmStorageConnection* 명령을 실행하여 해당 기능을 활성화해야 합니다.

> 가져오기 도구를 실행하는 동안이나 가져온 후에 가져오기 작업을 취소하려면 가져오기 작업의 일부로 생성된 SnapCenter 정책, 자격 증명 및 리소스 그룹을 수동으로 삭제해야 합니다.

결과

SnapCenter 백업 정책은 프로필, 일정 및 프로필을 사용하여 수행되는 작업에 대해 생성됩니다. 각 대상 데이터베이스에 대해서도 리소스 그룹이 생성됩니다.

데이터를 성공적으로 가져온 후, 가져온 데이터베이스와 연관된 일정은 SnapManager for Oracle 및 SnapManager for SAP에서 일시 중단됩니다.

가져온 후에는 SnapCenter 사용하여 가져온 데이터베이스나 파일 시스템을 관리해야 합니다.

가져오기 도구를 실행할 때마다 발생하는 로그는 */var/opt/snapcenter/spl/logs* 디렉토리에 spl_migration_timestamp.log라는 이름으로 저장됩니다. 이 로그를 참조하여 가져오기 오류를 검토하고 문제를 해결할 수 있습니다.

저작권 정보

상표 정보