Oracle 데이터베이스용 SnapCenter 플러그인을 설치합니다

SnapCenter Software 5.0

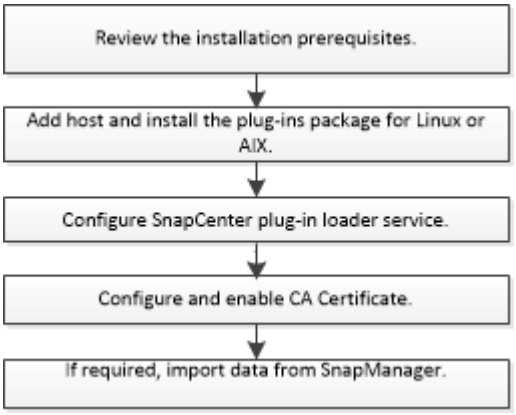
NetApp
July 18, 2024

목차

Oracle 데이터베이스용 SnapCenter 플러그인을 설치합니다

Oracle 데이터베이스용 SnapCenter 플러그인 설치 워크플로우

Oracle 데이터베이스를 보호하려면 Oracle 데이터베이스용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 Linux 또는 AIX용 플러그인 패키지를 설치하기 위한 사전 요구 사항

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

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.

  Oracle 데이터베이스용 SnapCenter 플러그인은 루트가 아닌 사용자가 설치할 수 있습니다. 그러나 비루트 사용자에 대한 sudo 권한을 구성하여 플러그인 프로세스를 설치하고 시작해야 합니다. 플러그인을 설치하면 프로세스가 루트가 아닌 효과적인 사용자로 실행됩니다.

- AIX 호스트에 AIX용 SnapCenter 플러그인 패키지를 설치하는 경우 디렉토리 레벨 심볼 링크를 수동으로 해결해야 합니다.

  AIX용 SnapCenter 플러그인 패키지는 파일 레벨 심볼 링크를 자동으로 확인하지만 java_home 절대 경로를 얻기 위한 디렉토리 레벨 심볼 링크는 확인하지는 않습니다.

- 설치 사용자에 대해 인증 모드를 Linux 또는 AIX로 사용하여 자격 증명을 작성합니다.
- Linux 또는 AIX 호스트에 Java 1.8.x 또는 Java 11, 64비트를 설치해야 합니다.

  Linux 호스트에 Java 11의 인증된 버전만을 설치했는지 확인합니다.

  Java를 다운로드하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

  - "모든 운영 체제에 대한 Java 다운로드"

◦ "AIX용 IBM Java"

- Linux 또는 AIX 호스트에서 실행 중인 Oracle 데이터베이스의 경우 Oracle 데이터베이스용 SnapCenter 플러그인과 UNIX용 SnapCenter 플러그인을 모두 설치해야 합니다.

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

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

SnapCenter에서는 /etc/fstab 파일의 UUID 매핑을 지원하지 않습니다.

- 플러그인 설치를 위한 기본 셸은 * bash * 이어야 합니다.

Linux 호스트 요구 사항

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

항목	요구 사항
운영 체제	• Red Hat Enterprise Linux • Oracle Linux Oracle Linux 또는 Red Hat Enterprise Linux 6.6 또는 7.0 운영 체제의 LVM에서 Oracle 데이터베이스를 사용하는 경우 최신 버전의 LVM(Logical Volume Manager)을 설치해야 합니다. • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	2 GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2 GB 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.

항목	요구 사항
필요한 소프트웨어 패키지	• Java 1.8.x(64비트) Oracle Java 및 OpenJDK • Java 11(64비트) Oracle Java 및 OpenJDK Linux 호스트에 Java 11의 인증된 버전만을 설치했는지 확인합니다. 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 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

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
- 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.

_C:\ProgramData\NetApp\SnapCenter\Package Repository_에 있는 * Oracle_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

사용자 지정 위치를 지정한 경우 위치는 _CUSTOM_PATH\NetApp\SnapCenter\Package Repository_입니다.

> 이 예제는 고유한 데이터를 만들기 위한 참조로만 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.

항목	요구 사항
운영 체제	AIX 7.1 이상
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	4 GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2 GB 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 1.8.x(64비트) IBM Java • Java 11(64비트) IBM Java 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 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

AIX 호스트에 대한 루트가 아닌 사용자에 대한 **sudo** 권한을 구성합니다

SnapCenter 4.4 이상에서는 루트가 아닌 사용자가 AIX용 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
- 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/*aix_user*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/netapp/snapcenter/SPL/설치/플러그인/제거
- /custom_location/NetApp/snapcenter/SPL/bin/SPL입니다
- 단계 *
  1. AIX용 SnapCenter 플러그인 패키지를 설치할 AIX 호스트에 로그인합니다.
  2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 행을 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/Con
fig_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: AIX_USER !visiblepw
Defaults: AIX_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.

_AIX_USER_는 사용자가 작성한 루트가 아닌 사용자의 이름입니다.

_C:\ProgramData\NetApp\SnapCenter\Package Repository_에 있는 * Oracle_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

사용자 지정 위치를 지정한 경우 위치는 _CUSTOM_PATH\NetApp\SnapCenter\Package Repository_입니다.

이 예제는 고유한 데이터를 만들기 위한 참조로만 사용해야 합니다.

자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. Linux 또는 AIX 호스트에 플러그인 패키지를 설치하기 위한 자격 증명을 작성해야 합니다.

- 이 작업에 대한 정보 *

이 자격 증명은 루트 사용자 또는 sudo 권한이 있는 비루트 사용자에 대해 생성되어 플러그인 프로세스를 설치 및 시작할 수 있습니다.

자세한 내용은 또는 을 참조하십시오 Linux 호스트에 대해 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다 AIX 호스트에 대한 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다

* 모범 사례: * 호스트를 구축하고 플러그인을 설치한 후에는 자격 증명을 생성할 수 있지만, 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후 자격 증명을 생성하는 것이 가장 좋습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 자격 증명 * 을 클릭합니다.
3. 새로 만들기 * 를 클릭합니다.
4. 자격 증명 페이지에 자격 증명 정보를 입력합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.

이 필드의 내용...	수행할 작업...
사용자 이름/암호	인증에 사용할 사용자 이름과 암호를 입력합니다. • 도메인 관리자 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자를 지정합니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. ◦ _NetBIOS\사용자 이름 _ ◦ _도메인 FQDN\사용자 이름 _ • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속하는 시스템의 경우 SnapCenter 플러그인을 설치할 시스템의 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
인증 모드	사용할 인증 모드를 선택합니다. 플러그인 호스트의 운영 체제에 따라 Linux 또는 AIX를 선택합니다.
sudo 권한을 사용합니다	루트가 아닌 사용자에 대한 자격 증명을 생성하는 경우 * sudo 권한 사용 * 확인란을 선택합니다.

5. 확인 * 을 클릭합니다.

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

Oracle 데이터베이스에 대한 자격 증명을 구성합니다

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

- 이 작업에 대한 정보 *

Oracle 데이터베이스에 지원되는 다양한 인증 방법을 검토해야 합니다. 자세한 내용은 을 "자격 증명에 대한 인증 방법입니다"참조하십시오.

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

Oracle 데이터베이스 인증을 사용하도록 설정한 경우 리소스 보기에 빨간색 자물쇠 아이콘이 표시됩니다.

데이터베이스를 보호하거나 리소스 그룹에 데이터베이스 자격 증명을 추가하여 데이터 보호 작업을 수행하려면 데이터베이스 자격 증명을 구성해야 합니다.

자격 증명을 생성하는 동안 잘못된 세부 정보를 지정하면 오류 메시지가 표시됩니다. 취소 * 를 클릭한 다음 다시 시도해야 합니다.

- 단계 *

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

   그런 다음 을 클릭하여 필터 창을 닫을 수 있습니다.

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 권한을 가지고 있어야 합니다.

   을 클릭하여 자격 증명을 만들 수도 있습니다.

6. Configure ASM settings 섹션의 * Use Existing Credential * 드롭다운 목록에서 ASM 인스턴스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   ASM 사용자는 sysasm 권한을 가지고 있어야 합니다.

   을 클릭하여 자격 증명을 만들 수도 있습니다.

7. RMAN 카탈로그 설정 구성 섹션의 * 기존 자격 증명 사용 * 드롭다운 목록에서 Oracle RMAN(Recovery Manager) 카탈로그 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   을 클릭하여 자격 증명을 만들 수도 있습니다.

   TNSName* 필드에 SnapCenter 서버가 데이터베이스와 통신하는 데 사용할 투명 네트워크 기질(TNS) 파일 이름을 입력합니다.

8. Preferred RAC Nodes * 필드에서 백업에 사용할 RAC(Real Application Cluster) 노드를 지정합니다.

   선호하는 노드는 RAC 데이터베이스 인스턴스가 있는 하나 또는 모든 클러스터 노드일 수 있습니다. 백업 작업은 기본 설정 순서대로 이러한 기본 설정 노드에서만 트리거됩니다.

   RAC One Node에서는 하나의 노드만 기본 노드에 나열되고 이 기본 설정 노드는 데이터베이스가 현재 호스팅되는 노드입니다.

   RAC One Node 데이터베이스의 페일오버 또는 재배치 후 SnapCenter 리소스 페이지에서 리소스를 새로 고치면 데이터베이스가 이전에 호스팅되었던 * 선호 RAC 노드 * 목록에서 호스트가 제거됩니다.
   데이터베이스가 재배치된 RAC 노드는 * RAC 노드 * 에 나열되며 기본 RAC 노드로 수동으로 구성해야 합니다.

자세한 내용은 을 "RAC 설정의 1차 노드"참조하십시오.

1. 확인 * 을 클릭합니다.

GUI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 설치하고 호스트를 추가합니다

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 대한 정보 *

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

플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당되어야 합니다.

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 유형으로 * Linux * 또는 * AIX * 를 선택합니다. SnapCenter 서버는 호스트를 추가한 다음 호스트에 플러그인이 설치되어 있지 않은 경우 Oracle 데이터베이스용 플러그인과 UNIX용 플러그인을 설치합니다.

이 필드의 내용...	수행할 작업...
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • Oracle RAC(Real Application Clusters) 환경의 모든 노드 노드 VIP 또는 스캔 IP는 지원되지 않습니다 SnapCenter를 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
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. 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 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
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	기본 경로는 _/opt/netapp/snapcenter_입니다. 선택적으로 경로를 사용자 지정할 수 있습니다.
Oracle RAC에 모든 호스트를 추가합니다	Oracle RAC의 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다. Flex ASM 설정에서 허브 또는 리프 노드인지 여부와 관계없이 모든 노드가 추가됩니다.
선택적 사전 설치 검사를 건너뜁니다	이미 플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.

7. 제출 * 을 클릭합니다.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구사항을 충족하는지 여부를 확인합니다.

   사전 확인 스크립트는 방화벽 거부 규칙에 지정된 플러그인 포트 방화벽 상태의 유효성을 검사하지 않습니다.

   최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다. 오류가 디스크 공간 또는 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 파일을 업데이트해야 합니다.

8. 지문을 확인한 다음 * 확인 및 제출 * 을 클릭합니다.

   클러스터 설정에서 클러스터의 각 노드에 대한 지문을 확인해야 합니다.

   SnapCenter는 ECDSA 알고리즘을 지원하지 않습니다.

동일한 호스트가 SnapCenter에 이전에 추가되었고 지문이 확인되었더라도 지문 확인은 필수입니다.

1. 설치 과정을 모니터링합니다.

   설치별 로그 파일은 _/custom_location/snapcenter/logs_에 있습니다.

결과 *

호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다. 아무 것도 표시되지 않으면 * 리소스 새로 고침 * 을 클릭합니다.

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 중
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기 중입니다

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.

Linux 또는 AIX용 플러그인 패키지를 설치하는 다른 방법

cmdlet 또는 CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 수동으로 설치할 수도

있습니다.

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

플러그인을 설치할 호스트에 * OpenSSL 1.0.2g * 가 설치되어 있는지 확인합니다.

다음 명령을 실행하여 바이너리 패키지의 서명을 확인합니다.

- 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_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

cmdlet을 사용하여 여러 원격 호스트에 설치합니다

여러 호스트에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치하려면 _Install-SmHostPackage_PowerShell cmdlet을 사용해야 합니다.

- 필요한 것 *

플러그인 패키지를 설치하려는 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 Linux 또는 AIX용 SnapCenter 플러그인 패키지용 SnapCenter 플러그인 패키지를 설치합니다.

   플러그인을 이미 수동으로 설치했고 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 여부를 확인하지 않으려는 경우 _-skipprecheck_옵션을 사용할 수 있습니다.

   사전 확인 스크립트는 방화벽 거부 규칙에 지정된 플러그인 포트 방화벽 상태의 유효성을 검사하지 않습니다.

1. 원격 설치를 위한 자격 증명을 입력합니다.

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.

클러스터 호스트에 설치합니다

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

클러스터 호스트의 각 노드에는 2개의 IP가 있습니다. IP 중 하나는 각 노드의 공용 IP이고, 두 번째 IP는 두 노드 간에 공유되는 클러스터 IP입니다.

- 단계 *

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

   SPL_ENABLED_PACNEWNES가 spl.properties 에 지정되지 않은 경우 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 매개 변수를 사용하여 노드의 기본 설정 IP를 설정합니다.
5. SnapCenter 서버 호스트에서 클러스터 IP에 대한 항목과 해당 DNS 이름을 _C:\Windows\System32\drivers\etc\hosts_에 추가합니다.
6. 호스트 이름에 대한 클러스터 IP를 지정하여 _Add-SmHost_cmdlet을 사용하여 SnapCenter 서버에 노드를 추가합니다.

노드 1에서 Oracle 데이터베이스를 검색하고(클러스터 IP가 노드 1에서 호스팅된다고 가정) 데이터베이스의 백업을 생성합니다. 페일오버가 발생하면 노드 1에서 생성된 백업을 사용하여 노드 2에서 데이터베이스를 복원할 수 있습니다. 노드 1에 생성된 백업을 사용하여 노드 2에 클론을 생성할 수도 있습니다.

다른 SnapCenter 작업이 실행 중인 동안 페일오버가 발생하면 오래된 볼륨, 디렉토리 및 잠금 파일이 있습니다.

Linux용 플러그인 패키지를 자동 모드로 설치합니다

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

- 필요한 것 *
- 플러그인 패키지를 설치하기 위한 사전 요구 사항을 검토해야 합니다.
- 디스플레이 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

  디스플레이 환경 변수가 설정된 경우 설정되지 않은 디스플레이를 실행한 다음 플러그인을 수동으로 설치해야 합니다.

- 이 작업에 대한 정보 *

콘솔 모드로 설치하는 동안 필요한 설치 정보를 제공해야 하지만 자동 모드 설치에서는 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 액세스할 수 있습니다.

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

```
./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. spL_enabled_plugins=SCO, SCU를 추가한 다음 SnapCenter 플러그인 로더 서비스를 다시 시작하려면 _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일을 편집합니다.

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

AIX용 플러그인 패키지를 자동 모드로 설치합니다

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

- 필요한 것 *
- 플러그인 패키지를 설치하기 위한 사전 요구 사항을 검토해야 합니다.
- 디스플레이 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

  디스플레이 환경 변수가 설정된 경우 설정되지 않은 디스플레이를 실행한 다음 플러그인을 수동으로 설치해야 합니다.

- 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 액세스할 수 있습니다.

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

```
./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. spL_enabled_plugins=SCO, SCU를 추가한 다음 SnapCenter 플러그인 로더 서비스를 다시 시작하려면 _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일을 편집합니다.

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

SnapCenter 플러그인 로더 서비스를 구성합니다

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

- 이 작업에 대한 정보 *

Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치한 후 SnapCenter 플러그인 로더 서비스가 자동으로 시작됩니다. SnapCenter 플러그인 로더 서비스가 자동으로 시작되지 않는 경우 다음을 수행해야 합니다.

- 플러그인이 작동하는 디렉토리가 삭제되지 않았는지 확인합니다
- Java Virtual Machine에 할당된 메모리 공간을 늘립니다

spl.properties 파일은 _/custom_location/NetApp/snapcenter/SPL/etc/_에 있으며 다음 매개 변수를 포함합니다. 기본값은 이러한 매개 변수에 할당됩니다.

매개 변수 이름입니다	설명
log_level 을 선택합니다	지원되는 로그 수준을 표시합니다. 가능한 값은 추적, 디버그, 정보, 경고, 오류, 치명적입니다.
SPL_protocol(프로토콜)	SnapCenter 플러그인 로더에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
SNAPCENTER_SERVER_PROTOCOL	SnapCenter 서버에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
skip_jAVHOME_update 를 선택합니다	기본적으로 SPL 서비스는 Java 경로를 감지하고 java_home 매개 변수를 업데이트합니다. 따라서 기본값은 false 로 설정됩니다. 기본 동작을 비활성화하고 Java 경로를 수동으로 수정하려면 TRUE로 설정할 수 있습니다.

매개 변수 이름입니다	설명
SPL_keystore_pass입니다	키 저장소 파일의 암호를 표시합니다. 암호를 변경하거나 새 키 저장소 파일을 만드는 경우에만 이 값을 변경할 수 있습니다.
SPL_PORT	SnapCenter 플러그인 로더 서비스가 실행 중인 포트 번호를 표시합니다. 기본값이 없는 경우 값을 추가할 수 있습니다. 플러그인을 설치한 후에는 값을 변경해서는 안 됩니다.
SNAPCENTER_SERVER_HOST	SnapCenter 서버의 IP 주소 또는 호스트 이름을 표시합니다.
SPL_keystore_path를 입력합니다	키 저장소 파일의 절대 경로를 표시합니다.
SNAPCENTER_SERVER_PORT	SnapCenter 서버가 실행 중인 포트 번호를 표시합니다.
logs_MAX_count	_/custom_location/snapcenter/SPL/logs_folder에 유지되는 SnapCenter 플러그인 로더 로그 파일의 수를 표시합니다. 기본값은 5000으로 설정됩니다. 카운트가 지정된 값보다 큰 경우 마지막으로 수정된 5000개의 파일이 유지됩니다. SnapCenter 플러그인 로더 서비스가 시작된 후 24시간마다 파일 수 검사가 자동으로 수행됩니다. spl.properties 파일을 수동으로 삭제하면 보존할 파일 수가 9999로 설정됩니다.
java_home입니다	SPL 서비스를 시작하는 데 사용되는 java_home의 절대 디렉토리 경로를 표시합니다. 이 경로는 설치 중에 그리고 SPL 시작 시 결정됩니다.
Log_MAX_SIZE(로그 최대 크기)	작업 로그 파일의 최대 크기를 표시합니다. 최대 크기에 도달하면 로그 파일이 압축되고 로그가 해당 작업의 새 파일에 기록됩니다.
최근 _ 일 _ 의 _ 로그 유지	로그가 유지되는 최대 일 수를 표시합니다.

매개 변수 이름입니다	설명
certificate_validation을 활성화합니다	호스트에 대해 CA 인증서 유효성 검사가 활성화되면 true를 표시합니다. spl.properties 를 편집하거나 SnapCenter GUI 또는 cmdlet을 사용하여 이 매개 변수를 활성화 또는 비활성화할 수 있습니다.

이러한 매개 변수 중 하나라도 기본값에 할당되지 않거나 값을 할당하거나 변경하려는 경우 spl.properties 파일을 수정할 수 있습니다. 또한 spl.properties 파일을 확인하고 파일을 편집하여 매개 변수에 할당된 값과 관련된 문제를 해결할 수도 있습니다. spl.properties 파일을 수정한 후 SnapCenter 플러그인 로더 서비스를 다시 시작해야 합니다.

- 단계 *
  1. 필요에 따라 다음 작업 중 하나를 수행합니다.
     - SnapCenter 플러그인 로더 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 로더 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 명령에 -force 옵션을 사용하면 SnapCenter 플러그인 로더 서비스를 강제로 중지할 수 있습니다. 그러나 기존 작업도 종료되므로 이 작업을 수행하기 전에 주의해야 합니다.

     - SnapCenter 플러그인 로더 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 로더 서비스의 상태를 찾습니다.
       - 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 로더 서비스에서 변경 사항을 찾습니다.
       - 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 SPL(Plug-in Loader) 서비스를 사용하여 CA 인증서를 구성합니다

SPL 키 저장소 및 해당 인증서의 암호를 관리하고, CA 인증서를 구성하고, SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, 설치된 디지털 인증서를 활성화하려면 SnapCenter 플러그인 로더 서비스를 사용하여 CA 서명 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

SPL은 '/var/opt/snapcenter/spl/etc'에 있는 'keystore.jks' 파일을 신뢰 저장소 및 키 저장소로 사용합니다.

SPL 키 저장소의 암호 및 사용 중인 CA 서명된 키 쌍의 별칭을 관리합니다

- 단계 *

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

   'PL_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>" -keystore keystore.jks
   ```

   spl.properties 파일의 SPL_keystore_pass 키에 대해서도 동일하게 업데이트하십시오.

3. 암호를 변경한 후 서비스를 다시 시작합니다.

SPL 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

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 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
 keytool -list -v -keystore keystore.jks
. 루트 또는 중간 인증서 추가:
```

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

ⓘ 루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

CA 서명 키 쌍을 SPL 신뢰 저장소에 구성합니다

CA 서명된 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

- 단계 *

1. SPL의 keystore/var/opt/snapcenter/SPL 등이 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

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

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

```
 keytool -list -v -keystore keystore.jks
. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지
확인합니다.
. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.
```

기본 SPL 키 저장소 암호는 spl.properties 파일의 SPL_keystore_pass 키 값입니다.

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

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

이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

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

SPL에 대한 CRL(인증서 해지 목록)을 구성합니다

SPL에 대해 CRL을 구성해야 합니다

- 이 작업에 대한 정보 *
- SPL은 사전 구성된 디렉터리에서 CRL 파일을 찾습니다.
- SPL에 대한 CRL 파일의 기본 디렉토리는 _ /var/opt/snapcenter/spl/etc/CRL_ 입니다.
- 단계 *
  1. spl.properties 파일의 기본 디렉터리를 SPL_CRL_PATH 키에 맞게 수정 및 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 활성화되거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- * * CA 인증서의 유효성 검사가 성공적으로 완료되었음을 나타냅니다.
- * * 는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- * * 는 연결 정보를 검색할 수 없음을 나타냅니다.

상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

SnapManager for Oracle 및 SnapManager for SAP에서 SnapCenter로 데이터를 가져옵니다

SnapManager for Oracle 및 SnapManager for SAP에서 SnapCenter로 데이터를 가져오면 이전 버전의 데이터를 계속 사용할 수 있습니다.

명령줄 인터페이스(Linux 호스트 CLI)에서 가져오기 도구를 실행하여 SnapManager for Oracle 및 SnapManager for SAP에서 SnapCenter로 데이터를 가져올 수 있습니다.

가져오기 도구는 SnapCenter에 정책 및 리소스 그룹을 만듭니다. SnapCenter에서 생성된 정책 및 리소스 그룹은 SnapManager for Oracle 및 SnapManager for SAP에서 이러한 프로파일을 사용하여 수행된 프로필과 작업에 해당합니다. SnapCenter 가져오기 도구는 SnapManager for Oracle 및 SnapManager for SAP 리포지토리 데이터베이스 및 가져올 데이터베이스와 상호 작용합니다.

- 프로파일을 사용하여 수행된 모든 프로파일, 스케줄 및 작업을 검색합니다.
- 프로필에 연결된 각 고유 작업 및 각 스케줄에 대한 SnapCenter 백업 정책을 생성합니다.
- 각 타겟 데이터베이스에 대한 리소스 그룹을 생성합니다.

가져오기 도구는 _/opt/NetApp/snapcenter/SPL/bin_에 있는 SC-migrate 스크립트를 실행하여 실행할 수 있습니다. 가져올 데이터베이스 호스트에 Linux용 SnapCenter 플러그인 패키지를 설치하면 SC-마이그레이션 스크립트가 _/opt/netapp/snapcenter/SPL/bin_에 복사됩니다.

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

SnapCenter는 7-Mode에서 작동하는 Data ONTAP를 지원하지 않습니다. 7-Mode 전환 툴을 사용하면 7-Mode에서 운영되는 Data ONTAP을 실행하는 시스템에 저장된 데이터와 구성을 ONTAP 시스템으로 마이그레이션할 수 있습니다.

데이터 가져오기에 지원되는 구성입니다

Oracle용 SnapManager 3.4.x 및 SAP용 SnapManager 3.4.x에서 SnapCenter로 데이터를 가져오기 전에 Oracle 데이터베이스용 SnapCenter 플러그인에서 지원되는 구성을 알고 있어야 합니다.

Oracle 데이터베이스용 SnapCenter 플러그인에서 지원되는 구성은 에 나와 "NetApp 상호 운용성 매트릭스 툴 "있습니다.

SnapCenter로 가져온 항목

프로파일을 사용하여 수행한 프로파일, 일정 및 작업을 가져올 수 있습니다.

SnapManager for Oracle 및 SnapManager for SAP에서	SnapCenter로
작업 및 일정이 없는 프로파일	정책은 기본 백업 유형을 온라인 으로, 백업 범위를 전체 로 하여 생성됩니다.
하나 이상의 작업이 있는 프로파일	여러 정책은 해당 프로파일을 사용하여 수행된 프로파일과 작업의 고유한 조합을 기반으로 생성됩니다. SnapCenter에서 생성된 정책에는 프로파일 및 해당 작업에서 가져온 아카이브 로그 잘라내기 및 보존 세부 정보가 포함됩니다.
Oracle RMAN(Recovery Manager) 구성을 사용한 프로파일	정책은 * Oracle Recovery Manager * 옵션을 활성화한 상태에서 * Catalog Backup을 사용하여 생성됩니다. SnapManager에서 외부 RMAN 카탈로그를 사용한 경우 SnapCenter에서 RMAN 카탈로그 설정을 구성해야 합니다. 기존 자격 증명을 선택하거나 새 자격 증명을 생성할 수 있습니다. RMAN이 SnapManager의 제어 파일을 통해 구성된 경우 SnapCenter에서 RMAN을 구성할 필요가 없습니다.
프로필에 연결된 스케줄입니다	스케줄에 대한 정책이 생성됩니다.
데이터베이스	가져온 각 데이터베이스에 대해 리소스 그룹이 만들어집니다. RAC(Real Application Clusters) 설정에서는 가져오기 도구를 실행하는 노드가 가져오기 후 기본 설정 노드가 되고 해당 노드에 대한 리소스 그룹이 생성됩니다.

프로필을 가져오면 백업 정책과 함께 검증 정책이 생성됩니다.

Oracle용 SnapManager와 SnapManager SAP 프로필, 일정 및 프로필을 사용하여 수행한 작업을 SnapCenter로 가져오는 경우 다른 매개 변수 값도 가져옵니다.

SnapManager for Oracle 및 **SnapManager for SAP** 매개 변수 및 값	**SnapCenter** 매개 변수 및 값	참고
백업 범위 • 가득 참 • 데이터 • 로그	백업 범위 • 가득 참 • 데이터 • 로그	
백업 모드 • 자동 • 온라인 • 오프라인	백업 유형 • 온라인 • 오프라인 종료	백업 모드가 자동인 경우 가져오기 도구는 작업이 수행될 때 데이터베이스 상태를 확인하고 백업 유형을 온라인 또는 오프라인 종료로 적절하게 설정합니다.
보존 • 일 • 카운트	보존 • 일 • 카운트	Oracle용 SnapManager와 SAP용 SnapManager는 일 및 수 모두를 사용하여 보존을 설정합니다. SnapCenter에는 days_or_Counts가 있습니다. 따라서 Oracle의 경우 SnapManager, SAP의 경우 SnapManager에서 일 수가 더 우선하기 때문에 일 수에 따라 보존 기간이 설정됩니다.
일정에 대한 정리 • 모두 • 시스템 변경 번호(SCN) • 날짜 • 지정된 시간, 일, 주 및 월 이전에 생성된 로그입니다	일정에 대한 정리 • 모두 • 지정된 시간 및 일 이전에 생성된 로그입니다	SnapCenter는 SCN, 날짜, 주 및 월을 기준으로 한 가지치기를 지원하지 않습니다.
통지 • 성공적인 작업을 위해 보낸 이메일입니다 • 실패한 작업에 대해서만 이메일이 전송되었습니다 • 성공 및 실패한 작업을 위해 전송된 이메일입니다	통지 • 항상 • 실패 시 • 경고 • 오류	이메일 알림을 가져옵니다. 그러나 SnapCenter GUI를 사용하여 SMTP 서버를 수동으로 업데이트해야 합니다. 이메일 제목은 구성할 수 있도록 비어 있습니다.

SnapCenter로 가져올 수 없는 항목

불러오기 도구는 모든 것을 SnapCenter로 불러오지 않습니다.

다음을 SnapCenter로 가져올 수 없습니다.

- 메타데이터 백업
- 부분 백업
- RDM(Raw Device Mapping) 및 VSC(Virtual Storage Console) 관련 백업
- Oracle용 SnapManager 및 SAP용 SnapManager 리포지토리에서 사용할 수 있는 역할 또는 자격 증명
- 검증, 복원 및 클론 작업과 관련된 데이터
- 작업을 위한 잘라내기
- SnapManager for Oracle 및 SnapManager for SAP 프로필에 지정된 복제 세부 정보입니다

  가져온 후에는 SnapCenter에서 생성한 해당 정책을 수동으로 편집하여 복제 세부 정보를 포함해야 합니다.

- 카탈로그 작성된 백업 정보

데이터 가져오기를 준비합니다

데이터를 SnapCenter로 가져오기 전에 가져오기 작업을 성공적으로 실행하기 위해 특정 작업을 수행해야 합니다.

- 단계 *

  1. 가져올 데이터베이스를 식별합니다.
  2. SnapCenter를 사용하여 데이터베이스 호스트를 추가하고 Linux용 SnapCenter 플러그인 패키지를 설치합니다.
  3. SnapCenter를 사용하여 호스트의 데이터베이스에서 사용되는 SVM(스토리지 가상 머신)의 연결을 설정합니다.
  4. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  5. 리소스 페이지에서 가져올 데이터베이스가 검색되어 표시되는지 확인합니다.

     가져오기 도구를 실행하려면 데이터베이스에 액세스할 수 있어야 하며 그렇지 않으면 리소스 그룹을 만들 수 없습니다.

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

  6. 가져오기 도구를 실행하는 사용자가 SnapManager SnapManager for Oracle 또는 SnapManager for SAP CLI 명령(예: 예약 일시 중지 명령)을 실행할 수 있는 충분한 권한을 가지고 있는지 확인합니다 SnapManager.
  7. Oracle용 SnapManager 또는 SAP용 SnapManager 호스트에서 다음 명령을 실행하여 스케줄을 일시 중지합니다.

     a. SnapManager for Oracle 호스트에서 스케줄을 일시 중지하려면 다음을 실행합니다.

- `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 자격 증명 세트 명령을 실행해야 합니다.

b. SnapManager for SAP 호스트의 스케줄을 일시 중지하려면 다음을 실행합니다.

- `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 집합 명령을 실행해야 합니다.

1. 호스트 이름 -F를 실행할 때 데이터베이스 호스트의 FQDN(정규화된 도메인 이름)이 표시되는지 확인합니다

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

데이터를 가져옵니다

데이터베이스 호스트에서 가져오기 도구를 실행하여 데이터를 가져올 수 있습니다.

- 이 작업에 대한 정보 *

가져온 후 생성되는 SnapCenter 백업 정책의 명명 형식은 다음과 같습니다.

- 작업 및 일정 없이 프로파일에 대해 생성된 정책에는 SM_profileName_online_full_default_m마이그레이션된 형식이 있습니다.

  프로파일을 사용하여 작업을 수행하지 않으면 해당 정책은 기본 백업 유형을 온라인 및 백업 범위를 전체 로 사용하여 생성됩니다.

- 하나 이상의 작업으로 프로파일에 대해 생성된 정책에는 SM_profileName_BACKUPMODE_BACKUPSCOPE_Migrated 형식이 있습니다.
- 프로필에 연결된 일정에 대해 생성된 정책에는 SM_profileName_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_Migrated 형식이 있습니다.
- 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 이름 및 암호를 입력합니다.

   자격 증명의 유효성을 검사한 후 SnapCenter와 연결이 설정됩니다.

4. SnapManager for Oracle 또는 SnapManager for SAP 리포지토리 데이터베이스 세부 정보를 입력합니다.

   저장소 데이터베이스에는 호스트에서 사용할 수 있는 데이터베이스가 나열됩니다.

5. 대상 데이터베이스 세부 정보를 입력합니다.

   호스트의 모든 데이터베이스를 가져오려면 All 을 입력합니다.

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

   가져오기 도구를 실행하는 동안 또는 가져온 후에 가져오기 작업을 취소하려면 가져오기 작업의 일부로 만든 SnapCenter 정책, 자격 증명 및 리소스 그룹을 수동으로 삭제해야 합니다.

- 결과 *

SnapCenter 백업 정책은 프로파일을 사용하여 수행하는 프로파일, 스케줄 및 작업에 대해 생성됩니다. 각 타겟 데이터베이스에 대해 리소스 그룹도 만들어집니다.

데이터를 성공적으로 가져오면 가져온 데이터베이스와 연결된 스케줄이 SnapManager for Oracle 및 SnapManager for SAP에서 일시 중단됩니다.

가져온 데이터베이스 또는 파일 시스템을 SnapCenter를 사용하여 관리해야 합니다.

가져오기 도구의 모든 실행에 대한 로그는 SPL_migration_timestamp.log라는 이름의 _/var/opt/snapcenter/SPL/logs_directory에 저장됩니다. 이 로그를 참조하여 가져오기 오류를 검토하고 문제를 해결할 수 있습니다.