



Unix 파일 시스템용 SnapCenter 플러그인을 설치합니다

SnapCenter Software 5.0

NetApp
July 18, 2024

목차

Unix 파일 시스템용 SnapCenter 플러그인을 설치합니다.....	1
Linux용 호스트 추가 및 플러그인 패키지 설치를 위한 사전 요구 사항	1
GUI를 사용하여 호스트를 추가하고 Linux용 플러그인 패키지를 설치합니다	2
SnapCenter 플러그인 로더 서비스를 구성합니다	5
Linux 호스트에서 SnapCenter SPL(Plug-in Loader) 서비스를 사용하여 CA 인증서를 구성합니다.....	8
플러그인에 대해 CA 인증서를 활성화합니다	10

Unix 파일 시스템용 SnapCenter 플러그인을 설치합니다

Linux용 호스트 추가 및 플러그인 패키지 설치를 위한 사전 요구 사항

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

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 루트 또는 루트 이외의 사용자에게 대해 암호 기반 인증을 사용하거나 SSH 키 기반 인증을 사용할 수 있습니다.

Unix 파일 시스템용 SnapCenter 플러그인은 루트가 아닌 사용자가 설치할 수 있습니다. 그러나 비루트 사용자에게 대한 sudo 권한을 구성하여 플러그인 프로세스를 설치하고 시작해야 합니다. 플러그인을 설치하면 프로세스가 루트가 아닌 효과적인 사용자로 실행됩니다.

- 설치 사용자에게 대해 인증 모드를 Linux로 사용하여 자격 증명을 생성합니다.
- Linux 호스트에 Java 1.8.x 또는 Java 11(64비트)을 설치해야 합니다.




Linux 호스트에 Java 11의 인증된 버전만을 설치했는지 확인합니다.

Java 다운로드에 대한 자세한 내용은 다음을 참조하십시오. "[모든 운영 체제에 대한 Java 다운로드](#)"

- 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	<ul style="list-style-type: none">• Red Hat Enterprise Linux• Oracle Linux• 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	<ul style="list-style-type: none"> • Java 1.8.x(64비트) Oracle Java 및 OpenJDK • Java 11(64비트) Oracle Java 및 OpenJDK <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Linux 호스트에 Java 11의 인증된 버전만을 설치했는지 확인합니다. </div> <p>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.</p>


지원되는 버전에 대한 최신 정보는 ["NetApp 상호 운용성 매트릭스 툴"](#) 참조하십시오.

GUI를 사용하여 호스트를 추가하고 Linux용 플러그인 패키지를 설치합니다

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

- 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 * 를 선택합니다.
호스트 이름입니다	<p>FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다.</p> <p>SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.</p> <p>SnapCenter를 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.</p>

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

5. 설치할 플러그인 선택 섹션에서 * Unix 파일 시스템 * 을 선택합니다.

6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	<p>기본 포트 번호를 유지하거나 포트 번호를 지정합니다.</p> <p>기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트 번호로 표시됩니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다. </div>
설치 경로	<p>기본 경로는 <code>_/opt/netapp/snapcenter_</code>입니다.</p> <p>선택적으로 경로를 사용자 지정할 수 있습니다. 사용자 지정 경로를 사용하는 경우 sudoers의 기본 콘텐츠가 사용자 지정 경로로 업데이트되었는지 확인합니다.</p>
선택적 사전 설치 검사를 건너뛰니다	<p>이미 플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.</p>

7. 제출 * 을 클릭합니다.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구 사항을 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.



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 *

호스트에 마운트된 모든 파일 시스템이 자동으로 검색되어 리소스 페이지 아래에 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.

SnapCenter 플러그인 로더 서비스를 구성합니다

SnapCenter 플러그인 로더 서비스는 SnapCenter 서버와 상호 작용하기 위해 Linux용 플러그인 패키지를 로드합니다. SnapCenter 플러그인 로더 서비스는 Linux용 SnapCenter 플러그인 패키지를 설치할 때 설치됩니다.

- 이 작업에 대한 정보 *

Linux용 SnapCenter 플러그인 패키지를 설치하면 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.

매개 변수 이름입니다	설명
skip_JAVHOME_update 를 선택합니다	<p>기본적으로 SPL 서비스는 Java 경로를 감지하고 java_home 매개 변수를 업데이트합니다.</p> <p>따라서 기본값은 false 로 설정됩니다. 기본 동작을 비활성화하고 Java 경로를 수동으로 수정하려면 TRUE로 설정할 수 있습니다.</p>
SPL_keystore_pass입니다	<p>키 저장소 파일의 암호를 표시합니다.</p> <p>암호를 변경하거나 새 키 저장소 파일을 만드는 경우에만 이 값을 변경할 수 있습니다.</p>
SPL_PORT	<p>SnapCenter 플러그인 로더 서비스가 실행 중인 포트 번호를 표시합니다.</p> <p>기본값이 없는 경우 값을 추가할 수 있습니다.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  플러그인을 설치한 후에는 값을 변경해서는 안 됩니다. </div>
SNAPCENTER_SERVER_HOST	<p>SnapCenter 서버의 IP 주소 또는 호스트 이름을 표시합니다.</p>
SPL_keystore_path를 입력합니다	<p>키 저장소 파일의 절대 경로를 표시합니다.</p>
SNAPCENTER_SERVER_PORT	<p>SnapCenter 서버가 실행 중인 포트 번호를 표시합니다.</p>
logs_MAX_count	<p>_/custom_location/snapcenter/SPL/logs_folder에 유지되는 SnapCenter 플러그인 로더 로그 파일의 수를 표시합니다.</p> <p>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.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  spl.properties 파일을 수동으로 삭제하면 보존할 파일 수가 9999로 설정됩니다. </div>
java_home입니다	<p>SPL 서비스를 시작하는 데 사용되는 java_home의 절대 디렉토리 경로를 표시합니다.</p> <p>이 경로는 설치 중에 그리고 SPL 시작 시 결정됩니다.</p>

매개 변수 이름입니다	설명
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.
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  
<AliasNameForCertificateToBeImported> -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 "<OriginalAliasName>" -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_cmdlet`을 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.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.