클라우드 커넥터

E-Series storage systems

NetApp
January 20, 2026

목차

클라우드 커넥터

SANtricity ® Cloud Connector 개요

SANtricity Cloud Connector는 호스트 기반 Linux 애플리케이션으로, E-Series 볼륨을 S3 불만 계정(예: Amazon Simple Storage Service 및 NetApp StorageGRID) 및 NetApp AltaVault 어플라이언스로 전체 블록 기반 및 파일 기반 백업 및 복구를 수행할 수 있습니다.

RedHat 및 SUSE Linux 플랫폼에 설치할 수 있는 SANtricity 클라우드 커넥터는 패키지 솔루션(.bin 파일)입니다. SANtricity 클라우드 커넥터를 설치한 후 애플리케이션을 구성하여 E-Series 볼륨의 백업 및 복원 작업을 AltaVault 어플라이언스 또는 기존 Amazon S3 또는 StorageGRID 계정에 수행할 수 있습니다. SANtricity 클라우드 커넥터를 통해 수행되는 모든 작업은 REST 기반 API를 사용합니다.

SANtricity 클라우드 커넥터 도구는 더 이상 사용되지 않으며 다운로드할 수 없습니다.

고려 사항

이러한 절차를 사용할 때는 다음 사항에 유의하십시오.

- 이 절차에서 설명하는 구성 및 백업/복원 작업은 SANtricity 클라우드 커넥터의 그래픽 사용자 인터페이스 버전에 적용됩니다.
- SANtricity 클라우드 커넥터 애플리케이션의 REST API 워크플로우는 이 절차에 설명되어 있지 않습니다. 숙련된 개발자의 경우 API 설명서에서 각 SANtricity 클라우드 커넥터 작업에 대해 엔드포인트를 사용할 수 있습니다. API 설명서는 브라우저를 통해 "http://<hostname.domain>:<port>/docs``으로 이동하여 액세스할 수 있습니다.

백업 유형

SANtricity 클라우드 커넥터는 이미지 기반 백업과 파일 기반 백업의 두 가지 백업 유형을 제공합니다.

- * 이미지 기반 백업 *

  이미지 기반 백업은 스냅샷 볼륨에서 원시 데이터 블록을 읽고 이를 이미지라고 하는 파일에 백업합니다. 스냅샷 볼륨의 모든 데이터 블록은 빈 블록, 삭제된 파일이 차지하는 블록, 파티셔닝과 관련된 블록, 파일 시스템 메타데이터 등을 포함하여 백업됩니다. 이미지 백업에서는 파티션 구성이나 파일 시스템에 관계없이 스냅샷 볼륨에 모든 정보를 저장할 수 있습니다.

  이미지는 백업 타겟에 단일 파일로 저장되지 않고 대신 64MB 크기의 일련의 데이터 청크로 분할됩니다. 데이터 청크를 통해 SANtricity Cloud Connector는 백업 타겟에 대한 여러 연결을 사용할 수 있으므로 백업 프로세스의 성능이 향상됩니다.

  StorageGRID 및 Amazon Web Services(S3)로 백업하는 경우 각 데이터 청크는 별도의 암호화 키를 사용하여 청크를 암호화합니다. 키는 사용자가 제공한 암호와 사용자 데이터의 SHA256 해시의 조합으로 구성된 SHA256 해시입니다. AltaVault로 백업할 경우 AltaVault가 이 작업을 수행하므로 SANtricity 클라우드 커넥터는 데이터 청크를 암호화하지 않습니다.

- * 파일 기반 백업 *

  파일 기반 백업은 파일 시스템 파티션에 포함된 파일을 읽고 64MB 크기의 일련의 데이터 청크로 백업합니다. 파일 기반 백업은 삭제된 파일 또는 파티션 분할과 파일 시스템 메타데이터를 백업하지 않습니다. 이미지 기반 백업과

마찬가지로 데이터 청크를 통해 SANtricity Cloud Connector는 백업 타겟에 대한 여러 연결을 사용할 수 있으므로 백업 프로세스의 성능이 향상됩니다.

StorageGRID 및 Amazon Web Services에 백업하는 경우 각 데이터 청크는 별도의 암호화 키를 사용하여 청크를 암호화합니다. 키는 사용자 제공 암호문과 사용자 데이터의 SHA256 해시의 조합으로 구성된 SHA256 해시입니다. AltaVault로 백업하는 경우 AltaVault가 이 작업을 수행하기 때문에 SANtricity 클라우드 커넥터에 의해 데이터 청크가 암호화되지 않습니다.

SANtricity Cloud Connector의 시스템 요구 사항

시스템은 SANtricity 클라우드 커넥터의 호환성 요구 사항을 충족해야 합니다.

호스트 하드웨어 요구 사항

하드웨어는 다음 최소 요구 사항을 충족해야 합니다.

- 최소 5GB의 메모리, 구성된 최대 힙 크기에 대해 4GB
- 소프트웨어 설치 시 최소 5GB의 사용 가능한 디스크 공간이 필요합니다

SANtricity 클라우드 커넥터를 사용하려면 SANtricity 웹 서비스 프록시를 설치해야 합니다. 웹 서비스 프록시를 로컬로 설치하거나 다른 서버에서 응용 프로그램을 원격으로 실행할 수 있습니다. SANtricity 웹 서비스 프록시 설치에 대한 자세한 내용은 를 참조하십시오 "웹 서비스 프록시 항목".

지원되는 브라우저

다음 브라우저는 SANtricity 클라우드 커넥터 응용 프로그램에서 지원됩니다(최소 버전 표시).

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

Microsoft Internet Explorer v11 브라우저 내에서 호환성 보기 설정을 사용할 때 SANtricity 클라우드 커넥터 응용 프로그램에 대한 API 문서가 로드되지 않습니다. Microsoft Internet Explorer v11 브라우저에서 API 문서가 제대로 표시되도록 하려면 호환성 보기 설정을 사용하지 않는 것이 좋습니다.

호환되는 스토리지 어레이 및 컨트롤러 펌웨어입니다

SANtricity 클라우드 커넥터 애플리케이션을 사용하기 전에 스토리지 어레이와 펌웨어의 호환성을 확인해야 합니다.

SANtricity 클라우드 커넥터의 호환 가능한 모든 스토리지 어레이 및 펌웨어의 전체 최신 목록은 을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

호환되는 운영 체제

SANtricity 클라우드 커넥터 4.0 응용 프로그램은 다음 운영 체제와 호환되고 지원됩니다.

운영 체제	버전	있습니다
Red Hat Enterprise Linux(RHEL)	7.x	64비트
SUSE Linux Enterprise Server(SLES)	12.x	64비트

지원되는 파일 시스템

SANtricity Cloud Connector 애플리케이션을 통해 백업 및 복구를 수행하려면 지원되는 파일 시스템을 사용해야 합니다.

SANtricity 클라우드 커넥터 애플리케이션에서 백업 및 복구 작업을 지원하는 파일 시스템은 다음과 같습니다.

- ext2
- ext3
- ext4

SANtricity 클라우드 커넥터를 설치합니다

SANtricity 클라우드 커넥터 패키지 솔루션(.bin 파일)은 RedHat 및 SUSE Linux 플랫폼에서만 사용할 수 있습니다.

호환되는 Linux 운영 체제에서 그래픽 모드 또는 콘솔 모드를 통해 SANtricity 클라우드 커넥터 응용 프로그램을 설치할 수 있습니다. 설치 프로세스 중에 SANtricity 클라우드 커넥터에 대한 비 SSL 및 SSL 포트 번호를 지정해야 합니다. SANtricity 클라우드 커넥터가 설치되면 데몬 프로세스로 실행됩니다.

SANtricity 클라우드 커넥터 도구는 더 이상 사용되지 않으며 다운로드할 수 없습니다.

시작하기 전에

다음 참고 사항을 검토하십시오.

- SANtricity 웹 서비스 프록시가 SANtricity 클라우드 커넥터와 동일한 서버에 이미 설치되어 있는 경우 비 SSL 포트 번호와 SSL 포트 번호 충돌 간에 충돌이 발생합니다. 이 경우 SANtricity 클라우드 커넥터 설치 중에 SSL이 아닌 포트와 SSL 포트에 적절한 번호를 선택합니다.
- 호스트에서 하드웨어 변경이 수행되는 경우 암호화 일관성을 보장하기 위해 SANtricity 클라우드 커넥터 애플리케이션을 다시 설치합니다.
- SANtricity 클라우드 커넥터 애플리케이션의 버전 3.1을 통해 생성된 백업은 SANtricity 클라우드 커넥터 애플리케이션의 버전 4.0과 호환되지 않습니다. 이러한 백업을 유지 관리하려면 이전 버전의 SANtricity 클라우드 커넥터를 계속 사용해야 합니다. SANtricity Cloud Connector의 3.1 및 4.0 릴리즈를 성공적으로 설치하려면 애플리케이션의 각 버전에 대해 고유한 포트 번호를 할당해야 합니다.

장치 매퍼 다중 경로(DM-MP) 설치

SANtricity 클라우드 커넥터를 실행하는 모든 호스트는 Linux 장치 매퍼 다중 경로(DM-MP)를 실행하고 다중 경로 도구 패키지를 설치해야 합니다.

SANtricity 클라우드 커넥터 검색 프로세스는 백업 또는 복원할 볼륨 및 파일을 검색하고 인식하기 위해 다중 경로 툴 패키지를 사용합니다. 장치 매퍼를 설정하고 구성하는 방법에 대한 자세한 내용은 에서 사용 중인 SANtricity 릴리스에 대한 _SANtricity 저장소 관리자 다중 경로 드라이버 안내서_를 참조하십시오 "E-Series 및 SANtricity 문서 리소스".

Cloud Connector를 설치합니다

Linux 운영 체제에 SANtricity 클라우드 커넥터를 그래픽 모드 또는 콘솔 모드로 설치할 수 있습니다.

그래픽 모드

그래픽 모드를 사용하여 Linux 운영 체제에 SANtricity 클라우드 커넥터를 설치할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터 설치를 위한 호스트 위치를 지정합니다.

단계

1. SANtricity 클라우드 커넥터 설치 파일을 원하는 호스트 위치로 다운로드합니다.
2. 터미널 창을 엽니다.
3. SANtricity 클라우드 커넥터 설치 파일이 포함된 디렉토리 파일로 이동합니다.
4. SANtricity 클라우드 커넥터 설치 프로세스를 시작합니다.

   ```
   ./cloudconnector-xxxx.bin -i gui
   ```

   이 명령에서 xxxx는 애플리케이션의 버전 번호를 지정합니다.

   설치 프로그램 창이 표시됩니다.

5. Introduction 문을 검토한 후 * Next * 를 클릭합니다.

   NetApp, Inc. 소프트웨어에 대한 라이센스 계약은 설치 프로그램 창에 표시됩니다.

6. 사용권 계약 조건에 동의하고 * 다음 * 을 클릭합니다.

   이전 릴리스의 SANtricity 클라우드 커넥터 페이지에서 생성된 백업이 표시됩니다.

7. 이전 릴리스의 SANtricity 클라우드 커넥터 메시지로 생성된 백업을 확인하려면 * 다음 * 을 클릭합니다.

   > ⓘ 이전 버전을 유지하면서 SANtricity 클라우드 커넥터 버전 4.0을 설치하려면 각 응용 프로그램 버전에 대해 고유한 포트 번호를 할당해야 합니다.

   설치 선택 페이지가 설치 프로그램 창에 표시됩니다. 설치할 위치 필드에는 기본 설치 폴더 'opt/netapp/sSANtricity_cloud_connector4/'가 표시됩니다

8. 다음 옵션 중 하나를 선택합니다.
   - 기본 위치를 그대로 사용하려면 * 다음 * 을 클릭합니다.
   - 기본 위치를 변경하려면 새 폴더 위치를 입력합니다. 비 SSL Jetty 포트 번호 입력 페이지가 표시됩니다. 기본값이 8080인 경우 비 SSL 포트에 할당됩니다.

9. 다음 옵션 중 하나를 선택합니다.
   - 기본 SSL 포트 번호를 적용하려면 * 다음 * 을 클릭합니다.
   - 기본 SSL 포트 번호를 변경하려면 원하는 새 포트 번호 값을 입력합니다.
10. 다음 옵션 중 하나를 선택합니다.
    - 기본 비 SSL 포트 번호를 그대로 사용하려면 * 다음 * 을 클릭합니다.
    - 기본 비 SSL 포트 번호를 변경하려면 원하는 새 포트 번호 값을 입력합니다. 사전 설치 요약 페이지가 표시됩니다.
11. 표시된 설치 전 요약을 검토하고 * 설치 * 를 클릭합니다.

    SANtricity 클라우드 커넥터 설치가 시작되고 Webserver 데몬 설정 프롬프트가 표시됩니다.

12. OK * 를 클릭하여 Webserver Daemon Setup 프롬프트를 확인합니다.

    Installation Complete(설치 완료) 메시지가 표시됩니다.

13. Done * 을 클릭하여 SANtricity 클라우드 커넥터 설치 프로그램을 종료합니다.

콘솔 모드

콘솔 모드를 사용하여 Linux 운영 체제에 SANtricity 클라우드 커넥터를 설치할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터 설치를 위한 호스트 위치를 지정합니다.

단계

1. SANtricity 클라우드 커넥터 설치 파일을 원하는 IO 호스트 위치로 다운로드합니다.
2. 터미널 창을 엽니다.
3. SANtricity 클라우드 커넥터 설치 파일이 포함된 디렉토리 파일로 이동합니다.
4. SANtricity 클라우드 커넥터 설치 프로세스를 시작합니다.

   ```
   ./cloudconnector-xxxx.bin –i console
   ```

   이 명령에서 xxxx는 애플리케이션의 버전 번호를 나타냅니다.

   SANtricity 클라우드 커넥터 설치 프로세스가 초기화됩니다.

5. 설치 프로세스를 진행하려면 * Enter * 를 누르십시오.

   NetApp, Inc. 소프트웨어에 대한 최종 사용자 라이센스 계약은 설치 프로그램 창에 표시됩니다.

   설치 프로세스를 취소하려면 설치 프로그램 창 아래에 quit를 입력합니다.

6. 최종 사용자 사용권 계약의 각 부분을 진행하려면 * Enter * 를 누르십시오.

   사용권 계약 수락 진술은 설치 프로그램 창 아래에 표시됩니다.

7. 최종 사용자 사용권 계약 조건에 동의하고 SANtricity 클라우드 커넥터 설치를 계속하려면 설치 프로그램 창에서 'Y'를 입력하고 * Enter * 를 누르십시오.

   이전 릴리스의 SANtricity 클라우드 커넥터 페이지에서 생성된 백업이 표시됩니다.

   최종 사용자 계약 조건에 동의하지 않으면 "N"을 입력하고 * Enter * 를 눌러 SANtricity 클라우드 커넥터의 설치 프로세스를 종료합니다.

8. 이전 릴리스의 SANtricity 클라우드 커넥터 메시지로 생성된 백업을 확인하려면 * Enter * 를 누르십시오.

   이전 버전을 유지하면서 SANtricity 클라우드 커넥터 버전 4.0을 설치하려면 각 응용 프로그램 버전에 대해 고유한 포트 번호를 할당해야 합니다.

   SANtricity 클라우드 커넥터에 대한 다음 기본 설치 폴더가 있는 설치 폴더 선택 메시지가 표시됩니다. ""/opt/netapp/sSANtricity_cloud_connector4/".

9. 다음 옵션 중 하나를 선택합니다.
   - 기본 설치 위치를 그대로 사용하려면 * Enter * 를 누릅니다.
   - 기본 설치 위치를 변경하려면 새 폴더 위치를 입력합니다. 비 SSL Jetty 포트 번호 입력 메시지가 표시됩니다. 기본값이 8080인 경우 비 SSL 포트에 할당됩니다.
10. 다음 옵션 중 하나를 선택합니다.
    - 기본 SSL 포트 번호를 그대로 사용하려면 * 다음 * 을 누릅니다.
    - 기본 SSL 포트 번호를 변경하려면 원하는 새 포트 번호 값을 입력합니다.
11. 다음 옵션 중 하나를 선택합니다.
    - 기본 비 SSL 포트 번호를 그대로 사용하려면 * Enter * 를 누릅니다.
    - 기본 비 SSL 포트 번호를 변경하려면 새 포트 번호 값을 입력합니다. SANtricity 클라우드 커넥터의 사전 설치 요약이 표시됩니다.
12. 표시된 사전 설치 요약을 검토하고 * Enter * 를 누릅니다.
13. Enter * 를 눌러 Webserver Daemon Setup 프롬프트를 확인합니다.

    Installation Complete(설치 완료) 메시지가 표시됩니다.

14. SANtricity 클라우드 커넥터 설치 프로그램을 종료하려면 * Enter * 를 누릅니다.

서버 인증서와 **CA** 인증서를 키 저장소에 추가합니다

브라우저에서 SANtricity 클라우드 커넥터 호스트로의 보안 https 연결을 사용하려면 SANtricity 클라우드 커넥터 호스트에서 자체 서명된 인증서를 수락하거나 브라우저와 SANtricity 클라우드 커넥터 응용 프로그램에서 인식되는 인증서와 신뢰 체인을 추가할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터 애플리케이션이 호스트에 설치되어 있어야 합니다.

단계

1. 'stemctl' 명령을 사용하여 서비스를 중지합니다.

2. 기본 설치 위치에서 작업 디렉토리에 액세스합니다.

   SANtricity 클라우드 커넥터의 기본 설치 위치는 '/opt/netapp/SANtricity_cloud_connector4'입니다.

3. 'keytool' 명령을 사용하여 서버 인증서 및 인증서 서명 요청(CSR)을 생성합니다.

   ◦ 예 *

```
keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
-sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
keystore_cloudconnect.jks -storepass changeit
keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
-storepass changeit -file cloudconnect.csr
```

4. 생성된 CSR을 선택한 CA(인증 기관)에 보냅니다.

   인증 기관이 인증서 요청에 서명하고 서명된 인증서를 반환합니다. 또한 CA 자체로부터 인증서를 받습니다. 이 CA 인증서를 키 저장소로 가져와야 합니다.

5. 인증서와 CA 인증서 체인을 "/<설치 경로>/작업/키 저장소" 응용 프로그램 키 저장소로 가져옵니다

   ◦ 예 *

```
keytool -import -alias ca-root -file root-ca.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
-keystore keystore_cloudconnect.jks -storepass <password>
```

6. 서비스를 다시 시작합니다.

StorageGRID 인증서를 키 저장소에 추가합니다

StorageGRID를 SANtricity 클라우드 커넥터 응용 프로그램의 대상 유형으로 구성하는 경우 먼저 SANtricity 클라우드 커넥터 키 저장소에 StorageGRID 인증서를 추가해야 합니다.

시작하기 전에

- 서명된 StorageGRID 인증서가 있습니다.
- 호스트에 SANtricity 클라우드 커넥터 애플리케이션이 설치되어 있습니다.

단계

1. 'stemctl' 명령을 사용하여 서비스를 중지합니다.
2. 기본 설치 위치에서 작업 디렉토리에 액세스합니다.

SANtricity 클라우드 커넥터의 기본 설치 위치는 '/opt/netapp/SANtricity_cloud_connector4'입니다.

3. StorageGRID 인증서를 "/<설치 경로>/작업/키 저장소" 응용 프로그램 키 저장소로 가져옵니다

   ◦ 예 *

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
/home/ictlabsg01.cer -keystore
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

4. 서비스를 다시 시작합니다.

SANtricity 클라우드 커넥터를 처음으로 구성합니다

설치가 완료되면 구성 마법사를 통해 SANtricity 클라우드 커넥터 응용 프로그램을 설정할 수 있습니다. SANtricity 클라우드 커넥터에 처음 로그인하면 구성 마법사가 표시됩니다.

SANtricity 클라우드 커넥터에 처음으로 로그인합니다

SANtricity 클라우드 커넥터를 처음으로 초기화하는 경우 응용 프로그램에 액세스하려면 기본 암호를 입력해야 합니다.

시작하기 전에

인터넷에 연결된 브라우저에 액세스할 수 있는지 확인합니다.

단계

1. 지원되는 브라우저를 엽니다.
2. 구성된 SANtricity 클라우드 커넥터 서버에 연결합니다(예: 'http://localhost:8080/`).

   SANtricity 클라우드 커넥터 애플리케이션의 초기 로그인 페이지가 표시됩니다.

3. Administrator Password(관리자 암호) 필드에 기본 암호 "password(암호)"를 입력합니다.
4. 로그인 * 을 클릭합니다.

   SANtricity 클라우드 커넥터 구성 마법사가 표시됩니다.

구성 마법사 사용

SANtricity 클라우드 커넥터에 처음 로그인하면 구성 마법사가 표시됩니다.

구성 마법사를 통해 관리자 암호, 웹 서비스 프록시 로그인 관리 자격 증명, 원하는 백업 대상 유형 및 SANtricity 클라우드 커넥터의 암호화 암호 구문을 설정합니다.

1단계**:** 관리자 암호를 설정합니다

관리자 암호 설정 페이지를 통해 SANtricity 클라우드 커넥터에 대한 후속 로그인에 사용되는 암호를 사용자 지정할 수 있습니다.

관리자 암호 설정 페이지를 통해 암호를 설정하면 SANtricity 클라우드 커넥터 응용 프로그램의 초기 로그인 중에 사용되는 기본 암호가 효과적으로 대체됩니다.

단계

1. 관리자 암호 설정 페이지의 * 새 관리자 암호 입력 * 필드에 SANtricity 클라우드 커넥터에 대해 원하는 로그인 암호를 입력합니다.
2. 새 관리자 암호 * 필드를 다시 입력하십시오. 필드에 첫 번째 필드의 암호를 다시 입력하십시오.
3. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터의 암호 설정이 수락되고 암호 설정 페이지가 구성 마법사 아래에 표시됩니다.

   사용자 정의 관리자 암호는 구성 마법사를 완료할 때까지 설정되지 않습니다.

2단계**:** 암호문 설정

암호화 암호 입력 페이지에서 8자에서 32자 사이의 영숫자 암호를 지정할 수 있습니다.

SANtricity 클라우드 커넥터 응용 프로그램에서 사용하는 데이터 암호화 키의 일부로 사용자 지정 암호가 필요합니다.

단계

1. 암호 정의 * 필드에 원하는 암호를 입력합니다.
2. 암호 구문 * 필드를 다시 입력하십시오. 필드에 첫 번째 필드의 암호를 다시 입력하십시오.
3. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터 애플리케이션에 대해 입력한 암호문이 수락되고 구성 마법사의 대상 유형 선택 페이지가 표시됩니다.

3단계**:** 대상 유형을 선택합니다

백업 및 복원 기능은 SANtricity 클라우드 커넥터를 통해 Amazon S3, AltaVault 및 StorageGRID 타겟 유형에 사용할 수 있습니다. 대상 유형 선택 페이지에서 SANtricity 클라우드 커넥터 애플리케이션에 대해 원하는 스토리지 타겟 유형을 지정할 수 있습니다.

시작하기 전에

AltaVault 마운트 지점, Amazon AWS 계정 또는 StorageGRID 계정 중 하나가 있는지 확인합니다.

단계

1. 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.
   - Amazon AWS
   - AltaVault
   - StorageGRID

선택한 옵션의 대상 유형 페이지가 구성 마법사에 표시됩니다.

2. AltaVault, Amazon AWS 또는 StorageGRID에 대한 적절한 구성 지침을 참조하십시오.

AltaVault 어플라이언스를 구성합니다

대상 유형 선택 페이지에서 AltaVault 어플라이언스 옵션을 선택하면 AltaVault 대상 유형의 구성 옵션이 표시됩니다.

시작하기 전에

- AltaVault 어플라이언스에 대한 NFS 마운트 경로가 있습니다.
- AltaVault 어플라이언스를 대상 유형으로 지정했습니다.

단계

1. NFS 마운트 경로 * 필드에 AltaVault 타겟 유형의 마운트 지점을 입력합니다.

   NFS 마운트 경로 * 필드의 값은 Linux 경로 형식을 따라야 합니다.

2. 선택한 타겟 유형에 구성 데이터베이스의 백업을 만들려면 이 대상에 구성 데이터베이스의 백업 저장 * 확인란을 선택합니다.

   연결을 테스트할 때 지정된 대상 유형에서 기존 데이터베이스 구성이 감지되면 SANtricity 클라우드 커넥터 호스트의 기존 데이터베이스 구성 정보를 구성 마법사 아래에 입력된 새 백업 정보로 대체할 수 있습니다.

3. 지정된 AltaVault 설정에 대한 연결을 테스트하려면 * 연결 테스트 * 를 클릭합니다.
4. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 지정된 대상 유형이 허용되고 웹 서비스 프록시 페이지가 구성 마법사에 표시됩니다.

5. "4단계: 웹 서비스 프록시에 연결"을 진행합니다.

Amazon AWS 계정을 구성합니다

대상 유형 선택 페이지에서 Amazon AWS 옵션을 선택하면 Amazon AWS 타겟 유형에 대한 구성 옵션이 표시됩니다.

시작하기 전에

- Amazon AWS 계정이 설정되었습니다.
- Amazon AWS를 타겟 유형으로 지정했습니다.

단계

1. 액세스 키 ID * 필드에 Amazon AWS 타겟의 액세스 ID를 입력합니다.
2. 비밀 액세스 키 * 필드에 대상의 비밀 액세스 키를 입력합니다.
3. [버킷 이름] * 필드에 대상의 버킷 이름을 입력합니다.
4. 선택한 타겟 유형에 구성 데이터베이스의 백업을 생성하려면 * 이 대상에 구성 데이터베이스의 백업 저장 * 확인란을 선택합니다.

데이터베이스를 잃어버린 경우 백업 대상의 데이터를 복원할 수 있도록 이 설정을 사용하는 것이 좋습니다.

연결을 테스트할 때 지정된 대상 유형에서 기존 데이터베이스 구성이 감지되면 SANtricity 클라우드 커넥터 호스트의 기존 데이터베이스 구성 정보를 구성 마법사 아래에 입력된 새 백업 정보로 대체할 수 있습니다.

5. Test Connection * 을 클릭하여 입력된 Amazon AWS 자격 증명을 확인합니다.
6. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 지정된 대상 유형이 허용되고 웹 서비스 프록시 페이지가 구성 마법사 아래에 표시됩니다.

7. "4단계: 웹 서비스 프록시에 연결"을 진행합니다.

StorageGRID 계정을 구성합니다

대상 유형 선택 페이지에서 StorageGRID 옵션을 선택하면 StorageGRID 대상 유형에 대한 구성 옵션이 표시됩니다.

시작하기 전에

- StorageGRID 계정이 설정되어 있습니다.
- SANtricity 클라우드 커넥터 키 저장소에 서명된 StorageGRID 인증서가 있습니다.
- 대상 유형으로 StorageGRID를 지정했습니다.

단계

1. URL * 필드에 Amazon S3 클라우드 서비스의 URL을 입력합니다
2. 액세스 키 ID * 필드에 S3 대상의 액세스 ID를 입력합니다.
3. 비밀 액세스 키 * 필드에 S3 대상의 비밀 액세스 키를 입력합니다.
4. Bucket Name * 필드에 S3 타겟의 버킷 이름을 입력합니다.
5. 경로 스타일 액세스를 사용하려면 * 경로 스타일 액세스 사용 * 확인란을 선택합니다.

   이 옵션을 선택하지 않으면 가상 호스트 스타일 액세스가 사용됩니다.

6. 선택한 타겟 유형에 구성 데이터베이스의 백업을 생성하려면 * 이 대상에 구성 데이터베이스의 백업 저장 * 확인란을 선택합니다.

   데이터베이스를 잃어버린 경우 백업 대상의 데이터를 복원할 수 있도록 이 설정을 사용하는 것이 좋습니다.

   연결을 테스트할 때 지정된 대상 유형에서 기존 데이터베이스 구성이 감지되면 SANtricity 클라우드 커넥터 호스트의 기존 데이터베이스 구성 정보를 구성 마법사에 입력한 새 백업 정보로 바꿀 수 있습니다.

7. Test Connection * 을 클릭하여 입력한 S3 자격 증명을 확인합니다.

일부 S3 호환 계정에는 보안 HTTP 연결이 필요할 수 있습니다. StorageGRID 인증서를 키 저장소에 배치하는 방법에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 인증서를 키 저장소에 추가합니다".

8. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 지정된 대상 유형이 허용되고 웹 서비스 프록시 페이지가 구성 마법사 아래에 표시됩니다.

9. "4단계: 웹 서비스 프록시에 연결"을 진행합니다.

4단계**:** 웹 서비스 프록시에 연결합니다

SANtricity 클라우드 커넥터와 함께 사용되는 웹 서비스 프록시의 로그인 및 연결 정보는 웹 서비스 프록시 URL 및 자격 증명 입력 페이지를 통해 입력됩니다.

시작하기 전에

SANtricity 웹 서비스 프록시에 대한 연결이 설정되어 있는지 확인합니다.

단계

1. URL* 필드에 SANtricity 클라우드 커넥터에 사용되는 웹 서비스 프록시의 URL을 입력합니다.
2. 사용자 이름 * 필드에 웹 서비스 프록시 연결의 사용자 이름을 입력합니다.
3. 암호 * 필드에 웹 서비스 프록시 연결의 암호를 입력합니다.
4. 입력한 웹 서비스 프록시 자격 증명에 대한 연결을 확인하려면 * 연결 테스트 * 를 클릭합니다.
5. 테스트 연결을 통해 입력한 웹 서비스 프록시 자격 증명을 확인한 후
6. 다음 * 을 클릭합니다

   SANtricity 클라우드 커넥터에 대한 웹 서비스 프록시 자격 증명이 수락되고 스토리지 배열 선택 페이지가 구성 마법사에 표시됩니다.

5단계**:** 스토리지 배열을 선택합니다

구성 마법사를 통해 입력한 SANtricity 웹 서비스 프록시 자격 증명을 기반으로 사용 가능한 스토리지 배열 목록이 스토리지 배열 선택 페이지에 표시됩니다. 이 페이지에서는 SANtricity 클라우드 커넥터가 백업 및 복원 작업에 사용하는 스토리지 어레이를 선택할 수 있습니다.

시작하기 전에

SANtricity 웹 서비스 프록시 응용 프로그램에 스토리지 배열이 구성되어 있는지 확인합니다.

SANtricity 클라우드 커넥터 애플리케이션에서 확인할 수 없는 스토리지 스토리지는 로그 파일에서 API 예외를 발생하게 됩니다. 이는 연결할 수 없는 스토리지에서 볼륨 목록을 가져올 때마다 SANtricity Cloud Connector 애플리케이션의 의도된 동작입니다. 로그 파일에서 이러한 API 예외를 방지하려면 스토리지 배열에서 직접 루트 문제를 해결하거나 SANtricity 웹 서비스 프록시 응용 프로그램에서 영향을 받는 스토리지 배열을 제거할 수 있습니다.

단계

1. 백업 및 복원 작업을 위해 SANtricity 클라우드 커넥터 애플리케이션에 할당할 스토리지 어레이 옆의 각 확인란을

선택합니다.

2. 다음 * 을 클릭합니다.

   선택한 스토리지 배열이 수락되고 호스트 선택 페이지가 구성 마법사에 표시됩니다.

   스토리지 배열 선택 페이지에서 선택한 스토리지 배열에 대해 유효한 암호를 구성해야 합니다. SANtricity 웹 서비스 프록시 API 설명서를 통해 스토리지 배열 암호를 구성할 수 있습니다.

6단계**:** 호스트를 선택합니다

구성 마법사를 통해 선택한 웹 서비스 프록시 호스팅 스토리지 어레이를 기반으로 사용 가능한 호스트를 선택하여 호스트 선택 페이지를 통해 백업 및 복구 대상 볼륨을 SANtricity 클라우드 커넥터 애플리케이션에 매핑할 수 있습니다.

시작하기 전에

SANtricity 웹 서비스 프록시를 통해 사용할 수 있는 호스트가 있는지 확인합니다.

단계

1. 나열된 스토리지 배열의 드롭다운 메뉴에서 원하는 호스트를 선택합니다.
2. 호스트 선택 페이지에 나열된 추가 스토리지 시스템에 대해 1단계를 반복합니다.
3. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 선택한 호스트가 수락되고 검토 페이지가 구성 마법사에 표시됩니다.

7단계**:** 초기 구성을 검토합니다

SANtricity 클라우드 커넥터 구성 마법사의 마지막 페이지에는 검토를 위해 입력된 결과가 요약되어 있습니다.

검증된 구성 데이터의 결과를 검토합니다.

- 모든 구성 데이터의 유효성을 성공적으로 확인 및 설정한 경우 * Finish * 를 클릭하여 구성 프로세스를 완료합니다.
- 구성 데이터의 섹션을 확인할 수 없는 경우 * Back * 을 클릭하여 구성 마법사의 해당 페이지로 이동하여 제출된 데이터를 수정합니다.

SANtricity 클라우드 커넥터에 로그인합니다

지원되는 브라우저에서 구성된 서버를 통해 SANtricity 클라우드 커넥터 응용 프로그램의 그래픽 사용자 인터페이스에 액세스할 수 있습니다. SANtricity 클라우드 커넥터 계정이 설정되어 있는지 확인합니다.

단계

1. 지원되는 브라우저에서 구성된 SANtricity 클라우드 커넥터 서버에 연결합니다(예: "http://localhost:8080/`).

   SANtricity 클라우드 커넥터 애플리케이션의 로그인 페이지가 표시됩니다.

2. 구성된 관리자 암호를 입력합니다.
3. 로그인 * 을 클릭합니다.

SANtricity 클라우드 커넥터 애플리케이션의 랜딩 페이지가 표시됩니다.

SANtricity Cloud Connector를 사용하여 E-Series 볼륨 백업을 생성하고 관리합니다

SANtricity 클라우드 커넥터 응용 프로그램의 왼쪽 탐색 패널에서 백업 옵션에 액세스할 수 있습니다. 백업 옵션은 새 이미지 기반 또는 파일 기반 백업 작업을 생성할 수 있는 백업 페이지를 표시합니다.

SANtricity Cloud Connector 애플리케이션의 * 백업 * 페이지를 사용하여 E-Series 볼륨의 백업을 생성 및 처리합니다. 이미지 기반 백업이나 파일 기반 백업을 만든 다음 이러한 작업을 즉시 또는 나중에 수행할 수 있습니다. 또한 마지막으로 수행된 전체 백업을 기준으로 전체 백업 또는 증분 백업을 수행하도록 선택할 수 있습니다. SANtricity 클라우드 커넥터 애플리케이션을 통해 수행된 마지막 전체 백업을 기준으로 최대 6개의 증분 백업을 수행할 수 있습니다.

SANtricity 클라우드 커넥터 애플리케이션에 나열된 백업 및 복원 작업에 대한 모든 타임스탬프는 현지 시간을 사용합니다.

새 이미지 기반 백업을 생성합니다

SANtricity 클라우드 커넥터 애플리케이션의 백업 페이지에 있는 생성 기능을 통해 새 이미지 기반 백업을 생성할 수 있습니다.

시작하기 전에

웹 서비스 프록시에서 SANtricity 클라우드 커넥터에 등록된 스토리지 배열이 있는지 확인합니다.

단계

1. 백업 페이지에서 * 생성 * 을 클릭합니다.

   백업 생성 창이 표시됩니다.

2. 이미지 기반 백업 생성 * 을 선택합니다.
3. 다음 * 을 클릭합니다.

   사용 가능한 E-Series 볼륨 목록이 백업 생성 창에 표시됩니다.

4. 원하는 E-Series 볼륨을 선택하고 * Next * 를 클릭합니다.

   백업 생성 확인 창의 * 백업 이름 지정 및 설명 * 페이지가 표시됩니다.

5. 자동 생성된 백업 이름을 수정하려면 * Job Name * 필드에 원하는 이름을 입력합니다.
6. 필요한 경우 * Job Description * 필드에 백업에 대한 설명을 추가합니다.

   백업 내용을 쉽게 식별할 수 있는 작업 설명을 입력해야 합니다.

7. 다음 * 을 클릭합니다.

선택한 이미지 기반 백업의 요약이 Create Backup 창의 * Review backup information * 페이지에 표시됩니다.

8. 선택한 백업을 검토하고 * Finish * 를 클릭합니다.

   Create Backup 창의 확인 페이지가 표시됩니다.

9. 다음 옵션 중 하나를 선택합니다.
   - * 예 * — 선택한 백업에 대한 전체 백업을 시작합니다.
   - * 아니요 * — 선택한 이미지 기반 백업에 대한 전체 백업이 수행되지 않습니다.

   > 선택한 이미지 기반 백업에 대한 전체 백업은 나중에 백업 페이지의 실행 기능을 통해 수행할 수 있습니다.

10. 확인 * 을 클릭합니다.

    선택한 E-Series 볼륨에 대한 백업이 시작되고 백업 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

새 폴더/파일 기반 백업을 생성합니다

SANtricity 클라우드 커넥터 애플리케이션의 백업 페이지에 있는 생성 기능을 통해 새 폴더/파일 기반 백업을 생성할 수 있습니다.

시작하기 전에

웹 서비스 프록시에서 SANtricity 클라우드 커넥터에 등록된 스토리지 배열이 있는지 확인합니다.

파일 기반 백업은 지정한 파일 시스템의 모든 파일을 무조건 백업합니다. 그러나 파일 및 폴더의 선택적 복원을 수행할 수 있습니다.

단계

1. 백업 페이지에서 * 생성 * 을 클릭합니다.

   백업 생성 창이 표시됩니다.

2. 폴더/파일 기반 백업 생성 * 을 선택합니다.
3. 다음 * 을 클릭합니다.

   백업에 사용할 수 있는 파일 시스템이 포함된 볼륨 목록이 백업 생성 창에 표시됩니다.

4. 원하는 볼륨을 선택하고 * 다음 * 을 클릭합니다.

   선택한 볼륨에서 사용 가능한 파일 시스템 목록이 Create Backup 창에 표시됩니다.

   > 파일 시스템이 나타나지 않으면 SANtricity 클라우드 커넥터 애플리케이션이 파일 시스템 유형을 지원하는지 확인하십시오. 자세한 내용은 을 참조하십시오 "지원되는 파일 시스템".

5. 백업할 폴더나 파일이 들어 있는 원하는 파일 시스템을 선택하고 * 다음 * 을 클릭합니다.

   백업 생성 확인 창의 * 백업 이름 지정 및 설명 * 페이지가 표시됩니다.

6. 자동 생성된 백업 이름을 수정하려면 * Job Name * 필드에 원하는 이름을 입력합니다.
7. 필요한 경우 * Job Description * 필드에 백업에 대한 설명을 추가합니다.

   백업 내용을 쉽게 식별할 수 있는 작업 설명을 입력해야 합니다.

8. 다음 * 을 클릭합니다.

   선택한 폴더/파일 기반 백업에 대한 요약이 Create Backup 창의 * Review backup information * 페이지에 표시됩니다.

9. 선택한 폴더/파일 기반 백업을 검토하고 * 마침 * 을 클릭합니다.

   Create Backup 창의 확인 페이지가 표시됩니다.

10. 다음 옵션 중 하나를 선택합니다.
    - * 예 * — 선택한 백업에 대한 전체 백업을 시작합니다.
    - * 아니요 * — 선택한 백업에 대한 전체 백업이 수행되지 않습니다.

      선택한 파일 기반 백업에 대한 전체 백업은 나중에 백업 페이지의 실행 기능을 통해 수행할 수도 있습니다.

11. 닫기 * 를 클릭합니다.

    선택한 E-Series 볼륨에 대한 백업이 시작되고 백업 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

전체 및 증분 백업을 실행합니다

백업 페이지의 실행 기능을 통해 전체 및 증분 백업을 수행할 수 있습니다. 증분 백업은 파일 기반 백업에만 사용할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터를 통해 백업 작업을 생성했는지 확인합니다.

단계

1. 백업 탭에서 원하는 백업 작업을 선택하고 * 실행 * 을 클릭합니다.

   이전에 수행된 초기 백업 없이 이미지 기반 백업 작업 또는 백업 작업을 선택할 때마다 전체 백업이 자동으로 수행됩니다.

   백업 실행 창이 표시됩니다.

2. 다음 옵션 중 하나를 선택합니다.
   - * 전체 * — 선택한 파일 기반 백업에 대한 모든 데이터를 백업합니다.
   - * Incremental * — 마지막으로 수행된 백업 이후 변경된 내용만 백업합니다.

SANtricity 클라우드 커넥터 애플리케이션을 통해 수행된 마지막 전체 백업을 기준으로 최대 6개의 증분 백업을 수행할 수 있습니다.

3. Run * 을 클릭합니다.

   백업 요청이 시작됩니다.

백업 작업을 삭제합니다

삭제 기능은 백업 세트와 함께 선택한 백업의 지정된 타겟 위치에서 백업된 데이터를 삭제합니다.

시작하기 전에

완료, 실패 또는 취소 상태의 백업이 있는지 확인합니다.

단계

1. 백업 페이지에서 원하는 백업을 선택하고 * 삭제 * 를 클릭합니다.

   전체 기본 백업을 삭제하도록 선택하면 관련된 모든 증분 백업도 삭제됩니다.

   Confirm Delete(삭제 확인) 창이 표시됩니다.

2. 삭제 작업을 확인하려면 * 유형 삭제 * 필드에 '삭제'를 입력합니다.
3. 삭제 * 를 클릭합니다.

   선택한 백업이 삭제됩니다.

SANtricity Cloud Connector에서 새 이미지 기반 또는 파일 기반 복원을 생성합니다

SANtricity 클라우드 커넥터 응용 프로그램의 왼쪽 탐색 패널에서 복원 옵션에 액세스할 수 있습니다. 복원 옵션은 새 이미지 기반 또는 파일 기반 복원 작업을 만들 수 있는 복원 페이지를 표시합니다.

SANtricity 클라우드 커넥터는 작업 개념을 사용하여 E-Series 볼륨의 실제 복원을 수행합니다. 복원을 수행하기 전에 작업에 사용할 E-Series 볼륨을 확인해야 합니다. 복원을 위해 E-Series 볼륨을 SANtricity 클라우드 커넥터 호스트에 추가한 후 SANtricity 클라우드 커넥터 애플리케이션의 '복원' 페이지를 사용하여 복원을 생성 및 처리할 수 있습니다.

SANtricity 클라우드 커넥터 애플리케이션에 나열된 백업 및 복원 작업에 대한 모든 타임스탬프는 현지 시간을 사용합니다.

새 이미지 기반 복원을 생성합니다

SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에 있는 만들기 기능을 통해 새 이미지 기반 복원을 만들 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터를 통해 이미지 기반 백업을 사용할 수 있는지 확인합니다.

단계

1. SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에서 * 생성 * 을 클릭합니다.

   Restore(복원) 창이 표시됩니다.

2. 원하는 백업을 선택합니다.
3. 다음 * 을 클릭합니다.

   백업 지점 선택 페이지가 복원 창에 표시됩니다.

4. 원하는 완료된 백업을 선택합니다.
5. 다음 * 을 클릭합니다.

   Restore(복원) 창에 Select Restore Target(대상 복원 선택) 페이지가 표시됩니다.

6. 복원 볼륨을 선택하고 * 다음 * 을 클릭합니다.

   Restore(복원) 창에 Review(검토) 페이지가 표시됩니다.

7. 선택한 복원 작업을 검토하고 * Finish * 를 클릭합니다.

   선택한 타겟 호스트 볼륨에 대한 복구가 시작되고 복구 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

새 파일 기반 복구를 생성합니다

SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에 있는 만들기 기능을 통해 새 파일 기반 복원을 만들 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터를 통해 파일 기반 백업을 사용할 수 있는지 확인합니다.

단계

1. SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에서 * 생성 * 을 클릭합니다.

   Restore(복원) 창이 표시됩니다.

2. Restore 창에서 원하는 파일 기반 백업을 선택합니다.
3. 다음 * 을 클릭합니다.

   백업 지점 선택 페이지가 복원 작업 생성 창에 표시됩니다.

4. 백업 지점 선택 페이지에서 원하는 완료된 백업을 선택합니다.
5. 다음 * 을 클릭합니다.

   복구 창에 사용 가능한 파일 시스템 또는 폴더/파일 목록이 표시됩니다.

6. 복원할 폴더 또는 파일을 선택하고 * 다음 * 을 클릭합니다.

Restore(복원) 창에 Select Restore Target(대상 복원 선택) 페이지가 표시됩니다.

7. 복원 볼륨을 선택하고 * 다음 * 을 클릭합니다.

   Restore(복원) 창에 Review(검토) 페이지가 표시됩니다.

8. 선택한 복원 작업을 검토하고 * Finish * 를 클릭합니다.

   선택한 타겟 호스트 볼륨에 대한 복구가 시작되고 복구 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

복원을 삭제합니다

삭제 기능을 사용하여 복원 페이지의 결과 목록 섹션에서 선택한 복원 항목을 삭제할 수 있습니다.

시작하기 전에

완료, 실패 또는 취소 상태의 복원 작업이 있는지 확인합니다.

단계

1. 복원 페이지에서 * 삭제 * 를 클릭합니다.

   Confirm Delete(삭제 확인) 창이 표시됩니다.

2. 삭제 작업을 확인하려면 * 유형 삭제 * 필드에 삭제 를 입력합니다.
3. 삭제 * 를 클릭합니다.

   일시 중지된 복구는 삭제할 수 없습니다.

   선택한 복원이 삭제됩니다.

SANtricity 클라우드 커넥터 설정을 수정합니다

설정 옵션을 사용하면 S3 계정, 관리되는 스토리지 배열 및 호스트, 웹 서비스 프록시 자격 증명에 대한 응용 프로그램의 현재 구성을 수정할 수 있습니다. 설정 옵션을 통해 SANtricity 클라우드 커넥터 응용 프로그램의 암호를 변경할 수도 있습니다.

S3 계정 설정을 수정합니다

S3 계정 설정 창에서 SANtricity 클라우드 커넥터 응용 프로그램에 대한 기존 S3 설정을 수정할 수 있습니다.

시작하기 전에

URL 또는 S3 버킷 레이블 설정을 수정할 때 SANtricity 클라우드 커넥터를 통해 구성된 기존 백업에 대한 액세스가 영향을 받는다는 점에 유의하십시오.

단계

1. 왼쪽 도구 모음에서 * 설정 > 구성 * 을 클릭합니다.

   설정 - 구성 페이지가 표시됩니다.

2. S3 계정 설정에 대한 * 설정 보기/편집 * 을 클릭합니다.

   S3 계정 설정 페이지가 표시됩니다.

3. URL 파일에 S3 클라우드 서비스의 URL을 입력합니다.
4. 액세스 키 ID * 필드에 S3 대상의 액세스 ID를 입력합니다.
5. 비밀 액세스 키 * 필드에 S3 대상의 액세스 키를 입력합니다.
6. S3 버킷 이름 * 필드에 S3 타겟의 버킷 이름을 입력합니다.
7. 필요한 경우 * 경로 스타일 액세스 사용 * 확인란을 선택합니다.
8. Test Connection * 을 클릭하여 입력한 S3 자격 증명에 대한 연결을 확인합니다.
9. 저장 * 을 클릭하여 수정 사항을 적용합니다.

   수정된 S3 계정 설정이 적용됩니다.

스토리지 시스템을 관리합니다

스토리지 배열 관리 페이지의 SANtricity 클라우드 커넥터 호스트에 등록된 웹 서비스 프록시에서 스토리지 배열을 추가하거나 제거할 수 있습니다.

스토리지 배열 관리 페이지에는 SANtricity 클라우드 커넥터 호스트에 등록할 수 있는 웹 서비스 프록시의 스토리지 배열 목록이 표시됩니다.

단계

1. 왼쪽 도구 모음에서 * 설정 > 스토리지 배열 * 을 클릭합니다.

   Settings - Storage Arrays(설정 - 스토리지 배열) 화면이 표시됩니다.

2. SANtricity 클라우드 커넥터에 스토리지 어레이를 추가하려면 * 추가 * 를 클릭합니다.
   a. Add Storage Arrays 창의 결과 목록에서 원하는 스토리지 배열 옆에 있는 각 확인란을 선택합니다.
   b. 추가 * 를 클릭합니다.

      선택한 스토리지 배열이 SANtricity 클라우드 커넥터에 추가되고 설정 - 스토리지 배열 화면의 결과 목록 섹션에 표시됩니다.

3. 추가된 스토리지 배열에 대한 호스트를 수정하려면 Settings(설정) - Storage Arrays(스토리지 배열) 화면의 Result list(결과 목록) 섹션에서 라인 항목에 대해 * Edit(편집) * 를 클릭합니다.
   a. Associated Host(연결된 호스트) 드롭다운 메뉴에서 스토리지 배열에 대해 원하는 호스트를 선택합니다.
   b. 저장 * 을 클릭합니다.

      선택한 호스트가 스토리지 배열에 할당됩니다.

4. SANtricity 클라우드 커넥터 호스트에서 기존 스토리지 배열을 제거하려면 하단 결과 목록에서 원하는 스토리지 배열을 선택하고 * Remove * 를 클릭합니다.
   a. 스토리지 배열 제거 확인 필드에 remove를 입력합니다.
   b. 제거 * 를 클릭합니다.

선택한 스토리지 배열이 SANtricity 클라우드 커넥터 호스트에서 제거됩니다.

웹 서비스 프록시 설정을 수정합니다

웹 서비스 프록시 설정 창에서 SANtricity 클라우드 커넥터 응용 프로그램에 대한 기존 웹 서비스 프록시 설정을 수정할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터와 함께 사용되는 웹 서비스 프록시는 적절한 어레이가 추가되고 해당 암호가 설정되어 있어야 합니다.

단계

1. 왼쪽 도구 모음에서 * 메뉴: 설정 [구성] * 을 클릭합니다.

   설정 - 구성 화면이 표시됩니다.

2. 웹 서비스 프록시에 대한 * 설정 보기/편집 * 을 클릭합니다.

   웹 서비스 프록시 설정 화면이 표시됩니다.

3. URL 필드에 SANtricity 클라우드 커넥터에 사용되는 웹 서비스 프록시의 URL을 입력합니다.
4. 사용자 이름 필드에 웹 서비스 프록시 연결의 사용자 이름을 입력합니다.
5. 암호 필드에 웹 서비스 프록시 연결의 암호를 입력합니다.
6. 입력한 웹 서비스 프록시 자격 증명에 대한 연결을 확인하려면 * 연결 테스트 * 를 클릭합니다.
7. 저장 * 을 클릭하여 수정 사항을 적용합니다.

SANtricity 클라우드 커넥터 암호를 변경합니다

암호 변경 화면에서 SANtricity 클라우드 커넥터 응용 프로그램의 암호를 변경할 수 있습니다.

단계

1. 왼쪽 도구 모음에서 * 메뉴: 설정 [구성] * 을 클릭합니다.

   설정 - 구성 화면이 표시됩니다.

2. SANtricity 클라우드 커넥터의 * 암호 변경 * 을 클릭합니다.

   암호 변경 화면이 표시됩니다.

3. 현재 암호 필드에 SANtricity 클라우드 커넥터 응용 프로그램의 현재 암호를 입력합니다.
4. 새 암호 필드에 SANtricity 클라우드 커넥터 응용 프로그램의 새 암호를 입력합니다.
5. 새 암호 확인 필드에 새 암호를 다시 입력합니다.
6. 새 암호를 적용하려면 * 변경 * 을 클릭합니다.

   수정된 암호는 SANtricity 클라우드 커넥터 응용 프로그램에 적용됩니다.

SANtricity 클라우드 커넥터를 제거합니다

그래픽 제거 프로그램 또는 콘솔 모드를 통해 SANtricity 클라우드 커넥터를 제거할 수 있습니다.

그래픽 모드를 사용하여 제거합니다

그래픽 모드를 사용하여 Linux 운영 체제에서 SANtricity 클라우드 커넥터를 제거할 수 있습니다.

단계

1. 터미널 창에서 SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉터리로 이동합니다.

   SANtricity 클라우드 커넥터의 제거 파일은 다음 기본 디렉토리 위치에서 사용할 수 있습니다.

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉토리에서 다음 명령을 실행합니다.

   ```
   ./uninstall_cloud_connector4 -i gui
   ```

   SANtricity 클라우드 커넥터의 제거 프로세스가 초기화됩니다.

3. 제거 창에서 * 제거 * 를 클릭하여 SANtricity 클라우드 커넥터 제거를 계속합니다.

   제거 프로세스가 완료되고 SANtricity 클라우드 커넥터 응용 프로그램이 Linux 운영 체제에서 제거됩니다.

콘솔 모드를 사용하여 제거합니다

콘솔 모드를 사용하여 Linux 운영 체제에서 SANtricity 클라우드 커넥터를 제거할 수 있습니다.

단계

1. 터미널 창에서 SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉터리로 이동합니다.

   SANtricity 클라우드 커넥터의 제거 파일은 다음 기본 디렉토리 위치에서 사용할 수 있습니다.

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉토리에서 다음 명령을 실행합니다.

   ```
   ./uninstall_cloud_connector4 -i console
   ```

   SANtricity 클라우드 커넥터의 제거 프로세스가 초기화됩니다.

3. 제거 창에서 * Enter * 를 눌러 SANtricity 클라우드 커넥터 제거를 계속합니다.

제거 프로세스가 완료되고 SANtricity 클라우드 커넥터 응용 프로그램이 Linux 운영 체제에서 제거됩니다.