보안 키 관리

SANtricity 11.8

NetApp
December 16, 2024

목차

보안 키 관리

보안 키를 변경합니다

언제든지 보안 키를 새 키로 바꿀 수 있습니다. 회사에서 보안 위반이 발생할 수 있으며 권한이 없는 직원이 드라이브 데이터에 액세스하지 못하도록 하려면 보안 키를 변경해야 할 수 있습니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 키 변경 * 을 선택합니다.

   보안 키 변경 대화 상자가 열립니다.

3. 다음 필드에 정보를 입력합니다.
   - * 보안 키 식별자 정의 * --(내부 보안 키에만 해당) 기본값(컨트롤러 펌웨어에 의해 생성되는 스토리지 배열 이름 및 타임스탬프)을 적용하거나 고유한 값을 입력합니다. 공백, 구두점 또는 기호 없이 최대 189자의 영숫자 문자를 입력할 수 있습니다.

     추가 문자는 자동으로 생성되며 입력하는 문자열의 양쪽 끝에 추가됩니다. 생성된 문자는 식별자가 고유한지 확인하는 데 도움이 됩니다.

   - * 암호문 정의/암호문 다시 입력 * — 이러한 각 필드에 암호문을 입력합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
     - 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
     - 숫자(하나 이상)
     - !, *, @(하나 이상)와 같은 영숫자 이외의 문자입니다.
4. 외부 보안 키의 경우 새 보안 키를 만들 때 이전 보안 키를 삭제하려면 대화 상자 아래쪽에 있는 "현재 보안 키 삭제… " 확인란을 선택합니다.

   - 나중에 사용할 수 있도록 항목을 기록해 두십시오. * — 보안 지원 드라이브를 스토리지 배열에서 이동해야 하는 경우, 드라이브 데이터를 잠금 해제하려면 식별자와 암호를 알아야 합니다.
5. 변경 * 을 클릭합니다.

   새 보안 키는 더 이상 유효하지 않은 이전 키를 덮어씁니다.

   다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

6. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

작업을 마친 후

키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

외부에서 내부 키 관리로 전환합니다

외부 키 서버에서 스토리지 배열에 사용되는 내부 방법으로 Drive Security의 관리 방법을 변경할 수 있습니다. 그런 다음 외부 키 관리를 위해 이전에 정의된 보안 키를 내부 키 관리에 사용합니다.

이 작업에 대해

이 작업에서는 외부 키 관리를 사용하지 않도록 설정하고 새 백업 복사본을 로컬 호스트에 다운로드합니다. 기존 키는 드라이브 보안에 계속 사용되지만 스토리지 시스템에서 내부적으로 관리됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 외부 키 관리 비활성화 * 를 선택합니다.

   외부 키 관리 비활성화 대화 상자가 열립니다.

3. 암호 정의/암호 다시 입력 * 에서 키 백업에 대한 암호 구문을 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.

   - 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
   - 숫자(하나 이상)
   - !, *, @(하나 이상)와 같은 영숫자 이외의 문자입니다.

   

   나중에 사용할 수 있도록 항목을 기록해 두십시오 _. 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터의 잠금을 해제하려면 식별자와 암호를 알아야 합니다.

4. 비활성화 * 를 클릭합니다.

   백업 키가 로컬 호스트에 다운로드됩니다.

5. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

결과

이제 드라이브 보안이 스토리지 어레이를 통해 내부적으로 관리됩니다.

작업을 마친 후

키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

키 관리 서버 설정을 편집합니다

외부 키 관리를 구성한 경우 언제든지 키 관리 서버 설정을 보고 편집할 수 있습니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 키 관리 서버 설정 보기/편집 * 을 선택합니다.
3. 다음 필드에서 정보를 편집합니다.

- * 키 관리 서버 주소 * — 키 관리에 사용되는 서버의 정규화된 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
- * 키 관리 포트 번호 * — KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트 번호를 입력합니다.
  - 선택 사항: * 키 서버 추가 * 를 클릭하여 다른 키 서버를 포함할 수 있습니다.

4. 저장 * 을 클릭합니다.

보안 키를 백업합니다

보안 키를 만들거나 변경한 후에는 원본이 손상되는 경우에 대비하여 키 파일의 백업 복사본을 만들 수 있습니다.

이 작업에 대해

이 작업에서는 이전에 만든 보안 키를 백업하는 방법에 대해 설명합니다. 이 절차를 수행하는 동안 백업에 대한 새 암호를 만듭니다. 이 암호문은 원래 키를 만들거나 마지막으로 변경할 때 사용한 암호문과 일치하지 않아도 됩니다. 암호는 생성 중인 백업에만 적용됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 백업 키 * 를 선택합니다.

   보안 키 백업 대화 상자가 열립니다.

3. 암호 구문 정의/암호 구문 다시 입력 * 필드에 이 백업의 암호 구문을 입력하고 확인합니다.

   값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.

   - 대문자(하나 이상)
   - 숫자(하나 이상)
   - 영숫자 이외의 문자(예:!, *, @(하나 이상)

   - 나중에 사용할 수 있도록 항목을 기록해 두십시오 *. 이 보안 키의 백업에 액세스하려면 암호문이 필요합니다.

4. 백업 * 을 클릭합니다.

   보안 키의 백업이 로컬 호스트에 다운로드되고 * 보안 키 백업 확인/기록 * 대화 상자가 열립니다.

   다운로드한 보안 키 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

5. 암호를 안전한 위치에 기록한 다음 * 닫기 * 를 클릭합니다.

작업을 마친 후

백업 보안 키의 유효성을 확인해야 합니다.

보안 키를 확인합니다

보안 키가 손상되지 않았는지 확인하고 올바른 암호문이 있는지 확인할 수 있습니다.

이 작업에 대해

이 작업에서는 이전에 만든 보안 키의 유효성을 검사하는 방법을 설명합니다. 이 단계는 키 파일이 손상되지 않고 암호 구문이 올바른지 확인하는 중요한 단계입니다. 이렇게 하면 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우 나중에 드라이브 데이터에 액세스할 수 있습니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 키 확인 * 을 선택합니다.

   보안 키 유효성 검사 대화 상자가 열립니다.

3. 찾아보기 * 를 클릭한 다음 키 파일(예:)을 `drivesecurity.slk` 선택합니다.
4. 선택한 키와 관련된 암호를 입력합니다.

   유효한 키 파일과 암호를 선택하면 * Validate * 버튼을 사용할 수 있게 됩니다.

5. Validate * 를 클릭합니다.

   유효성 검사 결과가 대화 상자에 표시됩니다.

6. 결과에 "보안 키 유효성 확인 성공"이 표시되면 * 닫기 * 를 클릭합니다. 오류 메시지가 나타나면 대화 상자에 표시되는 권장 지침을 따릅니다.

내부 키 관리 사용 시 드라이브 잠금을 해제합니다

내부 키 관리를 구성한 다음 나중에 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우, 드라이브의 암호화된 데이터에 액세스하려면 보안 키를 새 스토리지 배열에 다시 할당해야 합니다.

시작하기 전에

- 소스 스토리지(드라이브를 제거할 스토리지)에서 볼륨 그룹을 내보내고 드라이브를 제거했습니다. 대상 어레이에서 드라이브를 다시 설치했습니다.

  > 내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

  볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 "NetApp 기술 자료"참조하십시오. System Manager 또는 기존 시스템에서 관리하는 최신 어레이에 대한 적절한 지침을 따라야 합니다.

- 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
- 잠금을 해제할 드라이브와 연결된 보안 키를 알아야 합니다.

- 보안 키 파일은 관리 클라이언트(System Manager 액세스에 사용되는 브라우저가 있는 시스템)에서 사용할 수 있습니다. 드라이브를 다른 시스템에서 관리하는 스토리지 어레이로 이동하는 경우 보안 키 파일을 해당 관리 클라이언트로 이동해야 합니다.

이 작업에 대해

내부 키 관리를 사용하면 보안 키가 스토리지 배열에 로컬로 저장됩니다. 보안 키는 읽기/쓰기 액세스를 위해 컨트롤러와 드라이브에서 공유하는 일련의 문자입니다. 드라이브가 어레이에서 물리적으로 제거되어 다른 드라이브에 설치된 경우 올바른 보안 키를 제공할 때까지 드라이브가 작동할 수 없습니다.

> 컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 이 항목에서는 _INTERNAL_KEY 관리 사용 시 데이터 잠금 해제를 설명합니다. _EXTERNAL_KEY 관리를 사용한 경우 을 참조하십시오"외부 키 관리 사용 시 드라이브 잠금을 해제합니다". 컨트롤러 업그레이드를 수행하고 모든 컨트롤러를 최신 하드웨어로 교체하는 경우 E-Series 및 SANtricity 설명서 센터의 에 설명된 대로 서로 다른 단계를 수행해야 합니다."드라이브 잠금을 해제합니다"

다른 어레이에 보안 활성 드라이브를 재설치하면 해당 배열이 드라이브를 검색하고 "보안 키 필요" 상태와 함께 "주의 필요" 상태를 표시합니다. 드라이브 데이터의 잠금을 해제하려면 보안 키 파일을 선택하고 키에 대한 암호를 입력합니다. (이 암호는 스토리지 배열의 관리자 암호와 같지 않습니다.)

다른 보안 지원 드라이브가 새 스토리지 배열에 설치되어 있는 경우 가져오는 것과 다른 보안 키를 사용할 수 있습니다. 가져오기 프로세스 중에 이전 보안 키는 설치 중인 드라이브의 데이터 잠금을 해제하는 데만 사용됩니다. 잠금 해제 프로세스가 성공하면 새로 설치된 드라이브가 대상 스토리지 배열의 보안 키에 다시 입력됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 보안 드라이브 잠금 해제 * 를 선택합니다.

   보안 드라이브 잠금 해제 대화 상자가 열립니다. 보안 키가 필요한 모든 드라이브가 표에 나와 있습니다.

3. * 선택 사항: * 드라이브 번호 위로 마우스를 가져가면 드라이브 위치(쉘프 번호 및 베이 번호)가 표시됩니다.
4. 찾아보기 * 를 클릭한 다음 잠금을 해제할 드라이브에 해당하는 보안 키 파일을 선택합니다.

   선택한 키 파일이 대화 상자에 나타납니다.

5. 이 키 파일과 관련된 암호를 입력합니다.

   입력한 문자는 마스크됩니다.

6. 잠금 해제 * 를 클릭합니다.

   잠금 해제 작업이 성공하면 대화 상자에 "연결된 보안 드라이브가 잠금 해제되었습니다."라는 메시지가 표시됩니다.

결과

모든 드라이브가 잠겼다가 잠금 해제되면 스토리지 배열의 각 컨트롤러가 재부팅됩니다. 그러나 대상 스토리지 배열에 이미 일부 잠금 해제된 드라이브가 있는 경우 컨트롤러는 재부팅되지 않습니다.

작업을 마친 후

이제 대상 배열(새로 설치된 드라이브가 있는 배열)에서 볼륨 그룹을 가져올 수 있습니다.

내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 "NetApp 기술 자료"참조하십시오.

외부 키 관리 사용 시 드라이브 잠금을 해제합니다

외부 키 관리를 구성한 다음 나중에 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우, 드라이브의 암호화된 데이터에 액세스하려면 보안 키를 새 스토리지 배열에 다시 할당해야 합니다.

시작하기 전에

- 소스 스토리지(드라이브를 제거할 스토리지)에서 볼륨 그룹을 내보내고 드라이브를 제거했습니다. 대상 어레이에서 드라이브를 다시 설치했습니다.

  내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

  볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 "NetApp 기술 자료"참조하십시오. System Manager 또는 기존 시스템에서 관리하는 최신 어레이에 대한 적절한 지침을 따라야 합니다.

- 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
- 키 관리 서버의 IP 주소와 포트 번호를 알고 있어야 합니다.
- 스토리지 배열 컨트롤러의 서명된 클라이언트 인증서 파일이 있고, System Manager에 액세스하는 호스트에 해당 파일을 복사했습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다.
- 키 관리 서버에서 인증서 파일을 검색한 다음 System Manager에 액세스할 호스트에 해당 파일을 복사해야 합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에 루트, 중간 또는 서버 인증서를 사용할 수 있습니다.

서버 인증서에 대한 자세한 내용은 키 관리 서버 설명서를 참조하십시오.

이 작업에 대해

외부 키 관리를 사용하는 경우 보안 키는 보안 키를 안전하게 보호하도록 설계된 서버에 외부에 저장됩니다. 보안 키는 읽기/쓰기 액세스를 위해 컨트롤러와 드라이브에서 공유하는 일련의 문자입니다. 드라이브가 어레이에서 물리적으로 제거되어 다른 드라이브에 설치된 경우 올바른 보안 키를 제공할 때까지 드라이브가 작동할 수 없습니다.

컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 이 항목에서는 _EXTERNAL_KEY 관리 사용 시 데이터 잠금 해제를 설명합니다. internal_key 관리를 사용한 경우 를 참조하십시오"내부 키 관리 사용 시 드라이브 잠금을 해제합니다". 컨트롤러 업그레이드를 수행하고 모든 컨트롤러를 최신 하드웨어로 교체하는 경우 E-Series 및 SANtricity 설명서 센터의 에 설명된 대로 서로 다른 단계를 수행해야 합니다."드라이브 잠금을 해제합니다"

다른 어레이에 보안 활성 드라이브를 재설치하면 해당 배열이 드라이브를 검색하고 "보안 키 필요" 상태와 함께 "주의 필요" 상태를 표시합니다. 드라이브 데이터의 잠금을 해제하려면 보안 키 파일을 가져오고 키에 대한 암호를 입력합니다.

(이 암호는 스토리지 배열의 관리자 암호와 같지 않습니다.) 이 프로세스 중에 외부 키 관리 서버를 사용하도록 스토리지 배열을 구성하면 보안 키에 액세스할 수 있습니다. 보안 키를 연결 및 검색하려면 스토리지 배열에 대한 서버의 연락처 정보를 제공해야 합니다.

다른 보안 지원 드라이브가 새 스토리지 배열에 설치되어 있는 경우 가져오는 것과 다른 보안 키를 사용할 수 있습니다. 가져오기 프로세스 중에 이전 보안 키는 설치 중인 드라이브의 데이터 잠금을 해제하는 데만 사용됩니다. 잠금 해제 프로세스가 성공하면 새로 설치된 드라이브가 대상 스토리지 배열의 보안 키에 다시 입력됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 외부 키 생성 * 을 선택합니다.
3. 필수 연결 정보 및 인증서를 사용하여 마법사를 완료합니다.
4. 외부 키 관리 서버에 액세스하려면 * 통신 테스트 * 를 클릭합니다.
5. 보안 드라이브 잠금 해제 * 를 선택합니다.

   보안 드라이브 잠금 해제 대화 상자가 열립니다. 보안 키가 필요한 모든 드라이브가 표에 나와 있습니다.

6. * 선택 사항: * 드라이브 번호 위로 마우스를 가져가면 드라이브 위치(쉘프 번호 및 베이 번호)가 표시됩니다.
7. 찾아보기 * 를 클릭한 다음 잠금을 해제할 드라이브에 해당하는 보안 키 파일을 선택합니다.

   선택한 키 파일이 대화 상자에 나타납니다.

8. 이 키 파일과 관련된 암호를 입력합니다.

   입력한 문자는 마스크됩니다.

9. 잠금 해제 * 를 클릭합니다.

   잠금 해제 작업이 성공하면 대화 상자에 "연결된 보안 드라이브가 잠금 해제되었습니다."라는 메시지가 표시됩니다.

결과

모든 드라이브가 잠겼다가 잠금 해제되면 스토리지 배열의 각 컨트롤러가 재부팅됩니다. 그러나 대상 스토리지 배열에 이미 일부 잠금 해제된 드라이브가 있는 경우 컨트롤러는 재부팅되지 않습니다.

작업을 마친 후

이제 대상 배열(새로 설치된 드라이브가 있는 배열)에서 볼륨 그룹을 가져올 수 있습니다.

> 내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 "NetApp 기술 자료"참조하십시오.