드라이브 보안

SANtricity 11.7

NetApp
February 12, 2024

목차

드라이브 보안

드라이브 보안 개요

보안 키 관리 페이지에서 드라이브 보안 및 키 관리를 구성할 수 있습니다.

드라이브 보안이란 무엇입니까?

Drive Security 는 스토리지 어레이에서 제거할 때 보안이 설정된 드라이브의 데이터에 대한 무단 액세스를 방지하는 기능입니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다. FDE 또는 FIPS 드라이브를 어레이에서 물리적으로 제거할 경우, 해당 드라이브가 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 드라이브는 보안 잠금 상태가 됩니다. a_security key_는 이러한 유형의 드라이브와 스토리지 배열의 컨트롤러 간에 공유되는 문자의 문자열입니다.

자세한 내용:

- "드라이브 보안 기능의 작동 방식"
- "보안 키 관리의 작동 방식"
- "드라이브 보안 용어"

키 관리는 어떻게 구성합니까?

드라이브 보안을 구현하려면 어레이에 FDE 드라이브 또는 FIPS 드라이브가 설치되어 있어야 합니다. 이러한 드라이브의 키 관리를 구성하려면 메뉴 설정 [시스템 > 보안 키 관리]로 이동하여 컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 마지막으로 볼륨 설정에서 "보안 가능"을 선택하여 풀 및 볼륨 그룹에 대해 드라이브 보안을 설정합니다.

자세한 내용:

- "내부 보안 키를 생성합니다"
- "외부 보안 키를 만듭니다"
- "풀을 수동으로 생성합니다"
- "볼륨 그룹을 생성합니다"

드라이브의 잠금을 해제하려면 어떻게 해야 합니까?

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.

자세한 내용:

- "내부 키 관리 사용 시 드라이브 잠금을 해제합니다"
- "외부 키 관리 사용 시 드라이브 잠금을 해제합니다"

관련 정보

키 관리와 관련된 작업에 대해 자세히 알아보십시오.

- "키 관리 서버에서 인증에 CA 서명 인증서를 사용합니다"
- "보안 키를 백업합니다"

개념

드라이브 보안 기능의 작동 방식

드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다.

이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.

드라이브 보안을 구현하는 방법

드라이브 보안을 구현하려면 다음 단계를 수행하십시오.

1. 스토리지 어레이에 FDE 드라이브 또는 FIPS 드라이브와 같은 보안 지원 드라이브를 제공합니다. (FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.)
2. 컨트롤러 및 드라이브에서 읽기/쓰기 액세스를 위해 공유하는 일련의 문자인 보안 키를 생성합니다. 컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 외부 키 관리의 경우 키 관리 서버를 사용하여 인증을 설정해야 합니다.
3. 풀 및 볼륨 그룹에 대해 드라이브 보안 설정:
   - 풀 또는 볼륨 그룹을 생성합니다(후보 테이블의 * Secure-Capable * 열에서 * Yes * 를 찾습니다).
   - 새 볼륨을 생성할 때 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 * 보안 가능 * 옆에 * 예 * 가 표시됨).

드라이브 보안 작동 방식

FDE 또는 FIPS 중 어떤 보안 가능 드라이브도 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이 암호화 및 암호 해독은 성능 또는 사용자 워크플로에 영향을 주지 않습니다. 각 드라이브에는 드라이브에서 전송할 수 없는 고유한 암호화 키가 있습니다.

드라이브 보안 기능은 보안 기능이 있는 드라이브를 통해 추가 보호 계층을 제공합니다. 드라이브 보안을 위해 이러한 드라이브의 볼륨 그룹 또는 풀을 선택한 경우 드라이브는 데이터에 대한 액세스를 허용하기 전에 보안 키를 찾습니다. 드라이브의 기존 데이터에 영향을 주지 않고 언제든지 풀 및 볼륨 그룹에 대해 드라이브 보안을 설정할 수 있습니다. 그러나 드라이브의 모든 데이터를 지우지 않으면 드라이브 보안을 비활성화할 수 없습니다.

스토리지 어레이 레벨에서 드라이브 보안이 작동하는 방식

드라이브 보안 기능을 사용하면 스토리지 배열의 보안 지원 드라이브와 컨트롤러 간에 공유되는 보안 키를 만들 수 있습니다. 드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다.

보안 사용 드라이브가 스토리지 어레이에서 제거되어 다른 스토리지 배열에 다시 설치된 경우 드라이브는 보안 잠금 상태가 됩니다. 재배치된 드라이브는 데이터에 다시 액세스하기 전에 보안 키를 찾습니다. 데이터 잠금을 해제하려면 소스 스토리지 어레이에서 보안 키를 적용합니다. 잠금 해제 프로세스가 완료되면 다시 찾은 드라이브가 대상 스토리지 배열에 이미 저장된 보안 키를 사용하며 가져온 보안 키 파일이 더 이상 필요하지 않습니다.

내부 키 관리의 경우 실제 보안 키는 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 이 형식은 사람이 읽을 수 있는 형식도 아니며 사용자가 액세스할 수도 없습니다.

드라이브 보안이 볼륨 수준에서 작동하는 방식

보안 가능 드라이브에서 풀 또는 볼륨 그룹을 생성할 때 해당 풀 또는 볼륨 그룹에 대해 드라이브 보안을 설정할 수도 있습니다. Drive Security 옵션을 사용하면 드라이브 및 관련 볼륨 그룹과 풀의 보안이 __enabled_로 설정됩니다.

보안이 설정된 볼륨 그룹 및 풀을 생성하기 전에 다음 지침을 염두에 두십시오.

- 볼륨 그룹 및 풀은 전적으로 보안이 가능한 드라이브로 구성되어야 합니다. (FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.)
- 볼륨 그룹 및 풀이 최적의 상태여야 합니다.

보안 키 관리의 작동 방식

드라이브 보안 기능을 구현하는 경우 FIPS 또는 FDE(Secure-Enabled Drive)에 데이터 액세스를 위한 보안 키가 필요합니다. 보안 키는 이러한 유형의 드라이브와 스토리지 배열의 컨트롤러 사이에서 공유되는 문자의 문자열입니다.

드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다. 스토리지 어레이에서 보안 지원 드라이브를 제거하면 드라이브의 데이터가 잠깁니다. 드라이브가 다른 스토리지 배열에 다시 설치되면 데이터를 다시 액세스할 수 있도록 하기 전에 보안 키를 찾습니다. 데이터의 잠금을 해제하려면 원래 보안 키를 적용해야 합니다.

다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.

- 컨트롤러의 영구 메모리에서 내부 키 관리.
- 외부 키 관리 서버의 외부 키 관리.

내부 키 관리

내부 키는 컨트롤러의 영구 메모리에 액세스할 수 없는 위치에 유지되고 "숨김"됩니다. 내부 키 관리를 구현하려면 다음 단계를 수행하십시오.

1. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.

2. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
3. 식별자 및 암호 구문을 정의하는 내부 보안 키를 만듭니다. 식별자는 보안 키와 연결된 문자열이며, 컨트롤러와 키에 연결된 모든 드라이브에 저장됩니다. 암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 내부 키를 만들려면 설정 [시스템 > 보안 키 관리 > 내부 키 만들기] 메뉴로 이동합니다.

보안 키는 컨트롤러에 저장되어 있고 액세스할 수 없는 숨겨진 위치에 있습니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

외부 키 관리

외부 키는 KMIP(Key Management Interoperability Protocol)를 사용하여 별도의 키 관리 서버에 유지됩니다. 외부 키 관리를 구현하려면 다음 단계를 수행하십시오.

1. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
2. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
3. 서명된 클라이언트 인증서 파일을 가져옵니다. 클라이언트 인증서가 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP 요청을 신뢰할 수 있습니다.
   a. 먼저 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 설정 [인증서 > 키 관리 > CSR 완료] 메뉴로 이동합니다.
   b. 그런 다음 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청합니다. (CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드할 수도 있습니다.)
   c. 클라이언트 인증서 파일이 있는 경우 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.
4. 키 관리 서버에서 인증서 파일을 가져온 다음 System Manager에 액세스하는 호스트에 해당 파일을 복사합니다. 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.
5. 키 관리 서버의 IP 주소와 KMIP 통신에 사용되는 포트 번호를 정의하는 데 사용되는 외부 키를 생성합니다. 이 프로세스 중에 인증서 파일도 로드합니다. 외부 키를 만들려면 설정 [시스템 > 보안 키 관리 > 외부 키 만들기] 메뉴로 이동합니다.

입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

드라이브 보안 용어

드라이브 보안 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

기간	설명
드라이브 보안 기능	드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다. 이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.

기간	설명
FDE 드라이브	FDE(전체 디스크 암호화) 드라이브는 하드웨어 레벨의 디스크 드라이브에서 암호화를 수행합니다. 하드 드라이브에는 쓰기 중에 데이터를 암호화한 다음 읽기 중에 데이터를 해독하는 ASIC 칩이 포함되어 있습니다.
FIPS 드라이브	FIPS 드라이브는 FIPS(Federal Information Processing Standards) 140-2 레벨 2를 사용합니다. 이러한 드라이브는 강력한 암호화 알고리즘 및 방법을 보장하는 미국 정부 표준을 준수하는 FDE 드라이브입니다. FIPS 드라이브는 FDE 드라이브보다 보안 표준이 더 높습니다.
관리 클라이언트	System Manager 액세스를 위한 브라우저가 포함된 로컬 시스템(컴퓨터, 태블릿 등)
암호 구문	암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 드라이브 마이그레이션 또는 헤드 스왑의 결과로 백업된 보안 키를 가져올 때 보안 키를 암호화하는 데 사용된 것과 동일한 암호를 제공해야 합니다. 암호문은 8자에서 32자 사이여야 합니다.  Drive Security의 암호는 스토리지 배열의 관리자 암호와 무관합니다.
보안 지원 드라이브	보안이 가능한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있으며, 이 드라이브는 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이러한 드라이브는 드라이브 보안 기능을 사용하여 추가 보안을 위해 사용할 수 있으므로 보안 -_가능_으로 간주됩니다. 드라이브 보안 기능이 이러한 드라이브에 사용된 볼륨 그룹 및 풀에 대해 활성화된 경우 드라이브는 secure-_enabled_가 됩니다.
보안 지원 드라이브	보안 지원 드라이브는 드라이브 보안 기능과 함께 사용됩니다. 드라이브 보안 기능을 활성화한 다음 보안 -가능 드라이브의 풀 또는 볼륨 그룹에 드라이브 보안을 적용하면 드라이브는 보안- 사용 상태가 됩니다. 읽기 및 쓰기 액세스는 올바른 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다. 이렇게 추가된 보안으로 인해 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스가 방지됩니다.
보안 키	보안 키는 스토리지 어레이에서 보안 지원 드라이브와 컨트롤러 간에 공유되는 문자의 문자열입니다. 드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다. 스토리지 어레이에서 보안 지원 드라이브를 제거하면 드라이브의 데이터가 잠깁니다. 드라이브가 다른 스토리지 배열에 다시 설치되면 데이터를 다시 액세스할 수 있도록 하기 전에 보안 키를 찾습니다. 데이터의 잠금을 해제하려면 원래 보안 키를 적용해야 합니다. 다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다. • 내부 키 관리 — 컨트롤러의 영구 메모리에 보안 키를 만들고 관리합니다. • 외부 키 관리 — 외부 키 관리 서버에 보안 키를 만들고 유지 관리합니다.
보안 키 식별자입니다	보안 키 식별자는 키를 생성하는 동안 보안 키와 연결된 문자열입니다. 식별자는 컨트롤러와 보안 키와 연결된 모든 드라이브에 저장됩니다.

보안 키를 구성합니다

내부 보안 키를 생성합니다

드라이브 보안 기능을 사용하려면 스토리지 어레이에서 컨트롤러와 보안 가능 드라이브에서 공유하는 내부 보안 키를 생성해야 합니다. 내부 키는 컨트롤러의 영구 메모리에 유지됩니다.

시작하기 전에

- 스토리지 배열에 보안 가능 드라이브가 설치되어 있어야 합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
- 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.

FDE 및 FIPS 드라이브가 모두 스토리지 어레이에 설치된 경우 모두 동일한 보안 키를 공유합니다.

이 작업에 대해

이 작업에서는 내부 보안 키와 연결할 식별자와 암호를 정의합니다.

Drive Security의 암호는 스토리지 배열의 관리자 암호와 무관합니다.

단계

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

   아직 보안 키를 생성하지 않은 경우 보안 키 만들기 대화 상자가 열립니다.

3. 다음 필드에 정보를 입력합니다.

   ◦ * 보안 키 식별자 정의 * — 기본값(컨트롤러 펌웨어에 의해 생성되는 스토리지 배열 이름 및 타임 스탬프)을 그대로 사용하거나 값을 직접 입력할 수 있습니다. 공백, 구두점 또는 기호 없이 최대 189자의 영숫자 문자를 입력할 수 있습니다.

   입력한 문자열의 양쪽 끝에 추가된 추가 문자가 자동으로 생성됩니다. 생성된 문자는 식별자가 고유한지 확인합니다.

   ◦ * 암호문 정의/암호문 다시 입력 * — 암호문을 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. Create * 를 클릭합니다.

보안 키는 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 실제 키와 함께 암호화된 키 파일이 브라우저에서 다운로드됩니다.

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

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

결과

이제 보안 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

드라이브 전원을 껐다가 다시 켤 때마다 모든 보안 지원 드라이브는 보안 잠금 상태로 변경됩니다. 이 상태에서는 드라이브 초기화 중에 컨트롤러가 올바른 보안 키를 적용할 때까지 데이터에 액세스할 수 없습니다. 잠긴 드라이브를 물리적으로 제거하고 다른 시스템에 설치하는 경우 보안 잠금 상태는 데이터에 대한 무단 액세스를 방지합니다.

작업을 마친 후

키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

외부 보안 키를 만듭니다

키 관리 서버에서 드라이브 보안 기능을 사용하려면 스토리지 어레이에서 키 관리 서버와 보안 가능 드라이브가 공유하는 외부 키를 만들어야 합니다.

시작하기 전에

- 스토리지에 보안 가능 드라이브가 설치되어 있어야 합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.

  FDE 및 FIPS 드라이브가 모두 스토리지 어레이에 설치된 경우 모두 동일한 보안 키를 공유합니다.

- 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.
- 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

이 작업에서는 키 관리 서버의 IP 주소와 사용하는 포트 번호를 정의한 다음 외부 키 관리를 위해 인증서를 로드합니다.

단계

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

현재 내부 키 관리가 구성되어 있으면 대화 상자가 열리고 외부 키 관리로 전환할지 확인하는 메시지가 표시됩니다.

외부 보안 키 만들기 대화 상자가 열립니다.

3. 키 서버에 연결 * 에서 다음 필드에 정보를 입력합니다.
   - * 키 관리 서버 주소 * — 키 관리에 사용되는 서버의 정규화된 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
   - * 키 관리 포트 번호 * — KMIP 통신에 사용되는 포트 번호를 입력합니다. 키 관리 서버 통신에 사용되는 가장 일반적인 포트 번호는 5696입니다.
     - 선택 사항: * 백업 키 서버를 구성하려면 * 키 서버 추가 * 를 클릭한 다음 해당 서버의 정보를 입력합니다. 기본 키 서버에 연결할 수 없는 경우 두 번째 키 서버가 사용됩니다. 각 키 서버가 동일한 키 데이터베이스에 액세스할 수 있는지 확인합니다. 그렇지 않으면 어레이에서 오류를 게시하고 백업 서버를 사용할 수 없습니다.

     한 번에 하나의 키 서버만 사용됩니다. 스토리지 배열이 기본 키 서버에 도달할 수 없는 경우, 스토리지는 백업 키 서버에 접속하게 됩니다. 두 서버 간에 패리티를 유지해야 합니다. 그렇지 않으면 오류가 발생할 수 있습니다.

   - * 클라이언트 인증서 선택 * — 첫 번째 * 찾아보기 * 버튼을 클릭하여 스토리지 배열 컨트롤러의 인증서 파일을 선택합니다.
   - * 키 관리 서버의 서버 인증서 선택 * — 두 번째 * 찾아보기 * 버튼을 클릭하여 키 관리 서버의 인증서 파일을 선택합니다. 키 관리 서버에 대한 루트, 중간 또는 서버 인증서를 선택할 수 있습니다.
4. 다음 * 을 클릭합니다.
5. Create/Backup Key * 에서 보안을 위해 백업 키를 생성할 수 있습니다.
   - (권장) 백업 키를 만들려면 확인란을 선택한 상태로 두고 암호를 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 데이터를 잠금 해제하려면 암호를 알아야 합니다.

   +
   - 백업 키를 생성하지 않으려면 확인란을 선택 취소합니다.

     외부 키 서버에 액세스할 수 없고 백업 키가 없는 경우 다른 스토리지 어레이로 마이그레이션하면 드라이브의 데이터에 액세스할 수 없게 됩니다. 이 옵션은 System Manager에서 백업 키를 생성하는 유일한 방법입니다.
6. 마침 * 을 클릭합니다.

입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안 키의 복사본이 로컬 시스템에

저장됩니다.

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

7. 다운로드한 키 파일의 위치와 암호를 기록한 다음 * 닫기 * 를 클릭합니다.

   외부 키 관리를 위한 추가 링크가 포함된 다음 메시지가 페이지에 표시됩니다.

   ```
   Current key management method: External
   ```

8. 테스트 통신 * 을 선택하여 스토리지 어레이와 키 관리 서버 간의 연결을 테스트합니다.

   대화 상자에 검사 결과가 표시됩니다.

결과

외부 키 관리를 사용하도록 설정하면 보안 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

드라이브 전원을 껐다가 다시 켤 때마다 모든 보안 지원 드라이브는 보안 잠금 상태로 변경됩니다. 이 상태에서는 드라이브 초기화 중에 컨트롤러가 올바른 보안 키를 적용할 때까지 데이터에 액세스할 수 없습니다. 잠긴 드라이브를 물리적으로 제거하고 다른 시스템에 설치하는 경우 보안 잠금 상태는 데이터에 대한 무단 액세스를 방지합니다.

작업을 마친 후

키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

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 펌웨어에서 생성되는 스토리지 배열 이름 및 타임스탬프)을 그대로 사용하거나 값을 직접 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 클릭하고 키 파일(예: `drivesecurity.slk`)를 클릭합니다.
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 그룹 마이그레이션에 대한 자세한 지침은 에 나와 있습니다 "NetApp 기술 자료". 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 를 참조하십시오 "외부 키 관리 사용 시 드라이브 잠금을 해제합니다". 컨트롤러 업그레이드를 수행하고 모든 컨트롤러를 최신 하드웨어로 교체하려는 경우, 의 E-Series 및 SANtricity 설명서 센터에 설명된 대로 여러 단계를 수행해야 합니다 "드라이브 잠금을 해제합니다".

다른 어레이에서 보안 지원 드라이브를 재설치하면 해당 어레이에서 드라이브를 검색하고 "주의 필요" 상태와 함께 "보안 키 필요" 상태를 표시합니다. 드라이브 데이터의 잠금을 해제하려면 보안 키 파일을 선택하고 키의 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 그룹 마이그레이션에 대한 자세한 지침은 에 나와 있습니다 "NetApp 기술 자료".

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 그룹 마이그레이션에 대한 자세한 지침은 에 나와 있습니다 "NetApp 기술 자료". 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 교체하려는 경우, 의 E-Series 및 SANtricity 설명서 센터에 설명된 대로 여러 단계를 수행해야 합니다 "드라이브 잠금을 해제합니다".

다른 어레이에서 보안 지원 드라이브를 재설치하면 해당 어레이에서 드라이브를 검색하고 "주의 필요" 상태와 함께 "보안 키 필요" 상태를 표시합니다. 드라이브 데이터의 잠금을 해제하려면 보안 키 파일을 가져오고 키의 암호를 입력합니다. (이 암호는 스토리지 배열의 관리자 암호와 같지 않습니다.) 이 프로세스 중에 외부 키 관리 서버를 사용하도록 스토리지 배열을 구성한 다음 보안 키를 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 그룹 마이그레이션에 대한 자세한 지침은 에 나와 있습니다 "NetApp 기술 자료".

FAQ 를 참조하십시오

보안 키를 생성하기 전에 알아야 할 사항은 무엇입니까?

보안 키는 스토리지 시스템 내의 컨트롤러 및 보안 지원 드라이브에서 공유됩니다. 스토리지 배열에서 보안 지원 드라이브를 제거하면 보안 키가 무단 액세스로부터 데이터를 보호합니다.

다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.

- 컨트롤러의 영구 메모리에서 내부 키 관리.
- 외부 키 관리 서버의 외부 키 관리.

내부 키 관리

내부 키는 컨트롤러의 영구 메모리에 액세스할 수 없는 위치에 유지되고 "숨김"됩니다. 내부 보안 키를 생성하기 전에 다음을 수행해야 합니다.

1. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
2. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.

그런 다음 식별자 및 암호 구문을 정의하는 내부 보안 키를 만들 수 있습니다. 식별자는 보안 키와 연결된 문자열이며, 컨트롤러와 키에 연결된 모든 드라이브에 저장됩니다. 암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 작업을 마치면 보안 키가 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

외부 키 관리

외부 키는 KMIP(Key Management Interoperability Protocol)를 사용하여 별도의 키 관리 서버에 유지됩니다. 외부 보안 키를 만들기 전에 다음을 수행해야 합니다.

1. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
2. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.

3. 서명된 클라이언트 인증서 파일을 가져옵니다. 클라이언트 인증서가 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP 요청을 신뢰할 수 있습니다.
   a. 먼저 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 설정 [인증서 > 키 관리 > CSR 완료] 메뉴로 이동합니다.
   b. 그런 다음 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청합니다. (다운로드한 CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드할 수도 있습니다.)
   c. 클라이언트 인증서 파일이 있는 경우 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.
4. 키 관리 서버에서 인증서 파일을 가져온 다음 System Manager에 액세스하는 호스트에 해당 파일을 복사합니다. 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.

그런 다음 외부 키를 생성하여 키 관리 서버의 IP 주소와 KMIP 통신에 사용되는 포트 번호를 정의할 수 있습니다. 이 프로세스 중에 인증서 파일도 로드합니다. 작업을 마치면 입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

암호문을 정의해야 하는 이유는 무엇입니까?

암호 구문은 로컬 관리 클라이언트에 저장된 보안 키 파일을 암호화하고 해독하는 데 사용됩니다. 암호 구문이 없으면 보안 키를 해독할 수 없으며 다른 스토리지 배열에 다시 설치한 경우 보안 활성 드라이브에서 데이터의 잠금을 해제하는 데 사용할 수 없습니다.

보안 키 정보를 기록하는 것이 중요한 이유는 무엇입니까?

보안 키 정보가 손실되고 백업이 없는 경우, 보안 지원 드라이브를 재배치하거나 컨트롤러를 업그레이드할 때 데이터가 손실될 수 있습니다. 드라이브에서 데이터를 잠금 해제하려면 보안 키가 필요합니다.

보안 키 식별자, 연결된 암호 구문 및 보안 키 파일이 저장된 로컬 호스트의 위치를 기록해야 합니다.

보안 키를 백업하기 전에 알아야 할 내용은 무엇입니까?

원래 보안 키가 손상되고 백업이 없는 경우, 한 스토리지 어레이에서 다른 스토리지 어레이로 마이그레이션할 경우 드라이브의 데이터에 액세스할 수 없게 됩니다.

보안 키를 백업하기 전에 다음 지침을 염두에 두십시오.

- 원본 키 파일의 보안 키 식별자 및 암호를 알고 있어야 합니다.

> 내부 키만 식별자를 사용합니다. 식별자를 만들면 추가 문자가 자동으로 생성되고 식별자 문자열의 양쪽 끝에 추가됩니다. 생성된 문자는 식별자가 고유한지 확인합니다.

- 백업에 대한 새 암호를 만듭니다. 이 암호문은 원래 키를 만들거나 마지막으로 변경할 때 사용한 암호문과 일치하지 않아도 됩니다. 암호는 생성 중인 백업에만 적용됩니다.

드라이브 보안의 암호를 스토리지 배열의 관리자 암호와 혼동해서는 안 됩니다. Drive Security의 암호 구문은 보안 키의 백업을 보호합니다. 관리자 암호를 사용하면 전체 스토리지 시스템이 무단으로 액세스하지 못하도록 보호할 수 있습니다.

- 백업 보안 키 파일이 관리 클라이언트에 다운로드됩니다. 다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다. 보안 키 정보가 저장된 위치를 기록해 두십시오.

보안 드라이브를 잠금 해제하기 전에 알아야 할 사항은 무엇입니까?

보안 지원 드라이브에서 데이터의 잠금을 해제하려면 해당 보안 키를 가져와야 합니다.

보안 지원 드라이브를 잠금 해제하기 전에 다음 지침을 염두에 두십시오.

- 스토리지 배열에 이미 보안 키가 있어야 합니다. 마이그레이션된 드라이브는 대상 스토리지 배열에 다시 연결됩니다.
- 마이그레이션하는 드라이브의 경우 보안 키 식별자와 보안 키 파일에 해당하는 암호 구문을 알아야 합니다.
- 보안 키 파일은 관리 클라이언트(System Manager 액세스에 사용되는 브라우저가 있는 시스템)에서 사용할 수 있어야 합니다.
- 잠긴 NVMe 드라이브를 재설정하는 경우 드라이브의 보안 ID를 입력해야 합니다. 보안 ID를 찾으려면 드라이브를 물리적으로 제거하고 드라이브 레이블에서 PSID 문자열(최대 32자)을 찾아야 합니다. 작업을 시작하기 전에 드라이브를 다시 설치해야 합니다.

읽기/쓰기 접근성이란 무엇입니까?

드라이브 설정 창에는 드라이브 보안 속성에 대한 정보가 포함되어 있습니다. "읽기/쓰기 액세스 가능"은 드라이브의 데이터가 잠겨 있는지 여부를 표시하는 속성 중 하나입니다.

드라이브 보안 속성을 보려면 하드웨어 페이지로 이동합니다. 드라이브를 선택하고 * 설정 보기 * 를 클릭한 다음 * 추가 설정 표시 * 를 클릭합니다. 드라이브의 잠금이 해제될 때 페이지 하단에서 읽기/쓰기 액세스 가능 속성 값은 * 예 * 입니다. 읽기/쓰기 액세스 가능 속성 값은 드라이브가 잠겨 있을 때 * 아니오, 유효하지 않은 보안 키 * 입니다. 보안 키를 가져와 보안 드라이브의 잠금을 해제할 수 있습니다(설정 [시스템 > 보안 드라이브 잠금 해제] 메뉴로 이동).

보안 키 유효성 검사에 대해 알아야 할 내용은 무엇입니까?

보안 키를 만든 후에는 키 파일이 손상되지 않았는지 확인해야 합니다.

유효성 검사에 실패하면 다음을 수행합니다.

- 보안 키 식별자가 컨트롤러의 식별자와 일치하지 않는 경우 올바른 보안 키 파일을 찾은 다음 확인을 다시 시도하십시오.
- 컨트롤러가 유효성 검사를 위해 보안 키를 해독할 수 없는 경우 암호 구문을 잘못 입력했을 수 있습니다. 암호를 다시 확인하고 필요한 경우 다시 입력한 다음 확인을 다시 시도하십시오. 오류 메시지가 다시 나타나면 키 파일의 백업을 선택하고(있는 경우) 유효성 검사를 다시 시도하십시오.
- 여전히 보안 키의 유효성을 검사할 수 없는 경우 원본 파일이 손상되었을 수 있습니다. 키의 새 백업을 생성하고 해당 복사본을 확인합니다.

내부 보안 키와 외부 보안 키 관리의 차이점은 무엇입니까?

드라이브 보안 기능을 구현할 때 스토리지 배열에서 보안 지원 드라이브를 제거할 때 내부 보안 키 또는 외부 보안 키를 사용하여 데이터를 잠글 수 있습니다.

보안 키는 문자열을 말합니다. 이 문자열은 스토리지 어레이에서 보안이 설정된 드라이브와 컨트롤러 간에 공유됩니다. 내부 키는 컨트롤러의 영구 메모리에 유지됩니다. 외부 키는 KMIP(Key Management Interoperability Protocol)를 사용하여 별도의 키 관리 서버에 유지됩니다.

저작권 정보

상표 정보