



보안 키를 구성합니다

SANtricity 11.7

NetApp
February 12, 2024

목차

보안 키를 구성합니다	1
내부 보안 키를 생성합니다	1
외부 보안 키를 만듭니다	2

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 켜다가 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.

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.