



g SANtricity commands

NetApp
June 16, 2025

목차

- g 1
 - 인증 시작하기 - SANtricity CLI 1
 - 외부 키 관리 시작하기 - SANtricity CLI 1
 - 워크플로 단계 1
 - 내부 키 관리 시작하기 - SANtricity CLI 2
 - 워크플로 단계 2

g

인증 시작하기 - SANtricity CLI

인증을 위해서는 사용자가 할당된 로그인 자격 증명을 사용하여 시스템에 액세스해야 합니다. 각 사용자 로그인에는 특정 역할 및 액세스 권한이 포함된 사용자 프로필과 연결됩니다.

관리자는 다음과 같이 시스템 인증을 구현할 수 있습니다.

- 스토리지 어레이에 사전 정의된 사용자 및 역할을 포함하는 RBAC(역할 기반 액세스 제어) 기능을 사용합니다.
- LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스에 연결한 다음 LDAP 사용자를 스토리지 배열의 내장 역할에 매핑합니다.
- SAML(Security Assertion Markup Language) 2.0을 사용하여 IdP(Identity Provider)와 연결한 다음 사용자를 스토리지 배열의 내장 역할에 매핑합니다.



SAML은 스토리지 어레이에 포함된 기능(펌웨어 레벨 8.42 이상)이며 SANtricity 시스템 관리자 사용자 인터페이스에서만 구성할 수 있습니다.

외부 키 관리 시작하기 - SANtricity CLI

보안 키는 문자열을 말합니다. 이 문자열은 스토리지 어레이에서 보안이 설정된 드라이브와 컨트롤러 간에 공유됩니다. 외부 키 관리를 사용하는 경우 키 관리 서버에서 보안 키를 만들고 유지 관리합니다.

외부 키 관리 서버 및 보안 키 사용에 대한 개념적 정보는 SANtricity System Manager 온라인 도움말을 참조하십시오.

다음은 외부 보안 키를 구현하기 위한 기본 워크플로입니다.

1. * 인증서 서명 요청 생성 *
2. * KMIP 서버에서 클라이언트 및 서버 인증서를 얻습니다 *
3. * 클라이언트 인증서 설치 *
4. * KMIP 서버의 IP 주소와 포트 번호를 설정합니다. *
5. * KMIP 서버와의 통신 테스트 *
6. * 스토리지 배열 보안 키 생성 *
7. * 보안 키 유효성 검사 *

워크플로 단계

인증서 관리와 외부 키 관리 모두 SANtricity 11.40 릴리스의 새로운 보안 기능입니다. 시작하려면 다음 기본 단계를 사용하십시오.

1. 'Save storageArray keyManagementClientCSR' 명령어를 사용하여 인증서 서명 요청을 생성합니다. 을 참조하십시오 [키 관리 인증서 서명 요청을 생성합니다.](#)

2. KMIP 서버에서 클라이언트 및 서버 인증서를 요청합니다.
3. certificateType 매개 변수를 client로 설정한 상태에서 download storageArray keyManagementCertificate 명령을 사용하여 클라이언트 인증서를 설치합니다. 을 참조하십시오 [스토리지 배열 외부 키 관리 인증서를 설치합니다.](#)
4. certificateType 매개 변수를 'server'로 설정하고 download storageArray keyManagementCertificate 명령을 사용하여 서버 인증서를 설치합니다. 을 참조하십시오 [스토리지 배열 외부 키 관리 인증서를 설치합니다.](#)
5. Set storageArray externalKeyManagement 명령을 사용하여 키 관리 서버의 IP 주소와 포트 번호를 설정합니다. 을 참조하십시오 [외부 키 관리 설정을 지정합니다.](#)
6. 'tart storageArray externalKeyManagement test' 명령어를 사용하여 외부 키 관리 서버와의 통신을 테스트합니다. 을 참조하십시오 [외부 키 관리 통신을 테스트합니다.](#)
7. create storageArray securityKey 명령을 사용하여 보안 키를 생성합니다. 을 참조하십시오 [보안 키를 생성합니다.](#)
8. "validate storageArray securityKey" 명령을 사용하여 보안 키를 확인합니다. 을 참조하십시오 [내부 또는 외부 보안 키를 확인합니다.](#)

내부 키 관리 시작하기 - SANtricity CLI

보안 키는 문자열을 말합니다. 이 문자열은 스토리지 어레이에서 보안이 설정된 드라이브와 컨트롤러 간에 공유됩니다. 내부 키 관리를 사용하는 경우 컨트롤러의 영구 메모리에 보안 키를 만들고 유지 관리합니다.

내부 보안 키 사용에 대한 개념적 정보는 SANtricity System Manager 온라인 도움말을 참조하십시오.

다음은 내부 보안 키를 사용하기 위한 기본 워크플로입니다.

1. * 보안 키 생성 *
2. * 보안 키 설정 *
3. * 보안 키 유효성 검사 *

워크플로 단계

다음 명령을 실행하면 내부 보안 키로 시작할 수 있습니다.

1. Create storageArray securityKey 명령을 사용하여 스토리지 배열 보안 키를 생성합니다. 을 참조하십시오 [스토리지 배열 보안 키 생성.](#)
2. 'set storageArray securityKey' 명령어를 사용하여 스토리지 배열 보안 키를 설정합니다. 을 참조하십시오 [스토리지 배열 보안 키 설정.](#)
3. "validate storageArray securityKey" 명령을 사용하여 보안 키를 확인합니다. 을 참조하십시오 [스토리지 배열 보안 키의 유효성을 검사하는 중입니다.](#)

저작권 정보

Copyright © 2025 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.