g

SANtricity commands

NetApp
June 16, 2025

목차

g

인증 시작하기 - SANtricity CLI

인증을 위해서는 사용자가 할당된 로그인 자격 증명을 사용하여 시스템에 액세스해야 합니다. 각 사용자 로그인은 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 SANtrictity11.40 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 dowload 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

상표 정보