



데이터 보호

ASA r2

NetApp
September 26, 2024

목차

| | |
|--|---|
| 데이터 보호 | 1 |
| ASA R2 스토리지 시스템에서 유희 데이터를 암호화합니다 | 1 |
| ASA R2 스토리지 시스템에서 랜섬웨어 공격을 방어합니다 | 1 |
| ASA R2 스토리지 시스템에서 NVMe 연결을 보호합니다 | 2 |

데이터 보호

ASA R2 스토리지 시스템에서 유틸 데이터를 암호화합니다

유틸 상태의 데이터를 암호화할 때 스토리지 미디어가 용도 변경하거나 반환되거나 잘못 배치되거나 도난당하는 경우에는 읽을 수 없습니다. ONTAP System Manager를 사용하여 하드웨어 및 소프트웨어 수준에서 데이터를 암호화하여 이중 계층 보호를 제공할 수 있습니다.

NSE(NetApp 스토리지 암호화)는 자체 암호화 드라이브(SED)를 이용한 하드웨어 암호화를 지원합니다. SED는 데이터가 기록될 때 데이터를 암호화합니다. 각 SED에는 고유한 암호화 키가 포함되어 있습니다. SED에 저장된 암호화된 데이터는 SED의 암호화 키가 없으면 읽을 수 없습니다. SED에서 읽기를 시도하는 노드는 SED의 암호화 키에 액세스하려면 인증을 받아야 합니다. 노드는 키 관리자로부터 인증 키를 받은 다음 SED에 인증 키를 제공하여 인증됩니다. 인증 키가 유효한 경우 SED는 노드에 포함된 데이터에 액세스할 수 있는 암호화 키를 노드에 제공합니다.

ASA R2 온보드 키 관리자 또는 외부 키 관리자를 사용하여 노드에 인증 키를 제공합니다.

NSE 이외에 소프트웨어 암호화를 사용하여 데이터에 더 많은 보안 계층을 추가할 수도 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션의 * 암호화 * 에서 * 구성 * 을 선택합니다.
3. Key Manager를 설정한다.

| 옵션을 선택합니다 | 단계 |
|----------------------------|--|
| Onboard Key Manager를 구성합니다 | <ol style="list-style-type: none">a. Onboard Key Manager * 를 선택하여 키 서버를 추가합니다.b. 암호를 입력합니다. |
| 외부 키 관리자를 구성합니다 | <ol style="list-style-type: none">a. 외부 키 관리자 * 를 선택하여 키 서버를 추가합니다.b. + Add 키 서버를 추가하려면 선택합니다.c. KMIP 서버 CA 인증서를 추가합니다.d. KMIP 클라이언트 인증서를 추가합니다. |

4. 소프트웨어 암호화를 활성화하려면 * 듀얼 레이어 암호화 * 를 선택하십시오.
5. 저장 * 을 선택합니다.

다음 단계

이제 저장된 데이터를 암호화했습니다. NVMe/TCP 프로토콜을 사용하는 경우 ["네트워크를 통해 전송되는 모든 데이터를 암호화합니다"](#) NVMe/TCP 호스트와 ASA R2 시스템 간에 데이터를 암호화할 수 있습니다.

ASA R2 스토리지 시스템에서 랜섬웨어 공격을 방어합니다


랜섬웨어 공격에 대한 보호를 강화하기 위해 스냅샷을 원격 클러스터에 복제하고 대상 스냅샷을

잠가 변조 방지를 보장합니다. 잠긴 스냅샷은 실수로 또는 악의적으로 삭제할 수 없습니다. 스토리지 유닛이 랜섬웨어 공격에 의해 손상된 경우 잠긴 스냅샷을 사용하여 데이터를 복구할 수 있습니다.

SnapLock Compliance 클록을 초기화한다

무단 변경 방지 스냅샷을 생성하려면 로컬 및 대상 클러스터에서 SnapLock Compliance 클록을 초기화해야 합니다.

단계

1. 클러스터 > 개요 * 를 선택합니다.
2. 노드 * 섹션에서 * SnapLock Compliance 시계 초기화 * 를 선택합니다.
3. Initialize * 를 선택합니다.
4. 규정 준수 클록이 초기화되었는지 확인
 - a. 클러스터 > 개요 * 를 선택합니다.
 - b. Nodes * 섹션에서  선택한 다음 * SnapLock Compliance Clock * 을 선택합니다.

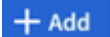

다음 단계

로컬 및 대상 클러스터에서 SnapLock Compliance 클록을 초기화한 후에는 을(를) 시작할 "잠긴 스냅샷이 있는 복제 관계를 생성합니다" 수 있습니다.

ASA R2 스토리지 시스템에서 NVMe 연결을 보호합니다

NVMe 프로토콜을 사용하는 경우 대역 내 인증을 구성하여 데이터 보안을 강화할 수 있습니다. 대역 내 인증을 통해 NVMe 호스트와 ASA R2 시스템 간에 안전한 양방향 및 단방향 인증을 수행할 수 있습니다. 모든 NVMe 호스트에서 대역 내 인증을 사용할 수 있습니다. NVMe/TCP 프로토콜을 사용하는 경우 TLS(전송 계층 보안)를 구성하여 NVMe/TCP 호스트와 ASA R2 시스템 간에 네트워크를 통해 전송되는 모든 데이터를 암호화함으로써 데이터 보안을 더욱 강화할 수 있습니다.

단계

1. Hosts * 를 선택한 다음 * NVMe * 를 선택합니다.
2. 을  선택합니다.
3. 호스트 이름을 입력한 다음 호스트 운영 체제를 선택합니다.
4. 호스트 설명을 입력한 다음 호스트에 접속할 스토리지 VM을 선택합니다.
5.  호스트 이름 옆의 을 선택합니다.
6. 대역내 인증 * 을 선택합니다.
7. NVMe/TCP 프로토콜을 사용하는 경우 * TLS(전송 계층 보안) 필요 * 를 선택합니다.
8. 추가 * 를 선택합니다.

결과

대역 내 인증 및/또는 TLS를 통해 데이터 보안이 강화됩니다.

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.