



## 보안 데이터 AFX

NetApp  
February 10, 2026

# 목차

- 보안 데이터 ..... 1
  - AFX 스토리지 시스템 데이터 보안을 준비하세요 ..... 1
    - 용어 및 옵션 ..... 1
    - 관련 정보 ..... 1
  - AFX 스토리지 시스템에서 저장 중인 데이터 암호화 ..... 1
  - AFX 스토리지 시스템의 보안 IP 연결 ..... 2
    - AFX 시스템에서 IPsec 구성 ..... 2
    - 하드웨어 오프로드 기능 ..... 3
    - 관련 정보 ..... 3

# 보안 데이터

## AFX 스토리지 시스템 데이터 보안을 준비하세요

AFX 데이터를 관리하기 전에 주요 개념과 기능에 대해 숙지해야 합니다.

### 용어 및 옵션

AFX 데이터 보안과 관련하여 알아야 할 용어가 몇 가지 있습니다.

#### 랜섬웨어

랜섬웨어는 사용자가 접근할 수 없도록 파일을 암호화하는 악성 소프트웨어입니다. 일반적으로 데이터를 해독하려면 어떤 유형의 지불이 요구됩니다. ONTAP ARP(자율 랜섬웨어 보호)와 같은 기능을 통해 랜섬웨어로부터 보호하는 솔루션을 제공합니다.

#### 암호화

암호화는 적절한 승인 없이는 쉽게 읽을 수 없는 안전한 형식으로 데이터를 변환하는 프로세스입니다. ONTAP 저장된 데이터를 보호하기 위해 소프트웨어 기반 및 하드웨어 기반 암호화 기술을 모두 제공합니다. 이렇게 하면 저장 매체가 다른 용도로 사용되거나, 반환되거나, 분실되거나, 도난당하더라도 해당 정보를 읽을 수 없게 됩니다. 이러한 암호화 솔루션은 외부 키 관리 서버나 ONTAP에서 제공하는 Onboard Key Manager를 사용하여 관리할 수 있습니다. 참조하다 ["AFX 스토리지 시스템에서 저장 중인 데이터 암호화"](#) 자세한 내용은.

#### 디지털 인증서 및 PKI

디지털 인증서는 공개 키의 소유권을 증명하는 데 사용되는 전자 문서입니다. 공개 키와 이와 관련된 개인 키는 다양한 방법으로 사용될 수 있는데, 일반적으로 TLS 및 IPsec와 같은 보다 큰 보안 프레임워크의 일부로서 신원을 확립하는 데 사용됩니다. 이러한 키와 지원 프로토콜 및 포맷 표준은 공개 키 인프라(PKI)의 기반을 형성합니다. 참조하다 ["AFX 스토리지 시스템에서 인증서 관리"](#) 자세한 내용은.

#### 인터넷 프로토콜 보안

IPsec은 IP 수준에서 네트워크 엔드포인트 간 트래픽 흐름에 대한 전송 중 데이터 암호화, 무결성 및 인증을 제공하는 인터넷 표준입니다. NFS 및 SMB와 같은 상위 레벨 프로토콜을 포함하여 ONTAP 과 클라이언트 간의 모든 IP 트래픽을 보호합니다. IPsec은 데이터에 대한 악의적인 재생 및 중간자 공격으로부터 보호해줍니다. 참조하다 ["AFX 스토리지 시스템의 보안 IP 연결"](#) 자세한 내용은.

### 관련 정보

- ["추가 AFX SVM 관리"](#)
- ["AFX 시스템 관리를 준비하세요"](#)

## AFX 스토리지 시스템에서 저장 중인 데이터 암호화

하드웨어 및 소프트웨어 수준에서 데이터를 암호화하여 이중 계층 보호를 구현할 수 있습니다. 저장 중인 데이터를 암호화하면 저장 매체가 다른 용도로 사용되거나, 반환되거나, 분실되거나, 도난당하더라도 해당 데이터를 읽을 수 없습니다.

NetApp Storage Encryption(NSE)은 SED(자체 암호화 드라이브)를 사용하여 하드웨어 암호화를 지원합니다. SED는 데이터가 기록되는 대로 암호화합니다. 각 SED에는 고유한 암호화 키가 포함되어 있습니다. SED에 저장된 암호화된

데이터는 SED의 암호화 키 없이는 읽을 수 없습니다. SED에서 읽으려는 노드는 SED의 암호화 키에 액세스하기 위해 인증을 받아야 합니다. 노드는 키 관리자로부터 인증 키를 얻은 다음 SED에 인증 키를 제시하여 인증됩니다. 인증 키가 유효하면 SED는 노드에 암호화 키를 제공하여 해당 노드가 포함하는 데이터에 액세스합니다.

#### 시작하기 전에

AFX 온보드 키 관리자나 외부 키 관리자를 사용하여 노드에 인증 키를 제공합니다. NSE 외에도 소프트웨어 암호화를 활성화하여 데이터의 보안을 한 단계 더 강화할 수 있습니다.

#### 단계

1. 시스템 관리자에서 \*클러스터\*를 선택한 다음 \*설정\*을 선택합니다.
2. 보안 섹션의 \*암호화\*에서 \*구성\*을 선택합니다.
3. 키 관리자를 구성합니다.

옵션	단계
온보드 키 관리자 구성	<ol style="list-style-type: none"> <li>a. *온보드 키 관리자*를 선택하여 키 서버를 추가하세요.</li> <li>b. 암호를 입력하세요.</li> </ol>
외부 키 관리자 구성	<ol style="list-style-type: none"> <li>a. 키 서버를 추가하려면 *외부 키 관리자*를 선택하세요.</li> <li>b. 선택하다 <b>+ Add</b> 주요 서버를 추가합니다.</li> <li>c. KMIP 서버 CA 인증서를 추가합니다.</li> <li>d. KMIP 클라이언트 인증서를 추가합니다.</li> </ol>

4. 소프트웨어 암호화를 활성화하려면 \*이중 계층 암호화\*를 선택하세요.
5. \*저장\*을 선택하세요.

#### 관련 정보

- ["암호화"](#)

## AFX 스토리지 시스템의 보안 IP 연결

IP 보안(IPsec)은 IP 수준에서 네트워크 엔드포인트 간 트래픽 흐름에 대한 데이터 암호화, 무결성 및 인증을 제공하는 인터넷 프로토콜 표준입니다. IPsec을 사용하면 AFX 클러스터와 클라이언트 간의 프런트엔드 네트워크 보안을 강화할 수 있습니다.

### AFX 시스템에서 IPsec 구성

AFX 스토리지 시스템의 IPsec 구성 절차는 하드웨어 오프로드 기능과 함께 사용되는 지원되는 네트워크 인터페이스 컨트롤러(NIC) 카드를 제외하고는 AFF 및 FAS 시스템과 동일합니다. 참조하다 ["ONTAP 네트워크에 대한 IP 보안 구성을 준비합니다."](#) 자세한 내용은.

## 하드웨어 오프로드 기능

암호화 및 무결성 검사와 같은 여러 IPsec 암호화 작업은 AFX 시스템에서 지원되는 NIC 카드로 오프로드할 수 있습니다. 이를 통해 IPsec으로 보호되는 네트워크 트래픽의 성능과 처리량이 크게 향상될 수 있습니다.



ONTAP 9.18.1부터 IPsec 하드웨어 오프로드 기능이 확장되어 IPv6 트래픽을 지원합니다.

다음 NIC 카드는 ONTAP 9.17.1부터 AFX 스토리지 시스템의 IPsec 하드웨어 오프로드 기능에 지원됩니다.

- X50130B(2p, 40G/100G 이더넷 컨트롤러)
- X50131B(2p, 40G/100G/200G/400G 이더넷 컨트롤러)

를 참조하세요 ["NetApp Hardware Universe"](#) AFX 시스템에서 실행되는 ONTAP 릴리스에 지원되는 카드에 대한 자세한 내용은 다음을 참조하세요.

## 관련 정보

- ["ONTAP 네트워크에 대한 IP 보안 구성을 준비합니다."](#)
- ["NetApp Hardware Universe"](#)

## 저작권 정보

Copyright © 2026 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.