



Sichere Daten

AFX

NetApp
January 21, 2026

Inhalt

- Sichere Daten. 1
 - Bereiten Sie sich auf die Sicherung Ihrer AFX-Speichersystemdaten vor 1
 - Terminologie und Optionen 1
 - Ähnliche Informationen 1
 - Verschlüsseln Sie ruhende Daten auf einem AFX-Speichersystem 2
- Sichere IP-Verbindungen auf Ihren AFX-Speichersystemen 3
 - Konfigurieren von IPsec auf einem AFX-System 3
 - Hardware-Entlastungsfunktion 3
 - Ähnliche Informationen 3

Sichere Daten

Bereiten Sie sich auf die Sicherung Ihrer AFX-Speichersystemdaten vor

Bevor Sie Ihre AFX-Daten verwalten, sollten Sie mit den wichtigsten Konzepten und Funktionen vertraut sein.

Terminologie und Optionen

Es gibt mehrere Begriffe im Zusammenhang mit der AFX-Datensicherheit, mit denen Sie vertraut sein sollten.

Ransomware

Ransomware ist Schadsoftware, die Dateien verschlüsselt und sie für den Benutzer unzugänglich macht. In der Regel wird eine Art Zahlung verlangt, um die Daten zu entschlüsseln. ONTAP bietet Lösungen zum Schutz vor Ransomware durch Funktionen wie den autonomen Ransomware-Schutz (ARP).

Verschlüsselung

Bei der Verschlüsselung handelt es sich um den Prozess der Konvertierung von Daten in ein sicheres Format, das ohne entsprechende Autorisierung nicht einfach gelesen werden kann. ONTAP bietet sowohl software- als auch hardwarebasierte Verschlüsselungstechnologien zum Schutz ruhender Daten. Dadurch wird sichergestellt, dass es nicht gelesen werden kann, wenn das Speichermedium zweckentfremdet, zurückgegeben, verlegt oder gestohlen wird. Diese Verschlüsselungslösungen können entweder mit einem externen Schlüsselverwaltungsserver oder dem von ONTAP bereitgestellten Onboard Key Manager verwaltet werden. Siehe ["Verschlüsseln Sie ruhende Daten auf einem AFX-Speichersystem"](#) für weitere Informationen.

Digitale Zertifikate und PKI

Ein digitales Zertifikat ist ein elektronisches Dokument, mit dem der Besitz eines öffentlichen Schlüssels nachgewiesen wird. Der öffentliche Schlüssel und der zugehörige private Schlüssel können auf verschiedene Weise verwendet werden, unter anderem zur Feststellung der Identität, typischerweise als Teil eines größeren Sicherheitsrahmens wie TLS und IPsec. Diese Schlüssel sowie die unterstützenden Protokolle und Formatierungsstandards bilden die Grundlage für die Public Key Infrastructure (PKI). Siehe ["Verwalten von Zertifikaten auf einem AFX-Speichersystem"](#) für weitere Informationen.

Internetprotokollsicherheit

IPsec ist ein Internetstandard, der die Verschlüsselung, Integrität und Authentifizierung von Daten während der Übertragung zwischen Netzwerkendpunkten auf IP-Ebene gewährleistet. Es sichert den gesamten IP-Verkehr zwischen ONTAP und Clients, einschließlich höherer Protokolle wie NFS und SMB. IPsec bietet Schutz vor böswilligen Replay- und Man-in-the-Middle-Angriffen auf Ihre Daten. Siehe ["Sichere IP-Verbindungen auf Ihren AFX-Speichersystemen"](#) für weitere Informationen.

Ähnliche Informationen

- ["Zusätzliche AFX SVM-Verwaltung"](#)
- ["Bereiten Sie sich auf die Verwaltung Ihres AFX-Systems vor"](#)

Verschlüsseln Sie ruhende Daten auf einem AFX-Speichersystem

Sie können Ihre Daten auf Hardware- und Softwareebene verschlüsseln, um einen zweischichtigen Schutz zu gewährleisten. Wenn Sie ruhende Daten verschlüsseln, können diese nicht gelesen werden, wenn das Speichermedium zweckentfremdet, zurückgegeben, verlegt oder gestohlen wird.

NetApp Storage Encryption (NSE) unterstützt die Hardwareverschlüsselung mithilfe von selbstverschlüsselnden Laufwerken (SEDs). SEDs verschlüsseln Daten beim Schreiben. Jedes SED enthält einen einzigartigen Verschlüsselungsschlüssel. Auf dem SED gespeicherte verschlüsselte Daten können ohne den Verschlüsselungsschlüssel des SED nicht gelesen werden. Knoten, die versuchen, von einem SED zu lesen, müssen authentifiziert werden, um auf den Verschlüsselungsschlüssel des SED zugreifen zu können. Knoten werden authentifiziert, indem sie einen Authentifizierungsschlüssel von einem Schlüsselmanager erhalten und diesen dann dem SED vorlegen. Wenn der Authentifizierungsschlüssel gültig ist, gibt das SED dem Knoten seinen Verschlüsselungsschlüssel, um auf die darin enthaltenen Daten zuzugreifen.

Bevor Sie beginnen

Verwenden Sie den integrierten AFX-Schlüsselmanager oder einen externen Schlüsselmanager, um Ihren Knoten Authentifizierungsschlüssel bereitzustellen. Zusätzlich zu NSE können Sie auch die Softwareverschlüsselung aktivieren, um Ihren Daten eine weitere Sicherheitsebene hinzuzufügen.

Schritte

1. Wählen Sie im Systemmanager **Cluster** und dann **Einstellungen**.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Verschlüsselung** die Option **Konfigurieren** aus.
3. Konfigurieren Sie den Schlüsselmanager.

Option	Schritte
Konfigurieren des Onboard-Schlüsselmanagers	<ol style="list-style-type: none">a. Wählen Sie Onboard Key Manager, um die Schlüsselservers hinzuzufügen.b. Geben Sie eine Passphrase ein.
Konfigurieren eines externen Schlüsselmanagers	<ol style="list-style-type: none">a. Wählen Sie Externer Schlüsselmanager aus, um die Schlüsselservers hinzuzufügen.b. Wählen + Add um die Schlüsselservers hinzuzufügen.c. Fügen Sie die CA-Zertifikate des KMIP-Servers hinzu.d. Fügen Sie die KMIP-Client-Zertifikate hinzu.

4. Wählen Sie **Dual-Layer-Verschlüsselung**, um die Softwareverschlüsselung zu aktivieren.
5. Wählen Sie **Speichern**.

Ähnliche Informationen

- ["Verschlüsselung"](#)

Sichere IP-Verbindungen auf Ihren AFX-Speichersystemen

IP Security (IPsec) ist ein Internetprotokollstandard, der Datenverschlüsselung, -integrität und -authentifizierung für den Datenverkehr zwischen Netzwerkendpunkten auf IP-Ebene bietet. Mit IPsec lässt sich die Sicherheit des Front-End-Netzwerks zwischen einem AFX-Cluster und den Clients verbessern.

Konfigurieren von IPsec auf einem AFX-System

Die IPsec-Konfigurationsverfahren für AFX-Speichersysteme sind die gleichen wie für AFF und FAS -Systeme, mit Ausnahme der unterstützten Netzwerkschnittstellenkarten (NIC), die mit der Hardware-Offload-Funktion verwendet werden. Siehe ["Bereiten Sie die Konfiguration der IP-Sicherheit für das ONTAP Netzwerk vor."](#) für weitere Informationen.

Hardware-Entlastungsfunktion

Mehrere IPsec-Kryptografieoperationen, wie Verschlüsselung und Integritätsprüfungen, können auf eine unterstützte Netzwerkkarte Ihres AFX-Systems ausgelagert werden. Dies kann die Leistung und den Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessern.



Ab ONTAP 9.18.1 wurde die IPsec-Hardware-Offload-Funktion erweitert, um IPv6-Datenverkehr zu unterstützen.

Die folgenden Netzwerkkarten werden für die IPsec-Hardware-Offload-Funktion auf AFX-Speichersystemen ab ONTAP 9.17.1 unterstützt:

- X50130B (2p, 40G/100G Ethernet-Controller)
- X50131B (2p, 40G/100G/200G/400G Ethernet-Controller)

Siehe die ["NetApp Hardware Universe"](#) Weitere Informationen zu den unterstützten Grafikkarten für die ONTAP Version auf Ihrem AFX-System finden Sie hier.

Ähnliche Informationen

- ["Bereiten Sie die Konfiguration der IP-Sicherheit für das ONTAP Netzwerk vor."](#)
- ["NetApp Hardware Universe"](#)

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.