



Datos seguros

AFX

NetApp
February 10, 2026

Tabla de contenidos

Datos seguros	1
Prepárese para proteger los datos de su sistema de almacenamiento AFX	1
Terminología y opciones	1
Información relacionada	1
Cifrar datos en reposo en un sistema de almacenamiento AFX	2
Conexiones IP seguras en sus sistemas de almacenamiento AFX	3
Configuración de IPsec en un sistema AFX	3
Función de descarga de hardware	3
Información relacionada	3

Datos seguros

Prepárese para proteger los datos de su sistema de almacenamiento AFX

Antes de administrar sus datos AFX, debe familiarizarse con los principales conceptos y capacidades.

Terminología y opciones

Hay varios términos relacionados con la seguridad de datos de AFX con los que debe estar familiarizado.

Ransomware

El ransomware es un software malicioso que cifra los archivos y los hace inaccesibles para el usuario. Generalmente se exige algún tipo de pago para descifrar los datos. ONTAP ofrece soluciones de protección contra ransomware a través de funciones como Autonomous Ransomware Protection (ARP).

Cifrado

El cifrado es el proceso de convertir datos a un formato seguro que no se puede leer fácilmente sin la autorización adecuada. ONTAP ofrece tecnologías de cifrado basadas en software y hardware para proteger los datos en reposo. Esto garantiza que no se pueda leer si el medio de almacenamiento se reutiliza, se devuelve, se extravía o se roba. Estas soluciones de cifrado se pueden gestionar mediante un servidor de administración de claves externo o mediante el administrador de claves integrado proporcionado por ONTAP. Referirse a "[Cifrar datos en reposo en un sistema de almacenamiento AFX](#)" Para más información.

Certificados digitales y PKI

Un certificado digital es un documento electrónico que se utiliza para demostrar la propiedad de una clave pública. La clave pública y la clave privada asociada se pueden utilizar de diversas maneras, incluso para establecer la identidad, generalmente como parte de un marco de seguridad más amplio, como TLS e IPsec. Estas claves, así como los protocolos de soporte y los estándares de formato, forman la base de la infraestructura de clave pública (PKI). Referirse a "[Administrar certificados en un sistema de almacenamiento AFX](#)" Para más información.

Seguridad del Protocolo de Internet

IPsec es un estándar de Internet que proporciona encriptación, integridad y autenticación de datos en tránsito para el tráfico que fluye entre puntos finales de la red a nivel de IP. Asegura todo el tráfico IP entre ONTAP y los clientes, incluidos los protocolos de nivel superior como NFS y SMB. IPsec brinda protección contra repeticiones maliciosas y ataques del tipo "man-in-the-middle" en sus datos. Referirse a "[Conexiones IP seguras en sus sistemas de almacenamiento AFX](#)" Para más información.

Información relacionada

- "[Administración adicional de AFX SVM](#)"
- "[Prepárese para administrar su sistema AFX](#)"

Cifrar datos en reposo en un sistema de almacenamiento AFX

Puede cifrar sus datos a nivel de hardware y software para obtener protección de doble capa. Cuando se cifran datos en reposo, no se pueden leer si el medio de almacenamiento se reutiliza, se devuelve, se extravía o se roba.

NetApp Storage Encryption (NSE) admite el cifrado de hardware mediante unidades de autocifrado (SED). Los SED cifran los datos a medida que se escriben. Cada SED contiene una clave de cifrado única. Los datos cifrados almacenados en la SED no se pueden leer sin la clave de cifrado de la SED. Los nodos que intentan leer desde un SED deben estar autenticados para acceder a la clave de cifrado del SED. Los nodos se autentican obteniendo una clave de autenticación de un administrador de claves y luego presentando dicha clave al SED. Si la clave de autenticación es válida, el SED le dará al nodo su clave de cifrado para acceder a los datos que contiene.

Antes de empezar

Utilice el administrador de claves integrado de AFX o un administrador de claves externo para entregar claves de autenticación a sus nodos. Además de NSE, también puedes habilitar el cifrado de software para agregar otra capa de seguridad a tus datos.

Pasos

1. En el Administrador del sistema, seleccione **Clúster** y luego **Configuración**.
2. En la sección **Seguridad**, en **Cifrado**, seleccione **Configurar**.
3. Configurar el administrador de claves.

Opción	Pasos
Configurar el administrador de claves integrado	<ol style="list-style-type: none">a. Seleccione Administrador de claves integrado para agregar los servidores de claves.b. Introduzca una frase de contraseña.
Configurar un administrador de claves externo	<ol style="list-style-type: none">a. Seleccione Administrador de claves externo para agregar los servidores de claves.b. Seleccionar  Add para agregar los servidores clave.c. Agregue los certificados CA del servidor KMIP.d. Agregue los certificados de cliente KMIP.

4. Seleccione **Cifrado de doble capa** para habilitar el cifrado de software.
5. Seleccione **Guardar**.

Información relacionada

- "Cifrado"

Conexiones IP seguras en sus sistemas de almacenamiento AFX

Seguridad IP (IPsec) es un estándar de protocolo de Internet que proporciona encriptación, integridad y autenticación de datos para el tráfico que fluye entre los puntos finales de la red a nivel de IP. Puede utilizar IPsec para mejorar la seguridad de la red front-end entre un clúster AFX y los clientes.

Configuración de IPsec en un sistema AFX

Los procedimientos de configuración de IPsec para los sistemas de almacenamiento AFX son los mismos que para los sistemas AFF y FAS , con la excepción de las tarjetas controladoras de interfaz de red (NIC) compatibles que se utilizan con la función de descarga de hardware. Referirse a "["Prepárese para configurar la seguridad IP para la red ONTAP."](#)" Para más información.

Función de descarga de hardware

Varias de las operaciones criptográficas de IPsec, como el cifrado y las comprobaciones de integridad, se pueden descargar a una tarjeta NIC compatible en su sistema AFX. Esto puede mejorar significativamente el rendimiento y el rendimiento del tráfico de red protegido por IPsec.



A partir de ONTAP 9.18.1, la función de descarga de hardware de IPsec se amplía para admitir el tráfico IPv6.

Las siguientes tarjetas NIC son compatibles con la función de descarga de hardware IPsec en sistemas de almacenamiento AFX a partir de ONTAP 9.17.1:

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

Consulte la "["NetApp Hardware Universe"](#)" para obtener más información sobre las tarjetas compatibles con la versión ONTAP que se ejecuta en su sistema AFX.

Información relacionada

- ["Prepárese para configurar la seguridad IP para la red ONTAP."](#)
- ["NetApp Hardware Universe"](#)

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.