



# **Proteja su red**

## ONTAP 9

NetApp  
February 12, 2026

This PDF was generated from [https://docs.netapp.com/es-es/ontap/networking/configure\\_network\\_security\\_using\\_federal\\_information\\_processing\\_standards\\_fips.html](https://docs.netapp.com/es-es/ontap/networking/configure_network_security_using_federal_information_processing_standards_fips.html) on February 12, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Tabla de contenidos

Proteja su red . . . . .	1
Configure la seguridad de red ONTAP mediante FIPS para todas las conexiones SSL . . . . .	1
Active FIPS . . . . .	2
Desactive FIPS . . . . .	2
Ver el estado de cumplimiento de normativas FIPS . . . . .	3
Configurar el cifrado en tiempo real de IPsec . . . . .	4
Prepárese para usar la seguridad IP en la red ONTAP . . . . .	4
Configure la seguridad IP para la red ONTAP . . . . .	8
Configurar el cifrado de red del clúster backend de ONTAP . . . . .	13
Habilitar o deshabilitar el cifrado para la comunicación de red del clúster . . . . .	14
Gestionar certificados de cifrado de red de clúster . . . . .	14
Configure políticas del firewall para las LIF en la red de ONTAP . . . . .	15
Políticas de firewall y LIF . . . . .	16
Configuración del servicio portmap . . . . .	17
Cree una política de firewall y asígnela a una LIF . . . . .	18
Comandos de ONTAP para gestionar el servicio y las políticas del firewall . . . . .	21

# Proteja su red

## Configure la seguridad de red ONTAP mediante FIPS para todas las conexiones SSL

ONTAP cumple con los Estándares Federales de Procesamiento de Información (FIPS) 140-2 para todas las conexiones SSL. Puede activar y desactivar el modo SSL FIPS, configurar los protocolos SSL globalmente y desactivar cualquier cifrado débil dentro de ONTAP.

De forma predeterminada, SSL en ONTAP se establece con la conformidad FIPS desactivada y con los siguientes protocolos TLS activados:

- TLSv1.3 (a partir de ONTAP 9.11.1)
- TLSv1.2

Las versiones anteriores de ONTAP tenían activados de forma predeterminada los siguientes protocolos TLS:

- TLSv1.1 (deshabilitado de forma predeterminada a partir de ONTAP 9.12.1)
- TLSv1 (deshabilitado de forma predeterminada a partir de ONTAP 9.8)

Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.

Si desea que las cuentas de administrador accedan a SVM con una clave pública SSH, debe asegurarse de que el algoritmo de clave de host sea compatible antes de habilitar el modo SSL FIPS.

**Nota:** la compatibilidad con el algoritmo de clave de host ha cambiado en ONTAP 9.11.1 y versiones posteriores.

Versión de ONTAP	Tipos de clave admitidos	Tipos de claves no compatibles
9.11.1 y posterior	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 y anteriores	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Las cuentas de clave pública SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave compatible antes de habilitar FIPS o la autenticación del administrador fallará.

Para obtener más información, consulte "[Habilite cuentas de clave pública de SSH](#)".

ONTAP 9.18.1 introduce soporte para los algoritmos criptográficos post-cuánticos ML-KEM, ML-DSA y SLH-DSA para SSL, proporcionando una capa adicional de seguridad contra posibles ataques futuros de computadoras cuánticas. Estos algoritmos solo están disponibles cuando [FIPS está desactivado](#). Los algoritmos criptográficos post-cuánticos se negocian cuando FIPS está deshabilitado y el par los admite.

## Active FIPS

Se recomienda que todos los usuarios seguros ajusten su configuración de seguridad inmediatamente después de instalar o actualizar el sistema. Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.



Cuando FIPS está habilitada, no se puede instalar ni crear un certificado con una longitud de clave RSA de 4096.

### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Habilitar FIPS:

```
security config modify * -is-fips-enabled true
```

3. Cuando se le solicite continuar, introduzca y

4. A partir de ONTAP 9.9.1, no es necesario reiniciar. Si está ejecutando ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster uno por uno.

### Ejemplo

Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
security config modify -is-fips-enabled true
```

```
Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

Obtenga más información sobre `security config modify` la configuración del modo FIPS SSL en el ["Referencia de comandos del ONTAP"](#).

## Desactive FIPS

A partir de ONTAP 9.18.1, SSL en ONTAP admite los algoritmos criptográficos de computación post-cuántica ML-KEM, ML-DSA y SLH-DSA. Estos algoritmos solo están disponibles cuando FIPS está deshabilitado y el par los admite.

## Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Para deshabilitar FIPS, escriba:

```
security config modify -is-fips-enabled false
```

3. Cuando se le solicite continuar, introduzca y.

4. A partir de ONTAP 9.9.1, no es necesario reiniciar. Si está ejecutando ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster.

Si necesita utilizar el protocolo SSLv3, debe deshabilitar FIPS siguiendo el procedimiento anterior. SSLv3 solo se puede habilitar cuando FIPS está deshabilitado.

Puedes habilitar SSLv3 con el siguiente comando. Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
security config modify -supported-protocols SSLv3
```

```
Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
```

```
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

## Ver el estado de cumplimiento de normativas FIPS

Puede ver si el clúster completo está ejecutando las opciones de configuración de seguridad actuales.

## Pasos

1. Si está ejecutando ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster uno por uno.
2. Ver el estado de cumplimiento actual:

```
security config show
```

```

cluster1::> security config show
Cluster      Supported
FIPS Mode   Protocols Supported Cipher Suites
-----
-----
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
TLSv1.2    TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
TLS_RSA_WITH_AES_256_CCM_8,
...

```

Obtenga más información sobre `security config show` en el ["Referencia de comandos del ONTAP"](#).

#### Información relacionada

- ["FIPS 203: Estándar de mecanismo de encapsulación de claves basado en retícula modular \(ML-KEM\)"](#)
- ["FIPS 204: Estándar de firma digital basado en retícula modular \(ML-DSA\)"](#)
- ["FIPS 205: Estándar de firma digital sin estado basada en hash \(SLH-DSA\)"](#)

## Configurar el cifrado en tiempo real de IPsec

### Prepárese para usar la seguridad IP en la red ONTAP

A partir de ONTAP 9.8, tiene la opción de usar la seguridad IP (IPsec) para proteger el tráfico de red. IPsec es una de las diversas opciones de cifrado de datos en movimiento o en tránsito disponibles con ONTAP. Debe prepararse para configurar IPsec antes de utilizarlo en un entorno de producción.

### Implementación de seguridad IP en ONTAP

IPSec es un estándar de Internet mantenido por el IETF. Proporciona cifrado e integridad de datos, así como autenticación para el tráfico que fluye entre los extremos de red a nivel de IP.

Con ONTAP, IPsec protege todo el tráfico IP entre ONTAP y los distintos clientes, incluidos los protocolos NFS, SMB e iSCSI. Además de la privacidad y la integridad de los datos, el tráfico de red está protegido contra varios ataques, como los ataques de repetición y de intermediario. ONTAP utiliza la implantación del modo de transporte IPsec. Aprovecha la versión 2 del protocolo de intercambio de claves de Internet (IKE) para negociar el material clave entre ONTAP y los clientes utilizando IPv4 o IPv6.

Cuando la funcionalidad IPsec está habilitada en un cluster, la red necesita una o más entradas en la base de datos de políticas de seguridad de ONTAP (SPD) que coincidan con las distintas características del tráfico. Estas entradas se asignan a los detalles de protección específicos necesarios para procesar y enviar los datos (por ejemplo, conjunto de cifrado y método de autenticación). También es necesario introducir el SPD correspondiente en cada cliente.

Para ciertos tipos de tráfico, es preferible otra opción de cifrado de datos en movimiento. Por ejemplo, para el cifrado del tráfico de interconexión de clústeres y NetApp SnapMirror, por lo general se recomienda el protocolo de seguridad de la capa de transporte (TLS) en lugar de IPsec. Esto se debe a que TLS ofrece un mejor rendimiento en la mayoría de las situaciones.

## Información relacionada

- ["Grupo de trabajo de ingeniería de Internet \(IETF\)"](#)
- ["RFC 4301: Arquitectura de seguridad para el protocolo de Internet"](#)

## Evolución de la implementación de ONTAP IPsec

IPsec se introdujo por primera vez en ONTAP 9.8. Su implementación ha seguido evolucionando en versiones posteriores de ONTAP, como se describe a continuación.

### ONTAP 9.18.1

La compatibilidad con la descarga de hardware de IPsec se extiende al tráfico IPv6.

### ONTAP 9.17.1

El soporte para la descarga de hardware IPsec se extiende a ["grupos de agregación de enlaces"](#) . ["Claves precompartidas poscuánticas \(PPK\)"](#) Son compatibles con la autenticación de claves precompartidas (PSK) de IPsec.

### ONTAP 9.16.1

Varias de las operaciones criptográficas, como el cifrado y las comprobaciones de integridad, se pueden descargar en una tarjeta NIC admitida. Consulte [Función de descarga de hardware IPsec](#) para obtener más información.

### ONTAP 9.12.1

La compatibilidad con el protocolo de host de interfaz IPsec está disponible en configuraciones FAS MetroCluster y MetroCluster IP. La compatibilidad de IPsec que se proporciona con los clústeres de MetroCluster se limita al tráfico del host de interfaz de usuario y no es compatible con las LIF de interconexión de clústeres de MetroCluster.

### ONTAP 9.10.1

Se pueden usar certificados para la autenticación IPsec, además de las claves de acceso predefinido (PSK). Antes de ONTAP 9.10.1, solo se admitían las PSK para la autenticación.

### ONTAP 9.9.1

Los algoritmos de cifrado utilizados por IPsec son validados por FIPS 140-2. Estos algoritmos son procesados por el módulo criptográfico de NetApp en ONTAP, que lleva la validación FIPS 140-2.

### ONTAP 9.8

La compatibilidad con IPsec está disponible inicialmente en función de la implementación del modo de transporte.

## Función de descarga de hardware IPsec

Si utiliza ONTAP 9.16.1 o posterior, tiene la opción de descargar ciertas operaciones de uso intensivo computacional, como el cifrado y las comprobaciones de integridad, a una tarjeta de controladora de interfaz de red (NIC) instalada en el nodo de almacenamiento. El rendimiento de las operaciones descargadas en la tarjeta NIC es aproximadamente del 5% o menos. Esto puede mejorar significativamente el rendimiento y el rendimiento del tráfico de red protegido por IPsec.

## Requisitos y recomendaciones

Hay varios requisitos que debe tener en cuenta antes de utilizar la función de descarga de hardware IPsec.

### Tarjetas Ethernet compatibles

Debe instalar y usar únicamente tarjetas Ethernet compatibles. Las siguientes tarjetas Ethernet son compatibles a partir de ONTAP 9.16.1:

- X50131A (controladora Ethernet 2P, 40G/100g/200g/400G)
- X60132A (controlador Ethernet 4p, 10G/25G)

ONTAP 9.17.1 agrega soporte para las siguientes tarjetas Ethernet:

- X50135A (controlador Ethernet 2p, 40G/100G)
- X60135A (controlador Ethernet 2p, 40G/100G)

Las tarjetas X50131A y X50135A son compatibles con las siguientes plataformas:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

Las tarjetas X60132A y X60135A son compatibles con las siguientes plataformas:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Ver el ["NetApp Hardware Universe"](#) para obtener más información sobre las plataformas y tarjetas compatibles.

### Ámbito del clúster

La función de descarga de hardware IPsec se configura globalmente para el cluster. Así que, por ejemplo, el comando `security ipsec config` se aplica a todos los nodos del clúster.

### Configuración consistente

Las tarjetas NIC admitidas deben instalarse en todos los nodos del clúster. Si solo hay disponible una tarjeta NIC compatible en algunos de los nodos, puede ver una degradación del rendimiento significativa tras una conmutación al nodo de respaldo si algunas de las LIF no están alojadas en una NIC compatible con la descarga.

### Desactive la reproducción anti-repetición

Debe desactivar la protección antireproducción IPsec en ONTAP (configuración predeterminada) y los clientes

IPsec. Si no está desactivada, la fragmentación y la multiruta (ruta redundante) no serán compatibles.

Si la configuración de IPsec de ONTAP se ha cambiado de la predeterminada para activar la protección contra la reproducción, utilice este comando para desactivarla:

```
security ipsec config modify -replay-window 0
```

Debe asegurarse de que la protección contra la reproducción IPsec está desactivada en el cliente. Consulte la documentación IPsec de su cliente para desactivar la protección contra la reproducción.

### Limitaciones

Hay varias limitaciones que debe considerar antes de usar la función de descarga de hardware IPsec.

#### IPv6

A partir de ONTAP 9.18.1, se admite IPv6 para la función de descarga de hardware IPsec. Antes de ONTAP 9.18.1, la descarga de hardware de IPsec no admite IPv6.

#### Núm.s de secuencia ampliados

Los números de secuencia extendida IPsec no son compatibles con la función de descarga de hardware. Solo se utilizan los números de secuencia normales de 32 bits.

#### Agregación de enlaces

A partir de ONTAP 9.17.1, puede utilizar la función de descarga de hardware de IPsec con un "[grupo de agregación de enlaces](#)".

Antes de la versión 9.17.1, la función de descarga de hardware de IPsec no admitía la agregación de enlaces. No se puede utilizar con una interfaz o un grupo de agregación de enlaces administrados a través de `network port ifgrp` comandos en la CLI de ONTAP .

#### Compatibilidad con la configuración de la interfaz de línea de comandos de ONTAP

Tres comandos CLI existentes se actualizan en ONTAP 9.16.1 para admitir la función de descarga de hardware IPsec como se describe a continuación. Consulte también "[Configure la seguridad IP en ONTAP](#)" para obtener más información.

Comando ONTAP	Actualizar
<code>security ipsec config show</code>	El parámetro booleano <code>Offload Enabled</code> muestra el estado actual de descarga de NIC.
<code>security ipsec config modify</code>	El parámetro <code>is-offload-enabled</code> se puede utilizar para activar o desactivar la función de descarga de NIC.
<code>security ipsec config show-ipsecsa</code>	Se han agregado cuatro contadores nuevos para mostrar el tráfico entrante y saliente en bytes y paquetes.

#### Soporte de configuración en la API de REST DE ONTAP

Dos extremos de API REST existentes se actualizan en ONTAP 9.16.1 para admitir la función de descarga de hardware IPsec como se describe a continuación.

Extremo de REST	Actualizar
/api/security/ipsec	El parámetro <code>offload_enabled</code> se ha agregado y está disponible con el método de PARCHE.
/api/security/ipsec/security_association	Se han agregado dos nuevos valores de contador para realizar un seguimiento del total de bytes y paquetes procesados por la función de descarga.

Obtenga más información sobre la API de REST DE ONTAP, incluida "[Novedades de la API de REST DE ONTAP](#)", en la documentación de automatización de ONTAP. También debe revisar la documentación de automatización de ONTAP para obtener detalles sobre "[Puntos finales IPsec](#)".

#### Información relacionada

- ["seguridad ipsec"](#)

## Configure la seguridad IP para la red ONTAP

Hay varias tareas que debe realizar para configurar y activar el cifrado en tiempo real de IPsec en el clúster de ONTAP.



Asegúrese de revisar "[Prepárese para usar la seguridad IP](#)" antes de configurar IPsec. Por ejemplo, es posible que deba decidir si desea utilizar la función de descarga de hardware IPsec disponible a partir de ONTAP 9.16.1.

#### Habilite IPsec en el clúster

Puede habilitar IPsec en el clúster para garantizar que los datos se cifran continuamente y estén seguros mientras están en tránsito.

#### Pasos

1. Detectar si IPsec está activada:

```
security ipsec config show
```

Si el resultado incluye IPsec Enabled: false, continúe con el siguiente paso.

2. Habilitar IPsec:

```
security ipsec config modify -is-enabled true
```

Puede activar la función de descarga de hardware IPsec mediante el parámetro booleano `is-offload-enabled`.

3. Vuelva a ejecutar el comando Discovery:

```
security ipsec config show
```

El resultado ahora incluye IPsec Enabled: true.

## Prepárese para la creación de directivas IPsec con autenticación de certificados

Puede omitir este paso si solo utiliza claves precompartidas (PSKs) para la autenticación y no utilizará la autenticación de certificados.

Antes de crear una política IPsec que utilice certificados para la autenticación, debe verificar que se cumplan los siguientes requisitos previos:

- Tanto ONTAP como el cliente deben tener instalado el certificado CA de la otra parte para que los certificados de la entidad final (ya sea ONTAP o el cliente) sean verificables por ambas partes
- Se instala un certificado para el LIF de ONTAP que participa en la política



Las LIF de ONTAP pueden compartir certificados. No es necesario realizar una asignación de uno a uno entre certificados y LIF.

### Pasos

1. Instale todos los certificados de CA utilizados durante la autenticación mutua, incluidas las CA de ONTAP y del lado del cliente, en la gestión de certificados de ONTAP a menos que ya esté instalado (como es el caso de una CA raíz autofirmado de ONTAP).

#### Comando de muestra

```
cluster::> security certificate install -vserver svm_name -type server-ca  
-cert-name my_ca_cert
```

2. Para asegurarse de que la CA instalada se encuentra dentro de la ruta de búsqueda de la CA IPsec durante la autenticación, agregue las CA de gestión de certificados ONTAP al módulo IPsec mediante el `security ipsec ca-certificate add` comando.

#### Comando de muestra

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs  
my_ca_cert
```

3. Cree e instale un certificado para que lo utilice la LIF de ONTAP. La entidad emisora de certificados de este certificado ya debe estar instalada en ONTAP y agregada a IPsec.

#### Comando de muestra

```
cluster::> security certificate install -vserver svm_name -type server -cert  
-name my_nfs_server_cert
```

Para obtener más información acerca de los certificados en ONTAP, consulte los comandos de certificado de seguridad en la documentación de ONTAP 9.

## Definir la base de datos de directivas de seguridad (SPD)

IPSec requiere una entrada SPD antes de permitir que el tráfico fluya por la red. Esto es cierto tanto si está utilizando un PSK como un certificado para la autenticación.

### Pasos

1. Utilice `security ipsec policy create` el comando para:
  - a. Seleccione la dirección IP de ONTAP o la subred de direcciones IP para participar en el transporte IPsec.

b. Seleccione las direcciones IP del cliente que se conectarán a las direcciones IP de ONTAP.



El cliente debe admitir la versión 2 de Exchange de claves de Internet (IKEv2) con una clave compartida previamente (PSK).

c. Opcionalmente, seleccione los parámetros de tráfico detallados, como los protocolos de capa superior (UDP, TCP, ICMP, etc.), los números de puerto local y los números de puerto remoto para proteger el tráfico. Los parámetros correspondientes son `protocols` , `local-ports` y `remote-ports` respectivamente.

Omita este paso para proteger todo el tráfico entre la dirección IP de ONTAP y la dirección IP del cliente. La protección de todo el tráfico es la opción predeterminada.

d. Introduzca PSK o la infraestructura de clave pública (PKI) para el `auth-method` parámetro del método de autenticación deseado.

i. Si introduce un PSK, incluya los parámetros y, a continuación, pulse `<enter>` para que el mensaje introduzca y verifique la clave precompartida.



Los `local-identity` parámetros y `remote-identity` son opcionales si tanto el host como el cliente utilizan strongSwan y no se ha seleccionado ninguna política de comodín para el host o el cliente.

ii. Si introduce un PKI, también debe introducir los `cert-name` `local-identity` `remote-identity` parámetros , ,. Si la identidad del certificado del lado remoto es desconocida o si se esperan varias identidades de cliente, introduzca la identidad especial `ANYTHING` .

e. A partir de ONTAP 9.17.1, ingrese opcionalmente una identidad de clave precompartida (PPK) postcuántica con la `ppk-identity` Parámetro. Las PPK ofrecen una capa adicional de seguridad contra posibles ataques futuros de computadoras cuánticas. Al ingresar una identidad PPK, se le solicitará que ingrese el secreto PPK. Las PPK solo son compatibles con la autenticación PSK.

Obtenga más información sobre `security ipsec policy create` en el "[Referencia de comandos del ONTAP](#)" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

El tráfico IP no puede fluir entre el cliente y el servidor hasta que ONTAP y el cliente hayan configurado las directivas IPsec coincidentes y las credenciales de autenticación (PSK o certificado) estén en su lugar en ambos lados.

## Usar identidades IPsec

Para el método de autenticación de clave precompartida, las identidades locales y remotas son opcionales si tanto el host como el cliente utilizan strongSwan y no se selecciona ninguna política de comodín para el host o el cliente.

Para el método de autenticación PKI/certificado, las identidades locales y remotas son obligatorias. Las identidades especifican qué identidad está certificada dentro del certificado de cada lado y se utilizan en el proceso de verificación. Si la identidad remota es desconocida o si podría ser muchas identidades diferentes, utilice la identidad especial ANYTHING .

### Acerca de esta tarea

En ONTAP, las identidades se especifican modificando la entrada SPD o durante la creación de la política SPD. El SPD puede ser una dirección IP o un nombre de identidad con formato de cadena.

### Pasos

1. Utilice el siguiente comando para modificar una configuración de identidad SPD existente:

```
security ipsec policy modify
```

### Comando de ejemplo

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

## Configuración de varios clientes IPsec

Cuando un pequeño número de clientes necesitan aprovechar IPsec, es suficiente utilizar una sola entrada SPD para cada cliente. Sin embargo, cuando cientos o incluso miles de clientes necesitan aprovechar IPsec, NetApp recomienda el uso de una configuración de varios clientes IPsec.

### Acerca de esta tarea

ONTAP admite la conexión de varios clientes a través de varias redes a una única dirección IP de SVM con IPsec habilitada. Para ello, utilice uno de los siguientes métodos:

- **Configuración de subred**

Para permitir que todos los clientes de una subred determinada (por ejemplo, 192.168.134.0/24) se conecten a una única dirección IP de SVM mediante una única entrada de política SPD, debe especificar el `remote-ip-subnets` formato de subred. Además, debe especificar el `remote-identity` campo con la identidad del lado del cliente correcta.

 Al utilizar una sola entrada de directiva en una configuración de subred, los clientes IPsec de esa subred comparten la identidad IPsec y la clave precompartida (PSK). Sin embargo, esto no es cierto con la autenticación de certificado. Cuando se utilizan certificados, cada cliente puede utilizar su propio certificado único o un certificado compartido para autenticarse. IPsec de ONTAP comprueba la validez del certificado en función de las CA instaladas en el almacén de confianza local. ONTAP también admite la comprobación de la lista de revocación de certificados (CRL).

- **Permitir la configuración de todos los clientes**

Para permitir que cualquier cliente, independientemente de su dirección IP de origen, se conecte a la dirección IP habilitada para IPsec de SVM, utilice el `0.0.0.0/0` comodín al especificar el `remote-ip`

subnets campo.

Además, debe especificar el `remote-identity` campo con la identidad del lado del cliente correcta. Para la autenticación del certificado, puede introducir ANYTHING.

Además, cuando `0.0.0.0/0` se utiliza el comodín, debe configurar un número de puerto local o remoto específico para utilizarlo. Por ejemplo, NFS port 2049.

## Pasos

a. Utilice uno de los siguientes comandos para configurar IPsec para varios clientes.

i. Si está utilizando **configuración de subred** para admitir varios clientes IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets  
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

### Comando de ejemplo

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets  
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity  
ontap_side_identity -remote-identity client_side_identity
```

i. Si está utilizando **Permitir que todos los clientes configuren** para admitir múltiples clientes IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local  
-ports port_number -local-identity local_id -remote-identity remote_id
```

### Comando de ejemplo

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets  
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local  
-identity ontap_side_identity -remote-identity client_side_identity
```

## Mostrar estadísticas de IPsec

A través de la negociación, se puede establecer un canal de seguridad denominado Asociación de seguridad IKE (SA) entre la dirección IP de la SVM de ONTAP y la dirección IP del cliente. Las unidades SAS IPsec se instalan en ambos extremos para que funcionen el cifrado y descifrado de datos. Puede utilizar comandos de estadísticas para comprobar el estado de las unidades SAS IPsec y SAS IKE.



Si está utilizando la función de descarga de hardware IPsec, se muestran varios contadores nuevos con el comando `security ipsec config show-ipsecsa`.

## Comandos de ejemplo

Comando de ejemplo IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Ejemplo de comando SA IPsec y salida:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
      Policy Local          Remote
Vserver    Name  Address      Address      Initiator-SPI      State
-----
-----
vs1        test34        192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Ejemplo de comando SA IPSec y salida:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
      Policy Local          Remote      Inbound  Outbound
Vserver    Name  Address      Address      SPI      SPI
State
-----
-----
vs1        test34        192.168.134.34  192.168.134.44  c4c5b3d6  c2515559
INSTALLED
```

#### Información relacionada

- ["instalación del certificado de seguridad"](#)
- ["seguridad ipsec"](#)

## Configurar el cifrado de red del clúster backend de ONTAP

A partir de ONTAP 9.18.1, puede configurar el cifrado de seguridad de la capa de transporte (TLS) para los datos en tránsito en la red del clúster de backend. Este cifrado protege los datos de los clientes almacenados en ONTAP cuando se transmiten entre nodos ONTAP en la red del clúster de backend.

#### Acerca de esta tarea

- El cifrado de red del clúster de backend está desactivado por defecto.
- Cuando el cifrado de la red del clúster de backend está habilitado, todos los datos del cliente almacenados en ONTAP se cifran cuando se transmiten entre los nodos ONTAP en la red del clúster de backend. Parte del tráfico de red del clúster, como los datos de la ruta de control, no está cifrado.
- Por defecto, el cifrado de la red del clúster de backend utilizará certificados autogenerados para cada nodo del clúster. Puede [Gestionar certificados de cifrado de red de clúster](#) en cada nodo se utilizará un certificado instalado personalizado.

## Antes de empezar

- Debes ser administrador de ONTAP en el admin Nivel de privilegios para realizar las siguientes tareas.
- Todos los nodos del clúster deben estar ejecutando ONTAP 9.18.1 o posterior para habilitar el cifrado de red del clúster de backend.

## Habilitar o deshabilitar el cifrado para la comunicación de red del clúster

### Pasos

1. Consulte el estado actual del cifrado de la red del clúster:

```
security cluster-network show
```

Este comando muestra el estado actual del cifrado de la red del clúster:

```
Cluster-1:::*> security cluster-network show
```

```
Enabled: true
```

```
Mode: tls
```

```
Status: READY
```

2. Habilitar o deshabilitar el cifrado de red del clúster de backend TLS:

```
security cluster-network modify -enabled <true|false>
```

Este comando habilita o deshabilita la comunicación cifrada para los datos de clientes en tránsito en la red del clúster de backend.

## Gestionar certificados de cifrado de red de clúster

1. Consulte la información actual del certificado de cifrado de la red del clúster:

```
security cluster-network certificate show
```

Este comando muestra la información actual del certificado de cifrado de la red del clúster:

security cluster-network certificate show		
Node	Certificate Name	CA
node1	-	Cluster-
1_Root_CA		
node2	-	Cluster-
1_Root_CA		
node3	google_issued_cert1	Google_CA1
node4	google_issued_cert2	Google_CA1

Se muestran el certificado y el nombre de la autoridad certificadora (CA) para cada nodo del clúster.

2. Modificar el certificado de cifrado de red del clúster para un nodo:

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Este comando modifica el certificado de cifrado de red del clúster para un nodo específico. El certificado debe estar instalado y firmado por una CA instalada antes de ejecutar este comando. Para obtener más información sobre la gestión de certificados, consulte "[Gestione certificados de ONTAP con System Manager](#)". Si -name Si no se especifica, se utiliza el certificado predeterminado generado automáticamente.

## Configure políticas del firewall para las LIF en la red de ONTAP

La configuración de un firewall mejora la seguridad del clúster y ayuda a evitar el acceso no autorizado al sistema de almacenamiento. De forma predeterminada, el firewall incorporado está configurado para permitir el acceso remoto a un conjunto específico de servicios IP para LIF de datos, gestión e interconexión de clústeres.

A partir de ONTAP 9,10.1:

- Las políticas de firewall quedan obsoletas y se reemplazan por las políticas de servicio de LIF. Anteriormente, el firewall incorporado se gestionaba mediante directivas de firewall. Esta funcionalidad ahora se logra usando una política de servicio de LIF.
- Todas las políticas de firewall están vacías y no abren ningún puerto en el firewall subyacente. En su lugar, se deben abrir todos los puertos con una política de servicio de LIF.
- No es necesario realizar ninguna acción después de una actualización a la versión 9.10.1 o posterior para pasar de políticas de firewall a políticas de servicio de LIF. El sistema crea automáticamente políticas de servicio de LIF coherentes con las políticas de firewall que se están usando en la versión anterior de ONTAP. Si utiliza scripts u otras herramientas que crean y gestionan políticas de firewall personalizadas, es posible que deba actualizar dichas secuencias de comandos para crear políticas de servicio personalizadas en su lugar.

Para obtener más información, consulte "["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#)".

Las políticas de firewall se pueden utilizar para controlar el acceso a protocolos de servicio de gestión como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS O SNMP. No se pueden establecer políticas de firewall para protocolos de datos como NFS o SMB.

Puede administrar el servicio y las políticas de firewall de las siguientes maneras:

- Activación o desactivación del servicio de firewall
- Mostrar la configuración actual del servicio de firewall
- Creación de una nueva directiva de firewall con el nombre de directiva y los servicios de red especificados
- Aplicar una política de firewall a una interfaz lógica
- Crear una nueva directiva de firewall que sea una copia exacta de una directiva existente

Puede usar esto para realizar una política con características similares dentro de la misma SVM o para copiar la política en una SVM diferente.

- Mostrar información acerca de las directivas de firewall
- Modificar las direcciones IP y las máscaras de red que utiliza una directiva de firewall
- Eliminar una política de firewall que no esté en uso en una LIF

## Políticas de firewall y LIF

Las políticas de firewall de LIF se utilizan para restringir el acceso al clúster en cada LIF. Debe entender cómo afecta la política de firewall predeterminada al acceso del sistema sobre cada tipo de LIF y cómo puede personalizar una política de firewall para aumentar o reducir la seguridad de una LIF.

Cuando se configura una LIF mediante `network interface create` o `network interface modify` el comando, el valor especificado para `-firewall-policy` el parámetro determina los protocolos de servicio y las direcciones IP que permiten acceder a la LIF. Obtenga más información sobre `network interface` en el "["Referencia de comandos del ONTAP"](#)".

En muchos casos puede aceptar el valor predeterminado de la política de firewall. En otros casos, es posible que deba restringir el acceso a determinadas direcciones IP y ciertos protocolos de servicio de gestión. Los protocolos de servicio de gestión disponibles incluyen SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS Y SNMP.

La política de firewall para todas las LIF de clúster se establece de forma predeterminada en "" y no se puede modificar.

En la siguiente tabla se describen las políticas de firewall predeterminadas que se asignan a cada LIF, en función de su rol (ONTAP 9.5 y versiones anteriores) o política de servicio (ONTAP 9.6 y versiones posteriores), al crear la LIF:

Política de firewall	Protocolos de servicio predeterminados	Acceso predeterminado	LIF aplicadas a.
gestión	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Cualquier dirección (0.0.0.0/0)	Gestión de clústeres, gestión de SVM y LIF de gestión de nodos

gestión de nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Cualquier dirección (0.0.0.0/0)	LIF de datos que también admiten el acceso a la gestión de la SVM
interconexión de clústeres	https, ndmp, ndmps	Cualquier dirección (0.0.0.0/0)	Todas las LIF de interconexión de clústeres
los datos	dns, ndmp, ndmps, portmap	Cualquier dirección (0.0.0.0/0)	Todos los LIF de datos

## Configuración del servicio portmap

El servicio portmap asigna los servicios RPC a los puertos en los que escuchan.

El servicio portmap siempre se pudo acceder en ONTAP 9.3 y versiones anteriores, se pasó a configurar en ONTAP 9.4 a través de ONTAP 9.6 y se gestiona automáticamente empezando por ONTAP 9.7.

- En ONTAP 9.3 y anteriores, siempre se pudo acceder al servicio portmap (rpcbind) en el puerto 111 en configuraciones de red que dependían del firewall integrado de ONTAP en lugar de un firewall de terceros.
- Desde ONTAP 9.4 a ONTAP 9.6, puede modificar las políticas de firewall para controlar si el servicio portmap es accesible en determinadas LIF.
- A partir de ONTAP 9.7, se elimina el servicio de firewall de portmap. En su lugar, el puerto portmap se abre automáticamente para todos los LIF que admiten el servicio NFS.

### El servicio Portmap se puede configurar en el firewall de ONTAP 9.4 a ONTAP 9.6.

En el resto de este tema se describe cómo configurar el servicio de firewall de portmap para versiones de ONTAP 9.4 a ONTAP 9.6.

En función de la configuración, es posible que no permita el acceso al servicio en tipos específicos de LIF, que suelen ser de gestión y LIF entre clústeres. En algunas circunstancias, puede que incluso no permita el acceso en las LIF de datos.

### Qué comportamiento se puede esperar

El comportamiento de ONTAP 9.4 a ONTAP 9.6 está diseñado para proporcionar una transición fluida durante la actualización. Si ya se está accediendo al servicio portmap a través de tipos específicos de LIF, continuará siendo accesible mediante estos tipos de LIF. Al igual que en ONTAP 9.3 y versiones anteriores, puede especificar los servicios a los que se puede acceder dentro del firewall en la política de firewall para el tipo de LIF.

Para que el comportamiento surta efecto, todos los nodos del clúster deben ejecutar de ONTAP 9.4 a ONTAP 9.6. Sólo se ve afectado el tráfico entrante.

Las nuevas reglas son las siguientes:

- Tras la actualización al lanzamiento del 9.4 al 9.6, ONTAP agrega el servicio portmap a todas las políticas de firewall existentes, predeterminadas o personalizadas.
- Cuando crea un nuevo clúster o un nuevo espacio IP, ONTAP agrega el servicio portmap solo a la política de datos predeterminada, no a las políticas de gestión o interconexión de clústeres predeterminadas.
- Puede agregar el servicio portmap a las políticas predeterminadas o personalizadas según sea necesario

y eliminar el servicio según sea necesario.

### Cómo agregar o quitar el servicio portmap

Para agregar el servicio portmap a una política de firewall de SVM o clúster (hacer que sea accesible dentro del firewall), introduzca:

```
system services firewall policy create -vserver SVM -policy  
mgmt|intercluster|data|custom -service portmap
```

Para quitar el servicio portmap de una política de firewall de SVM o clúster (hacer que sea inaccesible dentro del firewall), introduzca:

```
system services firewall policy delete -vserver SVM -policy  
mgmt|intercluster|data|custom -service portmap
```

Puede usar el comando `network interface modify` para aplicar la política del firewall a una LIF existente. Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

## Cree una política de firewall y asínjela a una LIF

Las políticas de firewall predeterminadas se asignan a cada LIF al crear la LIF. En muchos casos, la configuración predeterminada del firewall funciona bien y no es necesario modificarla. Si desea cambiar los servicios de red o las direcciones IP que pueden acceder a una LIF, puede crear una política de firewall personalizada y asignarla a la LIF.

### Acerca de esta tarea

- No puede crear una política de firewall con el `policy nombre` `data`, `intercluster`, `cluster`` o `mgmt`.

Estos valores se reservan para las políticas de firewall definidas por el sistema.

- No puede establecer ni modificar una política de firewall para las LIF del clúster.

La política de firewall para las LIF del clúster se establece en `0.0.0.0/0` para todos los tipos de servicios.

- Si necesita quitar un servicio de una política, debe eliminar la política de firewall existente y crear una nueva.
- Si IPv6 está habilitado en el clúster, puede crear políticas de firewall con direcciones IPv6.

Después de activar IPv6, `data`, `intercluster` y `mgmt` las políticas de firewall incluyen `::/0`, el comodín IPv6, en su lista de direcciones aceptadas.

- Cuando se usa System Manager para configurar la funcionalidad de protección de datos en todos los clústeres, se debe asegurarse de que las direcciones IP de LIF entre clústeres estén incluidas en la lista permitida y que el servicio HTTPS esté en las LIF entre clústeres y en los firewalls de propiedad de la empresa.

De forma predeterminada, la `intercluster` política de firewall permite el acceso desde todas las direcciones IP (`0.0.0.0/0`, o `::/0` para IPv6) y habilita los servicios HTTPS, NDMP y NDMPS. Si modifica esta política predeterminada o crea su propia política de firewall para las LIF de interconexión de clústeres, debe añadir cada dirección IP de la LIF entre clústeres a la lista permitida y habilitar el servicio HTTPS.

- A partir de ONTAP 9.6, los servicios de firewall HTTPS y SSH no son compatibles.

En ONTAP 9.6, los `management-https` y `management-ssh` servicios LIF y están disponibles para el acceso de gestión HTTPS y SSH.

## Pasos

1. Cree una política de firewall que estará disponible para las LIF en una SVM específica:

```
system services firewall policy create -vserver vserver_name -policy policy_name -service network_service -allow-list ip_address/mask
```

Puede usar este comando varias veces para agregar más de un servicio de red y una lista de direcciones IP permitidas para cada servicio de la directiva de firewall.

2. Compruebe que la política se ha agregado correctamente mediante `system services firewall policy show` el comando.
3. Aplique la política de firewall a una LIF:

```
network interface modify -vserver vserver_name -lif lif_name -firewall-policy policy_name
```

4. Compruebe que la política se ha agregado correctamente a la LIF mediante `network interface show -fields firewall-policy` el comando.

Obtenga más información sobre `network interface show` en el ["Referencia de comandos del ONTAP"](#).

## Ejemplo de creación de una política de firewall y asignación de ella a una LIF

El siguiente comando crea una política de firewall llamada `data_http` que permite el acceso al protocolo HTTP y HTTPS desde direcciones IP de la subred 10.10, aplica esa política a la LIF llamada `data1` en la SVM `vs1` y, a continuación, muestra todas las políticas de firewall del clúster:

```
system services firewall policy create -vserver vs1 -policy data_http -service http -allow-list 10.10.0.0/16
```

```

system services firewall policy show

Vserver Policy      Service      Allowed
----- -----
cluster-1
    data
        dns      0.0.0.0/0
        ndmp    0.0.0.0/0
        ndmps   0.0.0.0/0
cluster-1
    intercluster
        https   0.0.0.0/0
        ndmp    0.0.0.0/0
        ndmps   0.0.0.0/0
cluster-1
    mgmt
        dns      0.0.0.0/0
        http    0.0.0.0/0
        https   0.0.0.0/0
        ndmp    0.0.0.0/0
        ndmps   0.0.0.0/0
        ntp     0.0.0.0/0
        snmp    0.0.0.0/0
        ssh     0.0.0.0/0
vs1
    data_http
        http    10.10.0.0/16
        https   10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif          firewall-policy
----- -----
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt      mgmt
cluster-1 node1_mgmt1      mgmt
cluster-1 node2_mgmt1      mgmt
vs1      data1          data_http
vs3      data2          data

```

# Comandos de ONTAP para gestionar el servicio y las políticas del firewall

Puede utilizar `system services firewall` los comandos para gestionar el servicio de firewall, los `system services firewall policy` comandos para administrar las políticas de firewall y `network interface modify` el comando para gestionar la configuración del firewall para las LIF.

A partir de ONTAP 9.10.1:

- Las políticas de firewall quedan obsoletas y se reemplazan por las políticas de servicio de LIF. Anteriormente, el firewall incorporado se gestionaba mediante directivas de firewall. Esta funcionalidad ahora se logra usando una política de servicio de LIF.
- Todas las políticas de firewall están vacías y no abren ningún puerto en el firewall subyacente. En su lugar, se deben abrir todos los puertos con una política de servicio de LIF.
- No es necesario realizar ninguna acción después de una actualización a la versión 9.10.1 o posterior para pasar de políticas de firewall a políticas de servicio de LIF. El sistema crea automáticamente políticas de servicio de LIF coherentes con las políticas de firewall que se están usando en la versión anterior de ONTAP. Si utiliza scripts u otras herramientas que crean y gestionan políticas de firewall personalizadas, es posible que deba actualizar dichas secuencias de comandos para crear políticas de servicio personalizadas en su lugar.

Para obtener más información, consulte "["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#)".

Si desea...	Se usa este comando...
Active o desactive el servicio de firewall	<code>system services firewall modify</code>
Muestra la configuración actual del servicio de firewall	<code>system services firewall show</code>
Cree una política de firewall o agregue un servicio a una política de firewall existente	<code>system services firewall policy create</code>
Aplique una política de firewall a una LIF	<code>network interface modify -lif lifname -firewall-policy</code>
Modifique las direcciones IP y las máscaras de red asociadas a una directiva de firewall	<code>system services firewall policy modify</code>
Mostrar información acerca de las políticas de firewall	<code>system services firewall policy show</code>
Cree una nueva directiva de firewall que sea una copia exacta de una directiva existente	<code>system services firewall policy clone</code>
Eliminar una política de firewall que no esté usando una LIF	<code>system services firewall policy delete</code>

### Información relacionada

- "firewall de servicios de sistema"
- "modificación de la interfaz de red"

## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Impreso 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.