



Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere

Enterprise applications

NetApp
May 19, 2024

Tabla de contenidos

- Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere 1
 - Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere 1
 - Verificación de la integridad de las herramientas de ONTAP para los paquetes de instalación de VMware vSphere 1
 - Puertos y protocolos 3
 - Herramientas de ONTAP para puntos de acceso de VMware vSphere (Usuarios)..... 4
 - TLS mutuo (autenticación basada en certificados) 5
 - Certificado HTTPS de herramientas de ONTAP 11
 - Banner de inicio de sesión 12
 - Tiempo de espera de inactividad 12
 - Máximo de solicitudes simultáneas por usuario (Protección de seguridad de red :: Ataque DoS) 12
 - Configuración del Protocolo de hora de red (NTP) 13
 - Políticas de contraseñas 13

Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere

Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere

La guía de refuerzo de la seguridad para herramientas de ONTAP para VMware vSphere proporciona un conjunto completo de instrucciones para configurar los ajustes más seguros.

Estas guías se aplican tanto a las aplicaciones como al sistema operativo «guest» del propio dispositivo.

Verificación de la integridad de las herramientas de ONTAP para los paquetes de instalación de VMware vSphere

Existen dos métodos disponibles para que los clientes verifiquen la integridad de sus paquetes de instalación de herramientas de ONTAP.

1. Verificando las sumas de comprobación
2. Verificando la firma

Las sumas de comprobación se proporcionan en las páginas de descarga de los paquetes de instalación de OTV. Los usuarios deben verificar las sumas de comprobación de los paquetes descargados con la suma de comprobación proporcionada en la página de descarga.

Verificación de la firma del OVA de herramientas de ONTAP

El paquete de instalación de vApp se entrega en forma de tarball. Este tarball contiene certificados intermedios y raíz para el dispositivo virtual junto con un archivo README y un paquete OVA. El archivo README guía a los usuarios sobre cómo verificar la integridad del paquete OVA vApp.

Los clientes también deben cargar el certificado raíz e intermedio proporcionado en la versión 7.0U3E de vCenter y versiones posteriores. Para versiones de vCenter entre 7.0.1 y 7.0.U3E, la funcionalidad de verificación del certificado no es compatible con VMware. Los clientes no deberán cargar ningún certificado para las versiones de vCenter 6.x.

Cargar el certificado raíz de confianza en vCenter

1. Inicie sesión con VMware vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña de administrator@vsphere.local u otro miembro del grupo Administradores de inicio de sesión único de vCenter. Si especificó un dominio diferente durante la instalación, inicie sesión como administrator@mydomain.
3. Desplácese hasta la interfaz de usuario de Certificate Management: a. En el menú Inicio, seleccione Administración. b. En Certificados, haga clic en Gestión de certificados.
4. Si el sistema le solicita, introduzca las credenciales de vCenter Server.
5. En Certificados raíz de confianza, haga clic en Agregar.

6. Haga clic en Examinar y seleccione la ubicación del archivo .pem del certificado (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).
7. Haga clic en Añadir. El certificado se agrega a la tienda.

Consulte "[Agregue un certificado raíz de confianza al almacén de certificados](#)" si quiere más información. Al implementar una vApp (mediante el archivo OVA), la firma digital del paquete vApp se puede verificar en la página 'Detalles de revisión'. Si el paquete vApp descargado es genuino, la columna 'Publisher' muestra 'Trusted Certificate' (Certificado de confianza) (como en la siguiente captura de pantalla).

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Review details

Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere for netapp storage systems. For more information or support please visit https://www.netapp.com/
Download size	2.2 GB
Size on disk	3.9 GB (thin provisioned)
	53.0 GB (thick provisioned)

Activate

Go to Sys

CANCEL

BACK

NEXT

Verificación de la firma de las herramientas de ONTAP ISO y SRA tar.gz

NetApp comparte su certificado de firma de código con los clientes en la página de descarga del producto, junto con los archivos zip del producto para OTV-iso y sra.tgz.

Del certificado de firma de código, los usuarios pueden extraer la clave pública de la siguiente manera:

```
#> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

A continuación, se debe utilizar la clave pública para verificar la firma para iso y el zip del producto tgz como se muestra a continuación:

```
#> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
Ejemplo:
```

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK => response
```

Puertos y protocolos

A continuación se muestran los puertos y protocolos necesarios que permiten la comunicación entre herramientas de ONTAP para el servidor VMware vSphere y otras entidades como sistemas de almacenamiento gestionados, servidores y otros componentes.

Puertos de entrada y salida necesarios para OTV

Tenga en cuenta la siguiente tabla en la que se enumeran los puertos de entrada y salida necesarios para el correcto funcionamiento de las herramientas de ONTAP. Es importante asegurarse de que solo los puertos mencionados en la tabla estén abiertos para las conexiones de máquinas remotas, mientras que todos los demás puertos deben estar bloqueados para las conexiones de máquinas remotas. Esto ayudará a garantizar la seguridad de su sistema.

En la siguiente tabla se describen los detalles de los puertos abiertos.

Puerto TCP v4/v6 #	Dirección	Función
8143	entrante	Conexiones HTTPS para la API de REST
8043	entrante	Conexiones HTTPS
9060	entrante	Conexiones HTTPS Se utiliza para conexiones SOAP a través de HTTPS Este puerto se debe abrir para permitir que un cliente se conecte al servidor API de herramientas de ONTAP.
22	entrante	SSH (deshabilitado de forma predeterminada)
9080	entrante	Conexiones HTTPS - VP y SRA - conexiones internas sólo del bucle invertido
9083	entrante	Conexiones HTTPS - VP y SRA Se utiliza para conexiones SOAP a través de HTTPS
1162	entrante	VP paquetes de captura SNMP
8443	entrante	Complemento remoto

Puerto TCP v4/v6 #	Dirección	Función
1527	exclusivamente para uso interno	Puerto de base de datos Derby, solo entre este equipo y él mismo, conexiones externas no aceptadas — Solo conexiones internas
8150	exclusivamente para uso interno	El servicio de integridad de log se ejecuta en el puerto
443	bidireccional	Se utiliza para las conexiones a clústeres de ONTAP

Control del acceso remoto a la base de datos Derby

Los administradores pueden acceder a la base de datos derby con los siguientes comandos. Se puede acceder a él a través de las herramientas de ONTAP VM local, así como a un servidor remoto con los siguientes pasos:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

Ejemplo:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=
ij> show tables;
TABLE_SCHEM      |TABLE_NAME      |REMARKS
-----|-----|-----
SYS              |SYSALIASES      |
SYS              |SYSCHECKS       |
SYS              |SYSCOLPERMS     |
SYS              |SYSCOLUMNS     |
SYS              |SYSCONGLOMERATES|
SYS              |SYSCONSTRAINTS  |
SYS              |SYSDEPENDS      |
SYS              |SYSFILES        |
SYS              |SYSFOREIGNKEYS  |
SYS              |SYSKEYS         |
SYS              |SYSPERMS        |
```

Herramientas de ONTAP para puntos de acceso de VMware vSphere (Usuarios)

La instalación de ONTAP Tools para VMware vSphere crea y utiliza tres tipos de usuarios:

1. Usuario del sistema: La cuenta de usuario raíz
2. Usuario de la aplicación: El usuario administrador, el usuario de mantenimiento y las cuentas de usuario de base de datos
3. Usuario de soporte: La cuenta de usuario diag

1. Usuario del sistema

El usuario System(root) se crea mediante la instalación de herramientas de ONTAP en el sistema operativo subyacente (Debian).

- Un usuario predeterminado del sistema “root” se crea en Debian mediante la instalación de herramientas de ONTAP. Su valor predeterminado está desactivado y se puede activar de forma ad hoc a través de la consola 'antigua'.

2. Usuario de la aplicación

El usuario de la aplicación se denomina usuario local en las herramientas de ONTAP. Se trata de usuarios creados en la aplicación de herramientas de ONTAP. La siguiente tabla muestra los tipos de usuarios de la aplicación:

Usuario	Descripción
Usuario administrador	Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. La contraseña caducará en 90 días y se espera que los usuarios cambien la misma.
Usuario de mantenimiento	Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. Se trata de un usuario de mantenimiento y se crea para ejecutar las operaciones de la consola de mantenimiento.
Usuario de base de datos	Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. La contraseña caducará en 90 días y se espera que los usuarios cambien la misma.

3. Usuario de apoyo (usuario diag)

Durante la instalación de las herramientas de ONTAP, se crea un usuario de soporte. Este usuario se puede utilizar para acceder a las herramientas de ONTAP en caso de cualquier problema o interrupción en el servidor y para recopilar registros. De forma predeterminada, este usuario está desactivado, pero se puede activar de forma específica a través de la consola 'antigua'. Es importante tener en cuenta que este usuario se desactivará automáticamente después de un período de tiempo determinado.

TLS mutuo (autenticación basada en certificados)

Las versiones 9,7 y posteriores de ONTAP admiten la comunicación TLS mutua. A partir de ONTAP Tools para VMware y vSphere 9,12, el TLS mutuo se utiliza para la comunicación con clústeres recién añadidos (según la versión de ONTAP).

ONTAP

Para todos los sistemas de almacenamiento añadidos anteriormente: Durante una actualización, todos los sistemas de almacenamiento añadidos se volverán de confianza automáticamente y se configurarán los mecanismos de autenticación basados en certificados.

Como en la siguiente captura de pantalla, la página de configuración del clúster mostrará el estado de TLS mutuo (autenticación basada en certificado), configurado para cada clúster.

Storage Systems ?

ADD REDISCOVER ALL

Name	Type	IP Address	ONTAP Release	Status	Capacity	NFS VAAI	Supported Protocols
CL_sti21-vsim-ucs501m_1678878260	Cluster	10.234.85.142	9.12.0	Normal	20.42%		

Storage Systems per page: 10 1 Item

Cluster Add

Durante el flujo de trabajo de agregación de clústeres, si el clúster que se agrega admite MTLS, MTLS se configurará de forma predeterminada. El usuario no necesita realizar ninguna configuración para esto. La siguiente captura de pantalla muestra la pantalla presentada al usuario durante la adición del clúster.

Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.224.58.52

Name or IP address:

Username:

Password:

Port:

443

Advanced options

ONTAP Cluster Certificate:

Automatically fetch

Manually upload

CANCEL

ADD

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

Name or IP address:

Username:

Password:

Port:

Advanced options [>](#)

CANCEL

ADD

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.224.58.52

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES

CANCEL

ADD

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Hide certificate](#)

Certificate Information

This certificate identifies the 10.234.85.142 host.

Issued By

Name (CN or DN): C1_sti21-vsims-ucs581m_1678878260

Issued To

Name (CN or DN): C1_sti21-vsims-ucs581m_1678878260

Validity

Issued On: 03/15/2023 11:16:06

Expires On: 03/14/2024 11:16:06

Fingerprint Information

SHA-1 Fingerprint: 2C:38:E3:5C:4B:F3:5D:3F:39:C8:CE:4A:8
2:C1:A6:EE:34:53:A0:F3

SHA-256 Fingerprint: 05:0F:FE:CD:B0:C6:FC:6F:EB:8A:FC:86:F
7:E3:EF:D4:8D:CA:02:92:9B:E1:A4:70:84:
52:F8:76:98:64:FA:23

Do you want to trust this certificate?

NO

YES

Edición de clúster

Durante la operación de edición del clúster, existen dos situaciones:

- Si el certificado ONTAP caduca, el usuario tendrá que obtener el nuevo certificado y cargarlo.
- Si el certificado OTV caduca, el usuario puede regenerarlo marcando la casilla de verificación.
 - *Generar un nuevo certificado de cliente para ONTAP.*

Modify Storage System

Settings

Provisioning Options

IP address or hostname: 10.237.149.72

Port: 443

Username: admin

Password:

Upload Certificate (Optional) [BROWSE](#)

☐ Skip monitoring of this storage system

☒ Generate a new client certificate for ONTAP

CANCEL

OK



Certificado HTTPS de herramientas de ONTAP

De manera predeterminada, las herramientas de ONTAP utilizan un certificado autofirmado que se crea automáticamente durante la instalación para proteger el acceso HTTPS a la interfaz de usuario web. Las herramientas de ONTAP ofrecen las siguientes funciones:

1. Regenerar certificado HTTPS

Durante la instalación de las herramientas de ONTAP, se instala un certificado de CA HTTPS y el certificado se almacena en el almacén de claves. El usuario tiene la opción de regenerar el certificado HTTPS a través de la consola de mantenimiento.

Se puede acceder a las opciones anteriores en la consola *maint* navegando a '*Configuración de la aplicación*' → '*Volver a generar certificados*'.

Banner de inicio de sesión

Se muestra el siguiente banner de inicio de sesión después de que el usuario introduce un nombre de usuario en la pantalla de inicio de sesión. Tenga en cuenta que SSH está deshabilitado de forma predeterminada y solo permite inicios de sesión de una vez cuando se habilita desde la consola de VM.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Una vez que el usuario completa el inicio de sesión a través del canal SSH, se muestra el siguiente texto:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Tiempo de espera de inactividad

Para evitar el acceso no autorizado, se configura un tiempo de espera de inactividad, que cierra automáticamente la sesión de los usuarios inactivos durante un cierto período mientras se utilizan los recursos autorizados. Esto garantiza que solo los usuarios autorizados puedan acceder a los recursos y ayuda a mantener la seguridad.

- De forma predeterminada, las sesiones de vSphere Client se cierran tras 120 minutos de tiempo inactivo, lo cual requiere que el usuario inicie sesión nuevamente para reanudarse usando el cliente. Puede cambiar el valor de tiempo de espera editando el archivo `webclient.properties`. Puede configurar el tiempo de espera de vSphere Client "[Configure el valor de tiempo de espera del cliente de vSphere](#)"
- Las herramientas de ONTAP tienen un tiempo de cierre de sesión de la cli web de 30 minutos.

Máximo de solicitudes simultáneas por usuario (Protección de seguridad de red :: Ataque DoS)

Por defecto, el Núm. Máximo de solicitudes simultáneas por usuario es 48. El usuario root en las herramientas de ONTAP puede cambiar este valor en función de los

requisitos de su entorno. **Este valor no debe establecerse en un valor muy alto, ya que proporciona un mecanismo contra ataques de denegación de servicio (DoS).**

Los usuarios pueden modificar el número máximo de sesiones simultáneas y otros parámetros admitidos en el archivo `/opt/netapp/vscserver/etc/dosfilterParams.json`.

Podemos configurar el filtro con los siguientes parámetros:

- **delayMs**: El retraso en milisegundos dado a todas las solicitudes por encima del límite de tasa antes de que sean consideradas. Dar -1 para rechazar la solicitud.
- **throttleMs**: Cuánto tiempo esperar el semáforo de forma asíncrona.
- **maxRequestMs**: Cuánto tiempo se debe permitir que se ejecute esta solicitud.
- **ipWhitelist**: Una lista separada por comas de direcciones IP que no se limitará la tasa. (Pueden ser IP de vCenter, ESXi y SRA)
- **maxRequestsPerSec**: El número máximo de solicitudes de una conexión por segundo.

Valores predeterminados en el archivo `dosfilterParams`:

```
{ "delayMs": "-1",  
  "throttleMs": "1800000",  
  "maxRequestMs": "300000",  
  "ipWhitelist": "10.224.58.52",  
  "maxRequestsPerSec": "48" }
```

Configuración del Protocolo de hora de red (NTP)

A veces, pueden producirse problemas de seguridad debido a discrepancias en las configuraciones de tiempo de red. Es importante asegurarse de que todos los dispositivos dentro de una red tengan una configuración de tiempo precisa para evitar tales problemas.

Dispositivo virtual

Puede configurar los servidores NTP desde la consola de mantenimiento del dispositivo virtual. Los usuarios pueden agregar los detalles del servidor NTP en *Configuración del sistema* ⇒ *Agregar nuevo servidor NTP* opción

De forma predeterminada, el servicio para NTP es ntpd. Este es un servicio heredado y no funciona bien para máquinas virtuales en ciertos casos.

Debian

En Debian, el usuario puede acceder al archivo `/etc/ntp.conf` para obtener los detalles del servidor ntp.

Políticas de contraseñas

Los usuarios que implementen las herramientas de ONTAP por primera vez o que

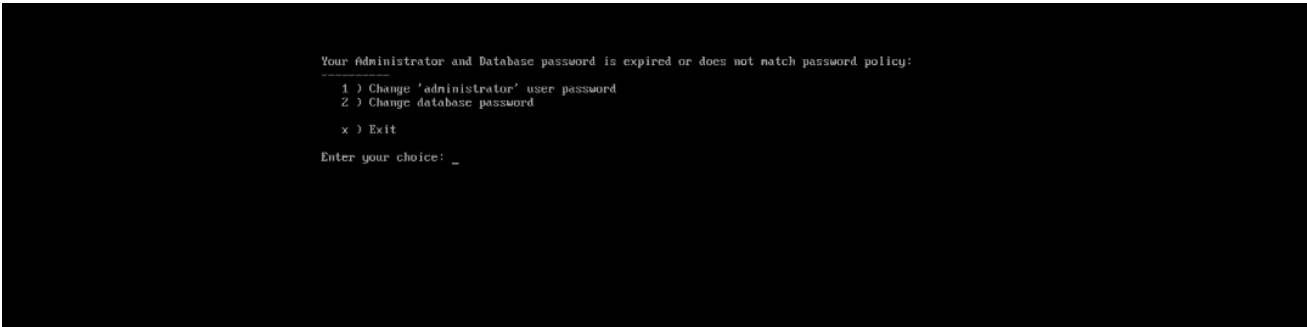
actualicen a la versión 9,12 o posterior deberán seguir la política de contraseñas seguras tanto para el administrador como para los usuarios de la base de datos. Durante el proceso de implementación, se solicitará a los nuevos usuarios que introduzcan sus contraseñas. Para los usuarios de brownfield que actualicen a la versión 9,12 o posterior, la opción de seguir la política de contraseñas seguras estará disponible en la consola de mantenimiento.

- Una vez que el usuario inicia sesión en la consola de mantenimiento, las contraseñas se verificarán con respecto al conjunto de reglas complejo y, si se detecta que no se siguen, se solicitará al usuario que restablezca la misma.
- La validez predeterminada de la contraseña es de 90 días y después de 75 días el usuario comenzará a recibir la notificación para cambiar la contraseña.
- Es necesario establecer una nueva contraseña en cada ciclo, el sistema no tomará la última contraseña como nueva contraseña.
- Cada vez que un usuario inicia sesión en la consola de mantenimiento, comprobará las políticas de contraseñas como las siguientes capturas de pantalla antes de cargar el menú principal:



```
Maintenance Console : "NetApp ONTAP tools for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
validating password policies
```

- Si no sigue la política de contraseñas o su configuración de actualización desde las herramientas de ONTAP 9,11 o anteriores. A continuación, el usuario verá la siguiente pantalla para restablecer la contraseña:



```
Your Administrator and Database password is expired or does not match password policy:
1 ) Change 'administrator' user password
2 ) Change database password
x ) Exit
Enter your choice: _
```

- Si el usuario intenta establecer una contraseña débil o da la última contraseña de nuevo, el usuario verá el siguiente error:


```
Changing password for administrator.

User: administrator
Enter new password:
Retype new password:

Password doesn't matches the password policy.
For security reasons, it is recommended to use a password that is of eight to thirty characters and
contains a minimum of one upper, one lower, one digit, and one special character.

Enter new password:
Retype new password:
Check if new decoder works ?
New decoder worked successfully
00-02/23 13:36:53 Your new password must be different

Error updating sra credential file

Press ENTER to continue._
```

Información de copyright

Copyright © 2024 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.