



# **Supervise los puertos de red**

## **ONTAP 9**

NetApp  
April 24, 2024

This PDF was generated from [https://docs.netapp.com/es-es/ontap/networking/monitor\\_the\\_health\\_of\\_network\\_ports.html](https://docs.netapp.com/es-es/ontap/networking/monitor_the_health_of_network_ports.html) on April 24, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos

- Supervise los puertos de red ..... 1
  - Supervise el estado de los puertos de red ..... 1
  - Supervisar la accesibilidad de los puertos de red (ONTAP 9,8 y posteriores) ..... 2
- Descripción general de los puertos ONTAP ..... 6
- Puertos internos ONTAP ..... 7

# Supervise los puertos de red

## Supervise el estado de los puertos de red

La gestión de ONTAP de los puertos de red incluye supervisión automática del estado y un conjunto de monitores de estado para ayudarle a identificar puertos de red que podrían no ser adecuados para alojar LIF.

### Acerca de esta tarea

Si un monitor de estado determina que un puerto de red no es bueno, advierte a los administradores a través de un mensaje de EMS o Marca el puerto como degradado. ONTAP evita el alojamiento de LIF en puertos de red degradados si existen destinos de conmutación al nodo de respaldo alternativos en buen estado para esa LIF. Un puerto puede degradarse debido a un evento de fallo de software, como el enlace flapping (enlaces que rebotan rápidamente entre arriba y abajo) o la partición de red:

- Los puertos de red del espacio IP del clúster se marcan como degradados cuando experimentan el enlace flopping o la pérdida de la capacidad de acceso de la capa 2 (L2) a otros puertos de red en el dominio de retransmisión.
- Los puertos de red de los espacios IP que no pertenecen al clúster se marcan como degradados cuando experimentan un enlace flapping.

Debe tener en cuenta los siguientes comportamientos de un puerto degradado:

- No se puede incluir un puerto degradado en una VLAN o en un grupo de interfaces.

Si un puerto del miembro de un grupo de interfaces se Marca como degradado, pero el grupo de interfaces sigue marcado como correcto, las LIF se pueden alojar en ese grupo de interfaces.

- Los LIF se migran automáticamente de puertos degradados a puertos en buen estado.
- Durante un evento de conmutación por error, no se considera un puerto degradado como destino de conmutación por error. Si no hay puertos en buen estado disponibles, puertos LIF degradados del host según la política de conmutación al respaldo normal.
- No puede crear, migrar o revertir un LIF a un puerto degradado.

Puede modificar el `ignore-health-status` configuración del puerto de red a `true`. Luego puede alojar una LIF en los puertos en buen estado.

### Pasos

1. Inicie sesión en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Compruebe qué monitores de estado están habilitados para supervisar el estado del puerto de red:

```
network options port-health-monitor show
```

El estado de un puerto está determinado por el valor de los monitores de estado.

Los siguientes monitores de estado están disponibles y están habilitados de manera predeterminada en ONTAP:

- Monitor de estado de enlace: Monitores de enlace flapping

Si un puerto tiene un enlace que flaquea más de una vez en cinco minutos, este puerto se marca como degradado.

- Monitor de estado de accesibilidad L2: Controla si todos los puertos configurados en el mismo dominio de difusión tienen accesibilidad L2 entre sí

Este monitor de estado genera problemas de accesibilidad L2 en todos los espacios IP; sin embargo, solo marca los puertos del espacio IP del clúster como degradados.

- Monitor CRC: Supervisa las estadísticas de CRC en los puertos

Este monitor de estado no marca un puerto como degradado, pero genera un mensaje de EMS cuando se observa una tasa de fallo de CRC muy alta.

3. Habilite o deshabilite cualquiera de los monitores de estado de un espacio IP según lo desee mediante el `network options port-health-monitor modify` comando.

4. Consulte el estado detallado de un puerto:

```
network port show -health
```

El resultado del comando muestra el estado del puerto, `ignore health status` configuración y lista de motivos por los que el puerto está marcado como degradado.

Un estado de estado de puerto puede ser `healthy` o `degraded`.

Si la `ignore health status` el ajuste es `true`, indica que el estado del puerto se ha modificado de `degraded` para `healthy` el administrador.

Si la `ignore health status` el ajuste es `false`, el estado del puerto lo determina automáticamente el sistema.

## Supervisar la accesibilidad de los puertos de red (ONTAP 9,8 y posteriores)

La supervisión de la accesibilidad está integrada en ONTAP 9.8 y versiones posteriores. Utilice esta supervisión para identificar cuándo la topología de red física no coincide con la configuración de ONTAP. En algunos casos, ONTAP puede reparar la accesibilidad de los puertos. En otros casos, se requieren pasos adicionales.

### Acerca de esta tarea

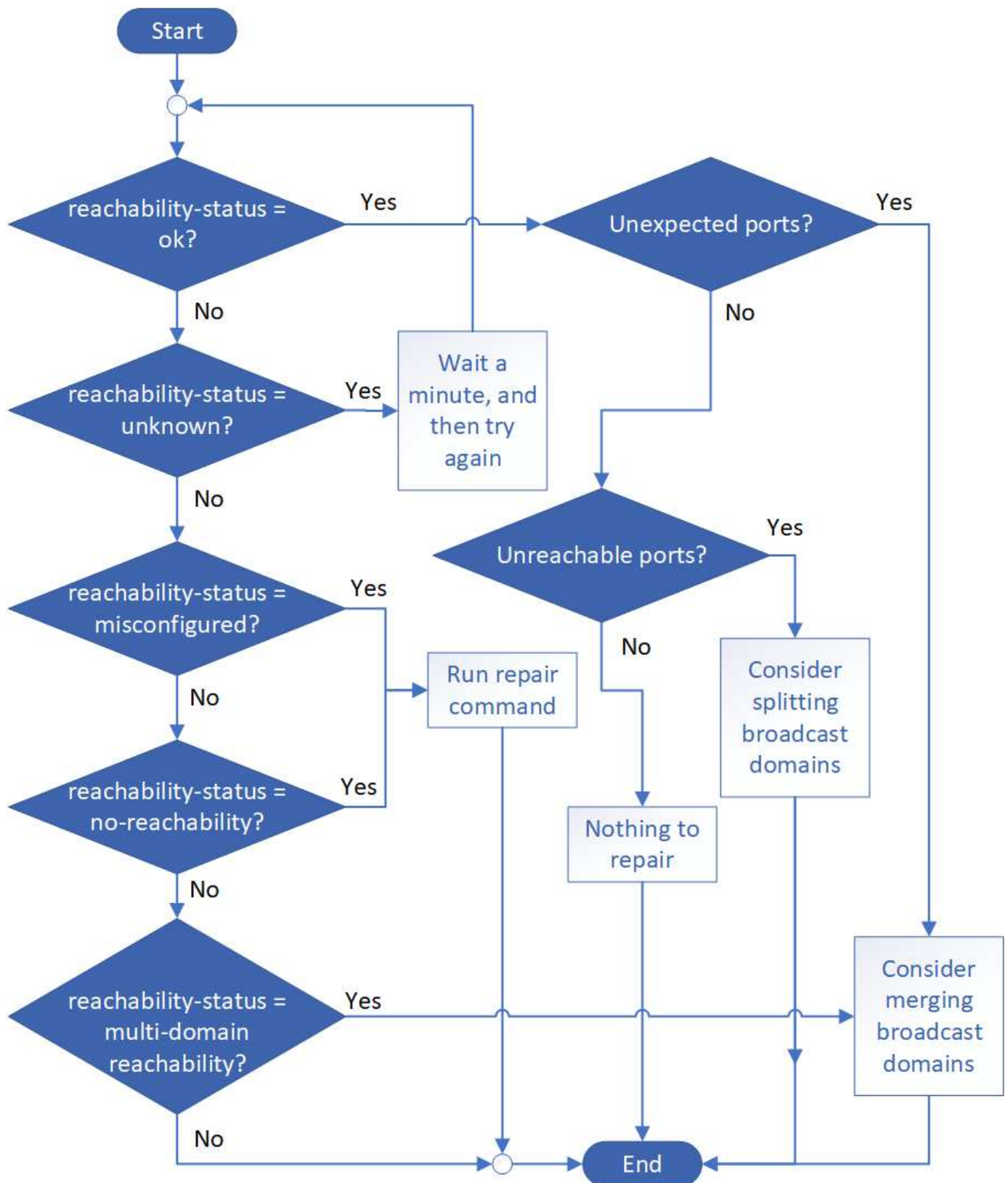
Utilice estos comandos para verificar, diagnosticar y reparar configuraciones incorrectas de red procedentes de la configuración de ONTAP que no coinciden con el cableado físico o la configuración del switch de red.

### Paso

1. Ver accesibilidad de puertos:

```
network port reachability show
```

2. Utilice el árbol de decisiones y la tabla siguientes para determinar el siguiente paso, si existe alguno.



Accesibilidad-estado	Descripción
----------------------	-------------

de acuerdo	<p>El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado. Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte la siguiente fila <i>inesperado ports</i>.</p> <p>Si el reachability-status es "ok", pero hay "puertos inaccesibles", considere dividir uno o más dominios de difusión. Para obtener más información, consulte la siguiente fila <i>ports</i> sin acceso.</p> <p>Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.</p>
Puertos inesperados	<p>El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast.</p> <p>Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión.</p> <p>Para obtener más información, consulte <a href="#">"Fusionar dominios de retransmisión"</a>.</p>
Puertos inaccesibles	<p>Si un solo dominio de difusión se ha particionado en dos conjuntos de accesibilidad diferentes, puede dividir un dominio de difusión para sincronizar la configuración de ONTAP con la topología de red física.</p> <p>Normalmente, la lista de puertos inaccesibles define el conjunto de puertos que se deben dividir en otro dominio de retransmisión después de verificar que la configuración física y de switch es correcta.</p> <p>Para obtener más información, consulte <a href="#">"Divida los dominios de retransmisión"</a>.</p>
función mal configurada	<p>El puerto no tiene posibilidad de recurrir a la capa 2 a su dominio de difusión asignado; sin embargo, el puerto tiene capacidad de acceso de capa 2 a un dominio de difusión diferente.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto al dominio de retransmisión al que se le habrá accesibilidad:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte <a href="#">"Reparar la accesibilidad del puerto"</a>.</p>
ausencia de accesibilidad	<p>El puerto no tiene posibilidad de recurrir a ningún dominio de difusión existente de capa 2.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto a un dominio de retransmisión creado automáticamente en el espacio IP predeterminado:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte <a href="#">"Reparar la accesibilidad del puerto"</a>.</p>

accesibilidad multi-dominio	<p>El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast.</p> <p>Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión.</p> <p>Para obtener más información, consulte <a href="#">"Fusionar dominios de retransmisión"</a> o <a href="#">"Reparar la accesibilidad del puerto"</a>.</p>
desconocido	Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.

Después de reparar un puerto, necesita comprobar y resolver las LIF y VLAN desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de interfaces. Para obtener más información, consulte ["Reparar la accesibilidad del puerto"](#).

## Descripción general de los puertos ONTAP

Algunos puertos conocidos se reservan para comunicaciones ONTAP con servicios específicos. Se producirán conflictos de puertos si un valor de puerto en el entorno de red de almacenamiento es el mismo que en el puerto ONTAP.

En la siguiente tabla se enumeran los puertos TCP y UDP que utiliza ONTAP.

Servicio	Puerto/protocolo	Descripción
ssh	22/TCP	Inicio de sesión seguro en shell
telnet	23/TCP	Inicio de sesión remoto
DNS	53/TCP	Cargue el DNS equilibrado
http	80/TCP	Protocolo de transferencia de Hyper Text
rpcind	111/TCP	Llamada a procedimiento remoto
rpcind	111/UDP	Llamada a procedimiento remoto
ntp	123/UDP	Protocolo de hora de red
msrpc	135/UDP	MSRPC
netbios-ssn	139/TCP	Sesión de servicio NetBIOS
snmp	161/UDP	Protocolo simple de gestión de red
https	443/TCP	HTTP sobre TLS
microsoft-ds	445/TCP	Microsoft-ds
montaje	635/TCP	Montaje NFS
montaje	635/UDP	Montaje NFS
nombre	953/UDP	Daemon de nombres



nfs	2049/UDP	Daemon de servidor NFS
nfs	2049/TCP	Daemon de servidor NFS
vrn	2050/TCP	Protocolo de volumen remoto de NetApp
iscsi	3260/TCP	Puerto de destino iSCSI
lockd	4045/TCP	Daemon de bloqueo NFS
lockd	4045/UDP	Daemon de bloqueo NFS
NSM	4046/TCP	Monitor de estado de red
NSM	4046/UDP	Monitor de estado de red
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS de multidifusión
HTTPS	5986/UDP	Puerto HTTPS: Protocolo binario de escucha
https	8443/TCP	Herramienta GUI de 7MTT a través de https
ndmp	10000/TCP	Protocolo de gestión de datos de red
Conexión de clústeres entre iguales	11104/TCP	Cluster peering, bidireccional
Cluster peering, bidireccional	11105/TCP	Conexión de clústeres entre iguales
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	acepte conexiones de control a través de tomas seguras
puerto de testigos cifs	40001/TCP	puerto de testigos cifs
tls	50000/TCP	Seguridad de la capa de transporte
iscsi	65200/TCP	Puerto iSCSI

## Puertos internos ONTAP

En la siguiente tabla se enumeran los puertos TCP y UDP que ONTAP utiliza internamente. Estos puertos se utilizan para establecer comunicación entre LIF dentro del clúster:

Puerto/protocolo	Descripción
514	Syslog
900	RPC de clúster de NetApp
902	RPC de clúster de NetApp
904	RPC de clúster de NetApp
905	RPC de clúster de NetApp

910	RPC de clúster de NetApp
911	RPC de clúster de NetApp
913	RPC de clúster de NetApp
914	RPC de clúster de NetApp
915	RPC de clúster de NetApp
918	RPC de clúster de NetApp
920	RPC de clúster de NetApp
921	RPC de clúster de NetApp
924	RPC de clúster de NetApp
925	RPC de clúster de NetApp
927	RPC de clúster de NetApp
928	RPC de clúster de NetApp
929	RPC de clúster de NetApp
931	RPC de clúster de NetApp
932	RPC de clúster de NetApp
933	RPC de clúster de NetApp
934	RPC de clúster de NetApp
935	RPC de clúster de NetApp
936	RPC de clúster de NetApp
937	RPC de clúster de NetApp
939	RPC de clúster de NetApp
940	RPC de clúster de NetApp
951	RPC de clúster de NetApp
954	RPC de clúster de NetApp
955	RPC de clúster de NetApp
956	RPC de clúster de NetApp
958	RPC de clúster de NetApp
961	RPC de clúster de NetApp
963	RPC de clúster de NetApp
964	RPC de clúster de NetApp
966	RPC de clúster de NetApp
967	RPC de clúster de NetApp
982	RPC de clúster de NetApp
983	RPC de clúster de NetApp

5125	Puerto de control alternativo para el disco
5133	Puerto de control alternativo para el disco
5144	Puerto de control alternativo para el disco
65502	SSH de alcance del nodo
65503	Uso compartido de LIF
7810	RPC de clúster de NetApp
7811	RPC de clúster de NetApp
7812	RPC de clúster de NetApp
7813	RPC de clúster de NetApp
7814	RPC de clúster de NetApp
7815	RPC de clúster de NetApp
7816	RPC de clúster de NetApp
7817	RPC de clúster de NetApp
7818	RPC de clúster de NetApp
7819	RPC de clúster de NetApp
7820	RPC de clúster de NetApp
7821	RPC de clúster de NetApp
7822	RPC de clúster de NetApp
7823	RPC de clúster de NetApp
7824	RPC de clúster de NetApp
8023	Telnet de alcance de nodo
8514	Alcance del nodo RSH
9877	Puerto de cliente KMIP (solo host local interno)

## 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.