



Configuraciones especiales

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/upgrade/concept_special_configurations_post_checks.html on September 12, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Configuraciones especiales 1
 - Consideraciones especiales tras una actualización de ONTAP 1
 - Verifique la configuración de red después de una actualización de ONTAP desde ONTAP 9,7x o una versión anterior 1
 - Quite el servicio LIF de EMS de las políticas de servicio de red 4
 - Comprobar el estado de redes y almacenamiento de las configuraciones de MetroCluster tras una actualización de ONTAP 5
 - Comprobar la configuración DE SAN tras una actualización 8
 - Vuelva a configurar las conexiones del servidor KMIP después de una actualización de ONTAP 9,2 o una versión anterior 9
 - Reubicar volúmenes de origen de reflejos de uso compartido de carga movidos después de una actualización de ONTAP 10
 - Cambio en las cuentas de usuario que pueden acceder a Service Processor 11

Configuraciones especiales

Consideraciones especiales tras una actualización de ONTAP

Si se configura el clúster con alguna de las siguientes funciones, es posible que deba realizar pasos adicionales después de actualizar el software ONTAP.

Pregúntese...	Si su respuesta es sí, entonces haga esto...
¿He actualizado desde ONTAP 9,7 o anterior a ONTAP 9,8 o posterior?	Compruebe la configuración de red Quite el servicio LIF EMS de las políticas de servicio de red que no proporcionan accesibilidad al destino EMS
¿Mi clúster está en una configuración MetroCluster?	Compruebe el estado de las redes y el almacenamiento
¿Tengo una configuración SAN?	Compruebe su configuración SAN
¿Actualizo desde ONTAP 9,3 o anterior? ¿Utilizo el cifrado del almacenamiento de NetApp?	Volver a configurar las conexiones del servidor KMIP
¿Tengo reflejos de uso compartido de carga?	Reubicar los volúmenes de origen de reflejos de uso compartido de carga movidos
¿Tengo cuentas de usuario para el acceso al procesador de servicio (SP) que se hayan creado antes de ONTAP 9,9.1?	Compruebe el cambio en las cuentas que pueden acceder a Service Processor

Verifique la configuración de red después de una actualización de ONTAP desde ONTAP 9,7x o una versión anterior

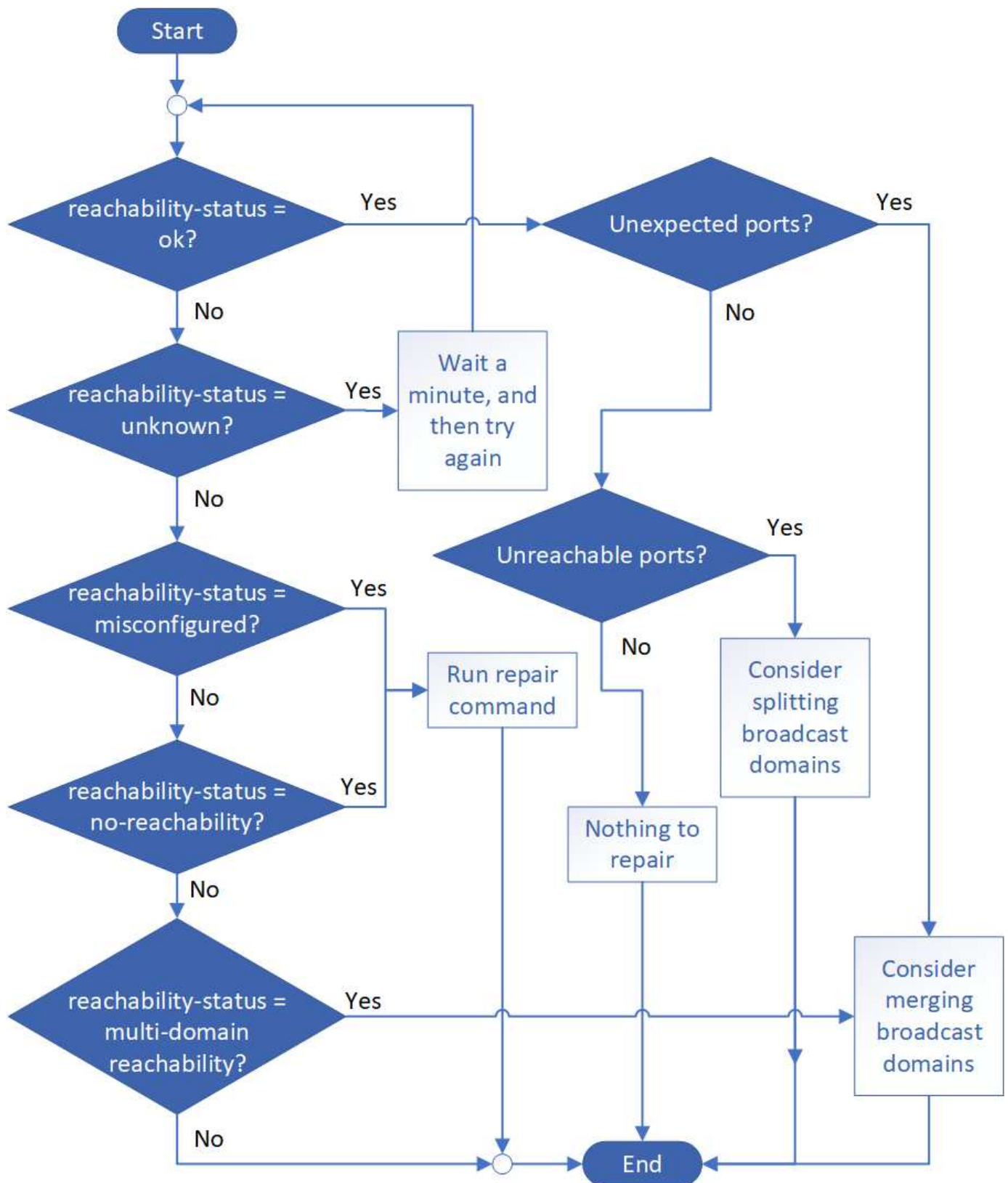
Después de realizar una actualización desde ONTAP 9,7x o anterior a ONTAP 9,8 o posterior, debe verificar la configuración de red. Después de la actualización, ONTAP supervisa automáticamente la accesibilidad de la capa 2.

Paso

1. Compruebe que cada puerto tiene accesibilidad al dominio de retransmisión esperado:

```
network port reachability show -detail
```

El resultado del comando contiene resultados de accesibilidad. Use el árbol de decisión y la tabla siguientes para comprender los resultados de la accesibilidad (estado de la accesibilidad) y determinar qué hacer, si es que hay algo, a continuación.



accesibilidad-estado	Descripción
----------------------	-------------

de acuerdo	<p>El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado.</p> <p>Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión".</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 "Divida los dominios de retransmisión".</p> <p>Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.</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 "Reparar la accesibilidad del puerto".</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 "Reparar la accesibilidad del puerto".</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 "Fusionar dominios de retransmisión" o "Reparar la accesibilidad del puerto".</p>
desconocido	<p>Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.</p>

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"](#).

Quite el servicio LIF de EMS de las políticas de servicio de red

Si tiene mensajes del sistema de gestión de eventos (EMS) configurados antes de actualizar de ONTAP 9.7 o anterior a ONTAP 9.8 o posterior, después de la actualización, es posible que los mensajes de EMS no se envíen.

Durante la actualización, Management-ems, que es el servicio LIF de EMS, se agrega a todas las políticas de servicio existentes. Esto permite enviar mensajes de EMS desde cualquiera de las LIF asociadas con cualquiera de las políticas de servicio. Si la LIF seleccionada no tiene accesibilidad al destino de notificaciones de eventos, el mensaje no se entrega.

Para evitar esto, después de la actualización, debe eliminar el servicio LIF de EMS de las políticas de servicio de red que no proporcionan accesibilidad al destino.

Pasos

1. Identificar las LIF y las políticas de servicio de red asociadas mediante las cuales se pueden enviar mensajes de EMS:

```
network interface show -fields service-policy -services management-ems
```

vserver	lif	service-policy
cluster-1	cluster_mgmt	default-management
cluster-1	node1-mgmt	default-management
cluster-1	node2-mgmt	default-management
cluster-1	inter_cluster	default-intercluster

4 entries were displayed.

2. Compruebe cada LIF para obtener conectividad con el destino EMS:

```
network ping -lif <lif_name> -vserver <svm_name> -destination  
<destination_address>
```

Realice esto en cada nodo.

Ejemplos

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Introduzca el nivel de privilegio avanzado:

```
set advanced
```

4. Para los LIF que no tienen habilidad, quite el servicio LIF Management-ems de las políticas de servicio correspondientes:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

5. Compruebe que el LIF de ems de gestión solo esté asociado a las LIF que proporcionan accesibilidad al destino de EMS:

```
network interface show -fields service-policy -services management-ems
```

Enlaces relacionados

["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#)

Comprobar el estado de redes y almacenamiento de las configuraciones de MetroCluster tras una actualización de ONTAP

Después de actualizar un clúster de ONTAP en una configuración de MetroCluster, debe comprobar el estado de las LIF, los agregados y los volúmenes de cada clúster.

1. Compruebe el estado de la LIF:

```
network interface show
```

En un funcionamiento normal, los LIF de las SVM de origen deben tener el estado de administrador de en activo y estar ubicados en sus nodos raíz. Los LIF para las SVM de destino no necesitan estar en marcha o ubicados en sus nodos iniciales. Sin embargo, todos los LIF tienen el estado de administrador activo,

pero no es necesario que estén ubicados en sus nodos iniciales.

```
cluster1::> network interface show
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					

Cluster					
	cluster1-a1_clus1	up/up	192.0.2.1/24	cluster1-01	e2a
true					
	cluster1-a1_clus2	up/up	192.0.2.2/24	cluster1-01	e2b
true					
cluster1-01					
	clus_mgmt	up/up	198.51.100.1/24	cluster1-01	e3a
true					
	cluster1-a1_inet4_intercluster1	up/up	198.51.100.2/24	cluster1-01	e3c
true					
	...				

27 entries were displayed.

2. Compruebe el estado de los agregados:

```
storage aggregate show -state !online
```

Este comando muestra todos los agregados que *not* están en línea. En el funcionamiento normal, todos los agregados ubicados en el sitio local deben estar en línea. Sin embargo, si la configuración de MetroCluster está de conmutación, los agregados raíz del sitio de recuperación ante desastres pueden estar sin conexión.

Este ejemplo muestra un clúster en funcionamiento normal:


```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

Este ejemplo muestra un clúster con conmutación de sitios, en el que los agregados raíz del sitio de recuperación ante desastres están sin conexión:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
aggr0_b1
0B            0B      0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
0B            0B      0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

3. Compruebe el estado de los volúmenes:

```
volume show -state !online
```

Este comando muestra los volúmenes que *not* están en línea.

Si la configuración de MetroCluster tiene un funcionamiento normal (no está en estado de conmutación por sitios), el resultado debe mostrar todos los volúmenes que pertenecen a las SVM secundarias del clúster (los que tienen el nombre de SVM anexado con "-mc").

Esos volúmenes solo entran en línea en caso de que se produzca un cambio.

Este ejemplo muestra un clúster con un funcionamiento normal, en el cual los volúmenes del sitio de recuperación ante desastres no están en línea.

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
vs2-mc    vol1             aggr1_b1      -          RW        -
-         -
vs2-mc    root_vs2        aggr0_b1      -          RW        -
-         -
vs2-mc    vol2            aggr1_b1      -          RW        -
-         -
vs2-mc    vol3            aggr1_b1      -          RW        -
-         -
vs2-mc    vol4            aggr1_b1      -          RW        -
-         -
5 entries were displayed.
```

4. Compruebe que no haya volúmenes incoherentes:

```
volume show -is-inconsistent true
```

Consulte el artículo de la base de conocimientos ["Volumen que muestra una incoherencia de WAFL"](#) sobre la forma de abordar los volúmenes incoherentes.

Comprobar la configuración DE SAN tras una actualización

Tras una actualización de ONTAP, en un entorno SAN, debe verificar que cada iniciador que esté conectado a una LIF antes de que la actualización se haya reconectado correctamente a la LIF.

1. Compruebe que cada iniciador está conectado a la LIF correcta.

Debe comparar la lista de iniciadores con la lista que ha realizado durante la preparación de la actualización. Si ejecuta ONTAP 9.11.1 o una versión posterior, use System Manager para ver el estado de conexión, ya que muestra mucho más clara que la interfaz de línea de comandos.

System Manager

- a. En el Administrador del sistema, haga clic en **hosts > grupos de iniciadores DE SAN**.

La página muestra una lista de iGroups. Si la lista es grande, puede ver páginas adicionales de la lista haciendo clic en los números de página en la esquina inferior derecha de la página.

Las columnas muestran información diversa sobre los iGroups. A partir de 9.11.1, también se muestra el estado de conexión del igroup. Pase el ratón sobre las alertas de estado para ver detalles.

CLI

- Mostrar iniciadores de iSCSI:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- Mostrar iniciadores de FC:

```
fcip initiator show -fields igroup,wwpn,lif
```

Vuelva a configurar las conexiones del servidor KMIP después de una actualización de ONTAP 9,2 o una versión anterior

Después de realizar la actualización desde ONTAP 9,2 o una versión anterior a ONTAP 9,3 o una versión posterior, debe volver a configurar todas las conexiones del servidor de gestión de claves externa (KMIP).

Pasos

1. Configure la conectividad del gestor de claves:

```
security key-manager setup
```

2. Añada sus servidores KMIP:

```
security key-manager add -address <key_management_server_ip_address>
```

3. Compruebe que los servidores KMIP están conectados:

```
security key-manager show -status
```

4. Consulte los servidores de claves:

```
security key-manager query
```

5. Cree una nueva clave de autenticación y contraseña:

```
security key-manager create-key -prompt-for-key true
```

La frase de contraseña debe tener un mínimo de 32 caracteres.

6. Consulte la nueva clave de autenticación:

```
security key-manager query
```

7. Asigne la nueva clave de autenticación a sus discos de cifrado automático (SED):

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```



Asegúrese de que está utilizando la nueva clave de autenticación de su consulta.

8. Si es necesario, asigne una clave FIPS al SED:

```
storage encryption disk modify -disk <disk_id> -fips-key-id  
<fips_authentication_key_id>
```

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

Reubicar volúmenes de origen de reflejos de uso compartido de carga movidos después de una actualización de ONTAP

Después de actualizar ONTAP, tiene que mover los volúmenes de origen de reflejos de uso compartido de carga nuevamente a sus ubicaciones previas a la actualización.

Pasos

1. Identifique la ubicación a la que se va a mover el volumen de origen de reflejos de uso compartido de carga mediante el registro creado antes de mover el volumen de origen de reflejos de uso compartido de carga.
2. Mueva el volumen de origen de reflejos de uso compartido de carga de vuelta a su ubicación original:

```
volume move start
```

Cambio en las cuentas de usuario que pueden acceder a Service Processor

Si ha creado cuentas de usuario en ONTAP 9,8 o una versión anterior que pueden acceder al procesador de servicio (SP) con un rol no de administrador y actualiza a ONTAP 9.9.1 o una versión posterior, cualquier valor que no sea administrador en la `-role` el parámetro se modifica a. `admin`.

Para obtener más información, consulte ["Cuentas que pueden acceder al SP"](#).

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.