



Supervisión del estado

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Supervisión del estado 1
 - Supervise el estado de la información general del sistema 1
 - Cómo funciona la supervisión del estado 1
 - Formas de responder a las alertas de estado del sistema 2
 - Personalización de alertas de estado del sistema 2
 - Cómo activan las alertas de estado los mensajes y eventos de AutoSupport. 3
 - Monitores de estado del clúster disponibles 3
 - Reciba alertas de estado del sistema automáticamente 5
 - Responda al estado degradado del sistema 5
 - Ejemplo de respuesta al estado degradado del sistema 6
 - Configurar la detección de switches de red de gestión y clústeres 9
 - Compruebe la supervisión de los switches de red de clúster y de gestión 10
 - Comandos para supervisar el estado del sistema 11
 - Muestra información del entorno 14

Supervisión del estado

Supervise el estado de la información general del sistema

Los monitores de estado supervisan proactivamente ciertas condiciones críticas de su clúster y generan alertas si detectan una falla o un riesgo. Si hay alertas activas, el estado del sistema informa de un estado degradado para el clúster. Las alertas incluyen la información que necesita para responder a un estado del sistema degradado.

Si el estado es degradado, puede ver detalles del problema, incluidas la causa probable y las acciones de recuperación recomendadas. Después de resolver el problema, el estado del sistema vuelve automáticamente a OK.

El estado del sistema refleja varios monitores de estado independientes. Un estado degradado en un monitor de estado individual provoca un estado degradado para el estado general del sistema.

Si quiere más información sobre cómo ONTAP admite los switches de clúster para supervisar el estado del sistema en el clúster, puede consultar el *Hardware Universe*.

["Los switches compatibles del Hardware Universe"](#)

Para obtener información detallada sobre las causas de los mensajes de AutoSupport del monitor de estado del switch de clúster (CSHM) y las acciones necesarias para resolver estas alertas, consulte el artículo de la base de conocimientos.

["Mensaje de AutoSupport: Proceso del monitor de estado CSHM"](#)

Cómo funciona la supervisión del estado

Los monitores de estado individuales tienen un conjunto de políticas que activan alertas cuando se dan ciertas condiciones. Comprender cómo funciona la supervisión del estado puede ayudarle a responder a problemas y controlar alertas futuras.

La supervisión del estado consta de los siguientes componentes:

- Monitores de salud individuales para subsistemas específicos, cada uno de los cuales tiene su propio estado de salud

Por ejemplo, el subsistema de almacenamiento tiene un monitor de estado de conectividad de nodo.

- Un monitor de estado general del sistema que consolida el estado de los monitores de estado individuales

Un estado degradado en cualquier subsistema único da como resultado un estado degradado para todo el sistema. Si ningún subsistema tiene alertas, el estado general del sistema es correcto.

Cada monitor de estado se compone de los siguientes elementos clave:

- Alertas que el monitor de estado puede generar potencialmente

Cada alerta tiene una definición, que incluye detalles como la gravedad de la alerta y su causa probable.

- Políticas de estado que identifican cuándo se activa cada alerta

Cada política de mantenimiento tiene una expresión de regla, que es la condición o cambio exactos que desencadena la alerta.

Un monitor de estado supervisa y valida continuamente los recursos en su subsistema para comprobar la condición o los cambios de estado. Cuando un cambio de condición o estado coincide con una expresión de regla de una política de estado, el monitor de estado genera una alerta. Una alerta hace que el estado del subsistema y su estado general del sistema se degraden.

Formas de responder a las alertas de estado del sistema

Cuando se produce una alerta de estado del sistema, puede reconocerla, obtener más información sobre él, reparar la condición subyacente y evitar que vuelva a producirse.

Cuando un monitor de estado genera una alerta, puede responder de cualquiera de las siguientes maneras:

- Obtenga información sobre la alerta, que incluye el recurso afectado, la gravedad de la alerta, la causa probable, el posible efecto y las acciones correctivas.
- Obtenga información detallada sobre la alerta, como el momento en que se planteó la alerta y si alguien más ya ha reconocido dicha alerta.
- Obtenga información relacionada con el estado del recurso o subsistema afectado, como una bandeja o un disco específicos.
- Reconozca la alerta para indicar que alguien está trabajando en el problema e identifíquese como el "acusador".
- Resuelva el problema siguiendo las acciones correctivas proporcionadas en la alerta, como la corrección de cableado para resolver un problema de conectividad.
- Elimine la alerta si el sistema no la borró automáticamente.
- Suprime una alerta para evitar que afecte al estado de un subsistema.

La supresión es útil cuando se entiende un problema. Después de suprimir una alerta, todavía puede ocurrir, pero el estado del subsistema se muestra como "ok-with-suppress". cuando se produce la alerta suprimida.

Personalización de alertas de estado del sistema

Puede controlar qué alertas genera un monitor de estado mediante la habilitación y la deshabilitación de las políticas de estado del sistema que definen cuándo se activan las alertas. Esto le permite personalizar el sistema de control del estado para su entorno concreto.

Puede obtener más información sobre el nombre de una política mediante la visualización de información detallada sobre una alerta generada o la visualización de definiciones de políticas para un monitor de estado, nodo o ID de alerta específicos.

Deshabilitar políticas de estado es diferente de suprimir alertas. Cuando se suprime una alerta, esta no afecta al estado del subsistema, pero aún puede aparecer la alerta.

Si deshabilita una política, la condición o el estado definidos en la expresión de regla de política ya no activan una alerta.

Ejemplo de una alerta que desea deshabilitar

Por ejemplo, supongamos que se produce una alerta que no le resulta útil. Utilice la `system health alert show -instance` Comando para obtener el ID de política de la alerta. El ID de política se utiliza en la `system health policy definition show` comando para ver información acerca de la política. Después de revisar la expresión de regla y otra información acerca de la directiva, decide deshabilitar la directiva. Utilice la `system health policy definition modify` comando para deshabilitar la política.

Cómo activan las alertas de estado los mensajes y eventos de AutoSupport

Las alertas de estado del sistema activan mensajes y eventos de AutoSupport en el sistema de gestión de eventos (EMS), lo que permite supervisar el estado del sistema mediante mensajes de AutoSupport y EMS, además de utilizar el sistema de supervisión de estado directamente.

El sistema envía un mensaje de AutoSupport dentro de los cinco minutos posteriores a una alerta. El mensaje AutoSupport incluye todas las alertas generadas desde el mensaje de AutoSupport anterior, a excepción de las alertas que duplican una alerta para el mismo recurso y la misma causa probable en la semana anterior.


Algunas alertas no activan mensajes de AutoSupport. Una alerta no activa un mensaje de AutoSupport si su política de estado deshabilita el envío de mensajes de AutoSupport. Por ejemplo, una directiva de estado podría deshabilitar los mensajes de AutoSupport de forma predeterminada porque AutoSupport ya genera un mensaje cuando se produce el problema. Puede configurar directivas para que no activen mensajes AutoSupport mediante el `system health policy definition modify` comando.

Puede ver una lista de todos los mensajes de AutoSupport activados por alertas enviados en la semana anterior mediante el `system health autosupport trigger history show` comando.

Las alertas también activan la generación de eventos en el EMS. Se genera un evento cada vez que se crea una alerta y se borra cada vez que se borra una alerta.

Monitores de estado del clúster disponibles

Existen varios monitores de estado que supervisan diferentes partes de un clúster. Los monitores de estado le ayudan a recuperarse de errores en sistemas ONTAP mediante la detección de eventos, el envío de alertas a usted y la eliminación de eventos según los borre.

Nombre del monitor de estado (identificador)	Nombre del subsistema (identificador)	Específico
Switch de clúster (switch de clúster)	Switch (Switch-Health)	<p>Supervisa los switches de red de clúster y los switches de red de gestión para obtener temperatura, utilización, configuración de interfaces, redundancia (solo switches de red de clúster) y funcionamiento de suministro de alimentación y ventilador. El monitor de estado del switch del clúster se comunica con los switches a través de SNMP. SNMPv2c es el valor predeterminado.</p> <div>  <p>A partir de ONTAP 9.2, este monitor puede detectar y generar informes cuando se ha reiniciado un switch de clúster desde el último periodo de sondeo.</p> </div>
Estructura MetroCluster	Conmutador	Supervisa la topología de la estructura del back-end de la configuración de MetroCluster y detecta mala configuración como el cableado y la división en zonas incorrectas y los fallos de ISL.
MetroCluster Salud	Interconexión, RAID y almacenamiento	Supervisa los adaptadores FC-VI, los adaptadores del iniciador FC, los agregados y discos subyacentes y los puertos entre clústeres
Conectividad de nodo (conexión por nodo)	Operaciones no disruptivas de CIFS (CIFS-NDO)	Supervisa conexiones SMB para proporcionar operaciones no disruptivas a aplicaciones de Hyper-V.
Almacenamiento (conexión SAS)	Supervisa las bandejas, los discos y los adaptadores a nivel de nodo para obtener las rutas y conexiones adecuadas.	Sistema

Nombre del monitor de estado (identificador)	Nombre del subsistema (identificador)	Específico
no aplicable	Agrega información de otros monitores de estado.	Conectividad del sistema (conexión del sistema)

Reciba alertas de estado del sistema automáticamente

Puede ver manualmente las alertas de estado del sistema usando la `system health alert show` comando. Sin embargo, debe suscribirse a mensajes específicos de Event Management System (EMS) para recibir notificaciones automáticamente cuando un monitor de estado genera una alerta.

Acerca de esta tarea

En el siguiente procedimiento se muestra cómo configurar notificaciones para todos los mensajes `hm.alert.levantados` y todos los mensajes `hm.alert.borrados`.

Todos los mensajes `hm.alert.levantados` y todos los mensajes `hm.alert.borrados` incluyen una captura SNMP. Los nombres de las capturas SNMP son `HealthMonitorAlertRaised` y `HealthMonitorAlertCleared`. Para obtener información acerca de las capturas SNMP, consulte *Network Management Guide*.

Pasos

1. Utilice la `event destination create` Comando para definir el destino al que desea enviar mensajes de EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilice la `event route add-destinations` comando para enrutar la `hm.alert.raised` y el `hm.alert.cleared` mensaje a un destino.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Información relacionada

["Gestión de redes"](#)

Responda al estado degradado del sistema

Cuando el estado del sistema es degradado, puede mostrar alertas, leer acerca de la causa probable y acciones correctivas, mostrar información sobre el subsistema degradado y resolver el problema. También se muestran alertas suprimidas para que pueda modificarlas y ver si se han reconocido.

Acerca de esta tarea

Puede detectar que se generó una alerta mediante un mensaje de AutoSupport o un evento de EMS, o mediante el `system health` comandos.

Pasos

1. Utilice la `system health alert show` comando para ver las alertas que están afectando al estado del sistema.
2. Lea la causa probable, el posible efecto y las acciones correctivas de la alerta para determinar si puede resolver el problema o necesita más información.
3. Si necesita más información, utilice `system health alert show -instance` comando para ver información adicional disponible para la alerta.
4. Utilice la `system health alert modify` con el `-acknowledge` parámetro para indicar que está trabajando en una alerta específica.
5. Tome medidas correctivas para resolver el problema como se describe en `Corrective Actions` campo de la alerta.

Las acciones correctivas pueden incluir reiniciar el sistema.

Cuando se resuelve el problema, la alerta se borra automáticamente. Si el subsistema no tiene otras alertas, el estado del subsistema cambia a. OK. Si el estado de todos los subsistemas es correcto, el estado general del sistema cambia a. OK.

6. Utilice la `system health status show` comando para confirmar que el estado del sistema es OK.

Si el estado del sistema no es OK, repetir este procedimiento.

Ejemplo de respuesta al estado degradado del sistema

Al revisar un ejemplo específico de estado del sistema degradado causado por una bandeja que carece de dos rutas a un nodo, puede ver lo que muestra la CLI cuando responde a una alerta.

Después de iniciar ONTAP, compruebe el estado del sistema y detecte que el estado es degradado:

```
cluster1::>system health status show
Status
-----
degraded
```

Muestra las alertas para averiguar dónde está el problema y ver que la bandeja 2 no tiene dos rutas al nodo 1:


```
cluster1::>system health alert show
      Node: node1
      Resource: Shelf ID 2
      Severity: Major
      Indication Time: Mon Nov 10 16:48:12 2013
      Probable Cause: Disk shelf 2 does not have two paths to controller
                      node1.
      Possible Effect: Access to disk shelf 2 via controller node1 will be
                      lost with a single hardware component failure (e.g.
                      cable, HBA, or IOM failure).
      Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert persists.
```

Se muestran detalles de la alerta para obtener más información, incluido el ID de alerta:

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
    Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
    hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
    Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
    Alerting Resource Name: Shelf ID 2

```

Reconoce la alerta para indicar que está trabajando en ella.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

Fije el cableado entre la bandeja 2 y la nodo 1 y, a continuación, reinicie el sistema. Luego, vuelva a comprobar el estado del sistema y compruebe que el estado es OK:

```
cluster1::>system health status show
Status
-----
OK
```

Configurar la detección de switches de red de gestión y clústeres

El monitor de estado del switch de clúster intenta automáticamente detectar los switches de red de gestión y clúster mediante el protocolo de detección de Cisco (CDP). Debe configurar el monitor de estado si no puede detectar automáticamente un switch o si no desea usar CDP para la detección automática.

Acerca de esta tarea

La `system cluster-switch show` el comando enumera los switches que detectó el monitor de estado. Si no ve un switch que esperaba ver en esa lista, el monitor de estado no podrá detectarlo automáticamente.

Pasos

1. Si desea utilizar CDP para la detección automática, haga lo siguiente:

a. Asegúrese de que el protocolo de descubrimiento de Cisco (CDP) está habilitado en los switches.

Consulte la documentación de su switch para obtener instrucciones.

b. Ejecute el siguiente comando en cada nodo del clúster para verificar si CDP está habilitado o deshabilitado:

```
run -node node_name -command options cdpd.enable
```

Si CDP está habilitado, vaya al paso d. Si CDP está desactivado, vaya al paso c.

c. Ejecute el siguiente comando para habilitar CDP:

```
run -node node_name -command options cdpd.enable on
```

Espere cinco minutos antes de pasar al siguiente paso.

a. Utilice la `system cluster-switch show` Para verificar si ONTAP ahora puede detectar automáticamente los switches.

2. Si el monitor de estado no puede detectar automáticamente un switch, use el `system cluster-switch create` comando para configurar la detección del switch:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Espere cinco minutos antes de pasar al siguiente paso.

3. Utilice la `system cluster-switch show` Comando para verificar que ONTAP puede detectar el switch al que ha añadido información.

Después de terminar

Compruebe que el monitor de estado puede supervisar los switches.

Compruebe la supervisión de los switches de red de clúster y de gestión

El monitor de estado del switch de clúster intenta supervisar automáticamente los switches que detecta; sin embargo, es posible que la supervisión no se produzca de manera automática si los switches no se han configurado correctamente. Debe verificar que el monitor de estado esté correctamente configurado para supervisar los switches.

Pasos

1. Para identificar los switches que detectó el monitor de estado del switch del clúster, introduzca el siguiente comando:

ONTAP 9,8 y versiones posteriores

```
system switch ethernet show
```

ONTAP 9,7 y anteriores

```
system cluster-switch show
```

Si la `Model` columna muestra el valor `OTHER`, Entonces ONTAP no puede supervisar el conmutador. ONTAP establece el valor en `OTHER` si un switch que detecta automáticamente no es compatible con la supervisión del estado.



Si un switch no se muestra en el resultado del comando, debe configurar la detección del switch.

2. Actualice al software de switch más reciente admitido y consulte el archivo de configuración (RCF) desde el sitio de soporte de NetApp.

["Página de descargas de soporte de NetApp"](#)

La cadena de comunidad en el RCF del conmutador debe coincidir con la cadena de comunidad que el monitor de estado está configurado para utilizar. De forma predeterminada, el monitor de estado utiliza la cadena de comunidad `cshml!`.



En este momento, el monitor de estado sólo admite SNMPv2.

Si necesita cambiar información sobre un switch que supervisa el clúster, puede modificar la cadena de comunidad que utiliza el monitor de estado mediante el siguiente comando:

ONTAP 9,8 y versiones posteriores

```
system switch ethernet modify
```

ONTAP 9,7 y anteriores

```
system cluster-switch modify
```

3. Compruebe que el puerto de gestión del switch está conectado a la red de gestión.

Esta conexión es necesaria para realizar consultas SNMP.

Comandos para supervisar el estado del sistema

Puede utilizar el `system health` comandos para mostrar información sobre el estado de los recursos del sistema, responder a las alertas y configurar alertas futuras. El uso de los comandos de la CLI le permite ver información en profundidad sobre la configuración del control del estado. Las páginas de manual de los comandos contienen más información.

Mostrar el estado del estado del sistema

Si desea...	Se usa este comando...
Muestre el estado del sistema, que refleja el estado general de cada monitor de estado	<code>system health status show</code>
Mostrar el estado de los subsistemas para los que está disponible la supervisión de estado	<code>system health subsystem show</code>

Mostrar el estado de conectividad de los nodos

Si desea...	Se usa este comando...
Muestra detalles acerca de la conectividad del nodo a la bandeja de almacenamiento, incluida la información de puertos, la velocidad del puerto de HBA, el rendimiento de I/O y la tasa de operaciones de I/O por segundo	<code>storage shelf show -connectivity</code> Utilice la <code>-instance</code> para mostrar información detallada de cada bandeja.
Muestra información sobre las unidades y los LUN de cabina, incluidos el espacio utilizable, los números de bandeja y bahía y el nombre del nodo propietario	<code>storage disk show</code> Utilice la <code>-instance</code> parámetro para mostrar información detallada acerca de cada unidad.

Si desea...	Se usa este comando...
Muestra información detallada sobre los puertos de las bandejas de almacenamiento, incluido el tipo de puerto, la velocidad y el estado	<pre>storage port show</pre> <p>Utilice la <code>-instance</code> parámetro para mostrar información detallada sobre cada adaptador.</p>

Gestionar la detección de switches de redes de gestión, almacenamiento y clúster

Si desea...	Utilice este comando. (ONTAP 9.8 y posterior)	Utilice este comando. (ONTAP 9.7 y anterior)
Muestre los switches que supervisa el clúster	<pre>system switch ethernet show</pre>	<pre>system cluster-switch show</pre>
Muestre los switches que el clúster supervisa actualmente, incluidos los switches que ha eliminado (que se muestran en la columna motivo del resultado del comando), y la información de configuración que necesita para el acceso de red a los switches de red de gestión y clúster. Este comando solo está disponible en el nivel de privilegios avanzado.	<pre>system switch ethernet show-all</pre>	<pre>system cluster-switch show-all</pre>
Configurar la detección de un switch no detectado	<pre>system switch ethernet create</pre>	<pre>system cluster-switch create</pre>
Modificar la información sobre un conmutador que supervisa el clúster (por ejemplo, nombre de dispositivo, dirección IP, versión SNMP y cadena de comunidad)	<pre>system switch ethernet modify</pre>	<pre>system cluster-switch modify</pre>
Desactive la supervisión de un interruptor	<pre>system switch ethernet modify -disable-monitoring</pre>	<pre>system cluster-switch modify -disable-monitoring</pre>
Desactive la detección y supervisión de un switch y elimine la información de configuración del switch	<pre>system switch ethernet delete</pre>	<pre>system cluster-switch delete</pre>

Si desea...	Utilice este comando. (ONTAP 9.8 y posterior)	Utilice este comando. (ONTAP 9.7 y anterior)
Eliminar permanentemente la información de configuración del conmutador almacenada en la base de datos (al hacerlo se vuelve a activar el descubrimiento automático del conmutador)	<code>system switch ethernet delete -force</code>	<code>system cluster-switch delete -force</code>
Active el registro automático para que se envíe con mensajes de AutoSupport.	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>




Responda a alertas generadas

Si desea...	Se usa este comando...
Muestra información sobre las alertas generadas, como el recurso y el nodo donde se activó la alerta, y la gravedad y la causa probable de la alerta	<code>system health alert show</code>
Muestra información sobre cada alerta generada	<code>system health alert show -instance</code>
Indique que alguien está trabajando en una alerta	<code>system health alert modify</code>
Reconozca una alerta	<code>system health alert modify -acknowledge</code>
Suprimir una alerta posterior para que no afecte al estado de un subsistema	<code>system health alert modify -suppress</code>
Eliminar una alerta que no se borró automáticamente	<code>system health alert delete</code>
Muestra información sobre los mensajes de AutoSupport que se han activado en la última semana, por ejemplo, para determinar si una alerta ha activado un mensaje de AutoSupport	<code>system health autosupport trigger history show</code>

Configurar alertas futuras

Si desea...	Se usa este comando...
Habilite o deshabilite la política que controla si un estado de recurso específico genera una alerta específica	<code>system health policy definition modify</code>

Muestra información acerca de cómo se configura la supervisión del estado

Si desea...	Se usa este comando...
Muestra información acerca de los monitores de estado, como sus nodos, nombres, subsistemas y estado	<pre>system health config show</pre> <div><p>Utilice la <code>-instance</code> parámetro para mostrar información detallada sobre cada monitor de estado.</p></div>
Muestre información sobre las alertas que un monitor de estado puede generar potencialmente	<pre>system health alert definition show</pre> <div><p>Utilice la <code>-instance</code> parámetro para mostrar información detallada sobre cada definición de alerta.</p></div>
Muestra información sobre las políticas de control de estado, que determinan cuándo se generan las alertas	<pre>system health policy definition show</pre> <div><p>Utilice la <code>-instance</code> parámetro para mostrar información detallada de cada política. Utilice otros parámetros para filtrar la lista de alertas, por ejemplo, el estado de la política (habilitada o no), el monitor de estado, las alertas, etc.</p></div>

Muestra información del entorno

Los sensores le ayudan a supervisar los componentes medioambientales de su sistema. La información que puede mostrar acerca de los sensores medioambientales incluye sus advertencias de tipo, nombre, estado, valor y umbral.

Paso

1. Para mostrar la información de los sensores medioambientales, utilice `system node environment sensors show` comando.

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.