Recuperación de fallos del nodo de administrador principal

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-115/maintain/copying-audit-logs-from-failed-primary-admin-node.html on October 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Recuperación de fallos del nodo de administrador principal . . . 1
- Al copiar los registros de auditoría del nodo de administración principal con errores . . . 1
- Reemplace el nodo de administrador principal . . . 2
- Configurar el nodo de administrador principal de reemplazo . . . 3
- Restaurar el registro de auditoría en el nodo de administración primario recuperado . . . 5
- Restablecer el emisor preferido en el nodo de administración principal recuperado . . . 6
- Restaurar la base de datos de nodos de administrador cuando se recupera un nodo de administrador principal . . . 6
- Restaurar las métricas de Prometheus al recuperar un nodo de administración principal . . . 8

Recuperación de fallos del nodo de administrador principal

Debe completar un conjunto específico de tareas para recuperar el sistema después de un fallo en un nodo de administrador principal. El nodo de administrador principal aloja el servicio Configuration Management Node (CMN) de la cuadrícula.

Acerca de esta tarea

Un nodo de administrador principal con fallos se debe reemplazar inmediatamente. El servicio nodo de gestión de configuración (CMN) del nodo de administración principal es responsable de emitir bloques de identificadores de objetos para la cuadrícula. Estos identificadores se asignan a los objetos a medida que se ingieren. Los objetos nuevos no se pueden procesar a menos que haya identificadores disponibles. La ingesta de objetos puede continuar mientras el CMN no está disponible porque el suministro de identificadores de aproximadamente un mes se almacena en caché en la cuadrícula. Sin embargo, después de que se agoten los identificadores almacenados en caché, no es posible añadir objetos nuevos.

> Debe reparar o sustituir un nodo de administrador principal con fallos dentro de un mes aproximadamente, o bien el grid podría perder su capacidad de procesar objetos nuevos. El período de tiempo exacto depende de la tasa de ingesta de objetos: Si necesita una evaluación más precisa del plazo para el grid, póngase en contacto con el soporte técnico.

Pasos

- "Al copiar los registros de auditoría del nodo de administración principal con errores"
- "Reemplace el nodo de administrador principal"
- "Configurar el nodo de administrador principal de reemplazo"
- "Restaurar el registro de auditoría en el nodo de administración primario recuperado"
- "Restablecer el emisor preferido en el nodo de administración principal recuperado"
- "Restaurar la base de datos de nodos de administrador cuando se recupera un nodo de administrador principal"
- "Restaurar las métricas de Prometheus al recuperar un nodo de administración principal"

Al copiar los registros de auditoría del nodo de administración principal con errores

Si puede copiar registros de auditoría del nodo de administración principal con errores, debe conservarlos para mantener el registro de la cuadrícula de la actividad y el uso del sistema. Es posible restaurar los registros de auditoría conservados al nodo administrador principal recuperado después de que esté activo y en ejecución.

Este procedimiento copia los archivos de registro de auditoría del nodo de administración con errores en una ubicación temporal en un nodo de grid independiente. Estos registros de auditoría conservados se pueden copiar en el nodo admin de reemplazo. Los registros de auditoría no se copian automáticamente al nuevo nodo de administración.

Según el tipo de error, es posible que no se puedan copiar los registros de auditoría de un nodo administrador con errores. Si la implementación solo tiene un nodo de administrador, el nodo de administrador recuperado

inicia la grabación de eventos en el registro de auditoría en un nuevo archivo vacío y se pierden datos registrados previamente. Si la implementación incluye más de un nodo de administrador, puede recuperar los registros de auditoría desde otro nodo de administración.

> Si no se puede acceder a los registros de auditoría en el nodo administrador con errores ahora, es posible que pueda acceder a ellos más adelante, por ejemplo, después de la recuperación del host.

1. Inicie sesión en el nodo de administrador con errores si es posible. De lo contrario, inicie sesión en el nodo de administración principal u otro nodo de administración, si está disponible.
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
2. Detenga el servicio AMS para evitar que cree un nuevo archivo de registro:`service ams stop`
3. Cambie el nombre del archivo audit.log para que no sobrescriba el archivo existente al copiarlo al nodo de administración recuperado.

   Cambie el nombre de audit.log por un nombre de archivo numerado único como aaaa-mm-dd.txt.1. Por ejemplo, puede cambiar el nombre del archivo audit.log a 2015-10-25.txt.1`cd /var/local/audit/export/`
4. Reinicie el servicio AMS: `service ams start`
5. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula independiente: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Cuando se lo pida, introduzca la contraseña de administrador.
6. Copie todos los archivos del registro de auditoría: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Cuando se lo pida, introduzca la contraseña de administrador.
7. Cerrar sesión como raíz: `exit`

Reemplace el nodo de administrador principal

Para recuperar un nodo de administrador principal, primero es necesario reemplazar el hardware físico o virtual.

Puede reemplazar un nodo de administración principal con fallos por un nodo de administración principal que se ejecute en la misma plataforma, o bien puede reemplazar un nodo de administración principal que se ejecute en VMware o un host Linux por un nodo de administración principal alojado en un dispositivo de servicios.

Utilice el procedimiento que coincida con la plataforma de reemplazo seleccionada para el nodo. Una vez completado el procedimiento de sustitución de nodo (que es adecuado para todos los tipos de nodos), dicho procedimiento le dirigirá al siguiente paso para la recuperación del nodo de administración principal.

Plataforma de sustitución	Procedimiento
VMware	"Reemplazar un nodo VMware"
Linux	"Reemplazar un nodo Linux"
Servicios de aplicaciones SG100 y SG1000	"Sustitución de un dispositivo de servicios"
OpenStack	Las operaciones de recuperación ya no son compatibles con los archivos de disco de máquinas virtuales y los scripts de OpenStack que proporciona NetApp. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para el sistema operativo Linux. A continuación, siga el procedimiento para reemplazar un nodo Linux.

Configurar el nodo de administrador principal de reemplazo

El nodo de reemplazo debe configurarse como nodo de administrador principal para el sistema StorageGRID.

Lo que necesitará

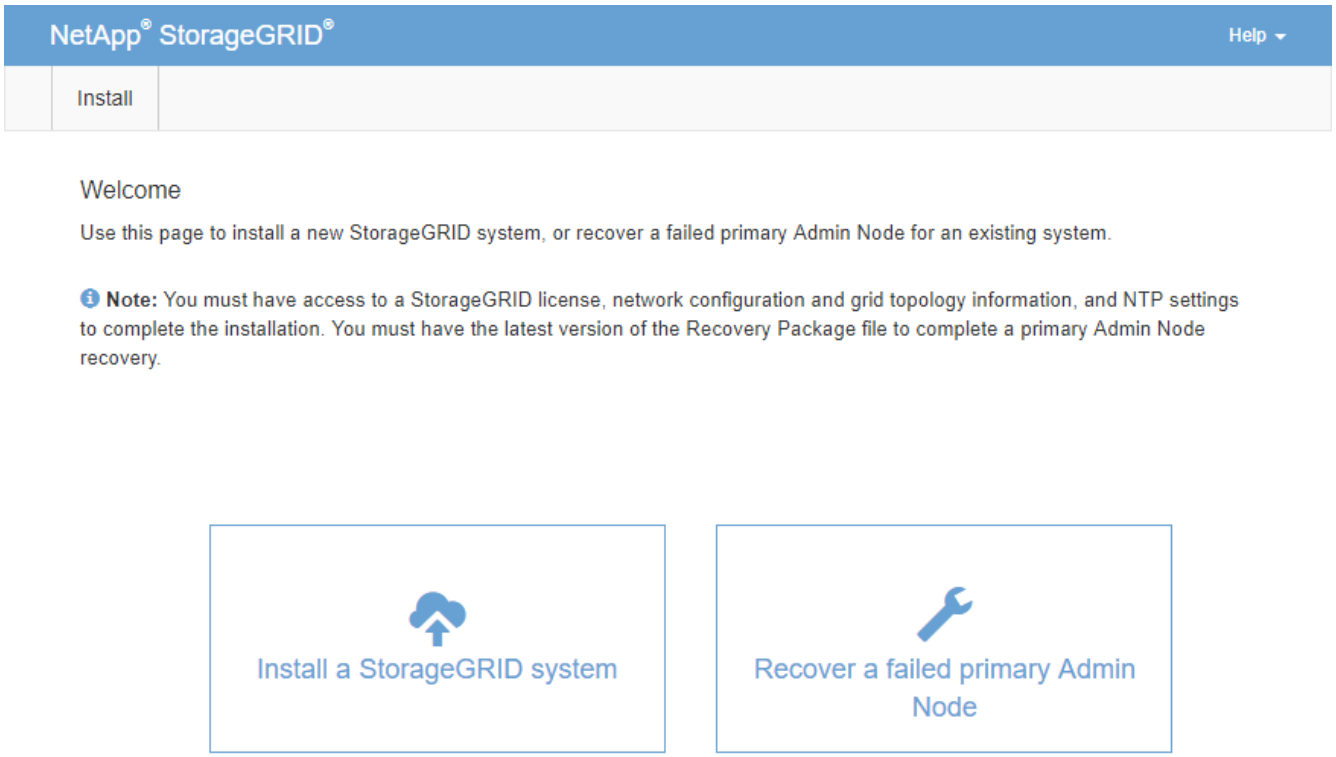
- Para los nodos de administración principales alojados en máquinas virtuales, la máquina virtual debe ponerse en marcha, encenderse e inicializarse.
- En el caso de los nodos de administrador principales alojados en un dispositivo de servicios, ha sustituido el dispositivo y ha instalado software. Consulte la guía de instalación del aparato.

  "SG100 servicios de aplicaciones SG1000"

- Debe tener el último backup del archivo de paquete de recuperación (`sgws-recovery-package-`*`id-revision`*`.zip`).
- Debe tener la clave de acceso de aprovisionamiento.

Pasos

1. Abra el explorador web y vaya a. `https://primary_admin_node_ip`.



2. Haga clic en **recuperar un nodo de administración principal con errores**.
3. Cargue la copia de seguridad más reciente del paquete de recuperación:
   a. Haga clic en **examinar**.
   b. Busque el archivo más reciente del paquete de recuperación para su sistema StorageGRID y haga clic en **Abrir**.
4. Introduzca la clave de acceso de aprovisionamiento.
5. Haga clic en **Iniciar recuperación**.

   Se inicia el proceso de recuperación. Es posible que Grid Manager no esté disponible durante unos minutos a medida que se inician los servicios necesarios. Una vez finalizada la recuperación, se muestra la página de inicio de sesión.

6. Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID y la confianza de la parte que confía para el nodo de administración que ha recuperado se configuró para utilizar el certificado de servidor de interfaz de gestión predeterminado, actualice (o elimine y vuelva a crear) la confianza de la parte que confía en el nodo en los Servicios de Federación de Active Directory (AD FS). Utilice el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.

   Para configurar la confianza de una parte de confianza, consulte las instrucciones para administrar StorageGRID. Para acceder al certificado de servidor predeterminado, inicie sesión en el shell de comandos del nodo de administración. Vaya a la `/var/local/mgmt-api` y seleccione el `server.crt` archivo.

7. Determine si necesita aplicar una revisión.
   a. Inicie sesión en Grid Manager con un navegador compatible.

b. Seleccione **Nodes**.

c. En la lista de la izquierda, seleccione el nodo de administración principal.

d. En la ficha Descripción general, observe la versión que aparece en el campo **Versión de software**.

e. Seleccione cualquier otro nodo de grid.

f. En la ficha Descripción general, observe la versión que aparece en el campo **Versión de software**.

- Si las versiones mostradas en los campos **Versión de software** son las mismas, no es necesario aplicar una revisión.
- Si las versiones que aparecen en los campos **Versión de software** son diferentes, debe aplicar una revisión para actualizar el nodo de administración principal recuperado a la misma versión.

Información relacionada

"Administre StorageGRID"

"Procedimiento de revisión de StorageGRID"

Restaurar el registro de auditoría en el nodo de administración primario recuperado

Si pudo conservar el registro de auditoría del nodo de administrador primario con errores, puede copiarlo al nodo de administrador principal que se está recuperando.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- Debe haber copiado los registros de auditoría en otra ubicación una vez que se produjo un error en el nodo de administración original.

Si falla un nodo de administrador, los registros de auditoría guardados en ese nodo de administrador se perderán potencialmente. Es posible conservar los datos que no se perderán al copiar los registros de auditoría del nodo administrador con errores y luego restaurar estos registros de auditoría en el nodo de administrador recuperado. Según el error, es posible que no se puedan copiar los registros de auditoría del nodo administrador con errores. En ese caso, si la implementación tiene más de un nodo de administración, puede recuperar los registros de auditoría de otro nodo de administración a medida que se replican los registros de auditoría a todos los nodos de administrador.

Si solo hay un nodo de administrador y el registro de auditoría no se puede copiar desde el nodo con errores, el nodo de administrador recuperado inicia el registro de eventos en el registro de auditoría como si la instalación es nueva.

Debe recuperar una Lo antes posible. de nodo de administrador para restaurar la funcionalidad de registro.

1. Inicie sesión en el nodo de administración recuperado:

   a. Introduzca el siguiente comando: `ssh admin@recovery_Admin_Node_IP`

   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Después de iniciar sesión como raíz, el símbolo del sistema cambia de `$` para `#`.

2. Compruebe qué archivos de auditoría se han conservado: `cd /var/local/audit/export`
3. Copie los archivos de registro de auditoría conservados en el nodo admin recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Cuando se lo pida, introduzca la contraseña de administrador.
4. Por motivos de seguridad, elimine los registros de auditoría del nodo de grid con errores después de verificar que se han copiado correctamente al nodo de administrador recuperado.
5. Actualice la configuración de usuario y grupo de los archivos de registro de auditoría en el nodo de administración recuperado: `chown ams-user:bycast *`
6. Cerrar sesión como raíz: `exit`

También debe restaurar cualquier acceso de cliente preexistente al recurso compartido de auditoría. Para obtener más información, consulte las instrucciones para administrar StorageGRID.

Información relacionada

"Administre StorageGRID"

Restablecer el emisor preferido en el nodo de administración principal recuperado

Si el nodo de administrador principal que se está recuperando está establecido actualmente como remitente preferido de notificaciones de alerta, notificaciones de alarma y mensajes de AutoSupport, debe volver a configurar este valor.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- El nodo de administrador recuperado debe estar instalado y en ejecución.

Pasos

1. Seleccione **Configuración** > **Configuración del sistema** > **Opciones de pantalla**.
2. Seleccione el nodo de administración recuperado de la lista desplegable **remitente preferido**.
3. Haga clic en **aplicar cambios**.

Información relacionada

"Administre StorageGRID"

Restaurar la base de datos de nodos de administrador cuando se recupera un nodo de administrador principal

Si desea conservar la información histórica sobre atributos, alarmas y alertas en un nodo de administración principal que tenga errores, puede restaurar la base de datos del nodo de administración. Solo puede restaurar esta base de datos si el sistema StorageGRID incluye otro nodo de administración.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- El sistema StorageGRID debe incluir al menos dos nodos de administración.
- Debe tener la `Passwords.txt` archivo.
- Debe tener la clave de acceso de aprovisionamiento.

Si falla un nodo de administrador, se pierde la información histórica almacenada en su base de datos de nodos de administrador. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Historial de alarmas
- Datos históricos de atributos, que se utilizan en los gráficos e informes de texto disponibles en la página **Support Tools Grid Topology**.

Cuando se recupera un nodo de administrador, el proceso de instalación del software crea una base de datos vacía Admin Node en el nodo recuperado. Sin embargo, la nueva base de datos sólo incluye información sobre servidores y servicios que actualmente forman parte del sistema o que se agregan más adelante.

Si restauró un nodo de administrador principal y el sistema StorageGRID tiene otro nodo de administración, puede restaurar la información histórica copiando la base de datos del nodo de administración desde un nodo de administración no primario (el *Source Admin Node*) en el nodo de administración primario recuperado. Si el sistema solo tiene un nodo de administrador principal, no puede restaurar la base de datos del nodo de administración.

> La copia de la base de datos del nodo de administración puede llevar varias horas. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración de origen.

1. Inicie sesión en el nodo de administrador de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Desde el nodo de administración de origen, detenga el servicio MI: `service mi stop`
3. En el nodo de administración de origen, detenga el servicio de la interfaz de programa de aplicaciones de gestión (API de gestión): `service mgmt-api stop`
4. Complete los siguientes pasos en el nodo de administración recuperado:
   a. Inicie sesión en el nodo de administración recuperado:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Detenga EL servicio MI: `service mi stop`
   c. Detenga el servicio API de gestión: `service mgmt-api stop`

d. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`

e. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

f. Copie la base de datos del nodo de administración de origen al nodo de administración recuperado: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Cuando se le solicite, confirme que desea sobrescribir la base DE datos MI en el nodo de administración recuperado.

   La base de datos y sus datos históricos se copian en el nodo de administración recuperado. Una vez realizada la operación de copia, el script inicia el nodo de administración recuperado.

h. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`

5. Reinicie los servicios en el nodo de administración de origen: `service servermanager start`

Restaurar las métricas de Prometheus al recuperar un nodo de administración principal

De manera opcional, puede conservar las métricas históricas que mantiene Prometheus en un nodo de administración principal que ha fallado. La métrica Prometheus solo se puede restaurar si su sistema StorageGRID incluye otro nodo de administración.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- El sistema StorageGRID debe incluir al menos dos nodos de administración.
- Debe tener la `Passwords.txt` archivo.
- Debe tener la clave de acceso de aprovisionamiento.

Si falla un nodo de administración, se pierden las métricas que se mantienen en la base de datos Prometheus del nodo de administración. Cuando recupera el nodo de administración, el proceso de instalación del software crea una nueva base de datos Prometheus. Una vez iniciado el nodo de administración recuperado, este registra las métricas como si hubiera realizado una nueva instalación del sistema StorageGRID.

Si restauró un nodo de administración principal y el sistema StorageGRID tiene otro nodo de administración, puede restaurar las métricas históricas copiando la base de datos Prometheus desde un nodo de administración no primario (el *source Admin Node*) en el nodo de administración principal recuperado. Si su sistema solo tiene un nodo de administración principal, no puede restaurar la base de datos Prometheus.

> La copia de la base de datos Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración de origen.

1. Inicie sesión en el nodo de administrador de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

2. Desde el nodo de administración de origen, detenga el servicio Prometheus: `service prometheus stop`
3. Complete los siguientes pasos en el nodo de administración recuperado:
    a. Inicie sesión en el nodo de administración recuperado:
        i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
        ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
        iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
        iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    b. Detenga el servicio Prometheus: `service prometheus stop`
    c. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`
    d. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.
    e. Copie la base de datos Prometheus del nodo de administración de origen al nodo de administración recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
    f. Cuando se le solicite, pulse **Intro** para confirmar que desea destruir la nueva base de datos Prometheus del nodo de administración recuperado.

        La base de datos Prometheus original y sus datos históricos se copian al nodo de administración recuperado. Una vez realizada la operación de copia, el script inicia el nodo de administración recuperado. Aparece el siguiente estado:

    Base de datos clonada, servicios de inicio

    a. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`
4. Reinicie el servicio Prometheus en el nodo de administración de origen.`service prometheus start`

Información de copyright

Copyright © 2025 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.