Endurecimiento del sistema

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-115/harden/hardening-storagegrid-system.html on October 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Endurecimiento del sistema . . . 1
Refuerzo de un sistema StorageGRID . . . 1
Consideraciones generales sobre el refuerzo de un sistema StorageGRID . . . 1
Directrices de refuerzo para las actualizaciones de software . . . 2
Actualice al software StorageGRID . . . 2
Actualizaciones a servicios externos . . . 2
Actualizaciones a hipervisores . . . 2
Actualizar a nodos Linux . . . 2
Directrices de refuerzo para redes de StorageGRID . . . 3
Directrices para la red Grid . . . 3
Directrices para la red de administración . . . 3
Directrices para la red de cliente . . . 3
Directrices de refuerzo para nodos de StorageGRID . . . 4
Configuración del firewall . . . 4
Virtualización, contenedores y hardware compartido . . . 4
Desactive los servicios no utilizados . . . 4
Proteja los nodos durante la instalación . . . 5
Directrices para los nodos de administrador . . . 5
Directrices para nodos de almacenamiento . . . 5
Directrices para los nodos de puerta de enlace . . . 6
Directrices para los nodos de dispositivos de hardware . . . 6
Directrices de refuerzo para certificados de servidor . . . 7
Otras directrices de endurecimiento . . . 8
Registros y mensajes de auditoría . . . 8
AutoSupport de NetApp . . . 8
Uso compartido de recursos de origen cruzado (CORS) . . . 9
Dispositivos de seguridad externos . . . 9

Endurecimiento del sistema

Conozca la configuración, las prácticas recomendadas y las recomendaciones del sistema para proteger un sistema StorageGRID de las amenazas de seguridad.

- "Refuerzo de un sistema StorageGRID"
- "Directrices de refuerzo para las actualizaciones de software"
- "Directrices de refuerzo para redes de StorageGRID"
- "Directrices de refuerzo para nodos de StorageGRID"
- "Directrices de refuerzo para certificados de servidor"
- "Otras directrices de endurecimiento"]

Refuerzo de un sistema StorageGRID

El endurecimiento del sistema es el proceso de eliminar tantos riesgos de seguridad como sea posible a través de un sistema StorageGRID.

Este documento proporciona una descripción general de las directrices generales específicas de StorageGRID. Estas directrices complementan las mejores prácticas estándar del sector para el endurecimiento del sistema. Por ejemplo, estas directrices asumen que utiliza contraseñas seguras para StorageGRID, utiliza HTTPS en lugar de HTTP y habilite la autenticación basada en certificados cuando esté disponible.

Al instalar y configurar StorageGRID, puede usar estas directrices para ayudarle a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad del sistema de información.

StorageGRID sigue la política de gestión de vulnerabilidades de *NetApp*. Las vulnerabilidades notificadas se verifican y se tratan de acuerdo con el proceso de respuesta a incidentes de seguridad del producto.

Consideraciones generales sobre el refuerzo de un sistema StorageGRID

Al reforzar un sistema StorageGRID, debe tener en cuenta lo siguiente:

- ¿Cuál de las tres redes StorageGRID que ha implementado? Todos los sistemas StorageGRID deben utilizar la red de cuadrícula, pero también puede utilizar la red de administración, la red de cliente o ambas. Cada red tiene diferentes consideraciones de seguridad.
- El tipo de plataformas que utiliza para los nodos individuales del sistema StorageGRID. Los nodos StorageGRID se pueden poner en marcha en máquinas virtuales VMware, en un contenedor Docker en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma tiene su propio conjunto de mejores prácticas de optimización.
- Qué confianza tienen las cuentas de inquilino. Si es un proveedor de servicios con cuentas de inquilino que no son de confianza, tendrá problemas de seguridad diferentes a si solo utiliza clientes internos de confianza.
- Los requisitos y convenciones de seguridad que siguen su organización. Es posible que deba cumplir requisitos normativos o corporativos específicos.

Información relacionada

"Política de manejo de vulnerabilidades"

Directrices de refuerzo para las actualizaciones de software

Debe mantener su sistema StorageGRID y los servicios relacionados actualizados para defender los ataques.

Actualice al software StorageGRID

Siempre que sea posible, debe actualizar el software StorageGRID a la versión principal más reciente o a la versión principal anterior. Mantener la StorageGRID actualizada ayuda a reducir la cantidad de tiempo que las vulnerabilidades conocidas están activas y reduce el área general de la superficie de ataque. Además, las versiones más recientes de StorageGRID a menudo contienen funciones de seguridad reforzada que no se incluyen en las versiones anteriores.

Cuando se necesita una corrección, NetApp prioriza la creación de actualizaciones para las versiones más recientes. Es posible que algunos parches no sean compatibles con versiones anteriores.

Para descargar las versiones y correcciones urgentes de StorageGRID más recientes, vaya a la página de descarga del software StorageGRID. Para obtener instrucciones paso a paso para actualizar el software StorageGRID, consulte las instrucciones para actualizar StorageGRID. Para obtener instrucciones sobre cómo aplicar una revisión, consulte las instrucciones de recuperación y mantenimiento.

Actualizaciones a servicios externos

Los servicios externos pueden tener vulnerabilidades que afectan indirectamente a StorageGRID. Debe asegurarse de que los servicios de los que depende StorageGRID se mantengan actualizados. Estos servicios incluyen LDAP, KMS (servidor KMIP o KMS), DNS y NTP.

Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

Actualizaciones a hipervisores

Si los nodos de StorageGRID se ejecutan en VMware u otro hipervisor, debe asegurarse de que el software y el firmware del hipervisor estén actualizados.

Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

Actualizar a nodos Linux

Si los nodos de StorageGRID utilizan plataformas host Linux, debe asegurarse de que las actualizaciones de seguridad y del kernel se apliquen al sistema operativo host. Además, debe aplicar actualizaciones de firmware al hardware vulnerable cuando estas actualizaciones estén disponibles.

Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

Información relacionada

"Descargas de NetApp: StorageGRID"

"Actualizar el software de"

"Mantener recuperar"

"Herramienta de matriz de interoperabilidad de NetApp"

Directrices de refuerzo para redes de StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Directrices para la red Grid

Debe configurar una red de red para todo el tráfico interno de StorageGRID. Todos los nodos de grid se encuentran en Grid Network, por lo que deben poder hablar con el resto de nodos.

Al configurar Grid Network, siga estas directrices:

- Asegúrese de que la red está protegida de clientes que no son de confianza, como los que están en Internet abierto.
- Cuando sea posible, utilice la red de red exclusiva para el tráfico interno. Tanto la red de administración como la red de cliente tienen restricciones de firewall adicionales que bloquean el tráfico externo a los servicios internos. Se admite el uso de Grid Network para el tráfico de clientes externos, pero este uso ofrece menos capas de protección.
- Si la implementación de StorageGRID abarca varios centros de datos, utilice una red privada virtual (VPN) o equivalente en la red de Grid para proporcionar protección adicional para el tráfico interno.
- Algunos procedimientos de mantenimiento requieren un acceso de shell seguro (SSH) en el puerto 22 entre el nodo de administrador principal y todos los demás nodos de grid. Use un firewall externo para restringir el acceso SSH a clientes de confianza.

Directrices para la red de administración

La red de administración suele utilizarse para tareas administrativas (empleados de confianza que utilizan Grid Manager o SSH) y para comunicarse con otros servicios de confianza como LDAP, DNS, NTP o KMS (o servidor KMIP). Sin embargo, StorageGRID no exige este uso interno.

Si utiliza la red de administración, siga estas directrices:

- Bloquee todos los puertos de tráfico internos en la red administrativa. Consulte la lista de puertos internos en la guía de instalación de su plataforma.
- Si los clientes que no son de confianza pueden acceder a la red de administración, bloquee el acceso a StorageGRID en la red de administración con un firewall externo.

Directrices para la red de cliente

La red de cliente suele utilizarse para los inquilinos y para comunicarse con servicios externos, como el servicio de replicación de CloudMirror o otro servicio de la plataforma. Sin embargo, StorageGRID no exige este uso interno.

Si está utilizando la red cliente, siga estas directrices:

- Bloquee todos los puertos de tráfico internos de la red cliente. Consulte la lista de puertos internos en la guía de instalación de su plataforma.

- Acepte tráfico de cliente entrante sólo en puntos finales configurados explícitamente. Consulte la información sobre la administración de redes de clientes que no son de confianza en las instrucciones para administrar StorageGRID.

Información relacionada

"Directrices de red"

"Imprimador de rejilla"

"Administre StorageGRID"

"Instale Red Hat Enterprise Linux o CentOS"

"Instalar Ubuntu o Debian"

"Instale VMware"

Directrices de refuerzo para nodos de StorageGRID

Los nodos StorageGRID se pueden poner en marcha en máquinas virtuales VMware, en un contenedor Docker en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma y cada tipo de nodo tiene su propio conjunto de prácticas recomendadas de endurecimiento.

Configuración del firewall

Como parte del proceso de endurecimiento del sistema, debe revisar las configuraciones de firewall externo y modificarlas para que el tráfico se acepte solo de las direcciones IP y en los puertos de los que se necesite estrictamente.

Los nodos que se ejecutan en plataformas VMware y dispositivos StorageGRID usan un firewall interno que se gestiona automáticamente. Aunque este firewall interno proporciona una capa adicional de protección contra algunas amenazas comunes, no elimina la necesidad de un firewall externo.

Para obtener una lista de todos los puertos internos y externos utilizados por StorageGRID, consulte la guía de instalación de su plataforma.

Virtualización, contenedores y hardware compartido

Para todos los nodos de StorageGRID, evite ejecutar StorageGRID en el mismo hardware físico que el software que no es de confianza. No asuma que las protecciones del hipervisor impedirán que el malware acceda a los datos protegidos con StorageGRID si tanto StorageGRID como el malware existen en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre aprovechan vulnerabilidades críticas en los procesadores modernos y permiten a los programas robar datos en memoria en el mismo equipo.

Desactive los servicios no utilizados

Para todos los nodos StorageGRID, debe deshabilitar o bloquear el acceso a los servicios que no se utilizan. Por ejemplo, si no tiene pensado configurar el acceso de cliente a los recursos compartidos de auditoría de CIFS o NFS, bloquee o deshabilite el acceso a estos servicios.

Proteja los nodos durante la instalación

No permita que los usuarios que no son de confianza accedan a los nodos de StorageGRID a través de la red cuando los nodos se están instalando. Los nodos no son totalmente seguros hasta que se han Unido a la cuadrícula.

Directrices para los nodos de administrador

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Cuando inicia sesión en el administrador de grid o en el administrador de inquilinos, se conecta a un nodo de administración.

Siga estas directrices para proteger los nodos de administrador en el sistema StorageGRID:

- Proteja todos los nodos de administrador de clientes que no son de confianza, como los que están en Internet abierto. Asegúrese de que ningún cliente que no sea de confianza puede acceder a un nodo de administración en la red de grid, la red de administración o la red de cliente.
- Los grupos StorageGRID controlan el acceso a las funciones de administrador de grid y administrador de inquilinos. Otorgue a cada grupo de usuarios los permisos mínimos necesarios para su función y utilice el modo de acceso de sólo lectura para evitar que los usuarios cambien la configuración.
- Cuando se utilizan extremos de equilibrador de carga de StorageGRID, use nodos de puerta de enlace en lugar de nodos de administrador para el tráfico de cliente que no es de confianza.
- Si tiene inquilinos que no son de confianza, no les permita tener acceso directo al administrador de inquilinos o a la API de gestión de inquilinos. En su lugar, para que los inquilinos que no son de confianza utilicen un portal de inquilinos o un sistema de gestión de inquilinos externo, que interactúa con la API de gestión de inquilinos.
- De manera opcional, use un proxy de administrador para obtener más control sobre la comunicación de AutoSupport desde los nodos de administrador al soporte de NetApp. Consulte los pasos para crear un proxy de administrador en las instrucciones para administrar StorageGRID.
- Opcionalmente, utilice los puertos restringidos 8443 y 9443 para separar las comunicaciones de Grid Manager y de arrendatario Manager. Bloquee el puerto compartido 443 y limite las solicitudes de inquilinos al puerto 9443 para obtener una protección adicional.
- De manera opcional, utilice nodos de administrador separados para los administradores de grid y los usuarios inquilinos.

Para obtener más información, consulte las instrucciones para administrar StorageGRID.

Directrices para nodos de almacenamiento

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Siga estas directrices para proteger los nodos de almacenamiento en el sistema StorageGRID.

- No habilite los servicios de salida para inquilinos que no sean de confianza. Por ejemplo, al crear la cuenta para un arrendatario que no sea de confianza, no permita que el arrendatario utilice su propio origen de identidad y no permita el uso de servicios de plataforma. Consulte los pasos para crear una cuenta de inquilino en las instrucciones para administrar StorageGRID.
- Utilice un equilibrador de carga de terceros para el tráfico de clientes que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques.
- Opcionalmente, utilice un proxy de almacenamiento para obtener más control sobre los pools de almacenamiento en cloud y la comunicación de servicios de plataforma de los nodos de almacenamiento a los servicios externos. Consulte los pasos para crear un proxy de almacenamiento en las instrucciones

para administrar StorageGRID.

- Opcionalmente, conéctese a servicios externos mediante la red cliente. A continuación, seleccione **Configuración** > **Configuración de red** > **Red de cliente no confiable** e indique que la Red de cliente en el nodo de almacenamiento no es de confianza. El nodo de almacenamiento ya no acepta tráfico entrante en la red cliente, pero sigue permitiendo solicitudes salientes para los servicios de plataforma.

Directrices para los nodos de puerta de enlace

Los nodos de puerta de enlace proporcionan una interfaz opcional de equilibrio de carga que las aplicaciones cliente pueden utilizar para conectarse a StorageGRID. Siga estas directrices para proteger cualquier nodo de puerta de enlace en el sistema StorageGRID:

- Configure y utilice puntos finales del equilibrador de carga en lugar de utilizar el servicio CLB en nodos de puerta de enlace. Consulte los pasos para gestionar el equilibrio de carga en las instrucciones para administrar StorageGRID.

  El servicio CLB está obsoleto.

- Utilice un equilibrador de carga de terceros entre el cliente y los nodos de puerta de enlace o de almacenamiento para buscar tráfico de cliente que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques. Si utiliza un equilibrador de carga de terceros, se puede configurar opcionalmente el tráfico de red para que pase por un extremo de equilibrador de carga interno o se envíe directamente a nodos de almacenamiento.
- Si utiliza puntos finales de equilibrador de carga, haga que los clientes se conecten a través de la red de cliente de forma opcional. A continuación, seleccione **Configuración** > **Configuración de red** > **Red de cliente no confiable** e indique que la Red de cliente en el nodo de puerta de enlace no es de confianza. El nodo Gateway sólo acepta tráfico entrante en los puertos configurados explícitamente como extremos equilibradores de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware StorageGRID están especialmente diseñados para su uso en un sistema StorageGRID. Algunos dispositivos se pueden usar como nodos de almacenamiento. Otros dispositivos se pueden usar como nodos de administrador o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o poner en marcha grids totalmente diseñados para todos los dispositivos.

Siga estas directrices para proteger cualquier nodo de dispositivo de hardware en el sistema StorageGRID:

- Si el dispositivo utiliza System Manager de SANtricity para la gestión de la controladora de almacenamiento, evite que los clientes que no son de confianza accedan a System Manager de SANtricity a través de la red.
- Si el dispositivo tiene un controlador de administración de placa base (BMC), tenga en cuenta que el puerto de administración del BMC permite un acceso bajo al hardware. Conecte el puerto de gestión de BMC sólo a una red de gestión interna segura y de confianza. Si no existe dicha red disponible, deje el puerto de administración del BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión al BMC.
- Si el dispositivo admite la administración remota del hardware de la controladora a través de Ethernet mediante el estándar de interfaz de gestión de plataforma inteligente (IPMI), bloquee el tráfico que no sea de confianza en el puerto 623.
- Si la controladora de almacenamiento del dispositivo incluye unidades FDE o FIPS y la función Drive

Security está habilitada, use SANtricity para configurar las claves de seguridad de unidades.

- Para dispositivos sin unidades FDE o FIPS, habilite el cifrado de nodos con un servidor de gestión de claves (KMS).

Consulte las instrucciones de instalación y mantenimiento de su dispositivo de hardware de StorageGRID.

Información relacionada

"Instale Red Hat Enterprise Linux o CentOS"

"Instalar Ubuntu o Debian"

"Instale VMware"

"Administre StorageGRID"

"Usar una cuenta de inquilino"

"SG100 servicios de aplicaciones SG1000"

"Dispositivos de almacenamiento SG5600"

"Dispositivos de almacenamiento SG5700"

"Dispositivos de almacenamiento SG6000"

Directrices de refuerzo para certificados de servidor

Debe sustituir los certificados predeterminados creados durante la instalación por sus propios certificados personalizados.

Para muchas organizaciones, el certificado digital autofirmado para el acceso web StorageGRID no cumple con sus políticas de seguridad de la información. En los sistemas de producción, debe instalar un certificado digital firmado por CA para utilizarlo en la autenticación de StorageGRID.

Específicamente, debe utilizar certificados de servidor personalizados en lugar de los siguientes certificados predeterminados:

- **Certificado del servidor de la interfaz de administración**: Se utiliza para asegurar el acceso a Grid Manager, al Gestor de arrendatarios, a la API de gestión de grid y a la API de administración de arrendatarios.
- **Object Storage API Service Endpoints Server Certificate**: Se utiliza para proteger el acceso a nodos de almacenamiento y nodos de puerta de enlace, que las aplicaciones cliente S3 y Swift utilizan para cargar y descargar datos de objeto.

> StorageGRID gestiona los certificados utilizados para los extremos del equilibrador de carga por separado. Para configurar certificados de equilibrador de carga, consulte los pasos para configurar los extremos de equilibrador de carga en las instrucciones para administrar StorageGRID.

Cuando utilice certificados de servidor personalizados, siga estas directrices:

- Los certificados deben tener un `subjectAltName` Que coincida con las entradas de DNS para StorageGRID. Para obtener más información, consulte la sección 4.2.1.6, "Nombre alternativo de la

expulsión" en "RFC 5280: Certificado PKIX y perfil CRL".

- Cuando sea posible, evite el uso de certificados comodín. Una excepción a esta directriz es el certificado para un extremo de estilo alojado virtual de S3, que requiere el uso de un comodín si los nombres de bloque no se conocen con anterioridad.
- Cuando debe utilizar comodines en los certificados, debe tomar medidas adicionales para reducir los riesgos. Utilice un patrón comodín como `*.s3.example.com`, y no utilice `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con acceso S3 de estilo de ruta como, por ejemplo `dc1-s1.s3.example.com/mybucket`.
- Establezca los tiempos de caducidad del certificado como cortos (por ejemplo, 2 meses) y utilice la API de gestión de grid para automatizar la rotación del certificado. Esto es especialmente importante para los certificados con caracteres comodín.

Además, los clientes deben usar una comprobación estricta del nombre de host al comunicarse con StorageGRID.

Otras directrices de endurecimiento

Además de seguir las directrices de refuerzo para redes y nodos de StorageGRID, debe seguir las directrices de refuerzo para otras áreas del sistema StorageGRID.

Registros y mensajes de auditoría

Proteja siempre los registros de StorageGRID y los resultados de mensajes de auditoría de forma segura. Los registros y mensajes de auditoría de StorageGRID proporcionan información de gran valor desde el punto de vista del soporte y la disponibilidad del sistema. Además, la información y los detalles que contienen los registros de StorageGRID y el resultado de un mensaje de auditoría suelen ser confidenciales.

Consulte las instrucciones para supervisar y solucionar problemas para obtener más información acerca de los registros de StorageGRID. Consulte las instrucciones de los mensajes de auditoría para obtener más información acerca de los mensajes de auditoría de StorageGRID.

AutoSupport de NetApp

La función AutoSupport de StorageGRID le permite supervisar de forma proactiva el estado del sistema y enviar automáticamente mensajes y detalles al soporte técnico de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera predeterminada, los mensajes de AutoSupport al soporte técnico de NetApp se habilitan cuando se configura StorageGRID por primera vez.

Es posible deshabilitar la función AutoSupport. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y resolución de problemas en caso de que se produzca un problema en su sistema StorageGRID.

AutoSupport admite HTTPS, HTTP y SMTP para los protocolos de transporte. Debido a la naturaleza sensible de los mensajes de AutoSupport, NetApp recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport a la compatibilidad de NetApp.

De manera opcional, se puede configurar un proxy de administrador para obtener más control sobre la comunicación de AutoSupport desde los nodos de administrador al soporte técnico de NetApp. Consulte los pasos para crear un proxy de administrador en las instrucciones para administrar StorageGRID.

Uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bloque de S3 si desea que dicho bloque y los objetos de ese bloque sean accesibles a las aplicaciones web de otros dominios. En general, no active CORS a menos que sea necesario. Si se requiere CORS, restringirlo a orígenes de confianza.

Consulte los pasos para configurar el uso compartido de recursos de origen cruzado (CORS) en las instrucciones para utilizar cuentas de arrendatario.

Dispositivos de seguridad externos

Una solución completa de consolidación debe abordar los mecanismos de seguridad fuera de StorageGRID. El uso de dispositivos de infraestructura adicionales para filtrar y limitar el acceso a StorageGRID es una forma efectiva de establecer y mantener una política de seguridad estricta. Estos dispositivos de seguridad externos incluyen firewalls, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda un equilibrador de carga de terceros para el tráfico de clientes que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques.

Información relacionada

"Solución de problemas de monitor"

"Revisar los registros de auditoría"

"Usar una cuenta de inquilino"

"Administre StorageGRID"

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.