Endurecimiento del sistema

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Endurecimiento del sistema

Consideraciones generales para el fortalecimiento del sistema

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

A medida que instala y configura StorageGRID, utilice estas pautas para ayudarlo a cumplir con los objetivos de seguridad prescritos en materia de confidencialidad, integridad y disponibilidad.

Ya debería estar utilizando las mejores prácticas estándar de la industria para el fortalecimiento del sistema. Por ejemplo, utiliza contraseñas seguras para StorageGRID, usa HTTPS en lugar de HTTP y habilita la autenticación basada en certificados cuando esté disponible.

StorageGRID sigue las "Política de gestión de vulnerabilidades de NetApp" . Las vulnerabilidades reportadas se verifican y abordan de acuerdo con el proceso de respuesta a incidentes de seguridad del producto.

Al fortalecer un sistema StorageGRID , tenga en cuenta lo siguiente:

- ¿*Cuál de las tres redes StorageGRID * ha implementado? Todos los sistemas StorageGRID deben usar la red Grid, pero también es posible que utilice 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 en su sistema StorageGRID . Los nodos StorageGRID se pueden implementar en máquinas virtuales VMware, dentro de un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma tiene su propio conjunto de mejores prácticas de fortalecimiento.
- **Qué tan confiables son las cuentas de los inquilinos**. Si usted es un proveedor de servicios con cuentas de inquilinos que no son de confianza, tendrá preocupaciones de seguridad diferentes que si solo utiliza inquilinos internos y de confianza.
- **Qué requisitos y convenciones de seguridad** sigue su organización. Es posible que deba cumplir con requisitos corporativos o regulatorios específicos.

Pautas de refuerzo para las actualizaciones de software

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

Actualizaciones del software StorageGRID

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

Consultar el "Herramienta de matriz de interoperabilidad de NetApp" (IMT) para determinar qué versión del software StorageGRID debería utilizar. Cuando se requiere una revisión, 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 revisiones más recientes de StorageGRID , vaya a "Descargas de NetApp : StorageGRID" .
- Para actualizar el software StorageGRID , consulte la"instrucciones de actualización" .
- Para aplicar una revisión, consulte la"Procedimiento de revisión de StorageGRID" .

Actualizaciones de servicios externos

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

Para obtener una lista de las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Actualizaciones de hipervisores

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

Para obtener una lista de las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Actualizaciones a nodos Linux

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

Para obtener una lista de las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Pautas de fortalecimiento para redes StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de red, lo que le permite configurar la red para cada nodo de red individual para que coincida con sus requisitos de seguridad y acceso.

Para obtener información detallada sobre las redes StorageGRID , consulte la"Tipos de red StorageGRID" .

Directrices para la red Grid

Debe configurar una red Grid para todo el tráfico interno de StorageGRID . Todos los nodos de la red están en la red de red y deben poder comunicarse con todos los demás nodos.

Al configurar la red Grid, siga estas pautas:

- Asegúrese de que la red esté protegida contra clientes que no sean de confianza, como aquellos en Internet abierto.
- Cuando sea posible, utilice la red Grid exclusivamente 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 la red Grid 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 Grid para brindar protección adicional para el tráfico interno.
- Algunos procedimientos de mantenimiento requieren acceso a shell seguro (SSH) en el puerto 22 entre el nodo de administración principal y todos los demás nodos de la red. Utilice un firewall externo para restringir el acceso SSH a clientes confiables.

Pautas para la red de administración

La red de administración generalmente se utiliza 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 internamente.

Si está utilizando la red de administración, siga estas pautas:

- Bloquear todos los puertos de tráfico interno en la red de administración. Ver el"lista de puertos internos" .
- Si los clientes no confiables 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 clientes

La red de cliente normalmente se utiliza para inquilinos y para comunicarse con servicios externos, como el servicio de replicación CloudMirror u otro servicio de plataforma. Sin embargo, StorageGRID no exige este uso internamente.

Si está utilizando la red de cliente, siga estas pautas:

- Bloquear todos los puertos de tráfico interno en la red del cliente. Ver el"lista de puertos internos" .
- Acepte el tráfico de clientes entrante solo en puntos finales configurados explícitamente. Ver la información sobre"gestión de controles de firewall" .

Pautas de refuerzo para nodos StorageGRID

Los nodos StorageGRID se pueden implementar en máquinas virtuales VMware, dentro de un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma y cada tipo de nodo tiene su propio conjunto de mejores prácticas de fortalecimiento.

Controlar el acceso remoto de IPMI a BMC

Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz IPMI remota permite el acceso de hardware de bajo nivel a sus dispositivos StorageGRID por parte de cualquier persona con una cuenta y contraseña de BMC . Si no necesita acceso IPMI remoto al BMC, desactive esta opción.

- Para controlar el acceso remoto de IPMI al BMC en Grid Manager, vaya a **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad** > **Dispositivos**:
  - Desmarque la casilla de verificación **Habilitar acceso IPMI remoto** para deshabilitar el acceso IPMI al BMC.
  - Seleccione la casilla de verificación **Habilitar acceso IPMI remoto** para habilitar el acceso IPMI al

BMC.

Configuración del firewall

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

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Debería"Administrar los controles internos del firewall" para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

En concreto, puedes gestionar estas áreas:

- **Direcciones privilegiadas**: puede permitir que direcciones IP o subredes seleccionadas accedan a puertos que estén cerrados por la configuración en la pestaña Administrar acceso externo.
- **Administrar acceso externo**: puedes cerrar puertos que están abiertos por defecto, o reabrir puertos previamente cerrados.
- **Red de cliente no confiable**: puede especificar si un nodo confía en el tráfico entrante de la red de cliente, así como los puertos adicionales que desea que estén abiertos cuando se configura la red de cliente no confiable.

Si bien 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"Referencia del puerto de red" .

Deshabilitar servicios no utilizados

Para todos los nodos de StorageGRID , debe deshabilitar o bloquear el acceso a los servicios no utilizados. Por ejemplo, si no planea utilizar DHCP, utilice el Administrador de cuadrícula para cerrar el puerto 68. Seleccione **CONFIGURACIÓN** > **Control de firewall** > **Administrar acceso externo**. A continuación, cambie el interruptor de estado del puerto 68 de **Abierto** a **Cerrado**.

Virtualización, contenedores y hardware compartido

Para todos los nodos de StorageGRID , evite ejecutar StorageGRID en el mismo hardware físico que software no confiable. No asuma que las protecciones del hipervisor evitarán que el malware acceda a los datos protegidos por StorageGRID si tanto StorageGRID como el malware existen en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre explotan vulnerabilidades críticas en los procesadores modernos y permiten que los programas roben datos de la memoria de la misma computadora.

Proteger los nodos durante la instalación

No permita que usuarios no confiables accedan a los nodos de StorageGRID a través de la red cuando se estén instalando los nodos. Los nodos no son completamente seguros hasta que se unen a la red.

Pautas para los nodos de administración

Los nodos de administración brindan servicios de gestión como configuración del sistema, monitoreo y registro. Cuando inicia sesión en Grid Manager o Tenant Manager, se conecta a un nodo de administración.

Siga estas pautas para proteger los nodos de administración en su sistema StorageGRID :

- Proteja todos los nodos de administración de clientes que no sean de confianza, como aquellos en Internet abierto. Asegúrese de que ningún cliente no confiable pueda acceder a ningún nodo de administración en la red Grid, la red de administración o la red de clientes.
- Los grupos de StorageGRID controlan el acceso a las funciones de Grid Manager y Tenant Manager. Otorgue a cada grupo de usuarios los permisos mínimos requeridos para su rol y utilice el modo de acceso de solo lectura para evitar que los usuarios cambien la configuración.
- Al utilizar puntos finales del balanceador de carga StorageGRID , utilice nodos de puerta de enlace en lugar de nodos de administración para el tráfico de clientes que no sean de confianza.
- Si tiene inquilinos que no son de confianza, no les permita tener acceso directo al Administrador de inquilinos ni a la API de administración de inquilinos. En su lugar, haga que los inquilinos que no sean de confianza utilicen un portal de inquilinos o un sistema de gestión de inquilinos externo, que interactúe con la API de gestión de inquilinos.
- Opcionalmente, utilice un proxy de administración para tener más control sobre la comunicación de AutoSupport desde los nodos de administración al soporte de NetApp . Vea los pasos para"creando un proxy de administrador" .
- Opcionalmente, utilice los puertos restringidos 8443 y 9443 para separar las comunicaciones entre Grid Manager y Tenant Manager. Bloquee el puerto compartido 443 y limite las solicitudes de inquilinos al puerto 9443 para obtener protección adicional.
- De manera opcional, utilice nodos de administración separados para administradores de red y usuarios inquilinos.

Para obtener más información, consulte las instrucciones para"administración de StorageGRID" .

Directrices para nodos de almacenamiento

Los nodos de almacenamiento administran y almacenan datos de objetos y metadatos. Siga estas pautas para proteger los nodos de almacenamiento en su sistema StorageGRID .

- No permita que clientes no confiables se conecten directamente a los nodos de almacenamiento. Utilice un punto final de balanceador de carga atendido por un nodo de puerta de enlace o un balanceador de carga de terceros.
- No habilite servicios salientes para inquilinos que no sean de confianza. Por ejemplo, al crear la cuenta para un inquilino que no es de confianza, no permita que el inquilino use su propia fuente de identidad y no permita el uso de los servicios de la plataforma. Vea los pasos para"crear una cuenta de inquilino" .
- Utilice un balanceador de carga de terceros para el tráfico de clientes que no sean de confianza. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.
- De manera opcional, utilice un proxy de almacenamiento para tener más control sobre los grupos de almacenamiento en la nube y la comunicación de los servicios de la plataforma desde los nodos de almacenamiento a los servicios externos. Vea los pasos para"creando un proxy de almacenamiento" .
- Opcionalmente, conéctese a servicios externos utilizando la red del cliente. Luego, seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall** > **Redes de cliente no confiables** e indique que la red de cliente en el nodo de almacenamiento no es confiable. El nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes para los servicios de plataforma.

Directrices para los nodos de enlace

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

- Configurar y utilizar puntos finales del balanceador de carga. Ver "Consideraciones para el equilibrio de carga" .
- Utilice un equilibrador de carga de terceros entre el cliente y el nodo de puerta de enlace o los nodos de almacenamiento para el tráfico de clientes no confiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques. Si utiliza un balanceador de carga de terceros, el tráfico de red puede configurarse opcionalmente para pasar por un punto final del balanceador de carga interno o enviarse directamente a los nodos de almacenamiento.
- Si está utilizando puntos finales de balanceador de carga, opcionalmente puede hacer que los clientes se conecten a través de la red del cliente. Luego, seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall** > **Redes de clientes no confiables** e indique que la red de clientes en el nodo de puerta de enlace no es confiable. El nodo de puerta de enlace solo acepta tráfico entrante en los puertos configurados explícitamente como puntos finales del equilibrador de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware StorageGRID están diseñados especialmente para su uso en un sistema StorageGRID . Algunos dispositivos pueden utilizarse como nodos de almacenamiento. Se pueden utilizar otros dispositivos como nodos de administración o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o implementar redes de dispositivos completamente diseñadas.

Siga estas pautas para proteger cualquier nodo de dispositivo de hardware en su sistema StorageGRID :

- Si el dispositivo utiliza SANtricity System Manager para la administración del controlador de almacenamiento, evite que los clientes no confiables accedan a SANtricity System Manager 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 de BMC permite el acceso al hardware de bajo nivel. Conecte el puerto de administración de BMC únicamente a una red de administración interna segura y confiable. Si no hay dicha red disponible, deje el puerto de administración de BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión de BMC .
- Si el dispositivo admite la administración remota del hardware del controlador a través de Ethernet utilizando el estándar de Interfaz de administración de plataforma inteligente (IPMI), bloquee el tráfico no confiable en el puerto 623.

> Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz IPMI remota permite el acceso de hardware de bajo nivel a sus dispositivos StorageGRID por parte de cualquier persona con una cuenta y contraseña de BMC . Si no necesita acceso IPMI remoto al BMC, deshabilite esta opción utilizando uno de los siguientes métodos: + En Grid Manager, vaya a **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad** > **Dispositivos** y desmarque la casilla de verificación **Habilitar acceso IPMI remoto**. + En la API de administración de Grid, use el punto final privado: `PUT /private/bmc` .

- Para los modelos de dispositivos que contienen unidades SED, FDE o FIPS NL-SAS que administra con SANtricity System Manager, "Habilitar y configurar SANtricity Drive Security" .

- Para los modelos de dispositivos que contienen SSD NVMe SED o FIPS que administra mediante el instalador de dispositivos StorageGRID y el administrador de red, "Habilitar y configurar el cifrado de unidad StorageGRID" .
- Para dispositivos sin unidades SED, FDE o FIPS, habilite y configure el cifrado del nodo de software StorageGRID "utilizando un servidor de administración de claves (KMS)" .

Pautas de refuerzo para TLS y SSH

Debe reemplazar los certificados predeterminados creados durante la instalación y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de endurecimiento de los certificados

Debe reemplazar los certificados predeterminados creados durante la instalación con sus propios certificados personalizados.

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

En concreto, debe utilizar certificados de servidor personalizados en lugar de estos certificados predeterminados:

- **Certificado de interfaz de administración**: se utiliza para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos.
- **Certificado API S3**: se utiliza para proteger el acceso a los nodos de almacenamiento y los nodos de puerta de enlace, que las aplicaciones cliente S3 utilizan para cargar y descargar datos de objetos.

Ver"Administrar certificados de seguridad" para obtener más detalles e instrucciones.

> StorageGRID administra los certificados utilizados para los puntos finales del equilibrador de carga por separado. Para configurar los certificados del balanceador de carga, consulte"Configurar los puntos finales del balanceador de carga" .

Al utilizar certificados de servidor personalizados, siga estas pautas:

- Los certificados deben tener una *`subjectAltName`* que coincide con las entradas DNS para StorageGRID. Para obtener más detalles, consulte la sección 4.2.1.6, "Nombre alternativo del sujeto", en "RFC 5280: Certificado PKIX y perfil CRL" .
- Siempre que sea posible, evite el uso de certificados comodín. Una excepción a esta directriz es el certificado para un punto final de estilo alojado virtual S3, que requiere el uso de un comodín si los nombres de los depósitos no se conocen de antemano.
- Cuando sea necesario utilizar comodines en los certificados, deberá tomar medidas adicionales para reducir los riesgos. Utilice un patrón comodín como `*.s3.example.com` , y no utilices el `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con acceso S3 de estilo de ruta, como `dc1-s1.s3.example.com/mybucket` .
- Establezca tiempos de vencimiento de certificados cortos (por ejemplo, 2 meses) y utilice la API de administración de cuadrícula para automatizar la rotación de certificados. Esto es especialmente importante para los certificados comodín.

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

Directrices de endurecimiento de las políticas TLS y SSH

Puede seleccionar una política de seguridad para determinar qué protocolos y cifrados se utilizan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras con servicios internos de StorageGRID .

La política de seguridad controla cómo TLS y SSH cifran los datos en movimiento. Como práctica recomendada, debe deshabilitar las opciones de cifrado que no sean necesarias para la compatibilidad de la aplicación. Utilice la política moderna predeterminada, a menos que su sistema necesite cumplir con los Criterios comunes o necesite utilizar otros cifrados.

Ver"Administrar la política TLS y SSH" para obtener detalles e instrucciones.

Otras pautas de endurecimiento

Además de seguir las pautas de fortalecimiento para las redes y los nodos de StorageGRID , debe seguir las pautas de fortalecimiento para otras áreas del sistema StorageGRID .

Contraseña de instalación temporal

Para proteger el sistema StorageGRID durante la instalación, configure una contraseña en la página de contraseña del instalador temporal en la interfaz de usuario de instalación de StorageGRID o en la API de instalación. Cuando se configura, esta contraseña se aplica a todos los métodos para instalar StorageGRID, incluida la interfaz de usuario, la API de instalación y `configure-storagegrid.py` guion.

Para obtener más información, consulte:

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"
- "Instalar StorageGRID en VMware"
- "Instalar el dispositivo StorageGRID"

Registros y mensajes de auditoría

Proteja siempre los registros de StorageGRID y la salida de mensajes de auditoría de manera segura. Los registros y mensajes de auditoría de StorageGRID proporcionan información invaluable desde el punto de vista de soporte y disponibilidad del sistema. Además, la información y los detalles contenidos en los registros de StorageGRID y en los mensajes de auditoría resultantes generalmente son de naturaleza confidencial.

Configure StorageGRID para enviar eventos de seguridad a un servidor syslog externo. Si utiliza la exportación de syslog, seleccione TLS y RELP/TLS para los protocolos de transporte.

Ver el"Referencia de archivos de registro" para obtener más información sobre los registros de StorageGRID . Ver"Mensajes de auditoría" para obtener más información sobre los mensajes de auditoría de StorageGRID .

AutoSupport de NetApp

La función AutoSupport de StorageGRID le permite monitorear de manera proactiva el estado de su sistema y enviar paquetes automáticamente al sitio de soporte de NetApp , al equipo de soporte interno de su organización o a un socio de soporte. De forma predeterminada, el envío de paquetes de AutoSupport a NetApp está habilitado cuando StorageGRID se configura por primera vez.

La función AutoSupport se puede desactivar. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y resolución de problemas en caso de que surja un problema en su sistema StorageGRID .

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

Intercambio de recursos entre orígenes (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bucket S3 si desea que ese bucket y los objetos que contiene sean accesibles para las aplicaciones web en otros dominios. En general, no habilite CORS a menos que sea necesario. Si se requiere CORS, limítelo a orígenes confiables.

Vea los pasos para"Configuración del uso compartido de recursos entre orígenes (CORS)" .

Dispositivos de seguridad externos

Una solución de fortalecimiento completa 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 eficaz de establecer y mantener una postura de seguridad estricta. Estos dispositivos de seguridad externos incluyen firewalls, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda un balanceador de carga de terceros para el tráfico de clientes que no son confiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.

Mitigación de ransomware

Ayude a proteger los datos de sus objetos de los ataques de ransomware siguiendo las recomendaciones en "Defensa contra ransomware con StorageGRID" .