Endurecimiento del sistema

StorageGRID software

NetApp
January 14, 2026

Tabla de contenidos

Endurecimiento del sistema

Consideraciones generales sobre el refuerzo del sistema

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

Al instalar y configurar StorageGRID, utilice estas directrices para ayudarle a cumplir los objetivos de seguridad prescritos en cuanto a 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. Estas mejores prácticas deben incluir seguridad física y ambiental que limite el acceso físico y proteja el centro de datos físico y la infraestructura de soporte. También debe consultar las normas y recomendaciones regulatorias aplicables para su negocio y geografía.

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.

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

- **Cuál de las tres redes StorageGRID** has 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 usas para los nodos individuales de tu sistema StorageGRID. Los nodos StorageGRID se pueden implementar en máquinas virtuales de VMware, en 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 optimización.
- **Cuán de confianza son 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.
- **Qué requisitos y convenciones de seguridad** sigue tu organización. Es posible que deba cumplir requisitos normativos o corporativos específicos.

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 refuerzo de la seguridad que no se incluyen en versiones anteriores.

Consulte el "Herramienta de matriz de interoperabilidad de NetApp" (IMT) para determinar qué versión del software de StorageGRID debe utilizar. 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 "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 a servicios externos

Los servicios externos pueden tener vulnerabilidades que afecten a StorageGRID indirectamente. Asegúrese 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 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.

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

Actualizaciones 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.

Para obtener una lista de las versiones compatibles, consulte la "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.

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

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 administrativa

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".
- 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 clientes

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".
- Acepte tráfico de cliente entrante sólo en puntos finales configurados explícitamente. Consulte la información sobre "gestión de controles de firewall".

Directrices de refuerzo para nodos de StorageGRID

Los nodos StorageGRID se pueden implementar en máquinas virtuales de VMware, en 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 prácticas recomendadas de endurecimiento.

Controlar el acceso remoto de IPMI a BMC

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

- Para controlar el acceso remoto de IPMI al BMC en Grid Manager, vaya a **Configuración** > **Seguridad** > **Configuración de seguridad** > **Dispositivos**:

- Desactive la casilla de verificación **Enable remote IPMI access** para desactivar el acceso IPMI a BMC.
- Seleccione la casilla de verificación **Enable remote IPMI access** para habilitar el acceso de IPMI a BMC.

Para obtener información adicional sobre el endurecimiento de BMC , consulte la "Controladores de administración de placa base Harden" Hoja informativa sobre ciberseguridad de la "Agencia de Seguridad Nacional (NSA)" y "Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA)" .

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.

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

Específicamente, puede gestionar estas áreas:

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

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"Puertos internos StorageGRID" y"Puertos que se utilizan para comunicaciones externas" .

Desactive los 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 el software que no es de confianza. No asuma que las protecciones del hipervisor evitarán que el malware acceda a los datos protegidos por StorageGRID si el StorageGRID y 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.

Proteja los nodos durante la instalación

No permita que usuarios que no sean de confianza accedan a los nodos StorageGRID a través de la red cuando se van a instalar los nodos. Los nodos no son totalmente seguros hasta que se han unido a la cuadrícula.

Limitar el acceso físico al hardware

Debe limitar el acceso físico a los nodos del dispositivo de hardware StorageGRID , así como a los hosts de máquinas virtuales VMware y a los hosts Linux que ejecutan StorageGRID , únicamente a los administradores autorizados. Algunos ejemplos de controles de acceso físico incluyen cerraduras, guardias, barreras físicas y videovigilancia.

Los nodos de dispositivos de hardware están diseñados para ser instalados y operados únicamente por administradores autorizados. No permita que administradores no autorizados accedan a los nodos del dispositivo de hardware.

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 permita que tengan 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.
- Opcionalmente, utilice un proxy de administrador para tener más control sobre la comunicación de AutoSupport de los nodos de administración a Soporte de NetApp. Consulte los pasos para "creando un proxy de administración".
- 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 de "Administración de 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 permita que los clientes que no son de confianza se conecten directamente con los nodos de almacenamiento. Utilice un punto final de equilibrio de carga servido por un nodo de gateway o un equilibrador de carga de terceros.
- No habilite los servicios de salida para inquilinos que no son de confianza. Por ejemplo, al crear la cuenta para un inquilino que no sea de confianza, no permita que el inquilino utilice su propia fuente de identidad y no permita el uso de servicios de plataforma. Consulte los pasos para "crear una cuenta de inquilino".
- 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 tener un mayor control sobre la comunicación de los pools de Cloud Storage y los servicios de plataforma de los nodos de almacenamiento a los servicios externos. Consulte los pasos para "creación de 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 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:

- Configurar y utilizar puntos finales del equilibrador de carga. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".
- 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 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 cliente no confiables** e indique que la red de cliente 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 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 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.

  Puede establecer una VLAN para aislar las conexiones de red de BMC y restringir el acceso a Internet de BMC a redes confiables. Para obtener información adicional sobre cómo aplicar la separación de VLAN, consulte la "Controladores de administración de placa base Harden" Hoja informativa sobre ciberseguridad de la "Agencia de Seguridad Nacional (NSA)" y "Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA)" .

  Si no hay disponible una red de administración interna segura y confiable, deje el puerto de administración de BMC desconectado o bloqueado. El soporte técnico podría solicitar acceso temporal durante un caso de soporte.

- 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.

> 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` .

+ También puedesdeshabilitar el acceso remoto a IPMI .

- Para los modelos de dispositivos que contienen unidades SED, FDE o FIPS NL-SAS que se gestionan con el administrador del sistema de SANtricity, "Habilite y configure 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, "Habilite y configure el cifrado de unidades StorageGRID" .
- Para dispositivos sin unidades SED, FDE o FIPS, utilice un servidor de administración de claves (KMS) para "Habilitar y configurar el cifrado del nodo de software StorageGRID" .

Información relacionada

"Obtenga información sobre la seguridad de la unidad en SANtricity System Manager"

Directrices de refuerzo para TLS y SSH

Debe controlar el acceso SSH, reemplazar los certificados TLS predeterminados y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de refuerzo para los certificados

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 de interfaz de administración**: Se utiliza para asegurar el acceso a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de administración de inquilinos.
- **Certificado de API S3**: Se utiliza para asegurar el acceso a los nodos de almacenamiento y los nodos de Gateway, que las aplicaciones cliente S3 utilizan para cargar y descargar datos de objetos.

Consulte "Gestionar certificados de seguridad" para obtener detalles e instrucciones.

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

Cuando utilice certificados de servidor personalizados, siga estas directrices:

- Los certificados deben tener una *subjectAltName* coincidencia con las entradas DNS de StorageGRID. Para obtener más información, consulte la sección 4,2.1,6, «Nombre alternativo del asunto» 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 punto final de estilo alojado virtual S3, que requiere el uso de un comodín si los nombres de depósito no se conocen por adelantado.
- 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 el `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con el acceso de estilo de ruta S3, como `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.

Directrices de endurecimiento para las políticas TLS y SSH

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

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, con FIPS 140-2 o necesite usar otros cifrados.

Consulte "Gestione la política TLS y SSH" para obtener detalles e instrucciones.

Administrar el acceso SSH externo

Para mejorar la seguridad del sistema, el acceso SSH externo está bloqueado de forma predeterminada. Habilite el acceso SSH solo cuando necesite realizar tareas que requieran acceso SSH entrante, como

resolución de problemas. Referirse a"Administrar el acceso SSH externo" para obtener detalles e instrucciones.

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.

Contraseña de instalación temporal

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

Para obtener más información, consulte:

- "Instalar StorageGRID en nodos basados en software"
- "Instale el dispositivo 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.

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

Consulte la "Referencia de archivos de registro" para obtener más información acerca de los registros de StorageGRID. Consulte "Auditar mensajes" para obtener más información sobre los mensajes de auditoría de StorageGRID.

AutoSupport de NetApp

La función AutoSupport de StorageGRID permite supervisar de forma proactiva el estado del sistema y enviar automáticamente paquetes al sitio de soporte de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera predeterminada, el envío de paquetes AutoSupport a NetApp se habilita cuando StorageGRID se configura 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 confidencial de los paquetes de AutoSupport, NetApp recomienda encarecidamente usar HTTPS como protocolo de transporte predeterminado para enviar paquetes de AutoSupport a NetApp.

Uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un depósito de S3 si desea

que las aplicaciones web de otros dominios puedan acceder a ese depósito y a los objetos de ese depósito. En general, no active CORS a menos que sea necesario. Si se requiere CORS, restringirlo a orígenes de confianza.

Vea los pasos para"Configuración de CORS para depósitos y objetos" .

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.

Mitigación de ransomware

Ayuda a proteger tus datos de objetos de ataques de ransomware siguiendo las recomendaciones en "Defensa contra ransomware con StorageGRID".