TR-4645: Funciones de seguridad

How to enable StorageGRID in your environment

NetApp
July 05, 2024

Tabla de contenidos

TR-4645: Funciones de seguridad

Protege los datos y metadatos de StorageGRID en un almacén de objetos

Descubra las funciones de seguridad integrales de la solución de almacenamiento de objetos de StorageGRID.

Esta es una descripción general de las muchas características de seguridad de NetApp® StorageGRID®, que cubren el acceso a datos, objetos y metadatos, el acceso administrativo y la seguridad de la plataforma. Se ha actualizado para incluir las últimas características lanzadas con StorageGRID 11,8.

La seguridad es una parte integral de la solución de almacenamiento de objetos de NetApp StorageGRID. La seguridad es especialmente importante porque muchos tipos de datos de contenido enriquecido que se adaptan perfectamente al almacenamiento de objetos también son confidenciales por naturaleza y sujetos a regulaciones y cumplimiento de normativas. A medida que las funcionalidades de StorageGRID continúan evolucionando, el software pone a su disposición muchas funciones de seguridad imprescindibles para proteger la política de seguridad de la organización y ayudar a la organización a cumplir las prácticas recomendadas del sector.

Este documento ofrece una descripción general de las muchas características de seguridad de StorageGRID 11,8, divididas en cinco categorías:

- Funciones de seguridad de acceso a los datos
- Funciones de seguridad de objetos y metadatos
- Funciones de seguridad de administración
- Funciones de seguridad de la plataforma
- Integración del cloud

Este documento está diseñado para ser una hoja de datos de seguridad; no detalla cómo configurar el sistema para que admita las características de seguridad enumeradas en que no están configuradas de forma predeterminada. El "Guía para el fortalecimiento de StorageGRID" está disponible en la página oficial "Documentación de StorageGRID" .

Además de las capacidades descritas en este informe, StorageGRID sigue el "Política de notificación y respuesta de vulnerabilidad de seguridad de los productos de NetApp". Las vulnerabilidades informadas se verifican y responden a ellas según el proceso de respuesta a incidentes de seguridad del producto.

NetApp StorageGRID ofrece funciones de seguridad avanzadas para casos de uso de almacenamiento de objetos empresariales muy exigentes.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- NetApp StorageGRID: Evaluación del cumplimiento de las normas SEC 17a-4(f), FINRA 4511(c) y CFTC 1,31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Página de documentación de StorageGRID 11,8 https://docs.netapp.com/us-en/storagegrid-118/

- Página de recursos de documentación de StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/

Términos y acrónimos

En esta sección se proporcionan definiciones de la terminología utilizada en el documento.

Término o acrónimo	Definición
S3	Servicio de almacenamiento simple.
Cliente	Una aplicación que puede interactuar con StorageGRID mediante el protocolo S3 para el acceso a los datos o el protocolo HTTP para la gestión.
Administrador de inquilinos	El administrador de la cuenta de inquilino de StorageGRID
Usuario inquilino	Un usuario dentro de una cuenta de inquilino de StorageGRID
TLS	Seguridad de la capa de transporte
ILM	Gestión del ciclo de vida de la información
LAN	Red de área local
Administrador de grid	El administrador del sistema StorageGRID
Cuadrícula	El sistema StorageGRID
Cucharón	Un contenedor para objetos almacenados en S3
LDAP	Protocolo ligero de acceso a directorios
SEG	Securities and Exchange Commission; regula los miembros, agentes y distribuidores de las operaciones
FINRA	Autoridad reguladora de la industria financiera; aplaza los requisitos de formato y medios de la norma SEC 17a-4(f)
CFTC	Commodity Futures Trading Comissions; regula el comercio de futuros de materias primas
NIST	Instituto Nacional de Estándares y Tecnología

Funciones de seguridad de acceso a los datos

Obtenga más información sobre las funciones de seguridad del acceso a los datos en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Seguridad de la capa de transporte configurable (TLS)	TLS establece un protocolo de apretón de manos para la comunicación entre un cliente y un nodo de pasarela StorageGRID, un nodo de almacenamiento o un extremo del balanceador de carga. StorageGRID admite los siguientes conjuntos de cifrado para TLS: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 Compatibilidad con TLS v1,2 y 1,3. SSLv3, TLS v1,1 y versiones anteriores ya no son compatibles.	Permite que un cliente y StorageGRID se identifiquen y autentiquen entre sí y se comuniquen con confidencialidad e integridad de los datos. Garantiza el uso de una versión de TLS reciente. Los cifrados ahora se pueden configurar en la configuración de configuración/seguridad	—

Función	Función	Impacto	Cumplimiento de normativas
Certificado de servidor configurable (punto final del equilibrador de carga)	Los administradores de grid pueden configurar puntos finales del equilibrador de carga para generar o utilizar un certificado de servidor.	Permite el uso de certificados digitales firmados por su entidad de certificación (CA) de confianza estándar para autenticar las operaciones de API de objetos entre grid y cliente por punto final de equilibrador de carga.	—
Certificado de servidor configurable (extremo de API)	Los administradores de grid pueden configurar de forma centralizada todos los puntos finales de la API de StorageGRID para que utilicen un certificado de servidor firmado por la CA de confianza de su organización.	Permite el uso de certificados digitales firmados por su CA de confianza estándar para autenticar operaciones de API de objetos entre un cliente y el grid.	—

Función	Función	Impacto	Cumplimiento de normativas
Multi-tenancy	StorageGRID admite varios inquilinos por grid, cada cliente cuenta con su propio espacio de nombres. Un inquilino proporciona un protocolo S3; de forma predeterminada, el acceso a bloques/contenedores y objetos está restringido a los usuarios de la cuenta. Los inquilinos pueden tener un usuario (por ejemplo, un despliegue empresarial, en el que cada usuario tiene su propia cuenta) o varios usuarios (por ejemplo, un despliegue de proveedor de servicios, en el que cada cuenta es una empresa y un cliente del proveedor de servicios). Los usuarios pueden ser locales o federados; los usuarios federados los define Active Directory o el protocolo ligero de acceso a directorios (LDAP). StorageGRID ofrece una consola por inquilino, en la que los usuarios inician sesión con las credenciales de cuentas locales o federadas. Los usuarios pueden acceder a informes visualizados sobre el uso de los inquilinos respecto de la cuota asignada por el administrador de grid, incluida la información de uso en datos y objetos almacenados por bloques. Los usuarios con permiso administrativo pueden llevar a cabo tareas de administración del sistema a nivel de inquilino, como gestionar usuarios y grupos y claves de acceso.	Permite que los administradores de StorageGRID alojen datos de varios inquilinos aislando el acceso de los inquilinos y establecer la identidad de usuario mediante la federación de usuarios con un proveedor de identidades externo, como Active Directory o LDAP.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
No rechazo de credenciales de acceso	Cada operación de S3 se identifica y se registra con una cuenta de inquilino, un usuario y una clave de acceso únicos.	Permite a los administradores de Grid establecer qué acciones de API realizan cada persona.	—

Función	Función	Impacto	Cumplimiento de normativas
Acceso anónimo deshabilitado	De forma predeterminada, el acceso anónimo está desactivado para las cuentas S3. Un solicitante debe tener una credencial de acceso válida para un usuario válido en la cuenta de inquilino para acceder a depósitos, contenedores u objetos dentro de la cuenta. El acceso anónimo a bloques u objetos de S3 se puede habilitar con una política de IAM explícita.	Permite a los administradores de Grid desactivar o controlar el acceso anónimo a bloques/contenedores y objetos.	—
WORM de cumplimiento de normativas	Diseñado para cumplir con los requisitos de la normativa SEC 17a-4(f) y validado por Cohasset. Los clientes pueden habilitar el cumplimiento de normativas a nivel del bucket. La retención se puede ampliar pero nunca se puede reducir. Las reglas de gestión de la vida útil de la información (ILM) aplican niveles de protección de datos mínimos.	Permite a los inquilinos con requisitos de retención de datos normativos para habilitar la protección WORM en los objetos almacenados y los metadatos de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
GUSANO	Los administradores de grid pueden habilitar WORM en toda la cuadrícula habilitando la opción Disable Client Modify, que impide que los clientes sobrescriban o eliminen objetos o metadatos de objetos en todas las cuentas de inquilino. S3 Los administradores de inquilinos también pueden habilitar WORM por inquilino, bloque o prefijo de objeto especificando la política de IAM, que incluye el permiso personalizado S3: PutOverwriteObject para la sobrescritura de objetos y metadatos.	Permite que los administradores de Grid y los administradores de inquilinos controlen la protección WORM en los objetos almacenados y los metadatos de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Función	Función	Impacto	Cumplimiento de normativas
Gestión de claves de cifrado del servidor host KM	Los administradores de grid pueden configurar uno o varios servidores de gestión de claves externos (KMS) en Grid Manager para proporcionar claves de cifrado para servicios de StorageGRID y aplicaciones de almacenamiento. Cada servidor de host KMS o clúster de servidores de host KMS utiliza el protocolo de interoperabilidad de gestión de claves (KMIP) para proporcionar una clave de cifrado a los nodos del dispositivo en el sitio de StorageGRID asociado.	Se logra el cifrado de los datos en reposo. Una vez cifrados los volúmenes del dispositivo, no puede acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el servidor host KMS.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Recuperación automatizada tras fallos	StorageGRID proporciona redundancia incorporada y conmutación por error automatizada. El acceso a las cuentas, los bloques y los objetos de inquilino puede continuar incluso si hay varios fallos, desde discos o nodos a sitios enteros. StorageGRID tiene en cuenta recursos y redirige automáticamente las solicitudes a los nodos y las ubicaciones de datos disponibles. Los sitios StorageGRID incluso pueden funcionar en modo interno; si una interrupción en WAN desconecta un sitio del resto del sistema, las operaciones de lectura y escritura pueden continuar con los recursos locales y la replicación se reanuda automáticamente cuando se restaura la WAN.	Permite a los administradores de Grid abordar el tiempo de actividad, los acuerdos de nivel de servicios y otras obligaciones contractuales, así como implementar planes de continuidad empresarial.	—

Función	Función	Impacto	Cumplimiento de normativas
Características de seguridad de acceso a datos específicas de S3	AWS Signature versión 2 y versión 4	Las solicitudes de API de firma proporcionan autenticación para las operaciones de API de S3. Amazon admite dos versiones de Signature Version 2 y 4. El proceso de firma verifica la identidad del solicitante, protege los datos en tránsito y protege contra posibles ataques de repetición.	Se alinea con la recomendación de AWS para la versión de firma 4 y permite la compatibilidad con versiones anteriores con aplicaciones anteriores con la versión de firma 2.
—	Bloqueo de objetos de S3	La función Bloqueo de objetos S3 de StorageGRID es una solución de protección de objetos equivalente a Bloqueo de objetos S3 en Amazon S3.	Permite a los inquilinos crear buckets con S3 Object Lock habilitado para cumplir con las regulaciones que requieren que ciertos objetos se conserven durante un período de tiempo fijo o indefinidamente.
Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)	Almacenamiento seguro de credenciales S3	Las claves de acceso S3 se almacenan en un formato protegido por una función de hash de contraseña (SHA-2).	Permite el almacenamiento seguro de claves de acceso mediante una combinación de longitud de clave (un número generado aleatoriamente 10^{31}) y un algoritmo de hash de contraseña.
—	Teclas de acceso S3 con límite de tiempo	Al crear una clave de acceso S3 para un usuario, los clientes pueden establecer una fecha y hora de caducidad en la clave de acceso.	Ofrece a los administradores de Grid la opción de aprovisionar claves de acceso S3 temporales.

Función	Función	Impacto	Cumplimiento de normativas
—	Múltiples claves de acceso por cuenta de usuario	StorageGRID permite crear varias claves de acceso y estar activas simultáneamente para una cuenta de usuario. Dado que cada acción de API se registra con una cuenta de usuario de inquilino y una clave de acceso, el no repudio se conserva a pesar de que hay varias claves activas.	Permite a los clientes rotar las claves de acceso sin interrupciones y permite que cada cliente tenga su propia clave, lo que desalienta el uso compartido de claves entre los clientes.
—	S3 Política de acceso de IAM	StorageGRID admite políticas de IAM S3, lo que permite a los administradores de Grid especificar control de acceso granular por inquilino, bloque o prefijo de objeto. StorageGRID también admite condiciones y variables de política de IAM, lo que permite políticas de control de acceso más dinámicas.	Permite a los administradores de Grid especificar el control de acceso por grupos de usuarios para todo el inquilino; también permite a los usuarios inquilinos especificar el control de acceso para sus propios bloques y objetos.
—	Cifrado del lado del servidor con claves gestionadas por StorageGRID (SSE)	StorageGRID admite SSE, lo que permite la protección multitenant de datos en reposo con claves de cifrado gestionadas por StorageGRID.	Permite a los inquilinos cifrar objetos. Se necesita una clave de cifrado para escribir y recuperar estos objetos.
Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)	Cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)	StorageGRID admite SSE-C, lo que permite la protección multitenant de los datos en reposo con claves de cifrado gestionadas por el cliente. Aunque StorageGRID gestiona todas las operaciones de cifrado y descifrado de objetos, con SSE-C, el cliente debe gestionar las claves de cifrado por sí mismo.	Permite a los clientes cifrar los objetos con claves que controlan. Se necesita una clave de cifrado para escribir y recuperar estos objetos.

Seguridad de objetos y metadatos

Explora las funciones de seguridad de objetos y metadatos en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Cifrado de objetos del lado del servidor del estándar de cifrado avanzado (AES)	StorageGRID proporciona cifrado de objetos en el servidor basado en AES 128 y AES 256. Los administradores de grid pueden activar el cifrado como valor predeterminado global. StorageGRID también admite el encabezado de cifrado de lado del servidor x-amz S3 para permitir habilitar o deshabilitar el cifrado por objeto. Cuando está activado, los objetos se cifran cuando se almacenan o están en tránsito entre los nodos de la cuadrícula.	Ayuda a proteger el almacenamiento y la transmisión de objetos, independientemente del hardware de almacenamiento subyacente.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Gestión de claves incorporada	Cuando se habilita el cifrado, cada objeto se cifra con una clave simétrica única generada aleatoriamente, que se almacena en StorageGRID sin acceso externo.	Permite el cifrado de objetos sin necesidad de gestión de claves externa.	
Discos de cifrado compatibles con el estándar de procesamiento de información federal (FIPS) 140-2	Los dispositivos StorageGRID SG5712, SG5760, SG6060 y SGF6024 ofrecen la opción de discos de cifrado conformes a la normativa FIPS 140-2-2. Las claves de cifrado para los discos pueden gestionarse opcionalmente un servidor KMIP externo.	Permite un almacenamiento seguro de datos, metadatos y objetos del sistema. También ofrece cifrado de objetos basado en software StorageGRID, que protege el almacenamiento y la transmisión de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Función	Función	Impacto	Cumplimiento de normativas
Exploración de integridad de fondo y reparación automática	StorageGRID usa un mecanismo interconectado compuesto por hashes, sumas de comprobación y comprobaciones de redundancia cíclicas (CRC) en el nivel de objeto y subobjeto para ofrecer protección frente a la incoherencia, manipulación o modificación de datos, tanto cuando los objetos se encuentran en almacenamiento como en tránsito. StorageGRID detecta automáticamente los objetos dañados o alterados, y los reemplaza mientras pone en cuarentena los datos modificados y alerta al administrador.	Permite a los administradores de Grid cumplir los acuerdos de nivel de servicios, las normativas y otras obligaciones relativas a la durabilidad de los datos. Ayuda a los clientes a detectar virus o ransomware que intentan cifrar, manipular o modificar datos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Retención y ubicación de objetos basadas en políticas	StorageGRID permite que los administradores de Grid configuren las reglas de ILM, las cuales especifican la retención de objetos, la ubicación, la protección, la transición y la caducidad. Los administradores de grid pueden configurar StorageGRID para que filtre objetos por sus metadatos y para aplicar reglas a distintos niveles de granularidad, incluidos todo el grid, inquilino, bloque, prefijo de clave o. y pares clave-valor de metadatos definidos por el usuario. StorageGRID ayuda a garantizar que los objetos se almacenan según las reglas de ILM durante sus ciclos de vida, a menos que el cliente los elimine de manera explícita.	Ayuda a aplicar la ubicación, la protección y la retención de los datos. Ayuda a los clientes a lograr el acuerdo de nivel de servicio en cuanto a durabilidad, disponibilidad y rendimiento.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Análisis de metadatos en segundo plano	StorageGRID analiza periódicamente los metadatos de objetos en segundo plano para aplicar cambios en la ubicación o la protección de los datos de objetos según lo especificado por ILM.	Ayuda a detectar objetos corruptos.	

Función	Función	Impacto	Cumplimiento de normativas
Coherencia ajustable	Los inquilinos pueden seleccionar niveles de coherencia en el nivel del bucket para garantizar que estén disponibles recursos, como la conectividad multisitio.	Proporciona la opción de confirmar las escrituras en el grid solo cuando hay un número necesario de sitios o recursos disponibles.	

Funciones de seguridad de administración

Descubra las funciones de seguridad de administración en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Certificado de servidor (interfaz de gestión de grid)	Los administradores de grid pueden configurar la interfaz de gestión de grid para que utilice un certificado de servidor firmado por la CA de confianza de su organización.	Permite el uso de certificados digitales firmados por su CA estándar y de confianza para autenticar el acceso de API y de interfaz de usuario de gestión entre un cliente de gestión y el grid.	—
Autenticación de usuario administrativa	Los usuarios administrativos se autentican con el nombre de usuario y la contraseña. Los usuarios y grupos administrativos pueden ser locales o federados, importados desde Active Directory o LDAP del cliente. Las contraseñas de la cuenta local se almacenan en un formato protegido por bcrypt; las contraseñas de la línea de comandos se almacenan en un formato protegido por SHA-2.	Autentica el acceso administrativo a la interfaz de usuario de gestión y las API.	—

Función	Función	Impacto	Cumplimiento de normativas
Soporte de SAML	StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2,0 (SAML 2,0). Cuando se habilita SSO, todos los usuarios deben estar autenticados por un proveedor de identidades externo antes de poder acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid o a la API de gestión de inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.	Permite niveles adicionales de seguridad para administradores de grid e inquilinos, como SSO y la autenticación multifactor (MFA).	NIST SP800-63
Control granular de permisos	Los administradores de grid pueden asignar permisos a roles y asignar roles a grupos de usuarios administrativos, lo que aplica qué tareas se permite que lleven a cabo los clientes administrativos desde la interfaz de usuario de gestión como las API.	Permite a los administradores de Grid gestionar el control de acceso de usuarios y grupos administradores.	—

Función	Función	Impacto	Cumplimiento de normativas
Registro de auditorías distribuido	StorageGRID ofrece una infraestructura de registro de auditorías incorporada y distribuida que se puede ampliar a cientos de nodos en hasta 16 sitios. Los nodos de software de StorageGRID generan mensajes de auditoría, que se transmiten a través de un sistema de retransmisión de auditoría redundante y, en última instancia, se capturan en uno o más repositorios de registros de auditoría. Eventos de captura de mensajes de auditoría con una granularidad a nivel de objeto, como operaciones de API S3 iniciadas por el cliente, eventos de ciclo de vida de los objetos por ILM, comprobaciones del estado de los objetos en segundo plano y cambios de configuración realizados desde las API o la interfaz de usuario de gestión. Los registros de auditoría se pueden exportar de los nodos de administrador mediante CIFS o NFS, lo cual permite los mensajes de auditoría por herramientas como Splunk y ELK. Existen cuatro tipos de mensajes de auditoría: • Mensajes de auditoría del sistema • Mensajes de auditoría del almacenamiento de objetos • Mensajes de auditoría de protocolo HTTP • Mensajes de auditoría de gestión	Proporciona a los administradores de Grid un servicio de auditoría probado y escalable y les permite extraer datos de auditoría para diversos objetivos. Entre estos objetivos se incluyen la solución de problemas, la auditoría del rendimiento del SLA, las operaciones de API de acceso a los datos del cliente y los cambios en la configuración de gestión.	—

Función	Función	Impacto	Cumplimiento de normativas
Auditoría del sistema	Los mensajes de auditoría del sistema capturan eventos relacionados con el sistema, como los estados de nodo de grid, la detección de objetos dañados, los objetos comprometidos en todas las ubicaciones especificadas por regla de ILM y el progreso de las tareas de mantenimiento en todo el sistema (tareas de grid).	Ayuda a los clientes a solucionar problemas del sistema y ofrece pruebas de que los objetos se almacenan según su acuerdo de nivel de servicio. Los acuerdos de nivel de servicio se implementan mediante reglas de ILM de StorageGRID y están protegidos para la integridad.	—
Auditoría de almacenamiento de objetos	Los mensajes de auditoría del almacenamiento de objetos capturan los eventos relacionados con el ciclo de vida y las transacciones de la API del objeto. Entre estos eventos se incluyen almacenamiento y recuperación de objetos, transferencias de grid-nodo a grid-nodo y verificaciones.	Ayuda a los clientes a auditar el progreso de los datos a través del sistema y si se están entregando el SLA, especificado como gestión del ciclo de vida de la información de StorageGRID.	—
Auditoría de protocolo HTTP	Los mensajes de auditoría del protocolo HTTP capturan las interacciones del protocolo HTTP relacionadas con las aplicaciones cliente y los nodos StorageGRID. Además, los clientes pueden capturar encabezados de solicitud HTTP específicos (como X-forward-for y metadatos de usuario [x-amz-meta-*]) en la auditoría.	Ayuda a los clientes a auditar las operaciones de API de acceso a los datos entre clientes y StorageGRID, y rastrea una acción en una cuenta de usuario individual y una clave de acceso. Los clientes también pueden registrar metadatos de usuario en auditorías y utilizar herramientas de extracción de registros como Splunk o ELK para buscar metadatos de objetos.	—
Auditoría de gestión	Los mensajes de auditoría de gestión registran las solicitudes del usuario administrador a las API o la interfaz de usuario de gestión (Grid Management Interface). Cada solicitud que no sea UNA solicitud GET o HEAD a la API registra una respuesta con el nombre de usuario, la IP y el tipo de solicitud a la API.	Ayuda a los administradores de Grid a establecer un registro de los cambios de configuración del sistema realizados por cada usuario desde qué IP de origen y qué IP de destino en qué momento.	—

Función	Función	Impacto	Cumplimiento de normativas
Soporte de TLS 1,3 para el acceso a la API e IU de gestión	TLS establece un protocolo de apretón de manos para la comunicación entre un cliente de administrador y un nodo de administrador de StorageGRID.	Permite a un cliente administrativo y a StorageGRID identificarse y autenticarse entre sí, y comunicarse con confidencialidad e integridad de los datos.	—
SNMPv3 para la supervisión de StorageGRID	SNMPv3 ofrece seguridad al ofrecer autenticación sólida y cifrado de datos para mayor privacidad. Con v3, las unidades de datos de protocolo se cifran, utilizando CBC-DES para su protocolo de cifrado. La autenticación de usuario de quién envió la unidad de datos de protocolo se proporciona mediante el protocolo de autenticación HMAC-SHA o HMAC-MD5. SNMPv2 y v1 siguen siendo compatibles.	Ayuda a los administradores de grid a supervisar el sistema StorageGRID mediante la activación de un agente SNMP en el nodo de administración.	—
Certificados de cliente para la exportación de métricas Prometheus	Los administradores de grid pueden cargar o generar certificados de cliente que se pueden utilizar para proporcionar acceso seguro y autenticado a la base de datos de StorageGRID Prometheus.	Los administradores de grid pueden utilizar certificados de cliente para supervisar StorageGRID externamente con aplicaciones como Grafana.	—

Funciones de seguridad de la plataforma

Obtenga más información sobre las características de seguridad de la plataforma en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Infraestructura de clave pública interna (PKI), certificados de nodo y TLS	StorageGRID utiliza una PKI interna y certificados de nodo para autenticar y cifrar la comunicación entre nodos. La comunicación entre nodos está protegida por TLS.	Ayuda a proteger el tráfico del sistema a través de LAN o WAN, especialmente en una implementación multisitio.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Función	Función	Impacto	Cumplimiento de normativas
Firewall de nodo	StorageGRID configura automáticamente tablas IP y reglas de firewall para controlar el tráfico de red entrante y saliente, así como para cerrar los puertos no utilizados.	Ayuda a proteger el sistema de StorageGRID, los datos y los metadatos frente al tráfico de red no solicitado.	—
Endurecimiento del SO	El sistema operativo básico de dispositivos físicos StorageGRID y nodos virtuales está reforzado; se eliminan los paquetes de software no relacionados.	Ayuda a minimizar posibles superficies de ataque.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Actualizaciones periódicas de la plataforma y del software	StorageGRID proporciona versiones regulares de software que incluyen sistemas operativos, binarios de aplicaciones y actualizaciones de software.	Ayuda a mantener el sistema StorageGRID actualizado con los binarios de software y aplicaciones actuales.	—
Inicio de sesión raíz desactivado a través de shell seguro (SSH)	El inicio de sesión raíz a través de SSH está deshabilitado en todos los nodos StorageGRID. El acceso SSH utiliza autenticación de certificados.	Ayuda a los clientes a protegerse contra posibles fallos remotos de contraseña del inicio de sesión root.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Sincronización de tiempo automatizada	StorageGRID sincroniza automáticamente los relojes del sistema de cada nodo en varios servidores de protocolo de tiempo de redes de tiempo (NTP) externos. Se requieren al menos cuatro servidores NTP de estrato 3 o posterior.	Asegura la misma referencia de tiempo en todos los nodos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Redes independientes para el tráfico de grid interno, de administración y de clientes	Los nodos de software y los dispositivos de hardware de StorageGRID admiten múltiples interfaces de red físicas y virtuales, para que los clientes puedan separar el tráfico de grid interno, de administración y de clientes en diferentes redes.	Permita a los administradores de Grid segregar el tráfico de red interno y externo y distribuir tráfico a través de redes con diferentes SLA.	—

Función	Función	Impacto	Cumplimiento de normativas
Varias interfaces de LAN virtual (VLAN)	StorageGRID admite la configuración de interfaces VLAN en sus redes de grid y cliente de StorageGRID.	Permita que los administradores de Grid dividan y aíslen el tráfico de aplicaciones para mejorar la seguridad, la flexibilidad y el rendimiento.	
Red cliente no confiable	La interfaz de red de cliente no confiable acepta conexiones entrantes solo en puertos que se han configurado explícitamente como puntos finales de equilibrio de carga.	Garantiza que las interfaces expuestas a redes que no son de confianza estén protegidas.	—
Firewall configurable	Gestionar puertos abiertos y cerrados para redes de administración, grid y cliente.	Permitir a los administradores de grid controlar el acceso a los puertos y administrar el acceso de dispositivos aprobados a los puertos.	
Comportamiento SSH mejorado	Al actualizar un nodo a StorageGRID 11,5, se generan nuevos certificados de host SSH y claves de host.	Mejora la protección contra ataques de hombre en el medio.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Cifrado de nodos	Como parte de la nueva función de cifrado del servidor host KMS, se agrega una nueva configuración de cifrado de nodos al instalador de dispositivos StorageGRID.	Este ajuste se debe activar durante la etapa de configuración de hardware de la instalación del dispositivo.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Integración del cloud

Comprende cómo StorageGRID se integra con los servicios en nube.

Función	Función	Impacto
Detección de virus basada en notificaciones	Los servicios de la plataforma StorageGRID admiten notificaciones de eventos. Las notificaciones de eventos se pueden usar con servicios de cloud computing externos para activar flujos de trabajo de análisis de virus en los datos.	Permite a los administradores inquilinos activar el análisis de virus de los datos mediante servicios de cloud computing externos.