Configurar ajustes de seguridad

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Configurar ajustes de seguridad

Administrar la política TLS y SSH

La política TLS y SSH determina 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. En general, utilice la política de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con los Criterios comunes o necesite utilizar otros cifrados.

> Algunos servicios de StorageGRID no se han actualizado para usar los cifrados en estas políticas.

Antes de empezar

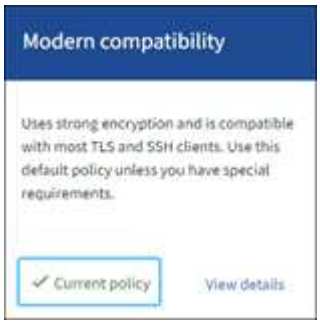
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

Seleccione una política de seguridad

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad**.

   La pestaña **Políticas TLS y SSH** muestra las políticas disponibles. La política actualmente activa se indica mediante una marca de verificación verde en el mosaico de políticas.



2. Revise los mosaicos para conocer las políticas disponibles.

Política	Descripción
Compatibilidad moderna (predeterminada)	Utilice la política predeterminada si necesita un cifrado fuerte y a menos que tenga requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.
Compatibilidad heredada	Utilice esta política si necesita opciones de compatibilidad adicionales para clientes más antiguos. Las opciones adicionales en esta política podrían hacerla menos segura que la política de compatibilidad moderna.

Política	Descripción
Criterios comunes	Utilice esta política si necesita la certificación Common Criteria.
FIPS estricto	Utilice esta política si necesita la certificación Common Criteria y usar el Módulo de seguridad criptográfica de NetApp 3.0.8 para conexiones de clientes externos a puntos finales de balanceador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento. **Nota**: Después de seleccionar esta política, todos los nodos deben estar"reiniciado de forma continua" para activar el módulo de seguridad criptográfica de NetApp . Utilice **Mantenimiento** > **Reinicio progresivo** para iniciar y supervisar los reinicios.
Costumbre	Cree una política personalizada si necesita aplicar sus propios cifrados.

3. Para ver detalles sobre los cifrados, protocolos y algoritmos de cada política, seleccione **Ver detalles**.
4. Para cambiar la política actual, seleccione **Usar política**.

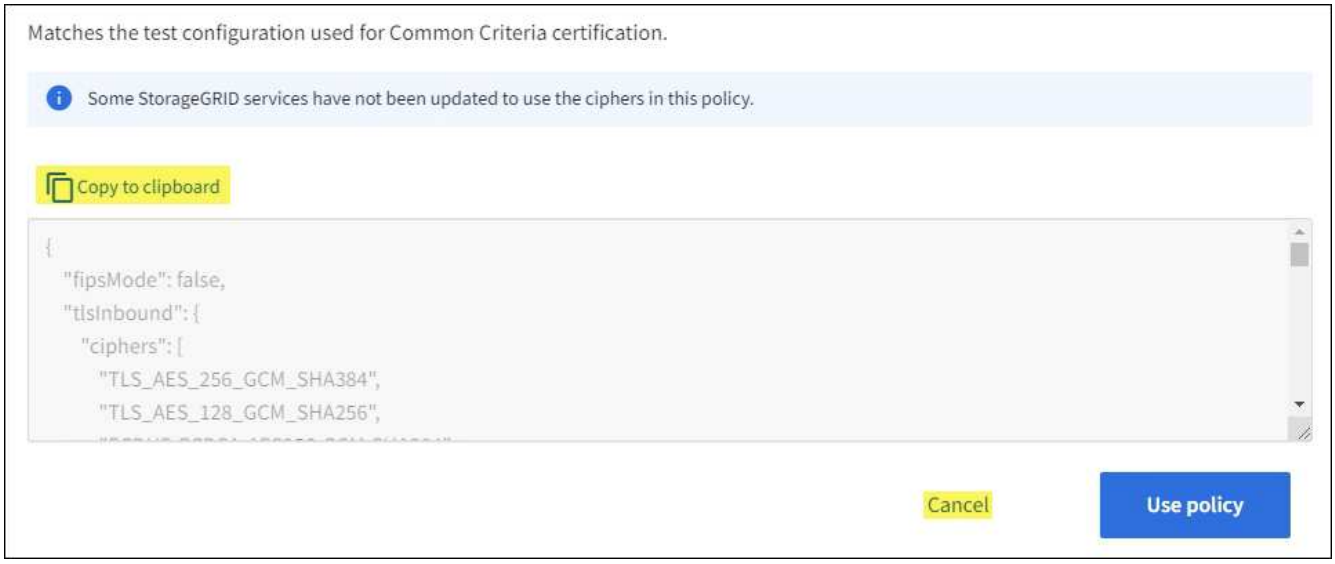
   Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Crear una política de seguridad personalizada

Puede crear una política personalizada si necesita aplicar sus propios cifrados.

Pasos

1. Desde el mosaico de la política que sea más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Seleccione **Copiar al portapapeles** y luego seleccione **Cancelar**.



3. Desde el mosaico **Política personalizada**, seleccione **Configurar y usar**.

4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Política de uso**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico Política personalizada.

6. Opcionalmente, seleccione **Editar configuración** para realizar más cambios en la nueva política personalizada.

Revertir temporalmente a la política de seguridad predeterminada

Si configuró una política de seguridad personalizada, es posible que no pueda iniciar sesión en Grid Manager si la política TLS configurada es incompatible con la"certificado de servidor configurado" .

Puede volver temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicie sesión en un nodo de administración:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

      Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Ejecute el siguiente comando:

   ```
   restore-default-cipher-configurations
   ```

3. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.
4. Siga los pasos enSeleccione una política de seguridad para configurar la política nuevamente.

Configurar la seguridad de la red y de los objetos

Puede configurar la seguridad de la red y de los objetos para cifrar los objetos almacenados, evitar ciertas solicitudes S3 o permitir que las conexiones de los clientes a los nodos de almacenamiento utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite el cifrado de todos los datos de los objetos a medida que se ingieren a través de S3. De forma predeterminada, los objetos almacenados no están cifrados, pero puede elegir cifrarlos utilizando el algoritmo de cifrado AES-128 o AES-256. Cuando habilita la configuración, todos los objetos recién ingeridos se cifran, pero no se realiza ningún cambio en los objetos almacenados existentes. Si deshabilita el cifrado, los objetos actualmente cifrados permanecerán cifrados, pero los objetos recién ingeridos no lo estarán.

La configuración de cifrado de objetos almacenados se aplica únicamente a los objetos S3 que no se han cifrado mediante cifrado a nivel de depósito o de objeto.

Para obtener más detalles sobre los métodos de cifrado de StorageGRID , consulte"Revisar los métodos de cifrado de StorageGRID" .

Evitar modificaciones del cliente

Evitar modificaciones del cliente es una configuración de todo el sistema. Cuando se selecciona la opción **Impedir modificación del cliente**, se rechazan las siguientes solicitudes.

API REST de S3

- Solicitudes de DeleteBucket
- Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

Habilitar HTTP para conexiones de nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Opcionalmente, puede habilitar HTTP para estas conexiones, por ejemplo, al probar una cuadrícula que no es de producción.

Utilice HTTP para las conexiones de nodo de almacenamiento solo si los clientes S3 necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento. No es necesario utilizar esta opción para clientes que solo usan conexiones HTTPS o para clientes que se conectan al servicio Load Balancer (porque puede"configurar cada punto final del balanceador de carga" para utilizar HTTP o HTTPS).

Ver"Resumen: Direcciones IP y puertos para conexiones de cliente" para conocer qué puertos utilizan los clientes S3 cuando se conectan a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccionar opciones

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes permiso de acceso root.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad**.
2. Seleccione la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utilice la configuración **Ninguno** (predeterminada) si no desea que se cifren los objetos almacenados, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación del cliente** si desea evitar que los clientes S3 realicen solicitudes específicas.

   > Si cambia esta configuración, tomará aproximadamente un minuto para que se aplique la nueva configuración. El valor configurado se almacena en caché para mejorar el rendimiento y la escala.

5. Opcionalmente, seleccione **Habilitar HTTP para conexiones de nodo de almacenamiento** si los clientes se conectan directamente a los nodos de almacenamiento y desea utilizar conexiones HTTP.

Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

6. Seleccione **Guardar**.

Cambiar la configuración de seguridad de la interfaz

La configuración de seguridad de la interfaz le permite controlar si se cierra la sesión de los usuarios si están inactivos durante más de la cantidad de tiempo especificada y si se incluye un seguimiento de pila en las respuestas de error de API.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"Permiso de acceso root" .

Acerca de esta tarea

La página **Configuración de seguridad** incluye las configuraciones de **Tiempo de espera de inactividad del navegador** y **Seguimiento de la pila de API de administración**.

Tiempo de espera por inactividad del navegador

Indica cuánto tiempo puede estar inactivo el navegador de un usuario antes de que se cierre la sesión. El valor predeterminado es 15 minutos.

El tiempo de espera por inactividad del navegador también está controlado por lo siguiente:

- Un temporizador StorageGRID independiente, no configurable, que se incluye para la seguridad del sistema. El token de autenticación de cada usuario expira 16 horas después de que el usuario inicia sesión. Cuando expira la autenticación de un usuario, ese usuario cierra la sesión automáticamente, incluso si el tiempo de espera de inactividad del navegador está deshabilitado o no se ha alcanzado el valor del tiempo de espera del navegador. Para renovar el token, el usuario deberá volver a iniciar sesión.
- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está habilitado para StorageGRID.

  Si SSO está habilitado y el navegador de un usuario expira, el usuario debe volver a ingresar sus credenciales de SSO para acceder a StorageGRID nuevamente. Ver "Configurar el inicio de sesión único" .

Seguimiento de la pila de la API de gestión

Controla si se devuelve un seguimiento de pila en las respuestas de error de API de Grid Manager y Tenant Manager.

Esta opción está deshabilitada de forma predeterminada, pero es posible que desee habilitar esta funcionalidad para un entorno de prueba. En general, debe dejar el seguimiento de pila deshabilitado en entornos de producción para evitar revelar detalles internos del software cuando ocurren errores de API.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad**.
2. Seleccione la pestaña **Interfaz**.

3. Para cambiar la configuración del tiempo de espera por inactividad del navegador:
   a. Expandir el acordeón.
   b. Para cambiar el período de tiempo de espera, especifique un valor entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
   c. Para desactivar esta función, desmarque la casilla de verificación.
   d. Seleccione **Guardar**.

      La nueva configuración no afecta a los usuarios que actualmente hayan iniciado sesión. Los usuarios deben iniciar sesión nuevamente o actualizar sus navegadores para que la nueva configuración de tiempo de espera surta efecto.

4. Para cambiar la configuración del seguimiento de la pila de la API de administración:
   a. Expandir el acordeón.
   b. Seleccione la casilla de verificación para devolver un seguimiento de la pila en las respuestas de error de API de Grid Manager y Tenant Manager.

      Deje el seguimiento de pila deshabilitado en entornos de producción para evitar revelar detalles internos del software cuando se producen errores de API.

   c. Seleccione **Guardar**.

Información de copyright

Información de la marca comercial