Configurar los ajustes de seguridad

StorageGRID software

NetApp
February 12, 2026

Tabla de contenidos

Configurar los ajustes de seguridad

Gestione la política TLS y SSH

La política de TLS y SSH determina qué protocolos y cifrados se usan para establecer conexiones TLS seguras con aplicaciones de cliente y conexiones SSH seguras a servicios StorageGRID internos.

La directiva de seguridad controla cómo TLS y SSH cifran los datos en movimiento. En general, utilice la directiva de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con Common Criteria o que necesite utilizar otros cifrados.

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

Antes de empezar

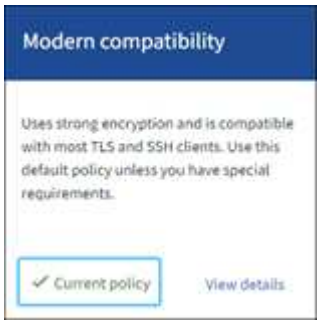
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

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 las pestañas para conocer las políticas disponibles.

Compatibilidad moderna (predeterminado)

Utilice la política predeterminada si necesita un cifrado fuerte y no tiene requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.

Compatibilidad con versiones anteriores

Utilice la política de compatibilidad heredada 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.

Criterios comunes

Utilice la política de Criterios Comunes si necesita la certificación de Criterios Comunes.

Estricta con FIPS

Utilice la política estricta FIPS si necesita la certificación Common Criteria y usar el módulo de seguridad criptográfica de NetApp (NCSM) 3.0.8 o el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 para conexiones de clientes externos a puntos finales del balanceador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento.

El módulo NCSM 3.0.8 y NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 se utilizan en las siguientes operaciones:

- NCSM
  - Conexiones TLS entre los siguientes servicios: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw y cache-svc
  - Conexiones TLS entre clientes y el servicio nginx-gw (puntos finales del balanceador de carga)
  - Conexiones TLS entre clientes y el servicio LDR
  - Cifrado de contenido de objetos para SSE-S3, SSE-C y la configuración de cifrado de objetos almacenados
  - Conexiones SSH

  Para obtener más información, consulte el Programa de validación de algoritmos criptográficos del NIST."Certificado #4838" .

- Módulo API criptográfica del kernel StorageGRID de NetApp

  El módulo NetApp StorageGRID Kernel Crypto API está presente únicamente en plataformas de dispositivos VM y StorageGRID .

  - Colección de entropía
  - Cifrado de nodos

  Para obtener más información, consulte el Programa de validación de algoritmos criptográficos del NIST."Certificados #A6242 a #A6257" y"Certificado de entropía n.° E223" .

Nota: Después de seleccionar esta política,"realizar un reinicio continuo" para que todos los nodos activen el NCSM. Utilice **Mantenimiento** > **Reinicio progresivo** para iniciar y supervisar los reinicios.

Personalizado

Cree una política personalizada si necesita aplicar sus propios cifrados.

De manera opcional, si su StorageGRID tiene requisitos de criptografía FIPS 140, habilite la función de modo FIPS para usar el módulo NCSM 3.0.8 y NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

a. Establezca el `fipsMode` parámetro a `true` .

b. Cuando se le solicite,"realizar un reinicio continuo" para que todos los nodos activen los módulos de criptografía. Utilice **Mantenimiento** > **Reinicio progresivo** para iniciar y supervisar los reinicios.

c. Seleccione **Soporte** > **Diagnóstico** para ver las versiones activas del módulo FIPS.

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

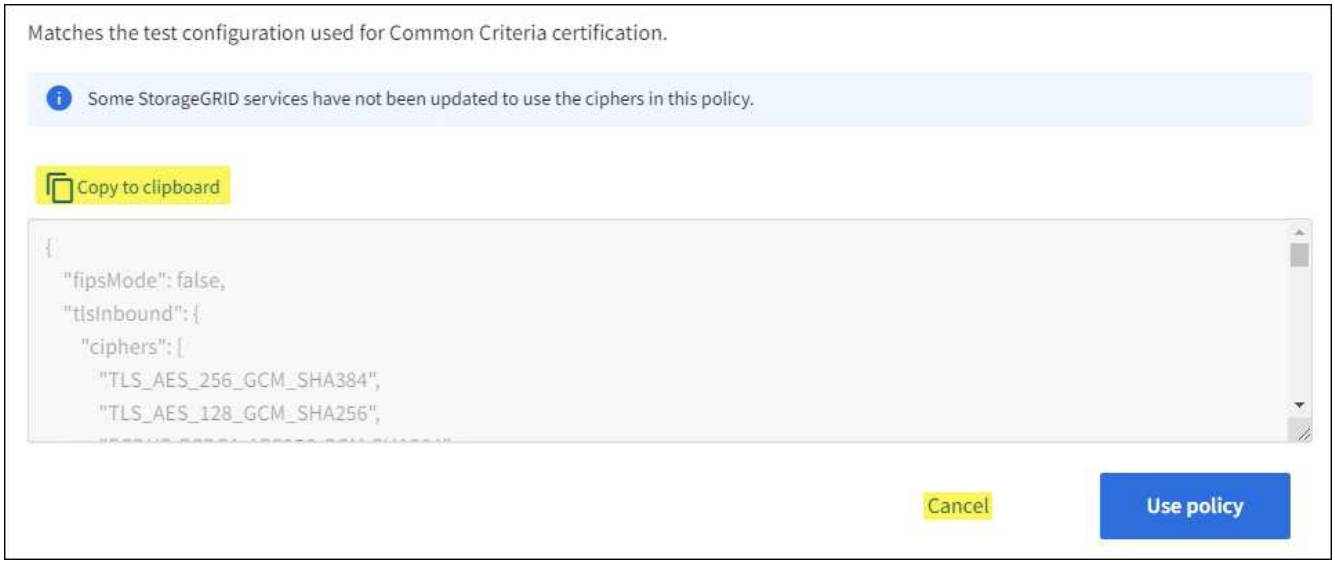
   Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Cree 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 es más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Selecciona **Copiar al portapapeles** y luego selecciona **Cancelar**.



3. En el mosaico **Política personalizada**, selecciona **Configurar y usar**.
4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Usar política**.

   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.

Vuelva temporalmente a la política de seguridad predeterminada

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

Puede revertir temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicie sesión en un nodo de administrador:
   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 raíz: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

2. Ejecute el siguiente comando:

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

3. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.
4. Siga los pasos de Seleccione una política de seguridad para volver a configurar la política.

Configure la seguridad de la red y de los objetos

Puede configurar la seguridad de red y de objetos para cifrar objetos almacenados, para evitar determinadas solicitudes S3 o para permitir que las conexiones de cliente 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 objetos tal como se ingieren a través de S3. De forma predeterminada, los objetos almacenados no se cifran, pero puede optar por cifrar objetos mediante el algoritmo de cifrado AES-128 o AES-256. Cuando se activa 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 cifrados actualmente permanecen cifrados, pero los objetos recién procesados no se cifran.

La configuración de cifrado de objetos almacenados se aplica solo a objetos S3 que no han sido cifrados por el cifrado a nivel de cubo o de objeto.

Para obtener más información sobre los métodos de cifrado StorageGRID, consulte "Consulte los métodos de cifrado de StorageGRID".

Impida la modificación del cliente

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

API REST DE S3

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

Active HTTP para las conexiones del nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea 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 utilizan conexiones HTTPS o para clientes que se conectan al servicio de equilibrio de carga (porque puede "configure cada punto final del equilibrador de carga"usar HTTP o HTTPS).

Consulte "Resumen: Direcciones IP y puertos para conexiones cliente"para saber qué usan los clientes de S3 de los puertos al conectarse a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccione las opciones

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tiene permiso de acceso raíz.

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 los objetos almacenados se cifren, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación de cliente** si desea evitar que los clientes de S3 realicen solicitudes específicas.

   Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

5. Opcionalmente, seleccione **Activar HTTP para conexiones de nodos de almacenamiento** si los clientes se conectan directamente a 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**.

Cambie la configuración de seguridad de la interfaz

La configuración de seguridad de la interfaz le permite controlar si los usuarios están

desconectados 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 la API.

Antes de empezar

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

Acerca de esta tarea

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

Tiempo de espera de inactividad del explorador

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

El tiempo de espera de inactividad del navegador también se controla mediante lo siguiente:

- Temporizador StorageGRID independiente no configurable, que se incluye para la seguridad del sistema. El token de autenticación de cada usuario caduca 16 horas después de que el usuario inicia sesión. Cuando caduca la autenticación de un usuario, ese usuario se cierra automáticamente, incluso si el tiempo de espera de inactividad del navegador está desactivado o no se ha alcanzado el valor del tiempo de espera del explorador. Para renovar el token, el usuario debe volver a iniciar sesión.
- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está activado 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 "Cómo funciona el SSO" .

Seguimiento de la pila de API de gestión

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

Esta opción está desactivada de forma predeterminada, pero es posible que desee activar esta funcionalidad para un entorno de prueba. En general, debe dejar el rastreo de pila desactivado en entornos de producción para evitar revelar detalles internos del software cuando se producen 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 de inactividad del navegador:
   a. Expande 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, desactive la casilla de verificación.
   d. Seleccione **Guardar**.

      La nueva configuración no afecta a los usuarios que están conectados actualmente. Los usuarios deben iniciar sesión de nuevo o actualizar sus exploradores para que la nueva configuración de tiempo de espera surta efecto.

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

      Deje desactivado el rastreo de pila en entornos de producción para evitar revelar los detalles internos del software cuando se produzcan errores de API.

   c. Seleccione **Guardar**.

Administrar el acceso SSH externo

Administre el acceso SSH para el tráfico entrante a la red bloqueando o permitiendo el acceso externo. La gestión del acceso externo SSH no tiene impacto en el tráfico entre nodos de la red.

Antes de empezar

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

Acerca de esta tarea

Para mejorar la seguridad del sistema, el acceso SSH externo está bloqueado de forma predeterminada. Si necesita realizar tareas que requieren acceso SSH entrante, como resolución de problemas, permita temporalmente el acceso externo. Cuando haya terminado la tarea, bloquee el acceso externo.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Configuración de seguridad**.
2. Seleccione la pestaña **Bloquear SSH**.
3. Utilice la opción **Bloquear acceso SSH entrante** para administrar el acceso SSH externo:
   a. Seleccione la casilla de verificación para bloquear el acceso (predeterminado).
   b. Desmarque la casilla de verificación para permitir el acceso.

      Requiere acceso al puerto 22 entre el portátil de servicio y todos los demás nodos de la red. Elimine el acceso al puerto 22 cuando complete la tarea de mantenimiento.

4. Seleccione **Guardar**.