Configurar los ajustes de seguridad

StorageGRID 11.7

NetApp
April 12, 2024

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 un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Seleccione una política de seguridad

Pasos

1. Selecciona **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 obtener más información sobre las políticas disponibles.

Política	Descripción
Compatibilidad moderna (predeterminado)	Use la directiva predeterminada si necesita cifrado seguro y a menos que tenga requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.
Compatibilidad con versiones anteriores	Utilice esta directiva si necesita opciones de compatibilidad adicionales para clientes antiguos. Las opciones adicionales de esta política podrían hacerlo menos seguro que la política de compatibilidad moderna.

Política	Descripción
Criterios comunes	Utilice esta política si necesita la certificación Common Criteria.
Estricta con FIPS	Use esta directiva si necesita la certificación de criterios comunes y necesita utilizar el módulo de seguridad criptográfica 3.0.0 de NetApp para conexiones de clientes externos a extremos del equilibrador de carga, tenant Manager y Grid Manager. El uso de esta política puede reducir el rendimiento.
Personalizado	Cree una política personalizada si necesita aplicar sus propios cifrados.

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 el "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 `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

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 ciertas solicitudes S3 y Swift, 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 bloques
- Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

API REST de Swift

- Eliminar solicitudes de contenedor
- Solicitudes para modificar cualquier objeto existente. Por ejemplo, se deniegan las siguientes operaciones: Put Overwrite, Delete, Metadata Update, etc.

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 nodos de almacenamiento solo si los clientes S3 y Swift necesitan establecer conexiones HTTP directamente a los nodos de almacenamiento. No es necesario que utilice esta opción para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio de Equilibrador de Carga (porque puede hacerlo "configure cada punto final del equilibrador de carga" Para usar HTTP o HTTPS).

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

Seleccione las opciones

Antes de empezar

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

Pasos

1. Selecciona **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 S3 y Swift 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**.

Cambiar el tiempo de espera de inactividad del navegador

Puede controlar si los usuarios de Grid Manager y de arrendatario Manager han cerrado la sesión si están inactivos durante más de un cierto período de tiempo.

Antes de empezar

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

Acerca de esta tarea

El tiempo de espera de inactividad del navegador es de forma predeterminada 15 minutos. Si el explorador de un usuario no está activo durante este período de tiempo, el usuario se cerrará la sesión.

Según sea necesario, puede aumentar o disminuir el período de tiempo de espera configurando la opción **Cerrar sesión de usuarios inactivos después**.

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. De forma predeterminada, 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 desconecta automáticamente, incluso si el tiempo de espera de inactividad del explorador 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 se activa SSO y se agota el tiempo de espera del explorador de un usuario, el usuario debe volver a introducir sus credenciales SSO para volver a acceder a StorageGRID. Consulte "Configurar el inicio de sesión único".

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.
2. Seleccione la pestaña **Tiempo de inactividad del navegador**.
3. En el campo **Cerrar sesión de usuarios inactivos después**, especifique un período de tiempo de espera del navegador entre 60 segundos y 7 días.

   Puede especificar el período de tiempo de espera del explorador en segundos, minutos, horas o días.

4. Seleccione **Guardar**. Si un explorador está inactivo durante la cantidad de tiempo especificada, el usuario se cierra sesión en Grid Manager o Tenant Manager.

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

Información de copyright

Información de la marca comercial