Gestionar la seguridad

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Gestionar la seguridad

Gestionar la seguridad

Puede configurar varias configuraciones de seguridad desde Grid Manager para ayudar a proteger su sistema StorageGRID .

Administrar el cifrado

StorageGRID ofrece varias opciones para cifrar datos. Debería"revise los métodos de cifrado disponibles" para determinar cuáles cumplen con sus requisitos de protección de datos.

Administrar certificados

Puede"configurar y administrar los certificados del servidor" Se utiliza para conexiones HTTP o los certificados de cliente utilizados para autenticar la identidad de un cliente o usuario en el servidor.

Configurar servidores de administración de claves

Usando un"servidor de gestión de claves" Le permite proteger los datos de StorageGRID incluso si se elimina un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo pueda comunicarse con el KMS.

> Para utilizar la administración de claves de cifrado, debe habilitar la configuración **Cifrado de nodo** para cada dispositivo durante la instalación, antes de agregar el dispositivo a la red.

Administrar la configuración del proxy

Si está utilizando servicios de la plataforma S3 o grupos de almacenamiento en la nube, puede configurar un"servidor proxy de almacenamiento" entre los nodos de almacenamiento y los puntos finales externos de S3. Si envía paquetes de AutoSupport mediante HTTPS o HTTP, puede configurar un"servidor proxy de administración" entre los nodos de administración y el soporte técnico.

Controlar cortafuegos

Para mejorar la seguridad de su sistema, puede controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en el"cortafuegos externo" . También puede controlar el acceso a la red de cada nodo configurando su"cortafuegos interno" . Puede evitar el acceso a todos los puertos excepto aquellos necesarios para su implementación.

Revisar los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para cifrar datos. Debe revisar los métodos disponibles para determinar cuáles cumplen con sus requisitos de protección de datos.

La tabla proporciona un resumen de alto nivel de los métodos de cifrado disponibles en StorageGRID.

Opción de cifrado	Cómo funciona	Se aplica a
Servidor de administración de claves (KMS) en Grid Manager	Tú"configurar un servidor de administración de claves" para el sitio StorageGRID y "Habilitar el cifrado de nodos para el dispositivo" . Luego, un nodo del dispositivo se conecta al KMS para solicitar una clave de cifrado de clave (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de dispositivo que tienen **Cifrado de nodo** habilitado durante la instalación. Todos los datos del dispositivo están protegidos contra pérdida física o eliminación del centro de datos. **Nota**: La administración de claves de cifrado con un KMS solo es compatible con nodos de almacenamiento y dispositivos de servicios.
Página de cifrado de unidad en el instalador del dispositivo StorageGRID	Si el dispositivo contiene unidades que admiten cifrado de hardware, puede establecer una frase de contraseña para la unidad durante la instalación. Cuando se establece una frase de contraseña de unidad, es imposible que alguien recupere datos válidos de unidades que se han eliminado del sistema, a menos que conozca la frase de contraseña. Antes de comenzar la instalación, vaya a **Configurar hardware** > **Cifrado de unidad** para establecer una frase de contraseña de unidad que se aplique a todas las unidades con cifrado automático administradas por StorageGRID en un nodo.	Dispositivos que contienen unidades con cifrado automático. Todos los datos de las unidades seguras están protegidos contra pérdida física o eliminación del centro de datos. El cifrado de unidad no se aplica a las unidades administradas SANtricity. Si tiene un dispositivo de almacenamiento con unidades de autocifrado y controladores SANtricity , puede habilitar la seguridad de la unidad en SANtricity.
Impulse la seguridad en SANtricity System Manager	Si la función Seguridad de la unidad está habilitada para su dispositivo StorageGRID , puede usar "SANtricity System Manager" para crear y gestionar la clave de seguridad. La clave es necesaria para acceder a los datos de las unidades protegidas.	Dispositivos de almacenamiento que tienen unidades de cifrado de disco completo (FDE) o unidades de cifrado automático. Todos los datos de las unidades seguras están protegidos contra pérdida física o eliminación del centro de datos. No se puede utilizar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio.

Opción de cifrado	Cómo funciona	Se aplica a
Cifrado de objetos almacenados	Habilitas el"Cifrado de objetos almacenados" opción en el Administrador de cuadrícula. Cuando esta opción está habilitada, todos los objetos nuevos que no estén cifrados en el nivel de depósito o en el nivel de objeto se cifran durante la ingesta.	Datos de objetos S3 recién ingeridos. Los objetos almacenados existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.
Cifrado de buckets S3	Emite una solicitud PutBucketEncryption para habilitar el cifrado para el depósito. Cualquier objeto nuevo que no esté cifrado a nivel de objeto se cifra durante la ingesta.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el depósito. Los objetos de bucket existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en buckets"
Cifrado del lado del servidor de objetos S3 (SSE)	Emite una solicitud S3 para almacenar un objeto e incluirlo `x-amz-server-side-encryption` encabezado de solicitud.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. StorageGRID administra las claves. "Utilice cifrado del lado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Emite una solicitud S3 para almacenar un objeto e incluye tres encabezados de solicitud. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. Las claves se administran fuera de StorageGRID. "Utilice cifrado del lado del servidor"

Opción de cifrado	Cómo funciona	Se aplica a
Cifrado de volumen externo o almacén de datos	Utilice un método de cifrado externo a StorageGRID para cifrar un volumen o almacén de datos completo, si su plataforma de implementación lo admite.	Todos los datos de objetos, metadatos y datos de configuración del sistema, asumiendo que cada volumen o almacén de datos está cifrado. Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados.
Cifrado de objetos fuera de StorageGRID	Utilice un método de cifrado externo a StorageGRID para cifrar datos y metadatos de objetos antes de que se ingieran en StorageGRID.	Solo datos de objeto y metadatos (los datos de configuración del sistema no están cifrados). Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados. "Amazon Simple Storage Service - Guía del usuario: Protección de datos mediante cifrado del lado del cliente"

Utilice múltiples métodos de cifrado

Dependiendo de sus requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

- Puede utilizar un KMS para proteger los nodos del dispositivo y también usar la función de seguridad de la unidad en SANtricity System Manager para "cifrar doblemente" los datos en las unidades con cifrado automático en los mismos dispositivos.
- Puede utilizar un KMS para proteger datos en los nodos del dispositivo y también utilizar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de sus objetos requieren cifrado, considere controlar el cifrado a nivel de depósito o de objeto individual. Habilitar múltiples niveles de cifrado tiene un costo de rendimiento adicional.

Administrar certificados

Administrar certificados de seguridad

Los certificados de seguridad son pequeños archivos de datos que se utilizan para crear conexiones seguras y confiables entre los componentes de StorageGRID y entre los componentes de StorageGRID y sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- Se requieren **certificados de servidor** cuando se utilizan conexiones HTTPS. Los certificados de servidor se utilizan para establecer conexiones seguras entre clientes y servidores, autenticando la identidad de un servidor ante sus clientes y proporcionando una ruta de comunicación segura para los datos. Tanto el servidor como el cliente tienen una copia del certificado.
- Los **certificados de cliente** autentican la identidad de un cliente o usuario en el servidor, proporcionando una autenticación más segura que las contraseñas solas. Los certificados de cliente no cifran los datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado del servidor, que contiene una clave pública. El cliente verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como servidor para algunas conexiones (como el punto final del equilibrador de carga) o como cliente para otras conexiones (como el servicio de replicación CloudMirror).

Certificado CA de Grid predeterminado

StorageGRID incluye una autoridad de certificación (CA) incorporada que genera un certificado CA de Grid interno durante la instalación del sistema. El certificado CA de Grid se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID . Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan totalmente con las políticas de seguridad de la información de su organización. Si bien puede utilizar el certificado CA de Grid para un entorno que no sea de producción, la mejor práctica para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa. También se admiten conexiones no seguras sin certificado, pero no se recomiendan.

- Los certificados CA personalizados no eliminan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones del servidor.
- Todos los certificados personalizados deben cumplir con los"Pautas de fortalecimiento del sistema para certificados de servidor" .
- StorageGRID admite la agrupación de certificados de una CA en un solo archivo (conocido como paquete de certificados de CA).

> ⓘ StorageGRID también incluye certificados CA del sistema operativo que son los mismos en todas las redes. En entornos de producción, asegúrese de especificar un certificado personalizado firmado por una autoridad de certificación externa en lugar del certificado CA del sistema operativo.

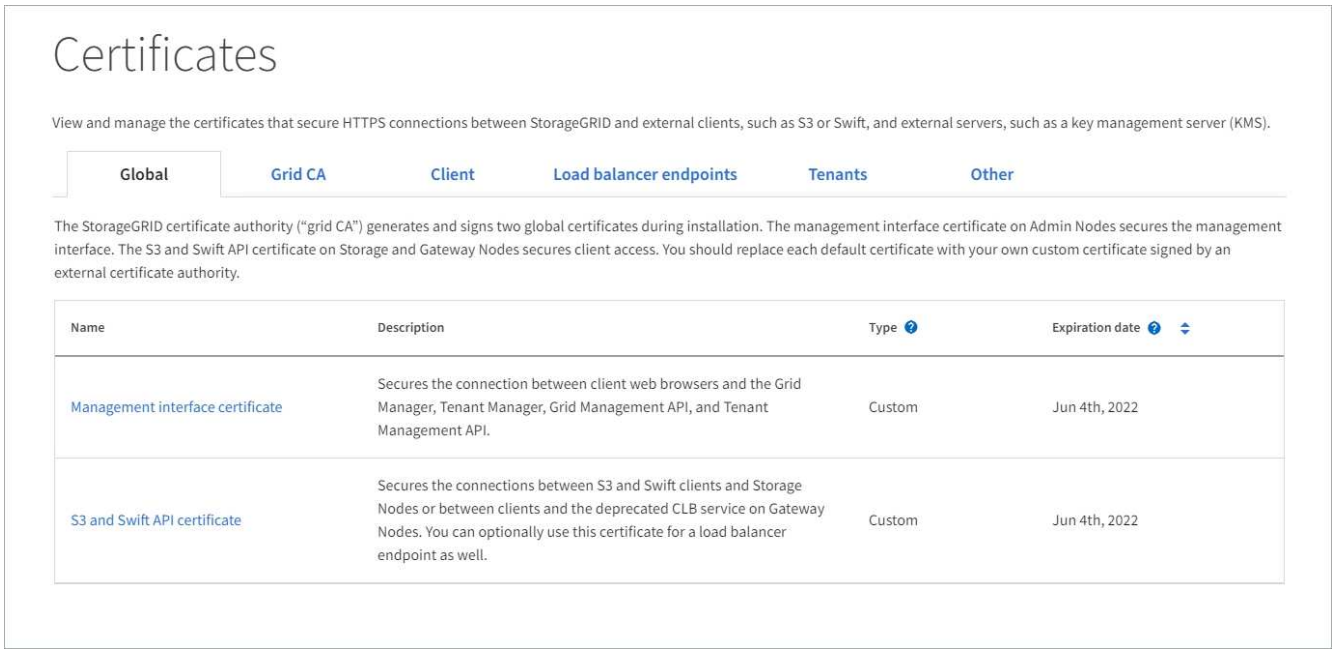
Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Debe tener todos los certificados necesarios para su configuración específica de StorageGRID listos antes de configurar el sistema.

Certificados de seguridad de acceso

Puede acceder a información sobre todos los certificados StorageGRID en una sola ubicación, junto con enlaces al flujo de trabajo de configuración para cada certificado.

Pasos

1. Desde Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.



2. Seleccione una pestaña en la página Certificados para obtener información sobre cada categoría de certificado y acceder a la configuración del certificado. Puedes acceder a una pestaña si tienes la"permiso apropiado" .

   - **Global**: protege el acceso a StorageGRID desde navegadores web y clientes API externos.
   - **Grid CA**: protege el tráfico interno de StorageGRID .
   - **Cliente**: protege las conexiones entre clientes externos y la base de datos StorageGRID Prometheus.
   - **Puntos finales del balanceador de carga**: protege las conexiones entre los clientes S3 y el balanceador de carga StorageGRID .
   - **Inquilinos**: protege las conexiones a servidores de federación de identidad o desde puntos finales de servicio de la plataforma a recursos de almacenamiento S3.
   - **Otro**: Protege las conexiones StorageGRID que requieren certificados específicos.

     A continuación se describe cada pestaña con enlaces a detalles adicionales del certificado.

Global

Los certificados globales protegen el acceso a StorageGRID desde navegadores web y clientes API S3 externos. La autoridad de certificación StorageGRID genera inicialmente dos certificados globales durante la instalación. La mejor práctica para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa.

- Certificado de interfaz de gestión:Asegura las conexiones del navegador web del cliente a las interfaces de administración de StorageGRID .
- Certificado API S3:Asegura las conexiones de API de cliente a los nodos de almacenamiento, nodos de administración y nodos de puerta de enlace, que las aplicaciones de cliente S3 utilizan para cargar y descargar datos de objetos.

La información sobre los certificados globales que están instalados incluye:

- **Nombre**: Nombre del certificado con enlace para administrar el certificado.
- **Descripción**
- **Tipo**: Personalizado o predeterminado. + Siempre debe utilizar un certificado personalizado para mejorar la seguridad de la red.
- **Fecha de vencimiento**: si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Puede:

- Reemplace los certificados predeterminados con certificados personalizados firmados por una autoridad de certificación externa para mejorar la seguridad de la red:
  - "Reemplazar el certificado de interfaz de administración generado por StorageGRID predeterminado"Se utiliza para conexiones de Grid Manager y Tenant Manager.
  - "Reemplazar el certificado de API S3"Se utiliza para conexiones de nodo de almacenamiento y punto final del equilibrador de carga (opcional).
- "Restaurar el certificado de interfaz de administración predeterminado" .
- "Restaurar el certificado API S3 predeterminado" .
- "Utilice un script para generar un nuevo certificado de interfaz de administración autofirmado" .
- Copiar o descargar el"certificado de interfaz de gestión" o"Certificado API S3" .

Red CA

ElCertificado de CA de Grid , generado por la autoridad de certificación de StorageGRID durante la instalación de StorageGRID , protege todo el tráfico interno de StorageGRID .

La información del certificado incluye la fecha de vencimiento del certificado y el contenido del certificado.

Puede"copiar o descargar el certificado de Grid CA" , pero no puedes cambiarlo.

Cliente

Certificados de cliente, generado por una autoridad de certificación externa, protege las conexiones entre las herramientas de monitoreo externas y la base de datos StorageGRID Prometheus.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede usar para acceder a la base de datos de Prometheus, junto con la fecha de

vencimiento del certificado.

Puede:

- "Cargar o generar un nuevo certificado de cliente."
- Seleccione un nombre de certificado para mostrar los detalles del certificado donde podrá:
  - "Cambiar el nombre del certificado del cliente."
  - "Establecer el permiso de acceso de Prometheus."
  - "Cargar y reemplazar el certificado del cliente."
  - "Copie o descargue el certificado del cliente."
  - "Eliminar el certificado del cliente."
- Seleccione **Acciones** para acceder rápidamente"editar" ,"adjuntar" , o"eliminar" un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez usando **Acciones** > **Eliminar**.

Puntos finales del balanceador de carga

Certificados de punto final del balanceador de cargaAsegure las conexiones entre los clientes S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración.

La tabla de puntos finales del equilibrador de carga tiene una fila para cada punto final del equilibrador de carga configurado e indica si se utiliza el certificado de API S3 global o un certificado de punto final del equilibrador de carga personalizado para el punto final. También se muestra la fecha de vencimiento de cada certificado.

> Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Puede:

- "Ver un punto final del balanceador de carga", incluidos los detalles de su certificado.
- "Especifique un certificado de punto final del equilibrador de carga para FabricPool."
- "Utilice el certificado API global de S3"en lugar de generar un nuevo certificado de punto final del equilibrador de carga.

Inquilinos

Los inquilinos pueden utilizarcertificados de servidor de federación de identidad ocertificados de punto final del servicio de plataforma para proteger sus conexiones con StorageGRID.

La tabla de inquilinos tiene una fila para cada inquilino e indica si cada inquilino tiene permiso para usar su propia fuente de identidad o servicios de plataforma.

Puede:

- "Seleccione un nombre de inquilino para iniciar sesión en el Administrador de inquilinos"
- "Seleccione un nombre de inquilino para ver los detalles de la federación de identidad del inquilino"
- "Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilinos"

- "Especifique un certificado de punto final del servicio de plataforma durante la creación del punto final"

Otro

StorageGRID utiliza otros certificados de seguridad para fines específicos. Estos certificados se enumeran por su nombre funcional. Otros certificados de seguridad incluyen:

- Certificados de grupo de almacenamiento en la nube
- Certificados de notificación de alertas por correo electrónico
- Certificados de servidor syslog externo
- Certificados de conexión de la federación de red
- Certificados de federación de identidad
- Certificados de servidor de administración de claves (KMS)
- Certificados de inicio de sesión único

La información indica el tipo de certificado que utiliza una función y las fechas de vencimiento de sus certificados de servidor y cliente, según corresponda. Al seleccionar un nombre de función, se abre una pestaña del navegador donde puede ver y editar los detalles del certificado.

> Solo puede ver y acceder a la información de otros certificados si tiene la"permiso apropiado" .

Puede:

- "Especifique un certificado de grupo de almacenamiento en la nube para S3, C2S S3 o Azure"
- "Especificar un certificado para notificaciones de alerta por correo electrónico"
- "Utilice un certificado para un servidor syslog externo"
- "Rotar certificados de conexión de federación de red"
- "Ver y editar un certificado de federación de identidad"
- "Cargar certificados de cliente y servidor del servidor de administración de claves (KMS)"
- "Especificar manualmente un certificado SSO para una relación de confianza de usuario autenticado"

Detalles del certificado de seguridad

A continuación se describe cada tipo de certificado de seguridad, con enlaces a las instrucciones de implementación.

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los navegadores web del cliente y la interfaz de administración de StorageGRID , lo que permite a los usuarios acceder a Grid Manager y Tenant Manager sin advertencias de seguridad. Este certificado también autentica las conexiones de la API de administración de red y la API de administración de inquilinos. Puede utilizar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.	**CONFIGURACIÓN** > **Seguridad** > **Certificados**, seleccione la pestaña **Global** y luego seleccione **Certificado de interfaz de administración**	"Configurar certificados de interfaz de administración"

Certificado API S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica conexiones seguras de cliente S3 a un nodo de almacenamiento y a puntos finales del balanceador de carga (opcional).	**CONFIGURACIÓN** > **Seguridad** > **Certificados**, seleccione la pestaña **Global** y luego seleccione **Certificado API S3**	"Configurar certificados de API S3"

Certificado de CA de Grid

Ver elDescripción del certificado de CA de Grid predeterminado .

Certificado de cliente administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Se instala en cada cliente, lo que permite que StorageGRID autentique el acceso de clientes externos. • Permite que los clientes externos autorizados accedan a la base de datos StorageGRID Prometheus. • Permite la monitorización segura de StorageGRID mediante herramientas externas.	**CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**	"Configurar certificados de cliente"

Certificado de punto final del balanceador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los clientes S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración. Puede cargar o generar un certificado de equilibrador de carga cuando configura un punto final de equilibrador de carga. Las aplicaciones cliente utilizan el certificado del equilibrador de carga cuando se conectan a StorageGRID para guardar y recuperar datos de objetos. También puedes utilizar una versión personalizada del globalCertificado API S3 Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar las conexiones del balanceador de carga, no es necesario cargar ni generar un certificado separado para cada punto final del balanceador de carga. **Nota:** El certificado utilizado para la autenticación del equilibrador de carga es el certificado más usado durante el funcionamiento normal de StorageGRID .	**CONFIGURACIÓN** > **Red** > **Puntos finales del balanceador de carga**	• "Configurar los puntos finales del balanceador de carga" • "Crear un punto final de balanceador de carga para FabricPool"

Certificado de punto final del grupo de almacenamiento en la nube

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde un grupo de almacenamiento en la nube StorageGRID a una ubicación de almacenamiento externa, como S3 Glacier o Microsoft Azure Blob Storage. Se requiere un certificado diferente para cada tipo de proveedor de nube.	**ILM** > **Grupos de almacenamiento**	"Crear un grupo de almacenamiento en la nube"

Certificado de notificación de alerta por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre un servidor de correo electrónico SMTP y StorageGRID que se utiliza para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren seguridad de la capa de transporte (TLS), debe especificar el certificado CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo electrónico SMTP requiere certificados de cliente para la autenticación.	**ALERTAS** > **Configuración de correo electrónico**	"Configurar notificaciones por correo electrónico para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID. **Nota:** No se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	**CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**	"Utilice un servidor syslog externo"

Certificado de conexión de federación de red

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema StorageGRID actual y otra red en una conexión de federación de redes.	**CONFIGURACIÓN** > **Sistema** > **Federación de red**	• "Crear conexiones de federación de red" • "Rotar certificados de conexión"

Certificado de federación de identidad

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidad externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidad, que permite que los grupos de administradores y los usuarios sean gestionados por un sistema externo.	**CONFIGURACIÓN** > **Control de acceso** > **Federación de identidades**	"Utilizar la federación de identidades"

Certificado de servidor de administración de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de administración de claves externo (KMS), que proporciona claves de cifrado a los nodos del dispositivo StorageGRID .	**CONFIGURACIÓN** > **Seguridad** > **Servidor de gestión de claves**	"Agregar servidor de administración de claves (KMS)"

Certificado de punto final de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión del servicio de la plataforma StorageGRID a un recurso de almacenamiento S3.	**Administrador de inquilinos** > **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**	"Crear punto final de servicios de plataforma" "Editar el punto final de los servicios de la plataforma"

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidad, como los Servicios de federación de Active Directory (AD FS) y StorageGRID , que se utilizan para solicitudes de inicio de sesión único (SSO).	**CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**	"Configurar el inicio de sesión único"

Ejemplos de certificados

Ejemplo 1: Servicio de balanceo de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Configura un punto final del equilibrador de carga y carga o genera un certificado de servidor en StorageGRID.
2. Configura una conexión de cliente S3 al punto final del equilibrador de carga y carga el mismo certificado en el cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al punto final del balanceador de carga mediante HTTPS.

4. StorageGRID responde con el certificado del servidor, que contiene una clave pública, y con una firma basada en la clave privada.
5. El cliente verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión utilizando la misma clave pública.
6. El cliente envía datos de objetos a StorageGRID.

Ejemplo 2: Servidor de administración de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Al utilizar el software de servidor de administración de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por una CA, un certificado de cliente público y la clave privada para el certificado de cliente.
2. Con Grid Manager, configura un servidor KMS y carga los certificados del servidor y del cliente y la clave privada del cliente.
3. Cuando un nodo StorageGRID necesita una clave de cifrado, realiza una solicitud al servidor KMS que incluye datos del certificado y una firma basada en la clave privada.
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde utilizando la conexión validada.

Tipos de certificados de servidor admitidos

El sistema StorageGRID admite certificados personalizados cifrados con RSA o ECDSA (algoritmo de firma digital de curva elíptica).

> El tipo de cifrado para la política de seguridad debe coincidir con el tipo de certificado del servidor. Por ejemplo, los cifrados RSA requieren certificados RSA y los cifrados ECDSA requieren certificados ECDSA. Ver "Administrar certificados de seguridad" . Si configura una política de seguridad personalizada que no es compatible con el certificado del servidor, puede"volver temporalmente a la política de seguridad predeterminada" .

Para obtener más información sobre cómo StorageGRID protege las conexiones de los clientes, consulte"Seguridad para clientes S3" .

Configurar certificados de interfaz de administración

Puede reemplazar el certificado de interfaz de administración predeterminado con un único certificado personalizado que permita a los usuarios acceder al Administrador de Grid y al Administrador de inquilinos sin encontrar advertencias de seguridad. También puede volver al certificado de interfaz de administración predeterminado o generar uno nuevo.

Acerca de esta tarea

De forma predeterminada, a cada nodo de administración se le emite un certificado firmado por la CA de la red. Estos certificados firmados por CA se pueden reemplazar por un único certificado de interfaz de administración personalizada común y su clave privada correspondiente.

Debido a que se utiliza un único certificado de interfaz de administración personalizado para todos los nodos de administración, debe especificar el certificado como comodín o como certificado multidominio si los clientes

necesitan verificar el nombre de host al conectarse al Administrador de red y al Administrador de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administración en la cuadrícula.

Debe completar la configuración en el servidor y, dependiendo de la autoridad de certificación raíz (CA) que esté utilizando, los usuarios también podrían necesitar instalar el certificado de CA de Grid en el navegador web que usarán para acceder a Grid Manager y Tenant Manager.

Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración del certificado de servidor para la interfaz de administración** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **Certificados** y mirando la fecha de vencimiento del certificado de la interfaz de administración en la pestaña Global.

Si accede al Administrador de red o al Administrador de inquilinos mediante un nombre de dominio en lugar de una dirección IP, el navegador muestra un error de certificado sin una opción para omitirlo si ocurre alguna de las siguientes situaciones:

- Su certificado de interfaz de administración personalizada caduca.
- TúRevertir de un certificado de interfaz de administración personalizado al certificado de servidor predeterminado .

Agregar un certificado de interfaz de administración personalizado

Para agregar un certificado de interfaz de administración personalizado, puede proporcionar su propio certificado o generar uno utilizando Grid Manager.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **Usar certificado personalizado**.
4. Subir o generar el certificado.

Subir certificado

Cargue los archivos de certificado de servidor necesarios.

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor**: el archivo de certificado de servidor personalizado (codificado en PEM).
- **Clave privada del certificado**: El archivo de clave privada del certificado del servidor personalizado(`.key`).

> Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete CA**: un único archivo opcional que contiene los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Expande **Detalles del certificado** para ver los metadatos de cada certificado que hayas cargado. Si cargó un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

  Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Guardar**. + El certificado de interfaz de administración personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generar certificado

Generar los archivos de certificado del servidor.

> La mejor práctica para un entorno de producción es utilizar un certificado de interfaz de administración personalizado firmado por una autoridad de certificación externa.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

   - Seleccione **Descargar certificado** para guardar el archivo del certificado.

     Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Seleccione **Guardar**. + El certificado de interfaz de administración personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Actualice la página para asegurarse de que el navegador web esté actualizado.

> Después de cargar o generar un nuevo certificado, espere hasta un día para que desaparezcan las alertas de vencimiento del certificado relacionadas.

6. Después de agregar un certificado de interfaz de administración personalizado, la página Certificado de interfaz de administración muestra información detallada de los certificados que están en uso. + Puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado de interfaz de administración predeterminado

Puede volver a utilizar el certificado de interfaz de administración predeterminado para las conexiones de Grid Manager y Tenant Manager.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **Usar certificado predeterminado**.

   Cuando restaura el certificado de interfaz de administración predeterminado, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado de interfaz de administración predeterminado se utiliza para todas las conexiones de nuevos clientes posteriores.

4. Actualice la página para asegurarse de que el navegador web esté actualizado.

Utilice un script para generar un nuevo certificado de interfaz de administración autofirmado

Si se requiere una validación estricta del nombre de host, puede utilizar un script para generar el certificado de interfaz de administración.

Antes de empezar

- Tienes"permisos de acceso específicos" .
- Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

La mejor práctica para un entorno de producción es utilizar un certificado firmado por una autoridad de certificación externa.

Pasos

1. Obtenga el nombre de dominio completo (FQDN) de cada nodo de administración.
2. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_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 `#` .

3. Configure StorageGRID con un nuevo certificado autofirmado.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Para `--domains` , utilice caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el comodín * para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com` .
   - Colocar `--type` a `management` para configurar el certificado de la interfaz de administración, que utilizan Grid Manager y Tenant Manager.
   - De forma predeterminada, los certificados generados son válidos por un año (365 días) y deben volver a crearse antes de que caduquen. Puedes utilizar el `--days` argumento para anular el período de validez predeterminado.

El período de validez de un certificado comienza cuando `make-certificate` se ejecuta. Debe asegurarse de que el cliente de administración esté sincronizado con la misma fuente de tiempo que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

La salida resultante contiene el certificado público que necesita su cliente de API de administración.

4. Seleccione y copie el certificado.

   Incluya las etiquetas BEGIN y END en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`
6. Confirme que se configuró el certificado:
   a. Acceda al Administrador de cuadrícula.
   b. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**
   c. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
7. Configure su cliente de administración para utilizar el certificado público que copió. Incluya las etiquetas BEGIN y END.

Descargue o copie el certificado de interfaz de administración

Puede guardar o copiar el contenido del certificado de la interfaz de administración para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione la pestaña **Servidor** o **Paquete CA** y luego descargue o copie el certificado.

Descargar archivo de certificado o paquete de CA

Descargar el certificado o paquete de CA `.pem` archivo. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

   Si está descargando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete de CA PEM

Copie el texto del certificado para pegarlo en otro lugar. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM**.

   Si está copiando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se copian juntos.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados de API S3

Puede reemplazar o restaurar el certificado de servidor que se utiliza para las conexiones de cliente S3 a los nodos de almacenamiento o a los puntos finales del equilibrador de carga. El certificado de servidor personalizado de reemplazo es específico para su organización.

Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver "StorageGRID 11.8: Configurar certificados de API de S3 y Swift" .

Acerca de esta tarea

De forma predeterminada, a cada nodo de almacenamiento se le emite un certificado de servidor X.509 firmado por la CA de la red. Estos certificados firmados por CA se pueden reemplazar por un único certificado de servidor personalizado común y su clave privada correspondiente.

Se utiliza un único certificado de servidor personalizado para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o un certificado multidominio si los clientes necesitan verificar el nombre de host al conectarse al punto final de almacenamiento. Defina el certificado personalizado de modo que coincida con todos los nodos de almacenamiento de la red.

Después de completar la configuración en el servidor, es posible que también necesite instalar el certificado CA de Grid en el cliente API S3 que usará para acceder al sistema, dependiendo de la autoridad de certificación raíz (CA) que esté utilizando.

> Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para la API S3** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **Certificados** y mirando la fecha de vencimiento del certificado de API S3 en la pestaña Global.

Puede cargar o generar un certificado API S3 personalizado.

Agregar un certificado API S3 personalizado

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione **Usar certificado personalizado**.
4. Subir o generar el certificado.

Subir certificado

Cargue los archivos de certificado de servidor necesarios.

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor**: el archivo de certificado de servidor personalizado (codificado en PEM).
- **Clave privada del certificado**: El archivo de clave privada del certificado del servidor personalizado(`.key`).

> Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete CA**: un único archivo opcional que contiene los certificados de cada autoridad de certificación emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Seleccione los detalles del certificado para mostrar los metadatos y PEM de cada certificado API S3 personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

  Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Guardar**.

  El certificado de servidor personalizado se utiliza para nuevas conexiones de cliente S3 posteriores.

Generar certificado

Generar los archivos de certificado del servidor.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para mostrar los metadatos y PEM del certificado API S3 personalizado que se generó.

   - Seleccione **Descargar certificado** para guardar el archivo del certificado.

     Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Seleccione **Guardar**.

   El certificado de servidor personalizado se utiliza para nuevas conexiones de cliente S3 posteriores.

5. Seleccione una pestaña para mostrar los metadatos del certificado de servidor StorageGRID predeterminado, un certificado firmado por CA que se cargó o un certificado personalizado que se generó.

   Después de cargar o generar un nuevo certificado, espere hasta un día para que desaparezcan las alertas de vencimiento del certificado relacionadas.

6. Actualice la página para asegurarse de que el navegador web esté actualizado.

7. Después de agregar un certificado API S3 personalizado, la página del certificado API S3 muestra información detallada del certificado API S3 personalizado que está en uso. + Puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado API S3 predeterminado

Puede volver a utilizar el certificado API S3 predeterminado para las conexiones de cliente S3 a los nodos de almacenamiento. Sin embargo, no puedes usar el certificado API S3 predeterminado para un punto final del balanceador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione **Usar certificado predeterminado**.

   Cuando restaura la versión predeterminada del certificado API S3 global, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado API S3 predeterminado se utilizará para las nuevas conexiones de clientes S3 posteriores a los nodos de almacenamiento.

4. Seleccione **Aceptar** para confirmar la advertencia y restaurar el certificado API S3 predeterminado.

   Si tiene permiso de acceso de root y se utilizó el certificado API S3 personalizado para las conexiones de puntos finales del balanceador de carga, se muestra una lista de puntos finales del balanceador de carga que ya no serán accesibles mediante el certificado API S3 predeterminado. Ir a"Configurar los puntos finales del balanceador de carga" para editar o eliminar los puntos finales afectados.

5. Actualice la página para asegurarse de que el navegador web esté actualizado.

Descargue o copie el certificado de API S3

Puede guardar o copiar el contenido del certificado API S3 para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione la pestaña **Servidor** o **Paquete CA** y luego descargue o copie el certificado.

Descargar archivo de certificado o paquete de CA

Descargar el certificado o paquete de CA `.pem` archivo. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

   Si está descargando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete de CA PEM

Copie el texto del certificado para pegarlo en otro lugar. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM**.

   Si está copiando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se copian juntos.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- "Utilice la API REST de S3"
- "Configurar nombres de dominio de puntos finales S3"

Copiar el certificado de CA de Grid

StorageGRID utiliza una autoridad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia si carga sus propios certificados.

Antes de empezar

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

Acerca de esta tarea

Si se ha configurado un certificado de servidor personalizado, las aplicaciones cliente deben verificar el servidor utilizando el certificado de servidor personalizado. No deben copiar el certificado CA del sistema StorageGRID .

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Grid CA**.
2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargar archivo de certificado

Descargar el certificado `.pem` archivo.

a. Seleccione **Descargar certificado**.
b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copie el texto del certificado para pegarlo en otro lugar.

a. Seleccione **Copiar certificado PEM**.
b. Pegue el certificado copiado en un editor de texto.
c. Guarde el archivo de texto con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta del nombre de host y no admiten la desactivación de la validación estricta del nombre de host, como los clientes ONTAP que usan FabricPool, puede generar o cargar un certificado de servidor cuando configura el punto final del equilibrador de carga.

Antes de empezar

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

Acerca de esta tarea

Cuando crea un punto final de balanceador de carga, puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una autoridad de certificación (CA) conocida. En entornos de producción, debe utilizar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar sin interrupciones. También son más seguros porque ofrecen una mejor protección contra ataques del tipo "man-in-the-middle".

Los siguientes pasos proporcionan pautas generales para los clientes S3 que utilizan FabricPool. Para obtener información y procedimientos más detallados, consulte"Configurar StorageGRID para FabricPool" .

Pasos

1. Opcionalmente, configure un grupo de alta disponibilidad (HA) para que lo utilice FabricPool .
2. Cree un punto final de balanceador de carga S3 para que lo utilice FabricPool .

Cuando crea un punto final de balanceador de carga HTTPS, se le solicita que cargue su certificado de servidor, la clave privada del certificado y el paquete de CA opcional.

3. Adjunte StorageGRID como un nivel de nube en ONTAP.

   Especifique el puerto del punto final del equilibrador de carga y el nombre de dominio completo utilizado en el certificado de CA que cargó. Luego, proporcione el certificado CA.

   > Si una CA intermedia emitió el certificado StorageGRID , debe proporcionar el certificado de CA intermedia. Si el certificado StorageGRID fue emitido directamente por la CA raíz, debe proporcionar el certificado de la CA raíz.

Configurar certificados de cliente

Los certificados de cliente permiten que los clientes externos autorizados accedan a la base de datos Prometheus de StorageGRID , lo que proporciona una forma segura para que las herramientas externas monitoreen StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de monitoreo externa, debe cargar o generar un certificado de cliente utilizando Grid Manager y copiar la información del certificado a la herramienta externa.

Ver"Administrar certificados de seguridad" y"Configurar certificados de servidor personalizados" .

> Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración de certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **Certificados** y mirando la fecha de vencimiento del certificado del cliente en la pestaña Cliente.

> Si está utilizando un servidor de administración de claves (KMS) para proteger los datos en nodos de dispositivos especialmente configurados, consulte la información específica sobre"Cargar un certificado de cliente KMS" .

Antes de empezar

- Tienes permiso de acceso root.
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Para configurar un certificado de cliente:
  - Tienes la dirección IP o el nombre de dominio del nodo de administración.
  - Si ha configurado el certificado de interfaz de administración de StorageGRID , tiene la CA, el certificado de cliente y la clave privada que se utilizan para configurar el certificado de interfaz de administración.
  - Para cargar su propio certificado, la clave privada del certificado está disponible en su computadora local.
  - La clave privada debe haber sido guardada o registrada en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
  - Tienes la dirección IP o el nombre de dominio del nodo de administración.

- Para cargar su propio certificado o un certificado nuevo, la clave privada, el certificado del cliente y la CA (si se utiliza) están disponibles en su computadora local.

Agregar certificados de cliente

Para agregar el certificado de cliente, utilice uno de estos procedimientos:

- Certificado de interfaz de administración ya configurado
- Certificado de cliente emitido por CA
- Certificado generado desde Grid Manager

Certificado de interfaz de administración ya configurado

Utilice este procedimiento para agregar un certificado de cliente si ya hay configurado un certificado de interfaz de administración mediante una CA proporcionada por el cliente, un certificado de cliente y una clave privada.

Pasos

1. En el Administrador de red, seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
5. Seleccione **Continuar**.
6. Para el paso **Adjuntar certificados**, cargue el certificado de la interfaz de administración.
   a. Seleccione **Subir certificado**.
   b. Seleccione **Explorar** y seleccione el archivo de certificado de la interfaz de administración(`.pem`).
      - Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

      El nuevo certificado aparece en la pestaña Cliente.
7. Configurar una herramienta de monitorización externa, como Grafana.

Certificado de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente administrador si no se configuró un certificado de interfaz de administración y planea agregar un certificado de cliente para Prometheus que utiliza un certificado de cliente emitido por una CA y una clave privada.

Pasos

1. Realice los pasos para"configurar un certificado de interfaz de administración" .
2. En el Administrador de red, seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.

3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
6. Seleccione **Continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado del cliente, la clave privada y los archivos del paquete de CA:
   a. Seleccione **Subir certificado**.
   b. Seleccione **Explorar** y seleccione el certificado del cliente, la clave privada y los archivos del paquete de CA(`.pem`).
      - Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

      Los nuevos certificados aparecen en la pestaña Cliente.
8. Configurar una herramienta de monitorización externa, como Grafana.

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente administrador si no se configuró un certificado de interfaz de administración y planea agregar un certificado de cliente para Prometheus que use la función de generar certificado en Grid Manager.

Pasos

1. En el Administrador de red, seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
5. Seleccione **Continuar**.
6. Para el paso **Adjuntar certificados**, seleccione **Generar certificado**.
7. Especifique la información del certificado:
   - **Asunto** (opcional): sujeto X.509 o nombre distinguido (DN) del propietario del certificado.
   - **Días de validez**: La cantidad de días que el certificado generado es válido, a partir del momento en que se genera.
   - **Agregar extensiones de uso de clave**: si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y de uso de clave extendida se agregan al certificado generado.

     Estas extensiones definen el propósito de la clave contenida en el certificado.

Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

8. Seleccione **Generar**.
9. Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en un lugar seguro.

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
   - Seleccione **Descargar certificado** para guardar el archivo del certificado.

     Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem` .

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar clave privada** para copiar la clave privada del certificado y pegarla en otro lugar.
   - Seleccione **Descargar clave privada** para guardar la clave privada como un archivo.

     Especifique el nombre del archivo de clave privada y la ubicación de descarga.

10. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

    El nuevo certificado aparece en la pestaña Cliente.

11. En el Administrador de red, seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Global**.
12. Seleccione **Certificado de interfaz de administración**.
13. Seleccione **Usar certificado personalizado**.
14. Cargue los archivos certificate.pem y private_key.pem desde eldetalles del certificado del cliente paso. No es necesario cargar el paquete CA.
    a. Seleccione **Cargar certificado** y luego seleccione **Continuar**.
    b. Subir cada archivo de certificado(`.pem`).
    c. Seleccione **Guardar** para guardar el certificado en el Administrador de Grid.

       El nuevo certificado aparece en la página de certificados de la interfaz de administración.

15. Configurar una herramienta de monitorización externa, como Grafana.

Configurar una herramienta de monitoreo externo

Pasos

1. Configure los siguientes ajustes en su herramienta de monitoreo externa, como Grafana.
   a. **Nombre**: Ingrese un nombre para la conexión.

      StorageGRID no requiere esta información, pero debe proporcionar un nombre para probar la conexión.

b. **URL**: Ingrese el nombre de dominio o la dirección IP del nodo de administración. Especifique HTTPS y el puerto 9091.

   Por ejemplo: `https://admin-node.example.com:9091`

c. Habilitar **Autenticación de cliente TLS** y **Con certificado CA**.

d. En Detalles de autenticación TLS/SSL, copie y pegue:

   - El certificado CA de la interfaz de administración para **CA Cert**
   - El certificado de cliente para **Certificado de cliente**
   - La clave privada de **Clave de cliente**

e. **ServerName**: Ingrese el nombre de dominio del nodo de administración.

   ServerName debe coincidir con el nombre de dominio tal como aparece en el certificado de la interfaz de administración.

2. Guarde y pruebe el certificado y la clave privada que copió de StorageGRID o de un archivo local.

   Ahora puede acceder a las métricas de Prometheus desde StorageGRID con su herramienta de monitoreo externa.

   Para obtener información sobre las métricas, consulte la"Instrucciones para monitorear StorageGRID" .

Editar certificados de cliente

Puede editar un certificado de cliente administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus o cargar un nuevo certificado cuando el actual haya expirado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.

   Las fechas de vencimiento de los certificados y los permisos de acceso de Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya caducó, aparece un mensaje en la tabla y se activa una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y luego seleccione **Editar nombre y permiso**
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
6. Seleccione **Continuar** para guardar el certificado en el Administrador de Grid.

   El certificado actualizado se muestra en la pestaña Cliente.

Adjuntar nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya expirado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de vencimiento de los certificados y los permisos de acceso de Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya caducó, aparece un mensaje en la tabla y se activa una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y luego seleccione una opción de edición.

Subir certificado

Copie el texto del certificado para pegarlo en otro lugar.

a. Seleccione **Cargar certificado** y luego seleccione **Continuar**.

b. Subir el nombre del certificado del cliente(`.pem`).

   Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   - Seleccione **Descargar certificado** para guardar el archivo del certificado.

     Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem` .

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

   El certificado actualizado se muestra en la pestaña Cliente.

Generar certificado

Generar el texto del certificado para pegarlo en otro lugar.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

   - **Asunto** (opcional): sujeto X.509 o nombre distinguido (DN) del propietario del certificado.
   - **Días de validez**: La cantidad de días que el certificado generado es válido, a partir del momento en que se genera.
   - **Agregar extensiones de uso de clave**: si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y de uso de clave extendida se agregan al certificado generado.

     Estas extensiones definen el propósito de la clave contenida en el certificado.

     Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en un lugar seguro.

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro

lugar.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

  Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado y pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como un archivo.

  Especifique el nombre del archivo de clave privada y la ubicación de descarga.

e. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

Descargar o copiar certificados de cliente

Puede descargar o copiar un certificado de cliente para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargar archivo de certificado

Descargar el certificado `.pem` archivo.

a. Seleccione **Descargar certificado**.
b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie el texto del certificado para pegarlo en otro lugar.

a. Seleccione **Copiar certificado PEM**.
b. Pegue el certificado copiado en un editor de texto.
c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Eliminar certificados de cliente

Si ya no necesita un certificado de cliente administrador, puede eliminarlo.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y luego confirme.

> Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la pestaña Cliente y luego seleccione **Acciones** > **Eliminar**.

Después de eliminar un certificado, los clientes que lo usaron deben especificar un nuevo certificado de cliente para acceder a la base de datos StorageGRID Prometheus.

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.
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**.

Configurar servidores de administración de claves

¿Qué es un servidor de administración de claves (KMS)?

Un servidor de administración de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos del dispositivo StorageGRID en el sitio StorageGRID asociado mediante el Protocolo de interoperabilidad de administración de claves (KMIP).

StorageGRID solo admite ciertos servidores de administración de claves. Para obtener una lista de productos y versiones compatibles, utilice el "Herramienta de matriz de interoperabilidad de NetApp (IMT)" .

Puede utilizar uno o más servidores de administración de claves para administrar las claves de cifrado de

nodo para cualquier nodo del dispositivo StorageGRID que tenga la configuración **Cifrado de nodo** habilitada durante la instalación. El uso de servidores de administración de claves con estos nodos de dispositivos le permite proteger sus datos incluso si se quita un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo pueda comunicarse con el KMS.

> StorageGRID no crea ni administra las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea utilizar un servidor de administración de claves externo para proteger los datos de StorageGRID , debe comprender cómo configurar ese servidor y cómo administrar las claves de cifrado. La realización de tareas de gestión de claves queda fuera del alcance de estas instrucciones. Si necesita ayuda, consulte la documentación de su servidor de administración de claves o comuníquese con el soporte técnico.

Configuración de KMS y dispositivos

Antes de poder usar un servidor de administración de claves (KMS) para proteger los datos de StorageGRID en los nodos del dispositivo, debe completar dos tareas de configuración: configurar uno o más servidores KMS y habilitar el cifrado de nodos para los nodos del dispositivo. Una vez completadas estas dos tareas de configuración, el proceso de gestión de claves se produce automáticamente.

El diagrama de flujo muestra los pasos de alto nivel para usar un KMS para proteger los datos de StorageGRID en los nodos del dispositivo.

El diagrama de flujo muestra la configuración de KMS y la configuración del dispositivo ocurriendo en paralelo; sin embargo, puede configurar los servidores de administración de claves antes o después de habilitar el cifrado de nodos para los nuevos nodos del dispositivo, según sus requisitos.

Configurar el servidor de administración de claves (KMS)

La configuración de un servidor de administración de claves incluye los siguientes pasos de alto nivel.

Paso	Referirse a
Acceda al software KMS y agregue un cliente para StorageGRID a cada KMS o clúster KMS.	"Configurar StorageGRID como cliente en el KMS"
Obtenga la información requerida para el cliente StorageGRID en el KMS.	"Configurar StorageGRID como cliente en el KMS"
Agregue el KMS al Grid Manager, asígnelo a un solo sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración del KMS.	"Agregar un servidor de administración de claves (KMS)"

Configurar el aparato

La configuración de un nodo de dispositivo para el uso de KMS incluye los siguientes pasos de alto nivel.

1. Durante la etapa de configuración de hardware de la instalación del dispositivo, utilice el instalador de

dispositivos StorageGRID para habilitar la configuración **Cifrado de nodo** para el dispositivo.

> No se puede habilitar la configuración **Cifrado de nodo** después de agregar un dispositivo a la red, y no se puede usar la administración de claves externa para dispositivos que no tengan habilitado el cifrado de nodo.

2. Ejecute el instalador del dispositivo StorageGRID . Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen del dispositivo, de la siguiente manera:
   - Las DEK se utilizan para cifrar los datos en cada volumen. Estas claves se generan mediante el cifrado de disco LUKS (configuración de clave unificada de Linux) en el sistema operativo del dispositivo y no se pueden modificar.
   - Cada DEK individual está encriptado por una clave de encriptación maestra (KEK). La KEK inicial es una clave temporal que cifra las DEK hasta que el dispositivo pueda conectarse al KMS.
3. Agregue el nodo del dispositivo a StorageGRID.

Ver "Habilitar el cifrado de nodos" Para más detalles.

Proceso de cifrado de gestión de claves (se produce automáticamente)

El cifrado de gestión de claves incluye los siguientes pasos de alto nivel que se realizan automáticamente.

1. Cuando instala un dispositivo que tiene el cifrado de nodo habilitado en la red, StorageGRID determina si existe una configuración de KMS para el sitio que contiene el nuevo nodo.
   - Si ya se ha configurado un KMS para el sitio, el dispositivo recibe la configuración de KMS.
   - Si aún no se ha configurado un KMS para el sitio, los datos del dispositivo continúan encriptados por la KEK temporal hasta que configure un KMS para el sitio y el dispositivo reciba la configuración del KMS.
2. El dispositivo utiliza la configuración de KMS para conectarse al KMS y solicitar una clave de cifrado.
3. El KMS envía una clave de cifrado al dispositivo. La nueva clave del KMS reemplaza la KEK temporal y ahora se utiliza para cifrar y descifrar las DEK de los volúmenes del dispositivo.

> Cualquier dato que exista antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifra con una clave temporal. Sin embargo, los volúmenes del dispositivo no deben considerarse protegidos contra la eliminación del centro de datos hasta que la clave temporal sea reemplazada por la clave de cifrado KMS.

4. Si el dispositivo se enciende o se reinicia, se vuelve a conectar al KMS para solicitar la clave. La clave, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o a un reinicio.

Consideraciones y requisitos para utilizar un servidor de administración de claves

Antes de configurar un servidor de administración de claves externo (KMS), debe comprender las consideraciones y los requisitos.

¿Qué versión de KMIP es compatible?

StorageGRID es compatible con KMIP versión 1.4.

"Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"

¿Cuáles son las consideraciones de la red?

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comunique a través del puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El puerto KMIP predeterminado es 5696.

Debe asegurarse de que cada nodo del dispositivo que utiliza cifrado de nodo tenga acceso a la red del KMS o del clúster KMS que configuró para el sitio.

¿Qué versiones de TLS son compatibles?

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID puede admitir el protocolo TLS 1.2 o TLS 1.3 cuando realiza conexiones KMIP a un KMS o un clúster KMS, según lo que admita el KMS y qué"Política de TLS y SSH" estás usando

StorageGRID negocia el protocolo y el cifrado (TLS 1.2) o el conjunto de cifrados (TLS 1.3) con el KMS cuando realiza la conexión. Para ver qué versiones de protocolo y cifrados/conjuntos de cifrados están disponibles, revise la `tlsOutbound` sección de la política TLS y SSH activa de la red (**CONFIGURACIÓN** > **Seguridad Configuración de seguridad**).

¿Qué dispositivos son compatibles?

Puede utilizar un servidor de administración de claves (KMS) para administrar las claves de cifrado para cualquier dispositivo StorageGRID en su red que tenga habilitada la configuración **Cifrado de nodo**. Esta configuración solo se puede habilitar durante la etapa de configuración de hardware de la instalación del dispositivo mediante el instalador de dispositivos StorageGRID .

> ⓘ No se puede habilitar el cifrado de nodos después de agregar un dispositivo a la red, y no se puede usar la administración de claves externa para dispositivos que no tengan habilitado el cifrado de nodos.

Puede utilizar el KMS configurado para dispositivos StorageGRID y nodos de dispositivos.

No se puede utilizar el KMS configurado para nodos basados en software (que no sean dispositivos), incluidos los siguientes:

- Nodos implementados como máquinas virtuales (VM)
- Nodos implementados dentro de motores de contenedores en hosts Linux

Los nodos implementados en estas otras plataformas pueden usar cifrado fuera de StorageGRID en el nivel de disco o de almacén de datos.

¿Cuándo debo configurar los servidores de administración de claves?

Para una nueva instalación, normalmente debe configurar uno o más servidores de administración de claves en Grid Manager antes de crear inquilinos. Esta orden garantiza que los nodos estén protegidos antes de que se almacenen datos de objetos en ellos.

Puede configurar los servidores de administración de claves en Grid Manager antes o después de instalar los nodos del dispositivo.

¿Cuántos servidores de gestión de claves necesito?

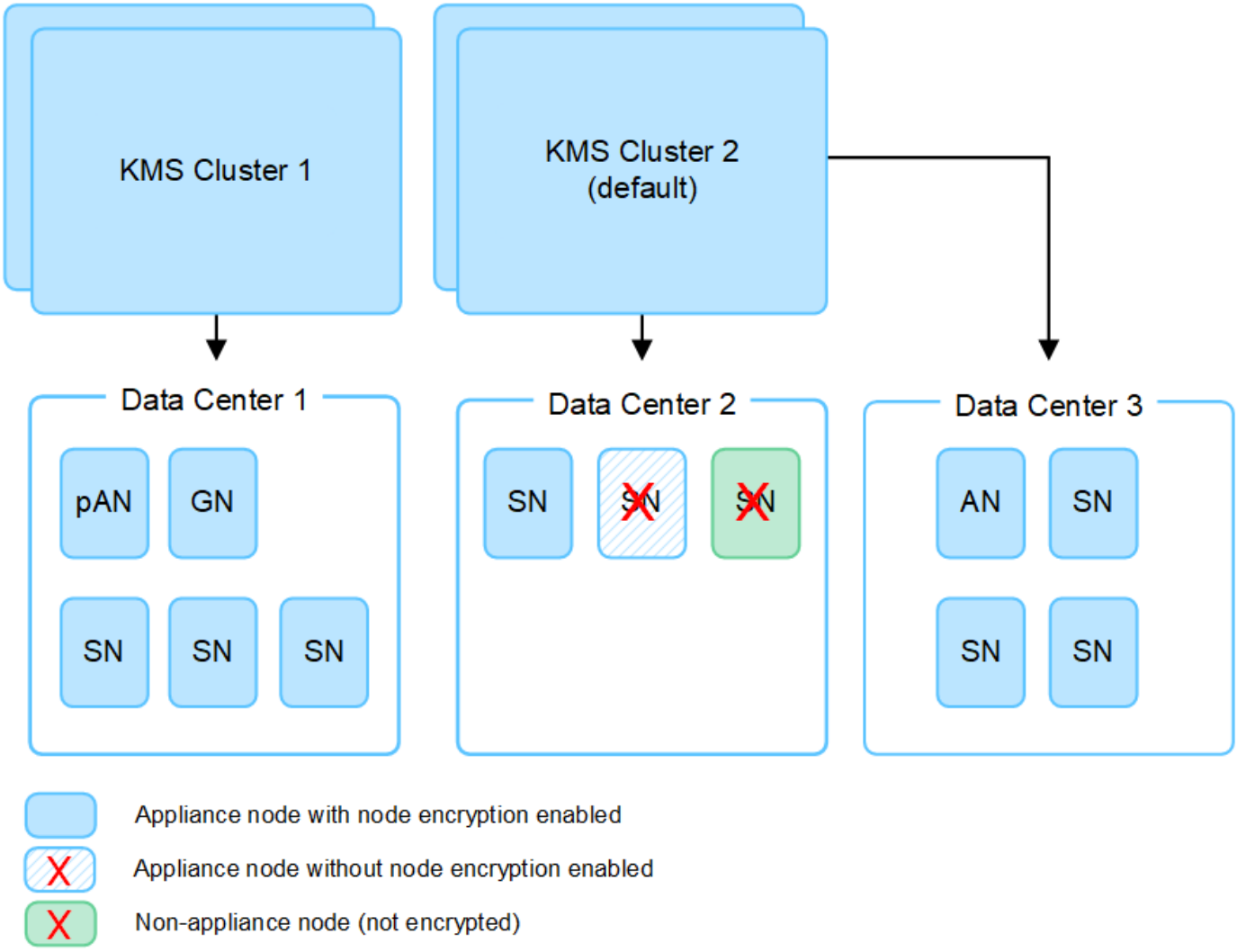
Puede configurar uno o más servidores de administración de claves externos para proporcionar claves de

cifrado a los nodos del dispositivo en su sistema StorageGRID . Cada KMS proporciona una única clave de cifrado a los nodos del dispositivo StorageGRID en un solo sitio o en un grupo de sitios.

StorageGRID admite el uso de clústeres KMS. Cada clúster KMS contiene varios servidores de administración de claves replicados que comparten configuraciones y claves de cifrado. Se recomienda el uso de clústeres KMS para la administración de claves porque mejora las capacidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supongamos que su sistema StorageGRID tiene tres sitios de centros de datos. Puede configurar un clúster KMS para proporcionar una clave a todos los nodos del dispositivo en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos del dispositivo en todos los demás sitios. Cuando agrega el segundo clúster KMS, puede configurar un KMS predeterminado para el Centro de datos 2 y el Centro de datos 3.

Tenga en cuenta que no puede usar un KMS para nodos que no sean dispositivos o para ningún nodo de dispositivo que no tuviera habilitada la configuración **Cifrado de nodo** durante la instalación.



¿Qué sucede cuando se gira una llave?

Como práctica recomendada de seguridad, debe realizar periódicamente"rotar la clave de cifrado" utilizado por cada KMS configurado.

Cuando la nueva versión de la clave esté disponible:

- Se distribuye automáticamente a los nodos del dispositivo cifrado en el sitio o sitios asociados con el KMS. La distribución debe ocurrir dentro de una hora después de que se gira la clave.
- Si el nodo del dispositivo cifrado está fuera de línea cuando se distribuye la nueva versión de la clave, el nodo recibirá la nueva clave tan pronto como se reinicie.
- Si por algún motivo no se puede usar la nueva versión de la clave para cifrar los volúmenes del dispositivo, se activa la alerta **Error en la rotación de la clave de cifrado KMS** para el nodo del dispositivo. Es posible que necesite ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo reutilizar un nodo de dispositivo después de haberlo cifrado?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID , primero debe desmantelar el nodo de la red para mover los datos del objeto a otro nodo. Luego, puede utilizar el instalador del dispositivo StorageGRID para "borrar la configuración de KMS" . Al borrar la configuración de KMS se deshabilita la configuración de **Cifrado de nodo** y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS para el sitio StorageGRID .

> Sin acceso a la clave de cifrado KMS, ya no se puede acceder a los datos que permanecen en el dispositivo y quedan bloqueados de forma permanente.

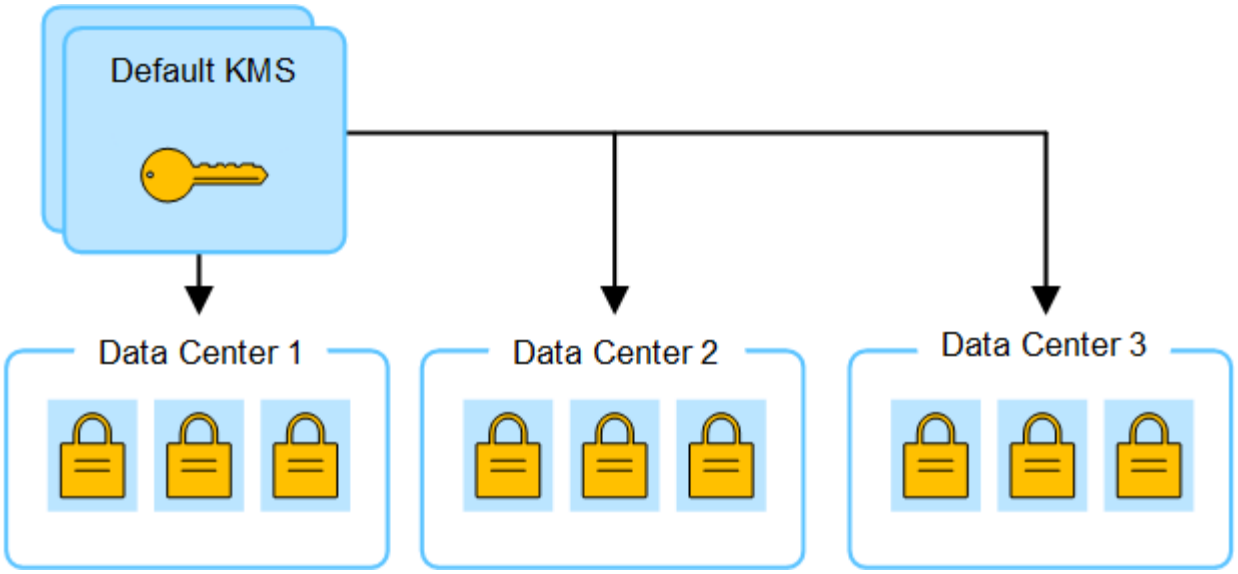
Consideraciones para cambiar el KMS de un sitio

Cada servidor de administración de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos del dispositivo en un solo sitio o en un grupo de sitios. Si necesita cambiar el KMS que se utiliza para un sitio, es posible que deba copiar la clave de cifrado de un KMS a otro.

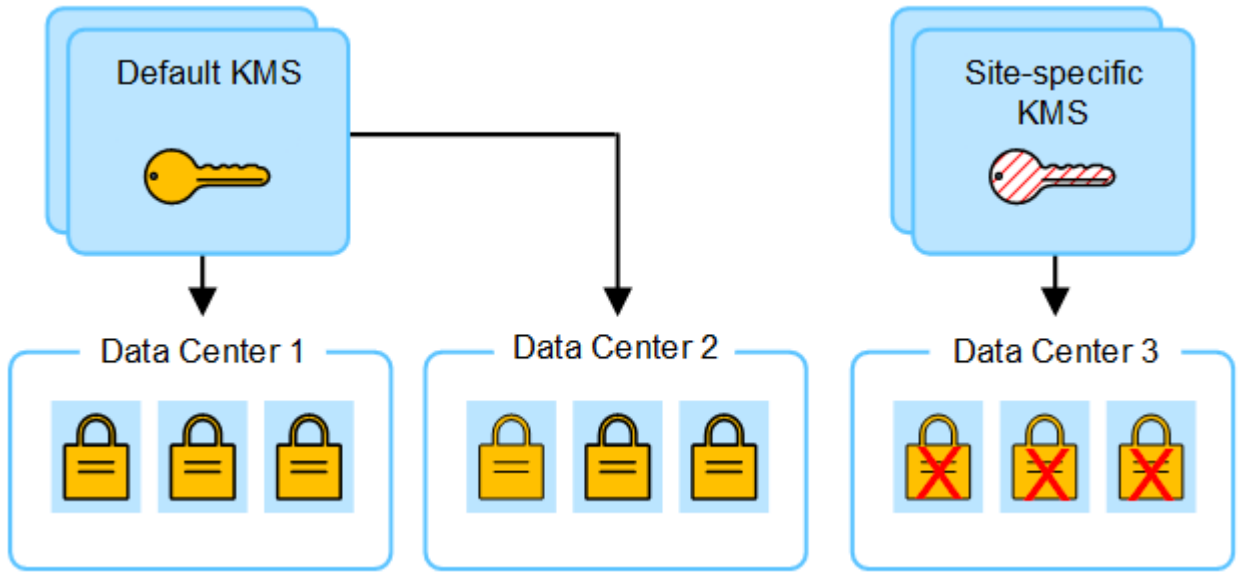
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo previamente cifrados en ese sitio se puedan descifrar usando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesites copiar la versión actual de la clave de cifrado del KMS original al nuevo KMS. Debe asegurarse de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

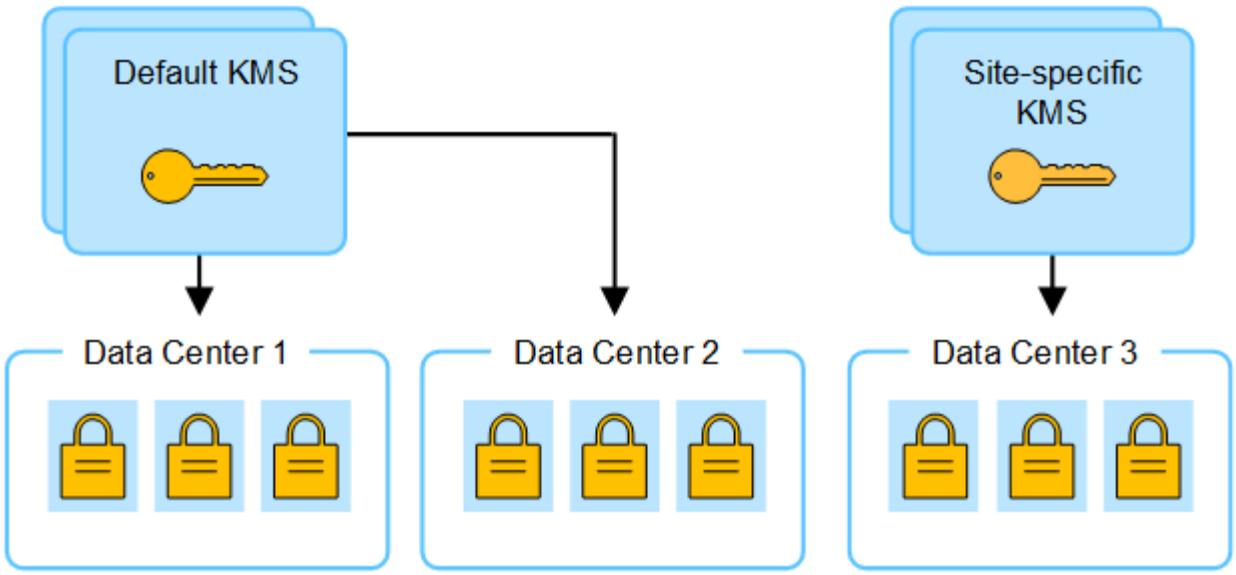
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos del dispositivo que tienen habilitada la configuración **Cifrado de nodo** se conectan al KMS y solicitan la clave de cifrado. Esta clave se utiliza para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar dichos dispositivos.



3. Decide agregar un KMS específico del sitio para un sitio (Centro de datos 3 en la figura). Sin embargo, debido a que los nodos del dispositivo ya están cifrados, se produce un error de validación cuando intenta guardar la configuración del KMS específico del sitio. El error se produce porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos en ese sitio.



4. Para solucionar el problema, copie la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, se copia la clave original a una nueva clave con el mismo alias. (La clave original se convierte en una versión anterior de la nueva clave). El KMS específico del sitio ahora tiene la clave correcta para descifrar los nodos del dispositivo en el Centro de datos 3, por lo que se puede guardar en StorageGRID.



Casos de uso para cambiar el KMS que se utiliza para un sitio

La tabla resume los pasos necesarios para los casos más comunes de cambio del KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos necesarios
Tiene una o más entradas KMS específicas del sitio y desea utilizar una de ellas como KMS predeterminado.	Editar el KMS específico del sitio. En el campo **Administra claves para**, seleccione **Sitios no administrados por otro KMS (KMS predeterminado)**. El KMS específico del sitio ahora se utilizará como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de administración de claves (KMS)"
Tienes un KMS predeterminado y agregas un nuevo sitio en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos del dispositivo en el nuevo sitio ya fueron cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un nuevo KMS. 2. Utilizando el Administrador de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Agregar un servidor de administración de claves (KMS)"
Desea que el KMS de un sitio utilice un servidor diferente.	1. Si los nodos del dispositivo en el sitio ya han sido cifrados por el KMS existente, utilice el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al nuevo KMS. 2. Utilizando el Administrador de cuadrícula, edite la configuración KMS existente e ingrese el nuevo nombre de host o dirección IP. "Agregar un servidor de administración de claves (KMS)"

Configurar StorageGRID como cliente en el KMS

Debe configurar StorageGRID como cliente para cada servidor de administración de claves externo o clúster KMS antes de poder agregar el KMS a StorageGRID.

> Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para obtener una lista de productos y versiones compatibles, utilice el "Herramienta de matriz de interoperabilidad de NetApp (IMT)" .

Pasos

1. Desde el software KMS, cree un cliente StorageGRID para cada KMS o clúster KMS que planee utilizar.

   Cada KMS administra una única clave de cifrado para los nodos de dispositivos StorageGRID en un solo sitio o en un grupo de sitios.

2. Cree una clave utilizando uno de los dos métodos siguientes:
   - Utilice la página de administración de claves de su producto KMS. Cree una clave de cifrado AES para cada KMS o clúster KMS.

     La clave de cifrado debe tener 2048 bits o más y debe ser exportable.

   - Haga que StorageGRID cree la clave. Se le avisará cuando realice la prueba y guarde después"cargando certificados de cliente" .
3. Registre la siguiente información para cada KMS o clúster KMS.

   Necesita esta información cuando agrega el KMS a StorageGRID:

   - Nombre de host o dirección IP para cada servidor.
   - Puerto KMIP utilizado por el KMS.
   - Alias de clave para la clave de cifrado en el KMS.
4. Para cada KMS o clúster KMS, obtenga un certificado de servidor firmado por una autoridad de certificación (CA) o un paquete de certificados que contenga cada uno de los archivos de certificado de CA codificados en PEM, concatenados en el orden de la cadena de certificados.

   El certificado del servidor permite que el KMS externo se autentique en StorageGRID.

   - El certificado debe utilizar el formato X.509 codificado en Base-64 de correo de privacidad mejorada (PEM).
   - El campo Nombre alternativo del sujeto (SAN) en cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que se conectará StorageGRID .

     > Al configurar el KMS en StorageGRID, debe ingresar los mismos FQDN o direcciones IP en el campo **Nombre de host**.

   - El certificado del servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que normalmente utiliza el puerto 5696.
5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada para el certificado de cliente.

   El certificado de cliente permite que StorageGRID se autentique ante el KMS.

Agregar un servidor de administración de claves (KMS)

Utilice el asistente del servidor de administración de claves StorageGRID para agregar cada KMS o clúster KMS.

Antes de empezar

- Usted ha revisado el"Consideraciones y requisitos para utilizar un servidor de administración de claves" .
- Tienes"configuró StorageGRID como cliente en el KMS" y tiene la información requerida para cada KMS o clúster KMS.
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

Acerca de esta tarea

Si es posible, configure cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no administrados por otro KMS. Si crea primero el KMS predeterminado, todos los dispositivos con nodos cifrados en la red se cifrarán con el KMS predeterminado. Si más adelante desea crear un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Ver"Consideraciones para cambiar el KMS de un sitio" Para más detalles.

Paso 1: Detalles del KMS

En el Paso 1 (Detalles de KMS) del asistente Agregar un servidor de administración de claves, debe proporcionar detalles sobre el KMS o el clúster de KMS.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.

   Aparece la página del servidor de administración de claves con la pestaña Detalles de configuración seleccionada.

2. Seleccione **Crear**.

   Aparece el paso 1 (detalles de KMS) del asistente Agregar un servidor de administración de claves.

3. Ingrese la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarle a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. **Nota**: Si no ha creado una clave con su producto KMS, se le solicitará que StorageGRID cree la clave.

Campo	Descripción
Administra claves para	El sitio StorageGRID que se asociará con este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no administrados por otro KMS. • Seleccione un sitio si este KMS administrará claves de cifrado para los nodos del dispositivo en un sitio específico. • Seleccione **Sitios no administrados por otro KMS (KMS predeterminado)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que agregue en expansiones posteriores. **Nota:** Se producirá un error de validación cuando guarde la configuración de KMS si selecciona un sitio que anteriormente fue cifrado por el KMS predeterminado pero no proporcionó la versión actual de la clave de cifrado original al nuevo KMS.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. **Nota:** El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor en el clúster.
5. Seleccione **Continuar**.

Paso 2: Cargar el certificado del servidor

En el paso 2 (Cargar certificado de servidor) del asistente Agregar un servidor de administración de claves, cargue el certificado de servidor (o paquete de certificados) para el KMS. El certificado del servidor permite que el KMS externo se autentique en StorageGRID.

Pasos

1. Desde el **Paso 2 (Cargar certificado de servidor)**, busque la ubicación del certificado de servidor o paquete de certificados guardado.
2. Subir el archivo del certificado.

   Aparecen los metadatos del certificado del servidor.

   Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en su propia pestaña.

3. Seleccione **Continuar**.

Paso 3: Cargar certificados de cliente

En el paso 3 (Cargar certificados de cliente) del asistente Agregar un servidor de administración de claves, cargue el certificado de cliente y la clave privada del certificado de cliente. El certificado de cliente permite que StorageGRID se autentique ante el KMS.

Pasos

1. Desde el **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.
2. Subir el archivo del certificado del cliente.

   Aparecen los metadatos del certificado del cliente.
3. Busque la ubicación de la clave privada para el certificado del cliente.
4. Sube el archivo de clave privada.
5. Seleccione **Probar y guardar**.

   Si no existe una clave, se le solicitará que StorageGRID cree una.

   Se prueban las conexiones entre el servidor de administración de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el nuevo servidor de administración de claves se agrega a la tabla en la página Servidor de administración de claves.

   > Inmediatamente después de agregar un KMS, el estado del certificado en la página del Servidor de administración de claves aparece como Desconocido. StorageGRID podría tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar su navegador web para ver el estado actual.
6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revise los detalles del mensaje y luego seleccione **Aceptar**.

   Por ejemplo, es posible que reciba un error 422: Entidad no procesable si falla una prueba de conexión.
7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Forzar guardado**.

   > Al seleccionar **Forzar guardado** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos del dispositivo que tengan el cifrado de nodo habilitado en el sitio afectado. Podría perder el acceso a sus datos hasta que se resuelvan los problemas.
8. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

   Se guarda la configuración del KMS pero no se prueba la conexión al KMS.

Administrar un KMS

Administrar un servidor de administración de claves (KMS) implica ver o editar detalles, administrar certificados, ver nodos cifrados y eliminar un KMS cuando ya no es

necesario.

Antes de empezar

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

Ver detalles de KMS

Puede ver información sobre cada servidor de administración de claves (KMS) en su sistema StorageGRID , incluidos los detalles de la clave y el estado actual de los certificados del servidor y del cliente.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.

   Aparece la página del servidor de administración de claves y muestra la siguiente información:

   - La pestaña Detalles de configuración enumera todos los servidores de administración de claves que están configurados.
   - La pestaña Nodos cifrados enumera todos los nodos que tienen el cifrado de nodo habilitado.

2. Para ver los detalles de un KMS específico y realizar operaciones en ese KMS, seleccione el nombre del KMS. La página de detalles del KMS enumera la siguiente información:

Campo	Descripción
Administra claves para	El sitio StorageGRID asociado con el KMS. Este campo muestra el nombre de un sitio StorageGRID específico o **Sitios no administrados por otro KMS (KMS predeterminado).**
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. Si hay un clúster de dos servidores de administración de claves, se enumeran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de administración de claves en un clúster, se incluye el nombre de dominio completo o la dirección IP del primer KMS junto con la cantidad de servidores de administración de claves adicionales en el clúster. Por ejemplo: `10.10.10.10 and 10.10.10.11` o `10.10.10.10 and 2 others` . Para ver todos los nombres de host en un clúster, seleccione un KMS y seleccione **Editar** o **Acciones** > **Editar**.

3. Seleccione una pestaña en la página de detalles de KMS para ver la siguiente información:

Pestaña	Campo	Descripción
Detalles clave	Nombre de la clave	El alias de clave para el cliente StorageGRID en el KMS.

Pestaña	Campo	Descripción
UID de clave	El identificador único de la última versión de la clave.	Última modificación
La fecha y hora de la última versión de la clave.	Certificado de servidor	Metadatos
Los metadatos del certificado, como el número de serie, la fecha y hora de vencimiento y el PEM del certificado.	Certificado PEM	El contenido del archivo PEM (correo con privacidad mejorada) del certificado.
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y hora de vencimiento y el PEM del certificado.

4. Con la frecuencia que requieran las prácticas de seguridad de su organización, seleccione **Rotar clave** o utilice el software KMS para crear una nueva versión de la clave.

   Cuando la rotación de clave es exitosa, se actualizan los campos UID de clave y Última modificación.

> Si rota la clave de cifrado utilizando el software KMS, rótela desde la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.
>
> Nunca intente rotar una clave cambiando el nombre de la clave (alias) para el KMS. StorageGRID requiere que todas las versiones de clave utilizadas anteriormente (así como cualquier versión futura) sean accesibles desde el KMS con el mismo alias de clave. Si cambia el alias de clave de un KMS configurado, es posible que StorageGRID no pueda descifrar sus datos.

Administrar certificados

Aborde rápidamente cualquier problema con el certificado del servidor o del cliente. Si es posible, reemplace los certificados antes de que caduquen.

> Debe abordar cualquier problema de certificado lo antes posible para mantener el acceso a los datos.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.
2. En la tabla, observe el valor de vencimiento del certificado para cada KMS.
3. Si la expiración del certificado para cualquier KMS es desconocida, espere hasta 30 minutos y luego actualice su navegador web.
4. Si la columna Vencimiento del certificado indica que un certificado ha vencido o está próximo a vencer,

seleccione el KMS para ir a la página de detalles del KMS.

a. Seleccione **Certificado de servidor** y verifique el valor del campo "Vence el".

b. Para reemplazar el certificado, seleccione **Editar certificado** para cargar un nuevo certificado.

c. Repita estos subpasos y seleccione **Certificado de cliente** en lugar de Certificado de servidor.

5. Cuando se activan las alertas **Expiración del certificado de CA de KMS**, **Expiración del certificado de cliente de KMS** y **Expiración del certificado de servidor de KMS**, tenga en cuenta la descripción de cada alerta y realice las acciones recomendadas.

   StorageGRID podría tardar hasta 30 minutos en obtener actualizaciones sobre la expiración del certificado. Actualice su navegador web para ver los valores actuales.

> Si obtiene un estado de **El estado del certificado del servidor es desconocido**, asegúrese de que su KMS permita obtener un certificado de servidor sin requerir un certificado de cliente.

Ver nodos cifrados

Puede ver información sobre los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Cifrado de nodo**.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.

   Aparece la página del Servidor de administración de claves. La pestaña Detalles de configuración muestra todos los servidores de administración de claves que se han configurado.

2. Desde la parte superior de la página, seleccione la pestaña **Nodos cifrados**.

   La pestaña Nodos cifrados enumera los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Cifrado de nodo**.

3. Revise la información en la tabla para cada nodo del dispositivo.

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, Administración o Puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde está instalado el nodo.
Nombre KMS	El nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Agregar un servidor de administración de claves (KMS)"

Columna	Descripción
UID de clave	El identificador único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, seleccione el texto. Un guion (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo y el KMS.
Estado	El estado de la conexión entre el KMS y el nodo del dispositivo. Si el nodo está conectado, la marca de tiempo se actualiza cada 30 minutos. El estado de la conexión puede tardar varios minutos en actualizarse después de los cambios de configuración de KMS. **Nota:** Actualice su navegador web para ver los nuevos valores.

4. Si la columna Estado indica un problema de KMS, solucione el problema de inmediato.

   Durante las operaciones normales de KMS, el estado será **Conectado a KMS**. Si un nodo se desconecta de la red, se muestra el estado de conexión del nodo (Administrativamente inactivo o Desconocido).

   Otros mensajes de estado corresponden a alertas de StorageGRID con los mismos nombres:

   - La configuración de KMS no se pudo cargar
   - Error de conectividad KMS
   - No se encontró el nombre de la clave de cifrado KMS
   - Error en la rotación de la clave de cifrado KMS
   - La clave KMS no pudo descifrar un volumen del dispositivo
   - KMS no está configurado

   Realice las acciones recomendadas para estas alertas.

> Debe abordar cualquier problema de inmediato para garantizar que sus datos estén completamente protegidos.

Editar un KMS

Es posible que necesite editar la configuración de un servidor de administración de claves, por ejemplo, si un certificado está a punto de caducar.

Antes de empezar

- Si planea actualizar el sitio seleccionado para un KMS, ha revisado el"Consideraciones para cambiar el KMS de un sitio" .
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra todos los servidores de administración de claves que se han configurado.

2. Seleccione el KMS que desea editar y seleccione **Acciones** > **Editar**.

   También puede editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualice los detalles en el **Paso 1 (detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarle a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de la clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente **Sitios no administrados por otro KMS (KMS predeterminado)**. Esta selección convierte un KMS específico del sitio en el KMS predeterminado, que se aplicará a todos los sitios que no tengan un KMS dedicado y a cualquier sitio agregado en una expansión. **Nota:** Si está editando un KMS específico del sitio, no podrá seleccionar otro sitio. Si está editando el KMS predeterminado, no podrá seleccionar un sitio específico.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. **Nota:** El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor en el clúster.
5. Seleccione **Continuar**.

   Aparece el paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de administración de claves.

6. Si necesita reemplazar el certificado del servidor, seleccione **Explorar** y cargue el nuevo archivo.
7. Seleccione **Continuar**.

   Aparece el paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de administración de claves.

8. Si necesita reemplazar el certificado del cliente y la clave privada del certificado del cliente, seleccione **Explorar** y cargue los nuevos archivos.
9. Seleccione **Probar y guardar**.

   Se prueban las conexiones entre el servidor de administración de claves y todos los nodos del dispositivo cifrados en los sitios afectados. Si todas las conexiones de nodo son válidas y se encuentra la clave correcta en el KMS, el servidor de administración de claves se agrega a la tabla en la página Servidor de administración de claves.

10. Si aparece un mensaje de error, revise los detalles del mensaje y seleccione **Aceptar**.

    Por ejemplo, es posible que reciba un error 422: Entidad no procesable si el sitio que seleccionó para este KMS ya está administrado por otro KMS o si falló una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar guardado**.

    > Al seleccionar **Forzar guardado** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos del dispositivo que tengan el cifrado de nodo habilitado en el sitio afectado. Podría perder el acceso a sus datos hasta que se resuelvan los problemas.

    Se guarda la configuración de KMS.

12. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

    Se guarda la configuración del KMS, pero no se prueba la conexión al KMS.

Eliminar un servidor de administración de claves (KMS)

Es posible que en algunos casos desees eliminar un servidor de administración de claves. Por ejemplo, es posible que desees eliminar un KMS específico del sitio si has dado de baja el sitio.

Antes de empezar

- Usted ha revisado el"Consideraciones y requisitos para utilizar un servidor de administración de claves" .
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

Acerca de esta tarea

Puedes eliminar un KMS en estos casos:

- Puede eliminar un KMS específico del sitio si el sitio se ha dado de baja o si no incluye nodos de dispositivos con cifrado de nodos habilitado.

- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tenga nodos de dispositivo con cifrado de nodo habilitado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.

   Aparece la página del servidor de administración de claves y muestra todos los servidores de administración de claves que se han configurado.

2. Seleccione el KMS que desea eliminar y seleccione **Acciones** > **Eliminar**.

   También puede eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirme que lo siguiente es verdadero:
   - Está eliminando un KMS específico del sitio para un sitio que no tiene ningún nodo de dispositivo con cifrado de nodo habilitado.
   - Está eliminando el KMS predeterminado, pero ya existe un KMS específico del sitio para cada sitio con cifrado de nodo.
4. Seleccione **Sí**.

   Se elimina la configuración de KMS.

Administrar la configuración del proxy

Configurar el proxy de almacenamiento

Si utiliza servicios de plataforma o grupos de almacenamiento en la nube, puede configurar un proxy no transparente entre los nodos de almacenamiento y los puntos finales externos de S3. Por ejemplo, es posible que necesite un proxy no transparente para permitir que los mensajes de servicios de la plataforma se envíen a puntos finales externos, como un punto final en Internet.

> Las configuraciones del proxy de almacenamiento configuradas no se aplican a los puntos finales de los servicios de la plataforma Kafka.

Antes de empezar

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

Acerca de esta tarea

Puede configurar los ajustes para un único proxy de almacenamiento.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Configuración de proxy**.
2. En la pestaña **Almacenamiento**, seleccione la casilla de verificación **Habilitar proxy de almacenamiento**.
3. Seleccione el protocolo para el proxy de almacenamiento.

4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Opcionalmente, ingrese el puerto utilizado para conectarse al servidor proxy.

   Deje este campo en blanco para utilizar el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

   Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos puntos finales para los servicios de la plataforma o los grupos de almacenamiento en la nube.

   > ⓘ Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Verifique la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma de StorageGRID no se bloqueen.
8. Si necesita deshabilitar un proxy de almacenamiento, desmarque la casilla de verificación y seleccione **Guardar**.

Configurar los ajustes del proxy de administración

Si envía paquetes de AutoSupport mediante HTTP o HTTPS, puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Para obtener más información sobre AutoSupport, consulte"Configurar AutoSupport" .

Antes de empezar

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

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de administrador.

Pasos

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

   Aparece la página Configuración de proxy. De forma predeterminada, Almacenamiento está seleccionado en el menú de pestañas.

2. Seleccione la pestaña **Admin**.
3. Seleccione la casilla de verificación **Habilitar proxy de administración**.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Opcionalmente, ingrese un nombre de usuario y una contraseña para el servidor proxy.

   Deje estos campos en blanco si su servidor proxy no requiere un nombre de usuario o una contraseña.

7. Seleccione una de las siguientes opciones:

- Si desea proteger la conexión al proxy de administración, seleccione **Verificar certificado de proxy**. Cargue un paquete de CA para verificar la autenticidad de los certificados SSL presentados por el servidor proxy de administración.

> AutoSupport on Demand, E-Series AutoSupport a través de StorageGRID y la determinación de ruta de actualización en la página Actualización de StorageGRID no funcionarán si se verifica un certificado de proxy.

Después de cargar el paquete de CA, aparecen sus metadatos.

- Si no desea validar certificados al comunicarse con el servidor proxy de administración, seleccione **No verificar certificado proxy**.

8. Seleccione **Guardar**.

   Una vez guardado el proxy de administración, se configura el servidor proxy entre los nodos de administración y el soporte técnico.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesita deshabilitar el proxy de administración, desmarque la casilla **Habilitar proxy de administración** y luego seleccione **Guardar**.

Controlar cortafuegos

Controlar el acceso al firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

Puede controlar el acceso a las interfaces de usuario y las API en los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse al Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si desea configurar el firewall interno de StorageGRID , consulte"Configurar el firewall interno" .

Puerto	Descripción	Si el puerto está abierto…
443	Puerto HTTPS predeterminado para nodos de administración	Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid, la API de administración de Grid, el Administrador de inquilinos y la API de administración de inquilinos. **Nota:** El puerto 443 también se utiliza para cierto tráfico interno.

Puerto	Descripción	Si el puerto está abierto…
8443	Puerto de Grid Manager restringido en los nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid y a la API de administración de Grid mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de inquilinos ni a la API de administración de inquilinos. • Las solicitudes de contenido interno serán rechazadas.
9443	Puerto de administrador de inquilinos restringido en nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de inquilinos y a la API de administración de inquilinos mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de Grid ni a la API de administración de Grid. • Las solicitudes de contenido interno serán rechazadas.

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

Información relacionada

- "Sign in en el Administrador de cuadrícula"
- "Crear una cuenta de inquilino"
- "Comunicaciones externas"

Administrar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su red.

- **Lista de direcciones privilegiadas**: utilice esta pestaña para permitir el acceso seleccionado a puertos cerrados. Puede agregar direcciones IP o subredes en notación CIDR que puedan acceder a puertos cerrados mediante la pestaña Administrar acceso externo.

- **Administrar acceso externo**: utilice esta pestaña para cerrar puertos que están abiertos de forma predeterminada o reabrir puertos previamente cerrados.
- **Red de cliente no confiable**: utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red de cliente.

  La configuración de esta pestaña anula la configuración de la pestaña Administrar acceso externo.

  - Un nodo con una red de cliente no confiable solo aceptará conexiones en los puertos de punto final del balanceador de carga configurados en ese nodo (puntos finales globales, de interfaz de nodo y enlazados al tipo de nodo).
  - Los puertos finales del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración en la pestaña Administrar redes externas.
  - Cuando es confiable, todos los puertos abiertos en la pestaña Administrar acceso externo son accesibles, así como también cualquier punto final del balanceador de carga abierto en la red del cliente.

> Las configuraciones que realice en una pestaña pueden afectar los cambios de acceso que realice en otra pestaña. Asegúrese de verificar la configuración en todas las pestañas para asegurarse de que su red se comporte de la manera esperada.

Para configurar los controles internos del firewall, consulte"Configurar los controles del firewall" .

Para obtener más información sobre firewalls externos y seguridad de red, consulte"Controlar el acceso al firewall externo" .

Lista de direcciones privilegiadas y pestañas para administrar acceso externo

La pestaña Lista de direcciones privilegiadas le permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de la red que están cerrados. La pestaña Administrar acceso externo le permite cerrar el acceso externo a puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada). Estas dos pestañas a menudo se pueden usar juntas para personalizar el acceso de red exacto que necesita permitir para su red.

> Las direcciones IP privilegiadas no tienen acceso al puerto de la red interna de forma predeterminada.

Ejemplo 1: Utilizar un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host con seguridad reforzada) para la administración de la red. Podrías utilizar estos pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para agregar la dirección IP del host de salto.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.

> Agregue la dirección IP privilegiada antes de bloquear los puertos 443 y 8443. Cualquier usuario actualmente conectado a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Después de guardar su configuración, todos los puertos externos en el nodo de administración de su red se

bloquearán para todos los hosts excepto el host de salto. Luego, puede utilizar el host de salto para realizar tareas de mantenimiento en su red de forma más segura.

Ejemplo 2: Bloquear puertos sensibles

Supongamos que desea bloquear puertos sensibles y el servicio en ese puerto (por ejemplo, SSH en el puerto 22). Podrías utilizar los siguientes pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para otorgar acceso solo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.

> ⚠ Agregue la dirección IP privilegiada antes de bloquear el acceso a cualquier puerto asignado para acceder a Grid Manager y al administrador de inquilinos (los puertos preestablecidos son 443 y 8443). Cualquier usuario actualmente conectado a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Después de guardar su configuración, el puerto 22 y el servicio SSH estarán disponibles para los hosts en la lista de direcciones privilegiadas. A todos los demás hosts se les negará el acceso al servicio sin importar de qué interfaz provenga la solicitud.

Ejemplo 3: Deshabilitar el acceso a servicios no utilizados

A nivel de red, podrías deshabilitar algunos servicios que no deseas utilizar. Por ejemplo, para bloquear el tráfico del cliente HTTP S3, deberá utilizar el interruptor en la pestaña Administrar acceso externo para bloquear el puerto 18084.

Pestaña Redes de clientes no confiables

Si utiliza una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles al aceptar tráfico de cliente entrante solo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente en cada nodo de la red es *confiable*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de la red en todos los"puertos externos disponibles" .

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red de cliente en cada nodo sea *no confiable*. Si la red de cliente de un nodo no es confiable, el nodo solo acepta conexiones entrantes en puertos configurados explícitamente como puntos finales del balanceador de carga. Ver"Configurar los puntos finales del balanceador de carga" y"Configurar los controles del firewall" .

Ejemplo 1: El nodo de puerta de enlace solo acepta solicitudes HTTPS S3

Supongamos que desea que un nodo de puerta de enlace rechace todo el tráfico entrante en la red del cliente, excepto las solicitudes HTTPS S3. Realizarías estos pasos generales:

1. Desde"Puntos finales del balanceador de carga" página, configure un punto final de balanceador de carga para S3 sobre HTTPS en el puerto 443.
2. Desde la página de control de Firewall, seleccione No confiable para especificar que la red de cliente en el nodo de puerta de enlace no es confiable.

Después de guardar su configuración, se descarta todo el tráfico entrante en la red de cliente del nodo de puerta de enlace, excepto las solicitudes HTTPS S3 en el puerto 443 y las solicitudes de eco ICMP (ping).

Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de la plataforma S3

Supongamos que desea habilitar el tráfico saliente de servicios de la plataforma S3 desde un nodo de almacenamiento, pero desea evitar cualquier conexión entrante a ese nodo de almacenamiento en la red del cliente. Realizarías este paso general:

- Desde la pestaña Redes de clientes no confiables de la página de control de Firewall, indique que la red de clientes en el nodo de almacenamiento no es confiable.

Después de guardar su configuración, el nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes a los destinos de servicios de plataforma configurados.

Ejemplo 3: Limitar el acceso a Grid Manager a una subred

Supongamos que desea permitir el acceso a Grid Manager solo en una subred específica. Realizarías los siguientes pasos:

1. Conecte la red de cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente no confiable para configurar la red de cliente como no confiable.
3. Cuando crea un punto final de balanceador de carga de interfaz de administración, ingrese el puerto y seleccione la interfaz de administración a la que accederá el puerto.
4. Seleccione **Sí** para Red de cliente no confiable.
5. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para hosts fuera de esa subred).

Después de guardar su configuración, solo los hosts en la subred que especificó podrán acceder al Administrador de Grid. Todos los demás hosts están bloqueados.

Configurar el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en sus nodos de StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Has revisado la información en"Administrar los controles del firewall" y"Pautas para establecer redes" .
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante solo en puntos finales configurados explícitamente, debe definir los puntos finales del equilibrador de carga.

> Al cambiar la configuración de la red del cliente, las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos de su red. Puede utilizar las pestañas de control de Firewall para abrir o cerrar puertos que están abiertos de manera predeterminada en la red de cuadrícula, la red de administración y la red de cliente. También puede crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos de la red que están cerrados. Si está utilizando una red de cliente, puede especificar si un nodo confía en el tráfico entrante de la red de cliente y puede configurar el acceso a puertos específicos en la red de cliente.

Limitar la cantidad de puertos abiertos a direcciones IP fuera de su red a solo aquellos que sean absolutamente necesarios mejora la seguridad de su red. Utilice la configuración de cada una de las tres pestañas de control del Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de los controles de firewall, incluidos ejemplos, consulte"Administrar los controles del firewall" .

Para obtener más información sobre firewalls externos y seguridad de red, consulte"Controlar el acceso al firewall externo" .

Controles de firewall de acceso

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall**.

   Las tres pestañas de esta página se describen en"Administrar los controles del firewall" .

2. Seleccione cualquier pestaña para configurar los controles del firewall.

   Puede utilizar estas pestañas en cualquier orden. Las configuraciones que establezca en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña podrían cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

Utilice la pestaña Lista de direcciones privilegiadas para otorgar a los hosts acceso a puertos que están cerrados de manera predeterminada o cerrados por la configuración de la pestaña Administrar acceso externo.

Las direcciones IP y subredes privilegiadas no tienen acceso a la red interna de forma predeterminada. Además, los puntos finales del balanceador de carga y los puertos adicionales abiertos en la pestaña Lista de direcciones privilegiadas son accesibles incluso si están bloqueados en la pestaña Administrar acceso externo.

> Las configuraciones en la pestaña Lista de direcciones privilegiadas no pueden anular las configuraciones en la pestaña Red de cliente no confiable.

Pasos

1. En la pestaña Lista de direcciones privilegiadas, ingrese la dirección o subred IP a la que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes privilegiados adicionales.

   > Agregue la menor cantidad posible de direcciones a la lista privilegiada.

3. Opcionalmente, seleccione *Permitir que las direcciones IP privilegiadas accedan a los puertos internos de StorageGRID *. Ver "Puertos internos de StorageGRID" .

   > Esta opción elimina algunas protecciones para los servicios internos. Déjelo deshabilitado si es posible.

4. Seleccione **Guardar**.

Gestionar el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de la red podrá acceder al puerto a menos que agregue la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar puertos que estén abiertos de forma predeterminada y solo puedes abrir puertos que hayas cerrado.

> Las configuraciones en la pestaña Administrar acceso externo no pueden anular las configuraciones en la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es confiable, el puerto SSH/22 se bloquea en la red del cliente incluso si está abierto en la pestaña Administrar acceso externo. Las configuraciones en la pestaña Red de cliente no confiable anulan los puertos cerrados (como 443, 8443, 9443) en la red del cliente.

Pasos

1. Seleccione **Administrar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada) para los nodos de su red.
2. Configure los puertos que desea abrir y cerrar utilizando las siguientes opciones:
   - Utilice el interruptor junto a cada puerto para abrir o cerrar el puerto seleccionado.
   - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.
   - Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.

   > Si cierra los puertos 443 o 8443 de Grid Manager, todos los usuarios que estén conectados actualmente en un puerto bloqueado, incluido usted, perderán el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

   > Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los puertos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier puerto externo ingresando un número de puerto. Puede ingresar un número de puerto parcial. Por ejemplo, si ingresa un **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Seleccione **Guardar**

Red de clientes no confiables

Si la red de cliente de un nodo no es confiable, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del balanceador de carga y, opcionalmente, puertos adicionales que seleccione en esta pestaña. También puede utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.

> Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Los cambios de configuración que realice en la pestaña **Red de cliente no confiable** anulan las configuraciones de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red de cliente no confiable**.
2. En la sección Establecer nuevo nodo predeterminado, especifique cuál debe ser la configuración predeterminada cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.

   - **Confiable** (predeterminado): cuando se agrega un nodo en una expansión, su red de cliente es confiable.
   - **No confiable**: cuando se agrega un nodo en una expansión, su red de cliente no es confiable.

   Según sea necesario, puede regresar a esta pestaña para cambiar la configuración de un nuevo nodo específico.

   > Esta configuración no afecta a los nodos existentes en su sistema StorageGRID .

3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de clientes solo en puntos finales del balanceador de carga configurados explícitamente o en puertos seleccionados adicionales:

   - Seleccione **No confiar en los nodos mostrados** para agregar todos los nodos que se muestran en la tabla a la lista de Red de clientes no confiables.
   - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos que se muestran en la tabla de la lista Red de clientes no confiables.
   - Utilice el interruptor junto a cada nodo para configurar la red del cliente como confiable o no confiable para el nodo seleccionado.

   Por ejemplo, puede seleccionar **No confiar en los nodos mostrados** para agregar todos los nodos a la lista de Red de clientes no confiables y luego usar el botón junto a un nodo individual para agregar ese único nodo a la lista de Red de clientes confiables.

   > Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo ingresando el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si ingresa un **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Seleccione **Guardar**.

   La nueva configuración del firewall se aplica y se ejecuta de inmediato. Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.