



Administrar la configuración de seguridad

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

- Administrar la configuración de seguridad 1
 - Gestionar certificados 1
 - Configuración de servidores de gestión de claves. 32
 - Administrar la configuración de proxy 61
 - Administrar redes de clientes que no son de confianza. 64

Administrar la configuración de seguridad

Gestionar certificados

Acerca de los certificados de seguridad

Los certificados de seguridad son archivos de datos pequeños que se utilizan para crear conexiones seguras y de confianza entre componentes de StorageGRID y entre 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, autenticar la identidad de un servidor a sus clientes y proporcionar una ruta de comunicación segura para los datos. Cada servidor y el cliente tienen una copia del certificado.
- **Los certificados de cliente** autentican una identidad de cliente o usuario al servidor, proporcionando una autenticación más segura que las contraseñas solamente. Los certificados de cliente no cifran datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado de 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 extremo de equilibrio de carga) o como cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Certificado de CA de cuadrícula predeterminado

StorageGRID incluye una entidad de certificación (CA) integrada que genera un certificado de CA de grid interno durante la instalación del sistema. El certificado de CA de cuadrícula se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una entidad de certificación externa (CA) puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de su empresa. Aunque se puede utilizar el certificado de CA de cuadrícula para un entorno que no sea de producción, la práctica recomendada para un entorno de producción es utilizar certificados personalizados firmados por una entidad de certificación externa. Las conexiones no seguras que no tienen ningún certificado también se admiten, pero no se recomienda.

- Los certificados de CA personalizados no quitan 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 el [directrices de optimización del sistema](#) para certificados de servidor.
- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).



StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Es necesario

tener preparados todos los certificados necesarios para la configuración específica de StorageGRID antes de configurar el sistema.

Acceda a los certificados de seguridad

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

1. En Grid Manager, seleccione **CONFIGURATON > Seguridad > certificados**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

GlobalGrid CAClientLoad balancer endpointsTenantsOther

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type	Expiration date
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Seleccione una ficha en la página certificados para obtener información sobre cada categoría de certificado y para acceder a la configuración de certificado. Sólo puede acceder a una ficha si tiene el permiso adecuado.
 - **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 Prometheus de StorageGRID.
 - **Puntos finales del equilibrador de carga:** Protege las conexiones entre los clientes S3 y Swift y el equilibrador de carga StorageGRID.
 - **Arrendatarios:** Protege las conexiones a servidores de federación de identidades o desde extremos de servicio de plataforma a recursos de almacenamiento S3.
 - **Otros:** Protege las conexiones StorageGRID que requieren certificados específicos.

Cada una de las pestañas se describe a continuación con enlaces a detalles de certificados adicionales.

Global

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

- [Certificado de interfaz de gestión](#): Protege las conexiones del explorador Web cliente a las interfaces de administración de StorageGRID.
- [Certificado API S3 y Swift](#): Protege las conexiones API de cliente a los nodos de almacenamiento, los nodos de administración y los nodos de puerta de enlace, que las aplicaciones de cliente S3 y Swift utilizan para cargar y descargar datos de objetos.

Entre la información sobre los certificados globales instalados se incluyen:

- **Nombre:** Nombre del certificado con enlace a la administración del certificado.
- **Descripción**
- **Tipo:** Personalizado o predeterminado. + debe usar siempre un certificado personalizado para mejorar la seguridad de la cuadrícula.
- **Fecha de vencimiento:** Si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Podrá:

- Sustituya los certificados predeterminados por certificados personalizados firmados por una autoridad de certificado externa para mejorar la seguridad de la cuadrícula:
 - [Reemplace el certificado de interfaz de gestión generado por StorageGRID predeterminado](#) Se utiliza para las conexiones del administrador de grid y del administrador de inquilinos.
 - [Reemplace el certificado API de S3 y Swift](#) Se utiliza para conexiones de nodo de almacenamiento, servicio CLB (obsoleto) y extremo de equilibrador de carga (opcional).
- [Restaurar el certificado de interfaz de gestión predeterminado.](#)
- [Restaurar el certificado API S3 y Swift predeterminado.](#)
- [Use un script para generar un nuevo certificado de interfaz de gestión autofirmado.](#)
- Copie o descargue el [certificado de interfaz de gestión](#) o. [Certificado API S3 y Swift](#).

CA de grid

La [Certificado de CA de grid](#), Generado por la autoridad de certificación StorageGRID durante la instalación de StorageGRID, protege todo el tráfico interno de StorageGRID.

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

Puede hacerlo [Copie o descargue el certificado de Grid CA](#), pero no puede cambiarlo.

Cliente

[Certificados de cliente](#), Generada por una autoridad de certificados externa, asegura las conexiones entre herramientas de supervisión externas y la base de datos Prometheus de StorageGRID.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede utilizar para el acceso a la base de datos Prometheus, junto con la fecha de caducidad del certificado.

Podrá:

- [Cargar o generar un nuevo certificado de cliente.](#)
- Seleccione un nombre de certificado para mostrar los detalles del certificado, donde podrá:
 - [Cambie el nombre del certificado de cliente.](#)
 - [Establezca el permiso de acceso Prometheus.](#)
 - [Cargue y reemplace el certificado de cliente.](#)
 - [Copie o descargue el certificado de cliente.](#)
 - [Quite el certificado de cliente.](#)
- Seleccione **acciones** para hacerlo rápidamente [editar](#), [asociar](#), o. [quitar](#) un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez utilizando **acciones** > **Quitar**.

Puntos finales del equilibrador de carga

[Certificados de punto final de equilibrador de carga](#), Que cargue o genere, proteja las conexiones entre los clientes S3 y Swift y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración.

La tabla de extremo de equilibrador de carga tiene una fila para cada extremo de equilibrador de carga configurado e indica si se está utilizando el certificado API global S3 y Swift o un certificado de extremo de equilibrador de carga personalizado para el extremo. También se muestra la fecha de caducidad de cada certificado.



Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Podrá:

- [Seleccione un nombre de extremo para abrir una ficha de explorador con información sobre el extremo de equilibrio de carga, incluidos los detalles de su certificado.](#)
- [Especifique un certificado de extremo de equilibrio de carga para FabricPool.](#)
- [Use el certificado global de la API de S3 y Swift](#) en lugar de generar un nuevo certificado de extremo de equilibrio de carga.

Clientes

Los inquilinos pueden usar [certificados de servidor de federación de identidades](#) o. [certificados de extremo de servicio de plataforma](#) Para asegurar sus conexiones con StorageGRID.

La tabla de arrendatarios tiene una fila para cada arrendatario e indica si cada arrendatario tiene permiso para utilizar su propio origen de identidad o servicios de plataforma.

Podrá:

- [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 identidades del inquilino](#)
- [Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilino](#)
- [Especifique un certificado de extremo de servicio de plataforma durante la creación del extremo](#)

Otros

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

- [Certificados de federación de identidades](#)
- [Certificados de Cloud Storage Pool](#)
- [Certificados de servidor de gestión de claves \(KMS\)](#)
- [Certificados de inicio de sesión único](#)
- [Certificados de notificación de alertas por correo electrónico](#)
- [Certificados de servidor de syslog externos](#)

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



Solo puede ver y acceder a la información de otros certificados si dispone del permiso correspondiente.

Podrá:

- [Ver y editar un certificado de federación de identidades](#)
- [Cargar certificados de servidor de gestión de claves \(KMS\) y de cliente](#)
- [Especifique un certificado de Cloud Storage Pool para S3, C2S S3 o Azure](#)
- [Especifique manualmente un certificado SSO para la confianza de la parte que confía](#)
- [Especifique un certificado para notificaciones de alertas por correo electrónico](#)
- [Especifique un certificado de servidor de syslog externo](#)

Detalles del certificado de seguridad

A continuación se describe cada tipo de certificado de seguridad, con vínculos a artículos que contienen instrucciones de implementación.

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	<p>Autentica la conexión entre los exploradores web del cliente y la interfaz de gestión de StorageGRID, lo que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin advertencias de seguridad.</p> <p>Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos.</p> <p>Puede usar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.</p>	CONFIGURACIÓN > Seguridad > certificados , seleccione la ficha Global y, a continuación, seleccione Certificado de interfaz de administración	Configure los certificados de interfaz de gestión

Certificado API S3 y Swift

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica conexiones de cliente S3 o Swift seguras con un nodo de almacenamiento, en el servicio Connection Load Balancer (CLB) obsoleto en un nodo de puerta de enlace y extremos de equilibrador de carga (opcional).	CONFIGURATION > Security > Certificates , seleccione la ficha Global y, a continuación, seleccione S3 y Swift API Certificate	Configure los certificados API S3 y Swift

Certificado de CA de grid

Consulte [Descripción de certificado de CA de cuadrícula predeterminada](#).

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	<p>Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos.</p> <ul style="list-style-type: none"> • Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID. • Permite una supervisión segura de StorageGRID mediante herramientas externas. 	<p>CONFIGURACIÓN > Seguridad > certificados y, a continuación, seleccione la ficha Cliente</p>	<p>Configurar certificados de cliente</p>

Certificado de punto final de equilibrador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	<p>Autentica la conexión entre clientes S3 o Swift y el servicio StorageGRID Load Balancer en nodos de puerta de enlace y nodos de administrador. Puede cargar o generar un certificado de equilibrador de carga al configurar un extremo de equilibrador de carga. Las aplicaciones cliente utilizan el certificado de equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objeto.</p> <p>También puede utilizar una versión personalizada del global Certificado API S3 y Swift Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar conexiones de equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada extremo de equilibrador de carga.</p> <p>Nota: el certificado utilizado para la autenticación del equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.</p>	CONFIGURACIÓN > Red > terminales de equilibrador de carga	<ul style="list-style-type: none"> • Configurar puntos finales del equilibrador de carga • Cree un extremo de equilibrador de carga para FabricPool

Certificado de federación de identidades

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

Certificado de extremo de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde el servicio de plataforma StorageGRID a un recurso de almacenamiento S3.	Administrador de inquilinos > ALMACENAMIENTO (S3) > terminales de servicios de plataforma	Cree un extremo de servicios de plataforma Editar extremo de servicios de plataforma

Certificado de extremo de Cloud Storage Pool

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión de un pool de almacenamiento en cloud de StorageGRID a una ubicación de almacenamiento externa, como S3 Glacier o el almacenamiento blob de Microsoft Azure. Se necesita un certificado diferente para cada tipo de proveedor de cloud.	ILM > piscinas de almacenamiento	Cree un pool de almacenamiento en el cloud

Certificado de servidor de gestión de claves (KMS)

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

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 identidades, como Active Directory Federation Services (AD FS), y StorageGRID, que se utilizan para solicitudes de inicio de sesión único (SSO).	CONFIGURACIÓN > Control de acceso > Single Sign-On	Configurar el inicio de sesión único

Certificado de notificación de alertas por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	<p>Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta.</p> <ul style="list-style-type: none"> • Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo SMTP requiere certificados de cliente para la autenticación. 	ALERTAS > Configuración de correo electrónico	Configure notificaciones por correo electrónico para las alertas

Certificado de servidor de syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	<p>Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID.</p> <p>Nota: no se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.</p>	CONFIGURACIÓN > Supervisión > servidor de auditoría y syslog y, a continuación, seleccione Configurar servidor de syslog externo	Configure un servidor de syslog externo

Ejemplos de certificados

Ejemplo 1: Servicio de equilibrador de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Se configura un extremo de equilibrador de carga y se carga o genera un certificado de servidor en StorageGRID.
2. Debe configurar una conexión de cliente S3 o Swift al extremo de equilibrio de carga y cargar el mismo

certificado en el cliente.

3. Cuando el cliente desea guardar o recuperar datos, se conecta al extremo de equilibrio de carga mediante HTTPS.
4. StorageGRID responde con el certificado de servidor, que contiene una clave pública y 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 objeto a StorageGRID.

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

En este ejemplo, StorageGRID actúa como cliente.

1. Con el software de servidor de gestión de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por CA, un certificado de cliente público y la clave privada del certificado de cliente.
2. Con el Administrador de grid, configura un servidor KMS y carga los certificados de servidor y cliente y la clave privada de 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 mediante la conexión validada.

Configurar certificados de servidor

Tipos de certificado de servidor admitidos

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

Para obtener más información sobre cómo protege StorageGRID las conexiones de cliente para la API DE REST, consulte [Use S3](#) o [Use Swift](#).

Configure los certificados de interfaz de gestión

Puede reemplazar el certificado de interfaz de gestión predeterminado por un único certificado personalizado que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin tener que encontrar advertencias de seguridad. También puede revertir al certificado de interfaz de gestión predeterminado o generar una nueva.

Acerca de esta tarea

De manera predeterminada, cada nodo del administrador se envía un certificado firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por una sola clave privada correspondiente y un certificado de interfaz de gestión personalizado común.

Dado que se utiliza un único certificado de interfaz de gestión personalizado para todos los nodos de administración, debe especificar el certificado como un comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse a Grid Manager y al Gestor de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administrador de la cuadrícula.

Debe completar la configuración en el servidor y, en función de la entidad emisora de certificados raíz (CA) que esté utilizando, los usuarios también pueden necesitar instalar el certificado de la CA de cuadrícula en el explorador Web que utilizarán para acceder a Grid Manager y al gestor de inquilinos.



Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor para la interfaz de administración** se activa cuando este certificado de servidor está a punto de caducar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > certificados** y mirando la fecha de caducidad del certificado de interfaz de administración en la ficha Global.



Si accede a Grid Manager o a Intenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el explorador mostrará un error de certificado sin una opción para omitir si se produce alguna de las siguientes situaciones:

- El certificado de la interfaz de gestión personalizada caduca.
- Usted [revertir de un certificado de interfaz de gestión personalizado al certificado de servidor predeterminado](#).

Añada un certificado de interfaz de gestión personalizado

Para agregar un certificado de interfaz de gestión personalizado, puede proporcionar su propio certificado o generar uno mediante el Gestor de cuadrícula.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor:** El archivo de certificado de servidor personalizado (codificado con PEM).
- **Clave privada de certificado:** Archivo de clave privada de certificado de servidor personalizado (.key).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

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

c. Expanda **Detalles del certificado** para ver los metadatos de cada certificado que haya cargado. Si cargó un paquete de CA opcional, cada certificado aparece 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 de 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 de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Guardar**. + el certificado de interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario Manager.

Generar certificado

Genere los archivos de certificado de servidor.



La práctica recomendada para un entorno de producción es usar un certificado de interfaz de gestión personalizado firmado por una entidad de certificación externa.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

- **Nombre de dominio:** Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
- **IP:** Una o varias direcciones IP que se incluirán en el certificado.
- **Asunto:** X.509 asunto o nombre distinguido (DN) del propietario del certificado.

- **Días válidos:** Número de días después de la creación que expira el certificado.

c. Seleccione **generar**.

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

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

Especifique el nombre del archivo de 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 para pegarlo en otro lugar.

e. Seleccione **Guardar**. + el certificado de interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario Manager.

5. Actualice la página para garantizar que se actualice el explorador web.



Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Después de añadir un certificado de interfaz de gestión personalizado, la página de certificado de interfaz de gestión muestra información detallada sobre certificados que están en uso. + puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado de interfaz de gestión predeterminado

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado predeterminado**.

Cuando restaura el certificado de interfaz de gestión predeterminado, los archivos de certificado de servidor personalizados que configuró se eliminan y no pueden recuperarse del sistema. El certificado de la interfaz de gestión predeterminado se utiliza para todas las conexiones de clientes nuevas subsiguientes.

4. Actualice la página para garantizar que se actualice el explorador web.

Use un script para generar un nuevo certificado de interfaz de gestión autofirmado

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

Lo que necesitará

- Tiene permisos de acceso específicos.

- Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

La práctica recomendada para un entorno de producción es usar un certificado firmado por una entidad de certificación externa.

Pasos

1. Obtenga el nombre de dominio completo (FQDN) de cada nodo de administrador.
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 `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
 - d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

3. Configure StorageGRID con un certificado autofirmado nuevo.

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

- Para `--domains`, Utilice comodines para representar los nombres de dominio completos de todos los nodos Admin. Por ejemplo: `*.ui.storagegrid.example.com` utiliza el comodín `*` que se va a representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.
- Configurado `--type` para `management` Para configurar el certificado de la interfaz de gestión, que utiliza el administrador de grid y el administrador de inquilinos.
- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede 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 gestión esté sincronizado con el mismo origen de hora que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

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

El resultado contiene el certificado público que necesita el cliente API de gestión.

4. Seleccione y copie el certificado.

Incluya las etiquetas INICIAL Y FINAL en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`
6. Confirme que se configuró el certificado:

- a. Acceda a Grid Manager.
 - b. Seleccione **CONFIGURACIÓN > Seguridad > certificados**
 - c. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
7. Configure el cliente de administración para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Descargue o copie el certificado de la interfaz de gestión

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el paquete de CA .pem archivo. Si utiliza un bundle 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 bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

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

Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

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

Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

- 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`

Configure los certificados API S3 y Swift

Es posible reemplazar o restaurar el certificado de servidor que se usa para conexiones de clientes S3 o Swift a nodos de almacenamiento, el servicio Connection Load Balancer

(CLB) obsoleto en los nodos de puerta de enlace o para cargar extremos de equilibrador. El certificado de servidor personalizado de reemplazo es específico de su organización.

Acerca de esta tarea

De forma predeterminada, cada nodo de almacenamiento recibe un certificado de servidor X.509 firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por un solo certificado de servidor personalizado común y una clave privada correspondiente.

Un único certificado de servidor personalizado se usa para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse al extremo de almacenamiento. Defina el certificado personalizado de forma que coincida con todos los nodos de almacenamiento de la cuadrícula.

Después de completar la configuración en el servidor, es posible que también necesite instalar el certificado de CA de grid en el cliente API S3 o Swift que usará para acceder al sistema, según la entidad de certificación (CA) raíz que use.



Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor global para API de S3 y Swift** se activa cuando el certificado de servidor raíz está a punto de caducar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > certificados** y mirando la fecha de caducidad del certificado API S3 y Swift en la ficha Global.

Puede cargar o generar un certificado API personalizado de S3 y Swift.

Añada un certificado API de S3 y Swift personalizado

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor:** El archivo de certificado de servidor personalizado (codificado con PEM).
- **Clave privada de certificado:** Archivo de clave privada de certificado de servidor personalizado (.key).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete CA:** Un único archivo opcional que contiene los certificados de cada autoridad de certificación de emisión intermedia. El archivo debe contener cada uno de los archivos de certificado de CA codificados con 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 de S3 y Swift personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado aparece 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 de 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 de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
- d. Seleccione **Guardar**.

El certificado de servidor personalizado se usa para conexiones posteriores de clientes S3 y Swift.

Generar certificado

Genere los archivos de certificado de servidor.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

- **Nombre de dominio:** Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
- **IP:** Una o varias direcciones IP que se incluirán en el certificado.
- **Asunto:** X.509 asunto o nombre distinguido (DN) del propietario del certificado.
- **Días válidos:** Número de días después de la creación que expira el certificado.

c. Seleccione **generar**.

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

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

Especifique el nombre del archivo de 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 para pegarlo en otro lugar.

e. Seleccione **Guardar**.

El certificado de servidor personalizado se usa para conexiones posteriores de clientes S3 y Swift.

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



Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Actualice la página para garantizar que se actualice el explorador web.

7. Después de añadir un certificado de API personalizado de S3 y Swift, la página de certificados de la API de S3 y Swift muestra información detallada de los certificados API personalizados de S3 y Swift que está en uso. + puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado API S3 y Swift predeterminado

Es posible revertir a usar el certificado API S3 y Swift predeterminado para conexiones de clientes S3 y Swift a nodos de almacenamiento, así como el servicio CLB obsoleto en los nodos de puerta de enlace. Sin embargo, no puede utilizar el certificado API S3 y Swift predeterminado para un extremo de equilibrio de carga.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione **utilizar certificado predeterminado**.

Cuando restaura la versión predeterminada del certificado API global S3 y Swift, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar desde el sistema. El certificado API S3 y Swift predeterminado se utilizará para las conexiones de clientes S3 y Swift posteriores a los nodos de almacenamiento, así como para el servicio CLB obsoleto en los nodos de puerta de enlace.

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

Si tiene permiso de acceso raíz y se utilizó el certificado de API Swift y S3 personalizado para conexiones de extremos de equilibrio de carga, se muestra una lista de extremos de equilibrio de carga que ya no se

podrán acceder mediante el certificado API predeterminado S3 y Swift. Vaya a [Configurar puntos finales del equilibrador de carga](#) para editar o eliminar los puntos finales afectados.

5. Actualice la página para garantizar que se actualice el explorador web.

Descargue o copie el certificado de la API S3 y Swift

Es posible guardar o copiar el contenido de los certificados API S3 y Swift para usarlos en otra parte.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el paquete de CA .pem archivo. Si utiliza un bundle 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 bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

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

Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

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

Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

- 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

- [Use S3](#)
- [Use Swift](#)
- [Configure los nombres de dominio de extremo API de S3](#)

Copie el certificado de la CA de cuadrícula

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

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tiene permisos de acceso específicos.

Acerca de esta tarea

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **CA** de cuadrícula.
2. En la sección **Certificado PEM** descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado .pem archivo.

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

Por ejemplo: storagegrid_certificate.pem

PEM de certificado de copia

Copie el texto del certificado que se va a pegar 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

Configure los certificados StorageGRID para FabricPool

En el caso de clientes S3 que realizan una validación de nombre de host estricta y no admiten la deshabilitación de la validación estricta de nombre de host, como clientes ONTAP que utilizan FabricPool, puede generar o cargar un certificado de servidor al configurar el extremo del equilibrador de carga.

Lo que necesitará

- Tiene permisos de acceso específicos.

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).

Acerca de esta tarea

Al crear un extremo de equilibrador de carga, se puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una entidad de certificación (CA) conocida. En los entornos de producción, se debe utilizar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar de forma no disruptiva. También son más seguros porque ofrecen una mejor protección contra los ataques de tipo "hombre en el medio".

En los siguientes pasos, se ofrecen directrices generales para clientes S3 que usan FabricPool. Para obtener información más detallada y procedimientos, consulte [Configure StorageGRID para FabricPool](#).



El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y no se recomienda su uso con FabricPool.

Pasos

1. Opcionalmente, configure un grupo de alta disponibilidad (ha) para que lo utilice FabricPool.
2. Cree un extremo de equilibrador de carga de S3 para que se utilice FabricPool.

Cuando crea un extremo de equilibrio de carga HTTPS, se le solicita que cargue el certificado de servidor, la clave privada de certificado y el paquete de CA opcional.

3. Adjuntar StorageGRID como nivel de cloud en ONTAP.

Especifique el puerto de extremo de equilibrio de carga y el nombre de dominio completo utilizado en el certificado de CA que ha cargado. A continuación, proporcione el certificado de CA.



Si una CA intermedia emitió el certificado StorageGRID, debe proporcionar el certificado de CA intermedio. Si la CA raíz emitió directamente el certificado StorageGRID, debe proporcionar el certificado de CA raíz.

Configurar certificados de cliente

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

Si necesita acceder a StorageGRID mediante una herramienta de supervisión externa, debe cargar o generar un certificado de cliente mediante el Gestor de cuadrícula y copiar la información de certificado a la herramienta externa.

Consulte la información acerca de [uso general de certificados de seguridad](#) y.. [configuración de certificados de servidor personalizados](#).



Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad de certificados de cliente configurados en la página certificados** se activa cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > certificados** y mirando la fecha de caducidad del certificado de cliente en la ficha Cliente.



Si usa un servidor de gestión de claves (KMS) para proteger los datos en los nodos de dispositivos especialmente configurados, consulte la información específica acerca de [Cargando un certificado de cliente KMS](#).

Lo que necesitará

- Tiene permiso de acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Para configurar un certificado de cliente:
 - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
 - Si configuró el certificado de interfaz de gestión StorageGRID, tiene la CA, el certificado de cliente y la clave privada utilizadas para configurar el certificado de interfaz de gestión.
 - Para cargar su propio certificado, la clave privada del certificado está disponible en su equipo local.
 - La clave privada debe haberse guardado o registrado en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
 - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
 - Para cargar su propio certificado o un nuevo certificado, la clave privada, el certificado de cliente y la CA (si se utiliza) están disponibles en su equipo local.

Añada certificados de cliente

Siga el procedimiento para agregar un certificado de cliente a su escenario:

- [El certificado de interfaz de gestión ya está configurado](#)
- [CERTIFICADO de cliente emitido por CA](#)
- [Certificado generado desde Grid Manager](#)

El certificado de interfaz de gestión ya está configurado

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

Pasos

1. En Grid Manager, seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.
4. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.
5. En la sección **Tipo de certificado**, cargue el certificado de interfaz de administración .pem archivo.
 - a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
 - b. Cargue el archivo de certificado de interfaz de gestión (.pem).
 - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

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

c. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

6. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.

a. **Nombre:** Escriba un nombre para la conexión.

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

b. **URL:** Introduzca 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. Activar **Licencia de cliente TLS y con CA Cert.**

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

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

e. **ServerName:** Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de la interfaz de gestión.

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

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener más información sobre las métricas, consulte [Instrucciones para supervisar StorageGRID](#).

CERTIFICADO de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y tiene previsto agregar un certificado de cliente para Prometheus que utilice un certificado de cliente emitido por CA y una clave privada.

Pasos

1. Siga los pasos a. [configure un certificado de interfaz de gestión](#).
2. En Grid Manager, seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.
5. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.

6. En la sección **Tipo de certificado**, cargue el certificado de cliente, la clave privada y el paquete de CA .pem archivos:
 - a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
 - b. Cargue un certificado de cliente, una clave privada y archivos de paquete de CA (.pem).
 - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en Grid Manager.

Los nuevos certificados aparecen en la ficha Cliente.

7. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.

- a. **Nombre:** Escriba un nombre para la conexión.

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

- b. **URL:** Introduzca 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. Activar **Licencia de cliente TLS y con CA Cert**.

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

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

- e. **ServerName:** Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de la interfaz de gestión.

- f. Guarde y pruebe el certificado y la clave privada que copió desde StorageGRID o un archivo local.

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener más información sobre las métricas, consulte [Instrucciones para supervisar StorageGRID](#).

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y planea agregar un certificado de cliente para Prometheus que utilice la función generar certificado en Grid Manager.

Pasos

1. En Grid Manager, seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación,

seleccione la ficha **Cliente**.

2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.
4. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.
5. En la sección **Tipo de certificado**, seleccione **generar certificado**.
6. Especifique la información del certificado:
 - **Nombre de dominio**: Uno o más nombres de dominio completos del nodo de administración que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
 - **IP**: Una o más direcciones IP del nodo de administración que se incluirán en el certificado.
 - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
7. Seleccione **generar**.
8. Seleccione **Detalles del certificado de 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 una ubicación segura.

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

Especifique el nombre del archivo de 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 para pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

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

9. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha **Cliente**.

10. En Grid Manager, seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **Global**.
11. Seleccione **Certificado de interfaz de administración**.
12. Seleccione **utilizar certificado personalizado**.
13. Cargue los archivos `certificate.pem` y `private_key.pem` desde el [detalles del certificado de cliente](#) paso. No es necesario cargar un paquete de CA.
 - a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
 - b. Cargue cada archivo de certificado (`.pem`).
 - c. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

14. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.

a. **Nombre:** Escriba un nombre para la conexión.

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

b. **URL:** Introduzca 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. Activar **Licencia de cliente TLS y con CA Cert.**

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

- El certificado de cliente de interfaz de gestión para **CA Cert** y **Cliente Cert**
- La clave privada de **clave de cliente**

e. **ServerName:** Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de la interfaz de gestión.

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

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener más información sobre las métricas, consulte [Instrucciones para supervisar StorageGRID](#).

Editar certificados de cliente

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

2. Seleccione el certificado que desea editar.

3. Seleccione **Editar** y, a continuación, seleccione **Editar nombre y permiso**

4. Introduzca un nombre de certificado que contenga al menos 1 y no más de 32 caracteres.

5. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.

6. Seleccione **continuar** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Adjunte un nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

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

Cargue el certificado

Copie el texto del certificado que se va a pegar en otro lugar.

- a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
- b. Cargue el nombre de certificado de cliente (.pem).

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

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

Especifique el nombre del archivo de 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 para pegarlo en otro lugar.
- c. Seleccione **Crear** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Generar certificado

Genere el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **generar certificado**.
- b. Especifique la información del certificado:
 - **Nombre de dominio:** Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
 - **IP:** Una o varias direcciones IP que se incluirán en el certificado.
 - **Asunto:** X.509 asunto o nombre distinguido (DN) del propietario del certificado.
 - **Días válidos:** Número de días después de la creación que expira el certificado.
- c. Seleccione **generar**.
- d. Seleccione **Detalles del certificado de 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 una ubicación segura.

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

Especifique el nombre del archivo de 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 para pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

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

e. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

Descargar o copiar certificados de cliente

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado `.pem` archivo.

- a. Seleccione **Descargar certificado**.
- b. Especifique el nombre del archivo de 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 que se va a pegar 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`

Quite certificados de cliente

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > certificados** y, a continuación, seleccione la ficha **Cliente**.

2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y, a continuación, confirme.



Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la ficha Cliente y, a continuación, seleccione **acciones > Eliminar**.

Una vez que se elimine un certificado, los clientes que lo hayan usado deben especificar un nuevo certificado de cliente para acceder a la base de datos Prometheus de StorageGRID.

Configuración de servidores de gestión de claves

Configurar servidores de gestión de claves: Descripción general

Puede configurar uno o más servidores de gestión de claves externos (KMS) para proteger los datos en nodos de dispositivo especialmente configurados.

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

Un servidor de gestión de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID en el sitio de StorageGRID asociado mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

Puede utilizar uno o varios servidores de gestión de claves para administrar las claves de cifrado de nodos para los nodos de dispositivo StorageGRID que tengan activada la configuración * cifrado de nodos* durante la instalación. El uso de servidores de gestión de claves con estos nodos de dispositivos le permite proteger los datos aunque se haya eliminado un dispositivo del centro de datos. Una vez que los volúmenes del dispositivo se han cifrado, no podrá acceder a ningún dato en el dispositivo a menos que el nodo se pueda comunicar con el KMS.




StorageGRID no crea ni gestiona las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea usar un servidor de gestión de claves externo para proteger los datos StorageGRID, debe comprender cómo configurar ese servidor y debe comprender cómo gestionar las claves de cifrado. La realización de tareas de gestión de claves supera el alcance de estas instrucciones. Si necesita ayuda, consulte la documentación del servidor de gestión de claves o póngase en contacto con el soporte técnico.

Consulte los métodos de cifrado de StorageGRID

StorageGRID proporciona una serie de opciones para cifrar datos. Debe revisar los métodos disponibles para determinar qué métodos cumplen 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 gestión de claves (KMS) en Grid Manager	Configure un servidor de administración de claves para el sitio StorageGRID (CONFIGURACIÓN > Seguridad > servidor de administración de claves) y active el cifrado de nodos para el dispositivo. A continuación, un nodo de dispositivo se conecta al KMS para solicitar una clave de cifrado (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	<p>Nodos de dispositivo con cifrado de nodos activado durante la instalación. Todos los datos del dispositivo están protegidos frente a la pérdida física o la eliminación del centro de datos.</p> <div>  <p>La gestión de claves de cifrado con un KMS solo es compatible con los nodos de almacenamiento y los dispositivos de servicio.</p> </div>
Drive Security en SANtricity System Manager	Si la función Drive Security está habilitada para un dispositivo de almacenamiento, es posible usar SANtricity System Manager para crear y gestionar la clave de seguridad. Se requiere la clave para acceder a los datos en las unidades seguras.	<p>Dispositivos de almacenamiento con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. No se puede utilizar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio.</p> <ul style="list-style-type: none"> • Dispositivos de almacenamiento SG6000 • Dispositivos de almacenamiento SG5700 • Dispositivos de almacenamiento SG5600
Opción de cuadrícula de cifrado de objetos almacenados	La opción cifrado de objetos almacenados se puede activar en Grid Manager (CONFIGURACIÓN > sistema > Opciones de cuadrícula). Cuando se habilita esta opción, todos los objetos nuevos que no se cifran a nivel de bloque o de objeto se cifran durante el procesamiento.	<p>Datos de objetos S3 y Swift recientemente procesados.</p> <p>Los objetos almacenados existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran.</p> <ul style="list-style-type: none"> • Configurar el cifrado de objetos almacenados

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de bloques de S3	Se emite una solicitud DE cifrado PUT Bucket para habilitar el cifrado en el bloque. Los objetos nuevos que no se cifren en el nivel de objeto se cifran durante el procesamiento.	<p>Solo datos de objetos S3 procesados recientemente.</p> <p>Debe especificarse el cifrado para el bloque. Los objetos de bloque existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran.</p> <ul style="list-style-type: none"> • Use S3
Cifrado del lado del servidor de objetos S3 (SSE)	Se emite una solicitud de S3 para almacenar un objeto e incluir el x-amz-server-side-encryption solicite el encabezado.	<p>Solo datos de objetos S3 procesados recientemente.</p> <p>Se debe especificar el cifrado para el objeto. Los metadatos de objetos y otros datos confidenciales no se cifran.</p> <p>StorageGRID gestiona las claves.</p> <ul style="list-style-type: none"> • Use S3
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	<p>Se emite una solicitud S3 para almacenar un objeto e incluir tres encabezados de solicitud.</p> <ul style="list-style-type: none"> • x-amz-server-side-encryption-customer-algorithm • x-amz-server-side-encryption-customer-key • x-amz-server-side-encryption-customer-key-MD5 	<p>Solo datos de objetos S3 procesados recientemente.</p> <p>Se debe especificar el cifrado para el objeto. Los metadatos de objetos y otros datos confidenciales no se cifran.</p> <p>Las claves se gestionan fuera de StorageGRID.</p> <ul style="list-style-type: none"> • Use S3
Cifrado de volúmenes o almacenes de datos externos	Si la plataforma de implementación lo admite, puede utilizar un método de cifrado fuera de StorageGRID para cifrar un volumen o almacén de datos completo.	<p>Todos los datos de objetos, metadatos y datos de configuración del sistema, suponiendo que se cifre cada volumen o almacén de datos.</p> <p>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.</p>

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de objetos fuera de StorageGRID	Se utiliza un método de cifrado fuera de StorageGRID para cifrar los metadatos y los datos de objetos antes de que se ingieran en StorageGRID.	<p>Solo datos de objetos y metadatos (los datos de configuración del sistema no están cifrados).</p> <p>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.</p> <ul style="list-style-type: none"> • "Amazon simple Storage Service - Guía para desarrolladores: Protección de datos mediante cifrado en el cliente"

Utilice varios métodos de cifrado

En función de los requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

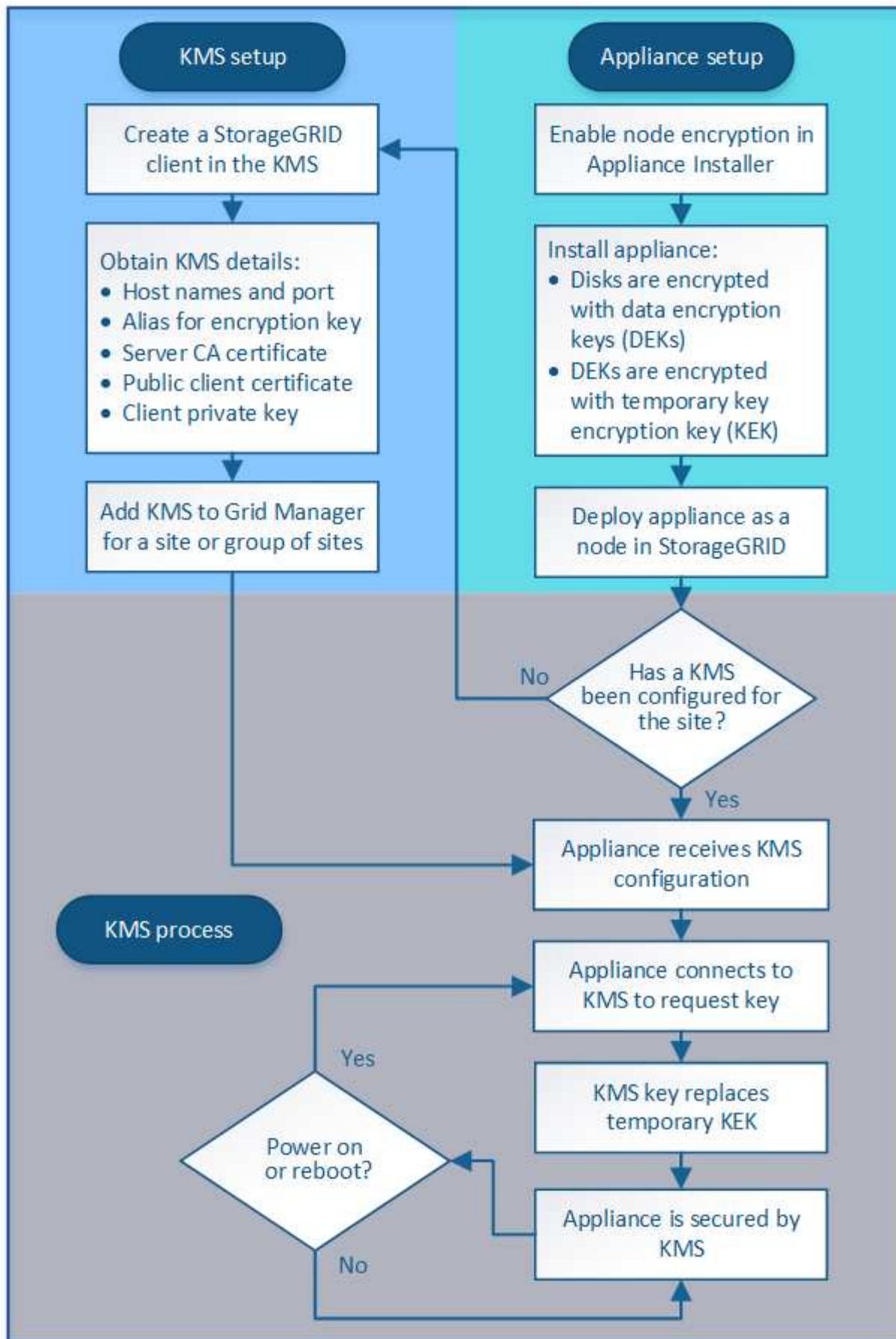
- Puede utilizar un KMS para proteger los nodos de dispositivos y también para usar la función de seguridad de unidades de System Manager de SANtricity a fin de «doble cifrado» de datos de las unidades de autocifrado de los mismos dispositivos.
- Puede usar un KMS para proteger los datos en los nodos del dispositivo y también puede usar la opción de cuadrícula de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de los objetos requiere cifrado, considere la posibilidad de controlar el cifrado en el nivel de bloque o de objeto individual. Habilitar varios niveles de cifrado tiene un coste de rendimiento adicional.

Información general de la configuración de KMS y dispositivos

Antes de poder usar un servidor de gestión de claves (KMS) para proteger los datos de StorageGRID en los nodos de los dispositivos, debe completar dos tareas de configuración: Configurar uno o más servidores KMS y habilitar el cifrado de nodos de los nodos de los dispositivos. Cuando estas dos tareas de configuración se completan, el proceso de gestión de claves se realiza de forma automática.

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



El diagrama de flujo muestra la configuración de KMS y la configuración de dispositivos que se producen en

paralelo; sin embargo, puede configurar los servidores de gestión de claves antes o después de habilitar el cifrado de nodos para los nodos de la aplicación nuevos, en función de sus requisitos.

Configurar el servidor de gestión de claves (KMS)

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

Paso	Consulte
Acceda al software KMS y añada un cliente para StorageGRID a cada clúster KMS o KMS.	Configure StorageGRID como cliente en KMS
Obtenga la información necesaria para el cliente StorageGRID en el KMS.	Configure StorageGRID como cliente en KMS
Agregue el KMS al Gestor de cuadrícula, asígnelo a un único sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración de KMS.	Añadir un servidor de gestión de claves (KMS)

Configure el aparato

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

1. Durante la fase de configuración de hardware de la instalación del dispositivo, utilice el instalador del dispositivo StorageGRID para activar el ajuste **cifrado de nodos** del dispositivo.



No puede activar el ajuste **cifrado de nodos** después de agregar un dispositivo a la cuadrícula y no puede utilizar la administración de claves externa para dispositivos que no tienen el cifrado de nodos activado.

2. Ejecute el instalador del dispositivo StorageGRID. Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen de la cabina, como se indica a continuación:
 - Los depósitos se utilizan para cifrar los datos en cada volumen. Estas claves se generan utilizando el cifrado de disco de Linux Unified Key Setup (LUKS) en el sistema operativo del dispositivo y no se pueden cambiar.
 - Cada DEK individual se cifra mediante una clave de cifrado de clave maestra (KEK). El KEK inicial es una clave temporal que cifra los depósitos hasta que el dispositivo pueda conectarse al KMS.
3. Añada el nodo del dispositivo a StorageGRID.

Si quiere más información, consulte lo siguiente:

- [Servicios de aplicaciones SG100 y SG1000](#)
- [Dispositivos de almacenamiento SG6000](#)
- [Dispositivos de almacenamiento SG5700](#)
- [Dispositivos de almacenamiento SG5600](#)

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. Al instalar un dispositivo con el cifrado de nodos activado en la cuadrícula, StorageGRID determina si existe una configuración KMS para el sitio que contiene el nodo nuevo.
 - 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, el KEK temporal continúa encriptando los datos del dispositivo hasta que configura un KMS para el sitio y el dispositivo recibe la configuración de KMS.
2. El dispositivo usa la configuración 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 sustituye al KEK temporal y ahora se utiliza para cifrar y descifrar los depósitos de los volúmenes del dispositivo.



Los datos que existan antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifran con una clave temporal. Sin embargo, los volúmenes de los dispositivos no se deben considerar protegidos de la eliminación del centro de datos hasta que la clave temporal se sustituya por la clave de cifrado KMS.

4. Si el dispositivo está encendido o reiniciado, se vuelve a conectar con el KMS para solicitar la clave. La tecla, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o un reinicio.

Consideraciones y requisitos para usar un servidor de gestión de claves

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

¿Cuáles son los requisitos de KMIP?

StorageGRID admite la versión KMIP 1.4.

["Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"](#)

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID admite los siguientes cifrados TLS v1.2 para KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Debe asegurarse de que cada nodo de dispositivo que utilice cifrado de nodo tenga acceso de red al clúster KMS o KMS configurado para el sitio.

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comuniquen a través del puerto que se utiliza para las comunicaciones del protocolo de interoperabilidad de gestión de claves (KMIP). El puerto KMIP predeterminado es 5696.

¿Qué dispositivos son compatibles?

Puede usar un servidor de administración de claves (KMS) para administrar las claves de cifrado de cualquier dispositivo StorageGRID de la cuadrícula que tenga activada la configuración **cifrado de nodos**. Este ajuste solo se puede habilitar durante la fase de configuración de hardware de la instalación del dispositivo mediante el instalador de StorageGRID Appliance.



No se puede habilitar el cifrado de nodos después de que se añade un dispositivo a la cuadrícula y no se puede usar la gestión de claves externa en los dispositivos que no tienen el cifrado de nodos habilitado.

Puede usar el KMS configurado para los siguientes dispositivos StorageGRID y nodos de dispositivos:

Dispositivo	Tipo de nodo
Aplicación de servicios SG1000	El nodo de administrador o el nodo de puerta de enlace
Servicio de atención al cliente SG100	El nodo de administrador o el nodo de puerta de enlace
Dispositivo de almacenamiento SG6000	Nodo de almacenamiento
Dispositivo de almacenamiento SG5700	Nodo de almacenamiento
Dispositivo de almacenamiento SG5600	Nodo de almacenamiento

No puede usar el KMS configurado para nodos basados en software (sin dispositivo), incluidos los siguientes:

- Nodos puestos en marcha como máquinas virtuales (VM)
- Nodos implementados en motores de contenedor en hosts Linux

Los nodos puestos en marcha en estas otras plataformas pueden utilizar el cifrado fuera de StorageGRID a nivel de almacén de datos o disco.

¿Cuándo se deben configurar los servidores de gestión de claves?

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

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

¿Cuántos servidores de gestión de claves necesito?

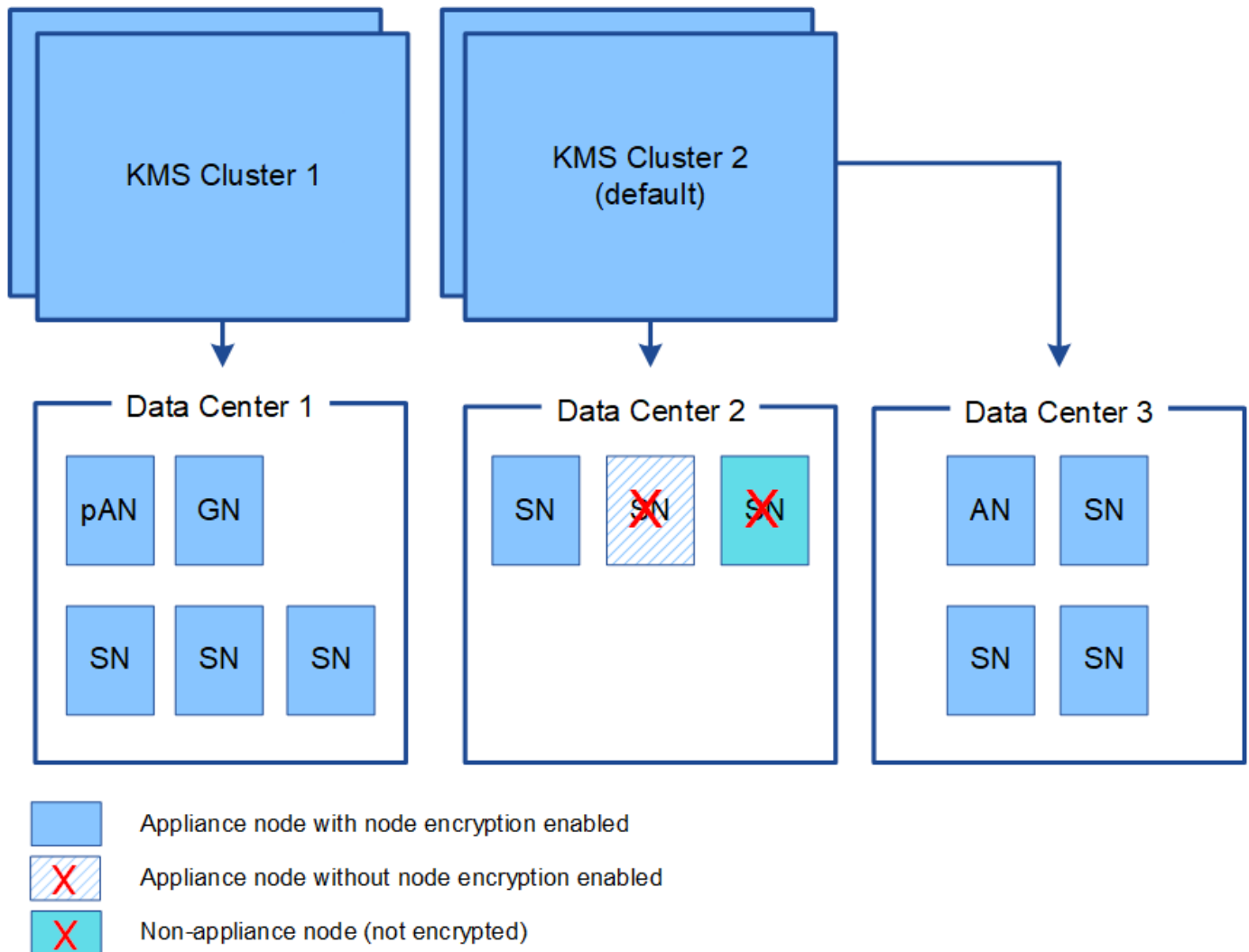
Puede configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de dispositivos en el sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de dispositivos StorageGRID en un único sitio o a un grupo de sitios.

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

Por ejemplo, supongamos que el sistema StorageGRID tiene tres sitios de centro de datos. Podría configurar un clúster KMS para proporcionar una clave a todos los nodos de dispositivos en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos de dispositivos de los demás sitios. Al

agregar 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 utilizar KMS para nodos que no son de dispositivo ni para los que no tenían activada la configuración de **cifrado de nodos** durante la instalación.



¿Qué ocurre cuando se gira una clave?

Como práctica recomendada para la seguridad, debe girar periódicamente la clave de cifrado utilizada por cada KMS configurado.

Al girar la clave de cifrado, utilice el software KMS para pasar de la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.



Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS en el Gestor de cuadrícula. En su lugar, gire la clave actualizando la versión de la clave en el software KMS. Utilice el mismo alias de clave para las claves nuevas que se usaron para las claves anteriores. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.

Cuando la nueva versión de clave esté disponible:

- Se distribuye automáticamente a los nodos de dispositivos cifrados del sitio o de los sitios asociados con el KMS. La distribución debe producirse dentro de una hora a partir de la cual se gira la clave.
- Si el nodo de dispositivo cifrado está sin conexión cuando se distribuye la nueva versión de clave, el nodo recibirá la nueva clave en cuanto se reinicie.
- Si la nueva versión de clave no se puede utilizar para cifrar los volúmenes del dispositivo por cualquier motivo, se activa la alerta **error de rotación de clave de cifrado KMS** para el nodo del dispositivo. Es posible que deba ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo reutilizar un nodo de dispositivo después de cifrar?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID, primero debe retirar el nodo grid para mover los datos del objeto a otro nodo. A continuación, puede usar el instalador del dispositivo StorageGRID para borrar la configuración de KMS. Al borrar la configuración KMS se deshabilita la configuración **cifrado de nodos** y se elimina la asociación entre el nodo del dispositivo y la configuración KMS del sitio StorageGRID.



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

Información relacionada

- [Servicios de aplicaciones SG100 y SG1000](#)
- [Dispositivos de almacenamiento SG6000](#)
- [Dispositivos de almacenamiento SG5700](#)
- [Dispositivos de almacenamiento SG5600](#)

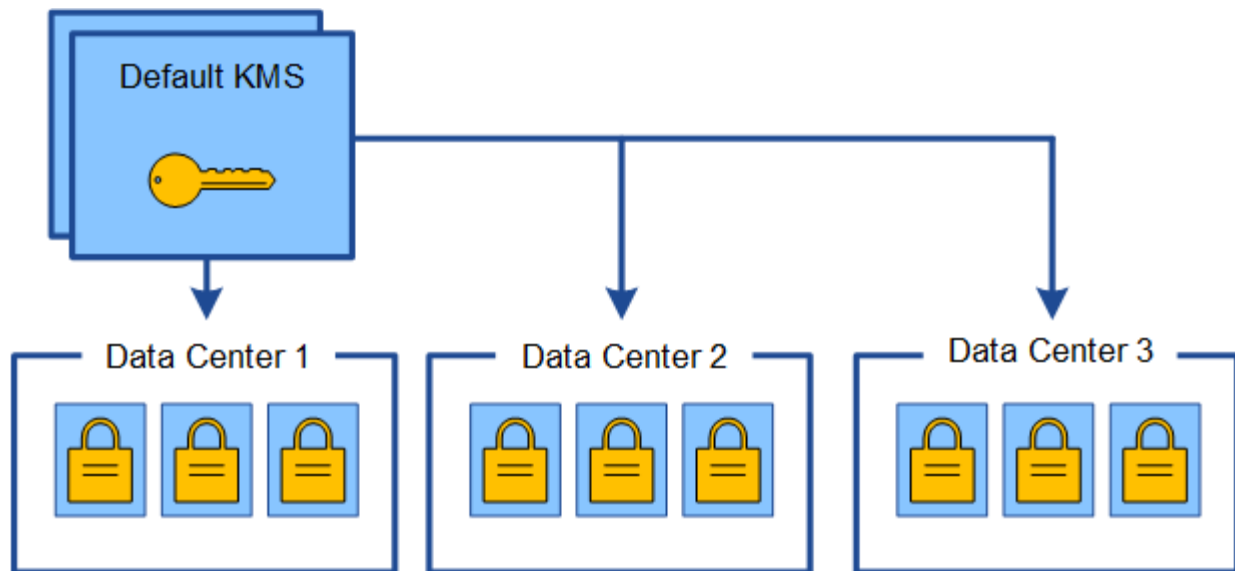
Consideraciones para cambiar el KMS de un sitio

Cada servidor de gestión de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos de dispositivos en un único sitio o en un grupo de sitios. Si necesita cambiar qué KMS se utiliza para un sitio, es posible que necesite copiar la clave de cifrado de un KMS a otro.

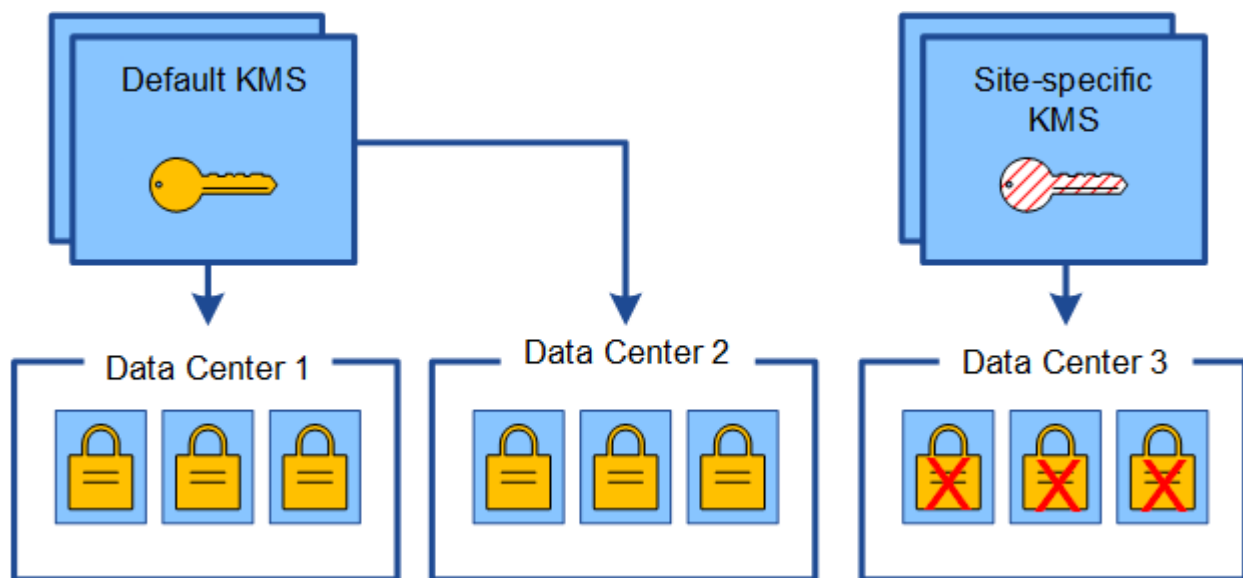
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original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

Por ejemplo:

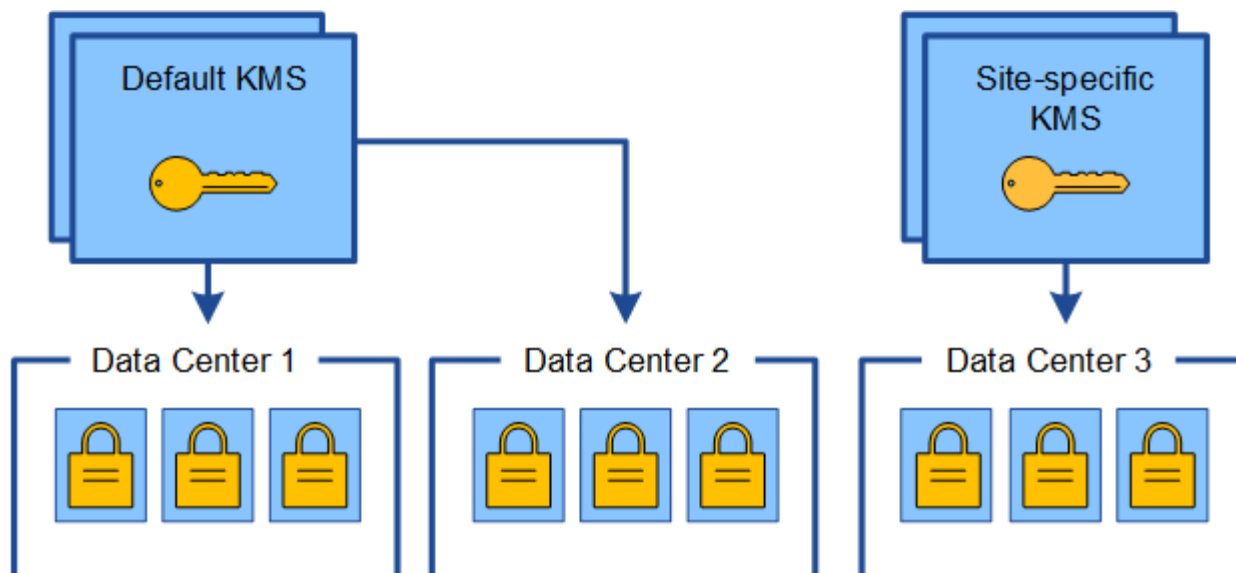
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa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



- Decide agregar un KMS específico de un sitio para un sitio (Data Center 3 en la figura). Sin embargo, como los nodos del dispositivo ya están cifrados, se produce un error de validación cuando se intenta guardar la configuración para el 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.



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



Utilice casos para cambiar qué KMS se utiliza para un sitio

La tabla resume los pasos necesarios para los casos más comunes para cambiar el KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos requeridos
Tiene una o más entradas KMS específicas del sitio y desea usar una de ellas como KMS predeterminado.	<p>Edite 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 se utilizará ahora como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado.</p> <p>Editar un servidor de gestión de claves (KMS)</p>
Tiene un KMS predeterminado y agrega un sitio nuevo en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	<ol style="list-style-type: none"> 1. Si los nodos del dispositivo en el sitio nuevo ya han sido cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un KMS nuevo. 2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio. <p>Añadir un servidor de gestión de claves (KMS)</p>

Caso de uso para cambiar el KMS de un sitio	Pasos requeridos
Desea que el KMS para un sitio utilice un servidor diferente.	<ol style="list-style-type: none"> 1. Si los nodos del dispositivo del sitio ya han sido cifrados por el KMS existente, use el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al KMS nuevo. 2. Con el Administrador de cuadrícula, edite la configuración de KMS existente e introduzca el nuevo nombre de host o la dirección IP. <p>Añadir un servidor de gestión de claves (KMS)</p>

Configure StorageGRID como cliente en KMS

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

Acerca de esta tarea

Estas instrucciones se aplican a Thales CipherTrust Manager k170v, versiones 2.0, 2.1 y 2.2. Si tiene preguntas sobre el uso de un servidor de gestión de claves diferente con StorageGRID, póngase en contacto con el soporte técnico.

"Thales CipherTrust Manager"

Pasos

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

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

2. Desde el software KMS, cree una clave de cifrado AES para cada clúster KMS o KMS.

La clave de cifrado debe ser exportable.

3. Registre la siguiente información de cada clúster KMS o KMS.

Necesitará esta información cuando agregue 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 del KMS.



La clave de cifrado ya debe existir en el KMS. StorageGRID no crea ni gestiona claves KMS.

4. Para cada clúster de KMS o KMS, obtenga un certificado de servidor firmado por una entidad de certificación (CA) o un paquete de certificado que contiene cada uno de los archivos de certificado de CA codificados con PEM, concatenado en el orden de la cadena de certificados.

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

- El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.
- El campo Nombre alternativo del asunto (SAN) de 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 introducir las mismas FQDN o direcciones IP en el campo **Nombre de host**.

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

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

Añadir un servidor de gestión de claves (KMS)

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

Lo que necesitará

- Ha revisado el [consideraciones y requisitos para usar un servidor de gestión de claves](#).
- Ya tienes [Se ha configurado StorageGRID como cliente en el KMS](#) y tiene la información necesaria para cada clúster KMS o KMS.
- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tiene el permiso acceso raíz.

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 aplica a todos los sitios no administrados por otro KMS. Si crea el KMS predeterminado primero, todos los dispositivos cifrados por nodo de la cuadrícula se cifrarán con el KMS predeterminado. Si desea crear más tarde un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulte [Consideraciones para cambiar el KMS de un sitio](#) para obtener más detalles.

Paso 1: Introduzca los detalles de KMS

En el paso 1 (introducir detalles de KMS) del asistente para agregar un servidor de administración de claves, se proporcionan detalles sobre el clúster KMS o KMS.

Pasos

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

Se muestra la página servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?

Key Name ?

Manages keys for ?

Hostname ?

Certificate Status ?

No key management servers have been configured. Select **Create**.

2. Seleccione **Crear**.

Paso 1 (introducir detalles de KMS) del asistente Añadir un servidor de gestión de claves aparece.

Add a Key Management Server



Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name ?	<input type="text"/>
Key Name ?	<input type="text"/>
Manages keys for ?	-- Choose One -- ▾
Port ?	<input type="text" value="5696"/>
Hostname ?	<input type="text"/>

+

Cancel

Next

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

Campo	Descripción
Nombre de visualización DE KMS	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.

Campo	Descripción
Nombre de la clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres.
Administra claves para	<p>El sitio StorageGRID que se asociará a este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS.</p> <ul style="list-style-type: none"> • Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos 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. <p>Nota: se producirá Un error de validación al guardar la configuración de KMS si selecciona un sitio que anteriormente estaba cifrado por el KMS predeterminado pero no proporciona la versión actual de la clave de cifrado original al nuevo KMS.</p>
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.
Nombre del host	<p>El nombre de dominio completo o la dirección IP del KMS.</p> <p>Nota: el campo SAN del certificado de servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.</p>

4. Si va a utilizar un clúster de KMS, seleccione el signo más **+** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **Siguiente**.

Paso 2: Cargar certificado de servidor

En el paso 2 (cargar certificado de servidor) del asistente Agregar un servidor de gestión de claves, carga el certificado de servidor (o el paquete de certificados) para el KMS. El certificado de servidor permite que el

KMS externo se autentique en StorageGRID.

Pasos

- 1. Desde **Paso 2 (cargar certificado de servidor)**, vaya a la ubicación del certificado de servidor o del paquete de certificados guardados.

Add a Key Management Server

1

Enter KMS
Details

2

Upload
Server
Certificate

3

Upload Client
Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ?

Browse

Cancel

Back

Next

- 2. Cargue el archivo de certificado.

Se muestran los metadatos del certificado del servidor.

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ

Browse

k170vCA.pem

Server Certificate Metadata

Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79

Cancel

Back

Next



Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en la pestaña correspondiente.

3. Seleccione **Siguiente**.

Paso 3: Cargar certificados de cliente

En el paso 3 (cargar certificados de cliente) del asistente Agregar un servidor de gestión de claves, carga el certificado de cliente y la clave privada del certificado de cliente. El certificado de cliente permite que StorageGRID se autentique en el KMS.

Pasos

1. Desde **Paso 3 (cargar certificados de cliente)**, vaya a la ubicación del certificado de cliente.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

Client Certificate Private Key ?

Browse

Cancel

Back

Save

2. Cargue el archivo de certificado de cliente.

Aparecen los metadatos del certificado de cliente.

3. Busque la ubicación de la clave privada del certificado de cliente.

4. Cargue el archivo de clave privada.

Aparecen los metadatos del certificado de cliente y la clave privada del certificado de cliente.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Cancel

Back

Save

5. Seleccione **Guardar**.

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



Inmediatamente después de añadir un KMS, el estado del certificado en la página servidor de gestión de claves aparece como Desconocido. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar el navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Guardar**, revise los detalles del mensaje y seleccione **Aceptar**.

Por ejemplo, puede recibir un error 422: Entidad no procesable si se produjo un error en una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Force Save**.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



Al seleccionar **Force Save**, 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 de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los 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.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

Ver detalles de KMS

Puede ver información sobre cada servidor de gestión de claves (KMS) del sistema StorageGRID, incluidos el estado actual de los certificados de servidor y de cliente.

Pasos

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

Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra cualquier servidor de gestión de claves configurado.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Revise la información de la tabla de cada KMS.

Campo	Descripción
Nombre de visualización DE KMS	Nombre descriptivo del KMS.
Nombre de la clave	El alias clave del cliente StorageGRID en el KMS.

Campo	Descripción
Administra claves para	<p>El sitio StorageGRID asociado con el KMS.</p> <p>Este campo muestra el nombre de un sitio StorageGRID específico o Sitios no administrados por otro KMS (KMS predeterminado).</p>
Nombre del hostl	<p>El nombre de dominio completo o la dirección IP del KMS.</p> <p>Si existe un clúster de dos servidores de gestión de claves, se muestran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de gestión de claves en un clúster, el nombre de dominio completo o la dirección IP del primer KMS se enumeran junto con la cantidad de servidores de gestión de claves adicionales en el clúster.</p> <p>Por ejemplo: 10.10.10.10 and 10.10.10.11 o. 10.10.10.10 and 2 others.</p> <p>Para ver todos los nombres de host de un clúster, seleccione un KMS y, a continuación, seleccione Editar.</p>
Estado del certificado	<p>Estado actual del certificado de servidor, del certificado de CA opcional y del certificado de cliente: Válido, caducado, casi expirado o desconocido.</p> <p>Nota: puede que StorageGRID tarde hasta 30 minutos en obtener actualizaciones del estado del certificado. Debe actualizar el navegador web para ver los valores actuales.</p>

- Si el estado de certificado es desconocido, espere hasta 30 minutos y, a continuación, actualice el explorador web.



Inmediatamente después de añadir un KMS, el estado del certificado en la página servidor de gestión de claves aparece como Desconocido. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar el explorador web para ver el estado real.

- Si la columna Estado del certificado indica que un certificado ha caducado o está a punto de expirar, envíe el Lo antes posible. del problema.

Consulte las acciones recomendadas para las alertas **KMS CA de vencimiento**, **KMS de vencimiento del certificado de cliente*** y **KMS de vencimiento del certificado de servidor*** en las instrucciones para [Supervisión y solución de problemas de StorageGRID](#).



Debe solucionar cualquier problema con los certificados Lo antes posible. para mantener el acceso a los datos.

Vea los nodos cifrados

Puede ver información acerca de los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

Pasos

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

Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra todos los servidores de gestión de claves que se configuraron.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. En la parte superior de la página, seleccione la ficha **nodos cifrados**.

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details


Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

La ficha nodos cifrados muestra los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name ?	Key UID ?	Status ?
SGA-010-096-104-67 	Storage Node	Data Center 1	Default KMS	41b0...5c57	 Connected to KMS (2021-03-12 10:59:32 MST)

3. Revise la información de la tabla de cada nodo del dispositivo.

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, administrador o puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde se instala el nodo.
Nombre de visualización DE KMS	<p>Nombre descriptivo del KMS utilizado para el nodo.</p> <p>Si no aparece ningún KMS, seleccione la ficha Detalles de configuración para agregar un KMS.</p> <p>Añadir un servidor de gestión de claves (KMS)</p>
UID de clave	<p>El ID único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, pase el cursor por la celda.</p> <p>Un guión (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo y el KMS.</p>
Estado	<p>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 que cambie la configuración de KMS.</p> <p>Nota: debe actualizar el explorador Web para ver los nuevos valores.</p>

4. Si la columna Estado indica un problema de KMS, resuelva el problema inmediatamente.

Durante las operaciones normales de KMS, el estado será **conectado a KMS**. Si un nodo está desconectado de la cuadrícula, se muestra el estado de conexión del nodo (administrativamente abajo o Desconocido).

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

- No se ha podido cargar la configuración DE KMS

- Error de conectividad DE KMS
- No se ha encontrado el nombre de la clave de cifrado DE KMS
- Error en la rotación de la clave de cifrado DE KMS
- LA clave KMS no pudo descifrar el volumen de un dispositivo
- KMS no está configurado

Consulte las acciones recomendadas para estas alertas en las instrucciones de [Supervisión y solución de problemas de StorageGRID](#).



Debe solucionar cualquier problema inmediatamente para garantizar que los datos están totalmente protegidos.

Editar un servidor de gestión de claves (KMS)

Es posible que deba editar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de expirar.

Lo que necesitará

- Ha revisado el [consideraciones y requisitos para usar un servidor de gestión de claves](#).
- 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](#).
- Tiene el permiso acceso raíz.

Pasos

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

Aparece la página servidor de gestión de claves para mostrar todos los servidores de gestión de claves configurados.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details **Encrypted Nodes**

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:


- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

<div> + Create Edit Remove </div>				
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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

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

Campo	Descripción
Nombre de visualización DE KMS	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	<p>El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres.</p> <p>Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de 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.</p> <div>  <p>Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS. En su lugar, gire la clave actualizando la versión de la clave en el software KMS. StorageGRID requiere que se pueda acceder a todas las versiones de claves usadas anteriormente (así como a las futuras) desde el KMS con el mismo alias de clave. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.</p> <p>Consideraciones y requisitos para usar un servidor de gestión de claves</p> </div>
Administra claves para	<p>Si va a editar un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione Sitios no administrados por otro KMS (KMS predeterminado). Esta selección convierte un KMS específico del sitio al KMS predeterminado, que se aplicará a todos los sitios que no tienen un KMS dedicado y a cualquier sitio agregado en una expansión.</p> <p>Nota: Si está editando un KMS específico del sitio, no puede seleccionar otro sitio. Si va a editar el KMS predeterminado, no puede seleccionar un sitio específico.</p>
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.
Nombre del host	<p>El nombre de dominio completo o la dirección IP del KMS.</p> <p>Nota: el campo SAN del certificado de servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.</p>

- Si va a configurar un clúster KMS, seleccione el signo más **+** para agregar un nombre de host para cada servidor del clúster.
- Seleccione **Siguiente**.

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

6. Si necesita sustituir el certificado del servidor, seleccione **examinar** y cargue el nuevo archivo.
7. Seleccione **Siguiente**.

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

8. Si necesita sustituir el certificado de cliente y la clave privada del certificado de cliente, seleccione **examinar** y cargue los nuevos archivos.
9. Seleccione **Guardar**.

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

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

Por ejemplo, puede recibir un error 422: Entidad no procesable si el sitio seleccionado para este KMS ya está administrado por otro KMS o si se produjo un error en una prueba de conexión.

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



Al seleccionar **Force Save**, 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 de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los 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.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

Quitar un servidor de gestión de claves (KMS)

En algunos casos, es posible quitar un servidor de gestión de claves. Por ejemplo, puede que desee quitar un KMS específico de un sitio si ha retirado del servicio el sitio.

Lo que necesitará

- Ha revisado el [consideraciones y requisitos para usar un servidor de gestión de claves](#).
- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tiene el permiso acceso raíz.

Acerca de esta tarea

Puede eliminar un KMS en los siguientes casos:

- Puede eliminar un KMS específico de un sitio si se ha dado de baja o si el sitio incluye ningún nodo de dispositivo con cifrado de nodo activado.
- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tiene nodos de dispositivo con cifrado de nodo activado.

Pasos

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

Aparece la página servidor de gestión de claves para mostrar todos los servidores de gestión de claves configurados.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

<div>+ Create Edit Remove</div>				
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Seleccione el botón de opción del KMS que desea quitar y seleccione **Quitar**.
3. Revise las consideraciones en el cuadro de diálogo de advertencia.

⚠ Warning

Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. Seleccione **OK**.

La configuración de KMS se elimina.

Administrar la configuración de proxy

Configure las opciones de proxy de almacenamiento

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

Lo que necesitará

- Tiene permisos de acceso específicos.
- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).

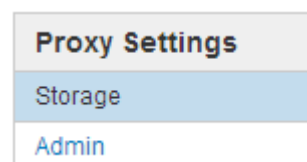
Acerca de esta tarea

Puede configurar los ajustes de un único proxy de almacenamiento.

Pasos

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

Se muestra la página Storage Proxy Settings. De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.



2. Active la casilla de verificación **Activar proxy de almacenamiento**.

Aparecen los campos para configurar un proxy de almacenamiento.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy ☒

Protocol ☒ HTTP ☐ SOCKS5

Hostname

Port (optional)

3. Seleccione el protocolo del proxy de almacenamiento no transparente.

4. Introduzca el nombre de host o la dirección IP del servidor proxy.

5. De manera opcional, introduzca el puerto utilizado para conectarse al servidor proxy.

Puede dejar este campo en blanco si utiliza 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 extremos para los servicios de plataforma o Cloud Storage Pools.



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

7. Compruebe la configuración del servidor proxy para asegurarse de que los mensajes de StorageGRID relacionados con el servicio de la plataforma no se bloqueen.

Después de terminar

Si necesita desactivar un proxy de almacenamiento, anule la selección de la casilla de verificación **Activar proxy de almacenamiento** y seleccione **Guardar**.

Información relacionada

- [Red y puertos para servicios de plataforma](#)
- [Gestión de objetos con ILM](#)

Configure los ajustes del proxy de administración

Si envía mensajes de AutoSupport con HTTP o HTTPS (consulte [Configure AutoSupport](#)), puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Lo que necesitará

- Tiene permisos de acceso específicos.
- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).

Acerca de esta tarea

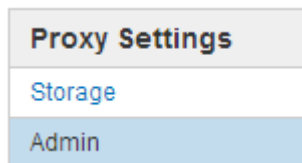
Puede configurar los ajustes de un único proxy de administración.

Pasos

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

Aparece la página Admin Proxy Settings (Configuración del proxy de administración). De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. En el menú de la barra lateral, seleccione **Admin**.



3. Active la casilla de verificación **Activar proxy de administración**.

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy ☒

Hostname

Port

Username (optional)

Password (optional)

4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Si lo desea, introduzca el nombre de usuario del proxy.

Deje este campo en blanco si el servidor proxy no requiere un nombre de usuario.

7. De forma opcional, introduzca la contraseña del proxy.

Deje este campo en blanco si el servidor proxy no requiere una contraseña.

8. Seleccione **Guardar**.

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



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

9. Si necesita desactivar el proxy, anule la selección de la casilla de verificación **Activar proxy de administración** y seleccione **Guardar**.

Administrar redes de clientes que no son de confianza

Administrar redes de clientes que no son de confianza: Descripción general

Si está utilizando una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles aceptando tráfico de cliente entrante sólo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente de cada nodo de cuadrícula es *Trusted*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de cuadrícula en todos los puertos externos disponibles (consulte la información acerca de las comunicaciones externas en [Directrices sobre redes](#)).

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red cliente de cada nodo sea *no confiable*. Si la red de cliente de un nodo no es de confianza, el nodo sólo acepta conexiones entrantes en los puertos configurados explícitamente como puntos finales de equilibrador de carga. Consulte [Configurar puntos finales del equilibrador de carga](#).

Ejemplo 1: Gateway Node solo acepta solicitudes HTTPS S3

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

1. En la página Load Balancer Endpoints, configure un extremo de equilibrador de carga para S3 a través de HTTPS en el puerto 443.
2. En la página redes de cliente no fiables, especifique que la red de cliente del nodo de puerta de enlace no sea de confianza.

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

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

Supongamos que desea habilitar el tráfico saliente del servicio de la plataforma S3 desde un nodo de almacenamiento, pero desea impedir las conexiones entrantes a ese nodo de almacenamiento en la red cliente. Debe realizar este paso general:

- En la página redes de cliente no fiables, indique que la red de clientes del nodo de almacenamiento no es de confianza.

Después de guardar la configuración, el nodo de almacenamiento ya no acepta ningún tráfico entrante en la red cliente, pero continúa permitiendo solicitudes salientes a Amazon Web Services.

Especifique que la red de cliente del nodo no es de confianza

Si utiliza una red de cliente, puede especificar si la red de cliente de cada nodo es de

confianza o no es de confianza. También puede especificar la configuración predeterminada para los nuevos nodos agregados en una ampliación.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tiene el permiso acceso raíz.
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante sólo en puntos finales configurados explícitamente, ha definido los puntos finales del equilibrador de carga.



Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > redes de cliente no fiables**.

En la página redes de cliente no fiables se enumeran todos los nodos del sistema StorageGRID. La columna motivo no disponible incluye una entrada si la red de cliente del nodo debe ser de confianza.

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network

Default

☒ Trusted

☐ Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

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.
 - **Trusted:** Cuando se agrega un nodo en una expansión, su red de cliente es de confianza.

- **No fiable:** Cuando se agrega un nodo en una expansión, su red cliente no es de confianza. Según sea necesario, puede volver a esta página para cambiar la configuración de un nuevo nodo concreto.



Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

3. En la sección **Seleccionar nodos de red de cliente no confiable**, seleccione los nodos que deben permitir conexiones de cliente sólo en puntos finales de equilibrador de carga configurados explícitamente.

Puede seleccionar o anular la selección de la casilla de comprobación en el título para seleccionar o anular la selección de todos los nodos.

4. Seleccione **Guardar**.

Las nuevas reglas de firewall se agregan y aplican inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.