



# **Configuración de servidores de gestión de claves**

## **StorageGRID**

NetApp  
April 10, 2024

# Tabla de contenidos

- Configuración de servidores de gestión de claves. . . . . 1
  - Configurar servidores de gestión de claves: Descripción general . . . . . 1
  - Consulte los métodos de cifrado de StorageGRID . . . . . 1
  - Información general de la configuración de KMS y dispositivos . . . . . 4
  - Consideraciones y requisitos para usar un servidor de gestión de claves . . . . . 7
  - Consideraciones para cambiar el KMS de un sitio . . . . . 10
  - Configure StorageGRID como cliente en KMS . . . . . 13
  - Añadir un servidor de gestión de claves (KMS). . . . . 14
  - Ver detalles de KMS. . . . . 22
  - Vea los nodos cifrados . . . . . 24
  - Editar un servidor de gestión de claves (KMS) . . . . . 26
  - Quitar un servidor de gestión de claves (KMS) . . . . . 29

# 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 ( <b>CONFIGURACIÓN &gt; Seguridad &gt; servidor de administración de claves</b> ) 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 <b>cifrado de nodos</b> 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"> <li>• <a href="#">Dispositivos de almacenamiento SG6000</a></li> <li>• <a href="#">Dispositivos de almacenamiento SG5700</a></li> <li>• <a href="#">Dispositivos de almacenamiento SG5600</a></li> </ul>
Opción de cuadrícula de cifrado de objetos almacenados	La opción <b>cifrado de objetos almacenados</b> se puede activar en Grid Manager ( <b>CONFIGURACIÓN &gt; sistema &gt; Opciones de cuadrícula</b> ). 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"> <li>• <a href="#">Configurar el cifrado de objetos almacenados</a></li> </ul>

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"> <li>• <a href="#">Use S3</a></li> </ul>
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"> <li>• <a href="#">Use S3</a></li> </ul>
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"> <li>• x-amz-server-side-encryption-customer-algorithm</li> <li>• x-amz-server-side-encryption-customer-key</li> <li>• x-amz-server-side-encryption-customer-key-MD5</li> </ul>	<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"> <li>• <a href="#">Use S3</a></li> </ul>
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"> <li>• <a href="#">"Amazon simple Storage Service - Guía para desarrolladores: Protección de datos mediante cifrado en el cliente"</a></li> </ul>

## Utilice varios métodos de cifrado

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

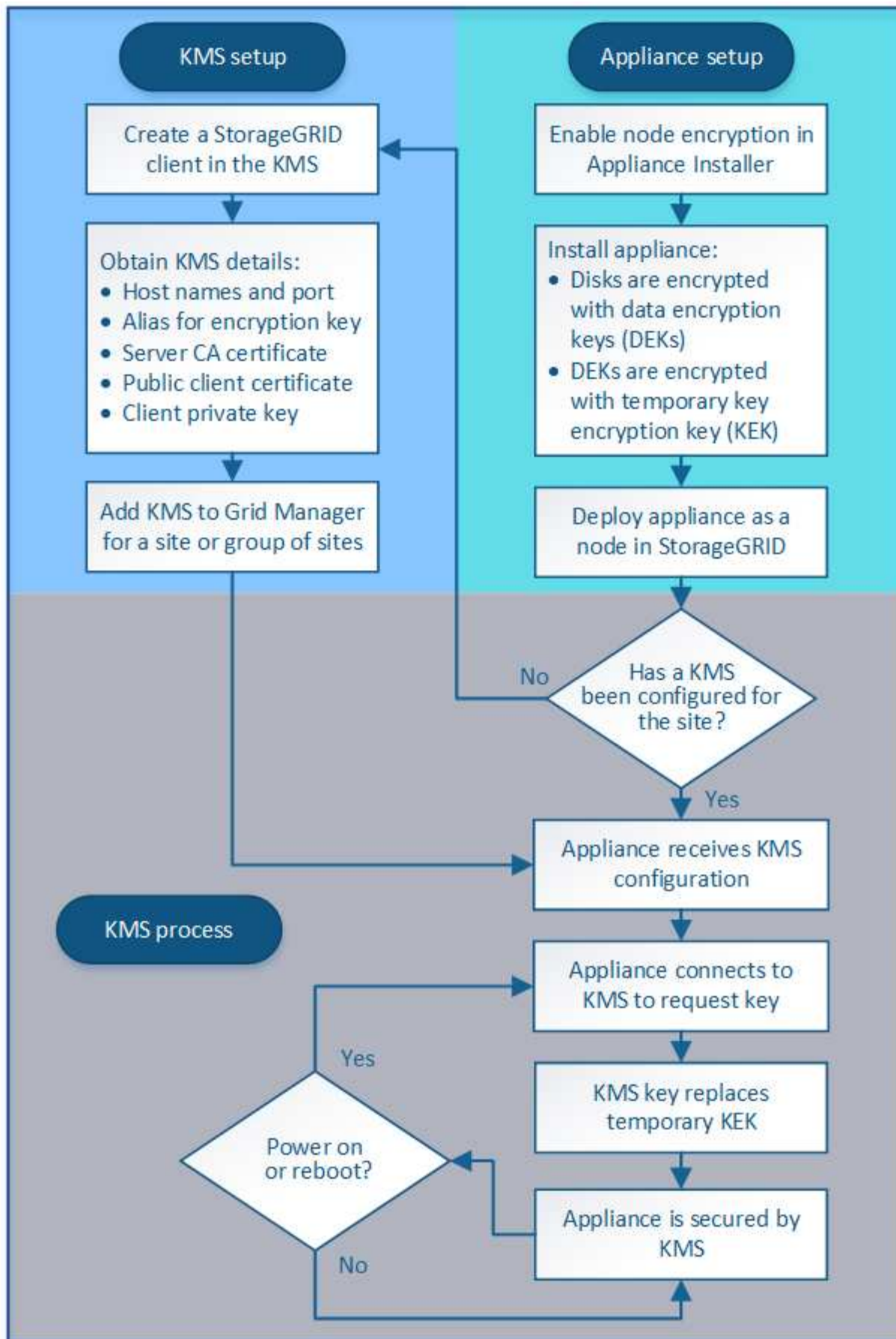
- Puede utilizar un KMS para proteger los nodos de dispositivos y también para usar la función de seguridad de unidades de System Manager de SANtricity a fin de «doble cifrado» de datos de las unidades de autocifrado de los mismos dispositivos.
- Puede usar un KMS para proteger los datos en los nodos 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.	<a href="#">Configure StorageGRID como cliente en KMS</a>
Obtenga la información necesaria para el cliente StorageGRID en el KMS.	<a href="#">Configure StorageGRID como cliente en KMS</a>
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.	<a href="#">Añadir un servidor de gestión de claves (KMS)</a>

## 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.

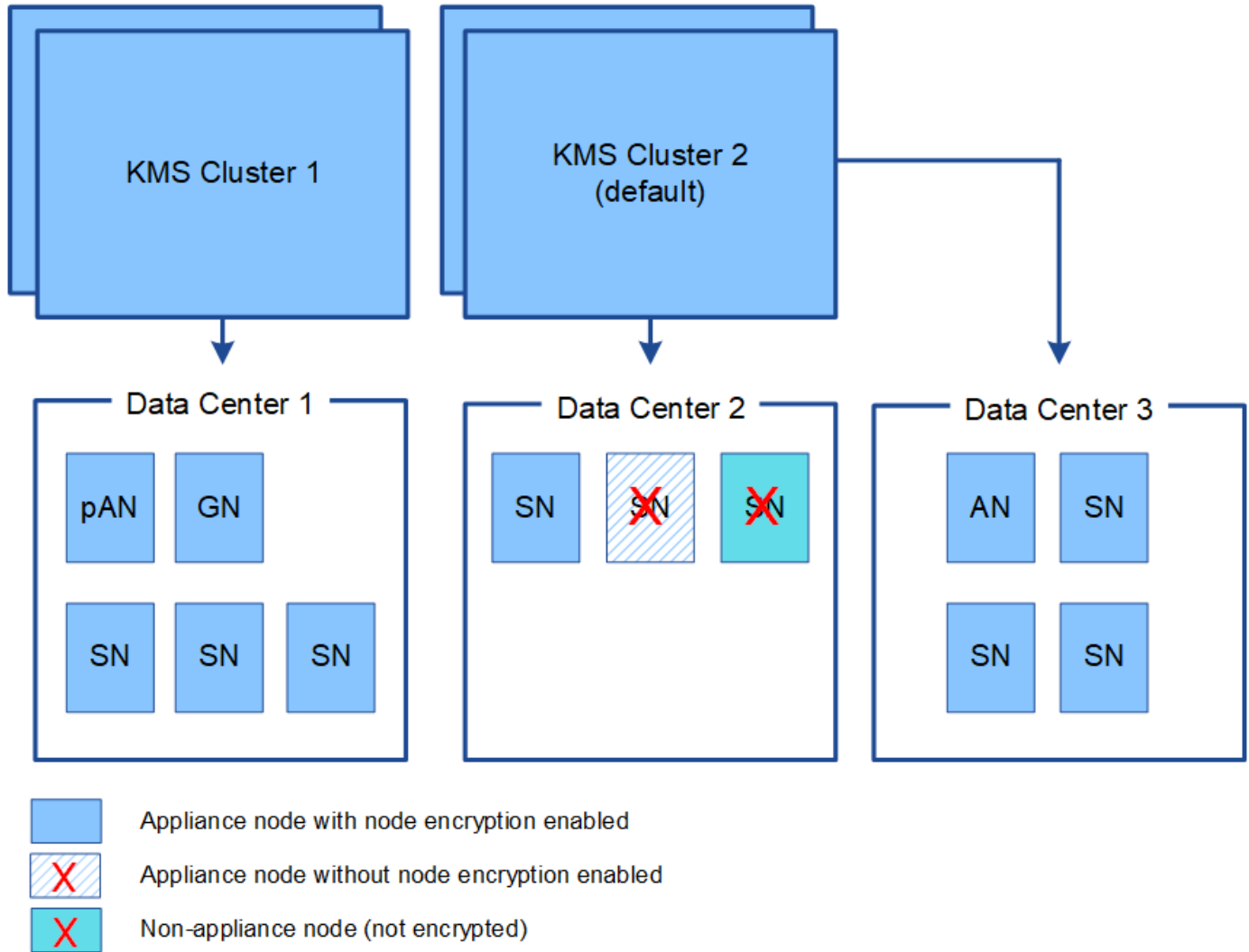
## ¿Cuántos servidores de gestión de claves necesito?

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

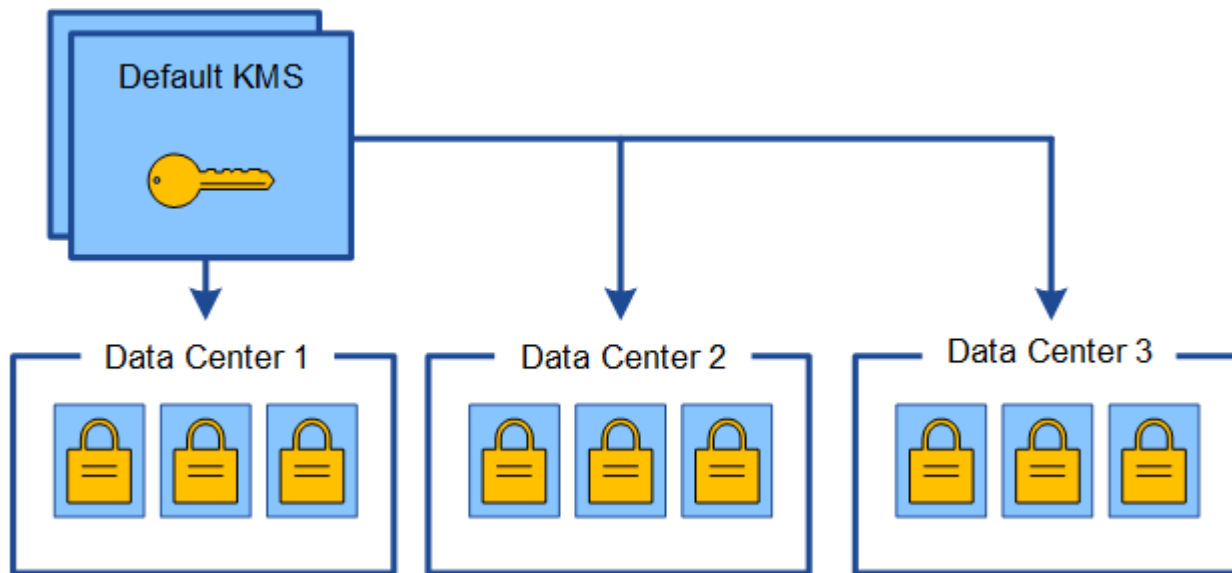
Cada servidor de gestión de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos de dispositivos en un único sitio o en un grupo de sitios. Si necesita cambiar qué KMS se utiliza para un sitio, es posible que necesite copiar la clave de cifrado de un KMS a otro.

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.

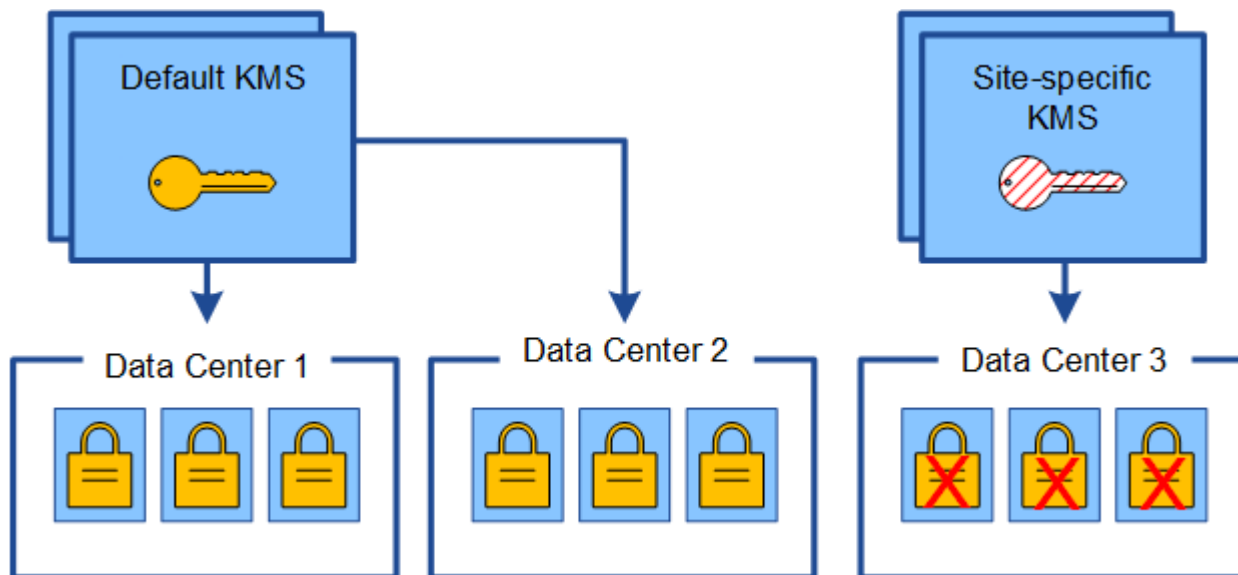
Por ejemplo:

1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.

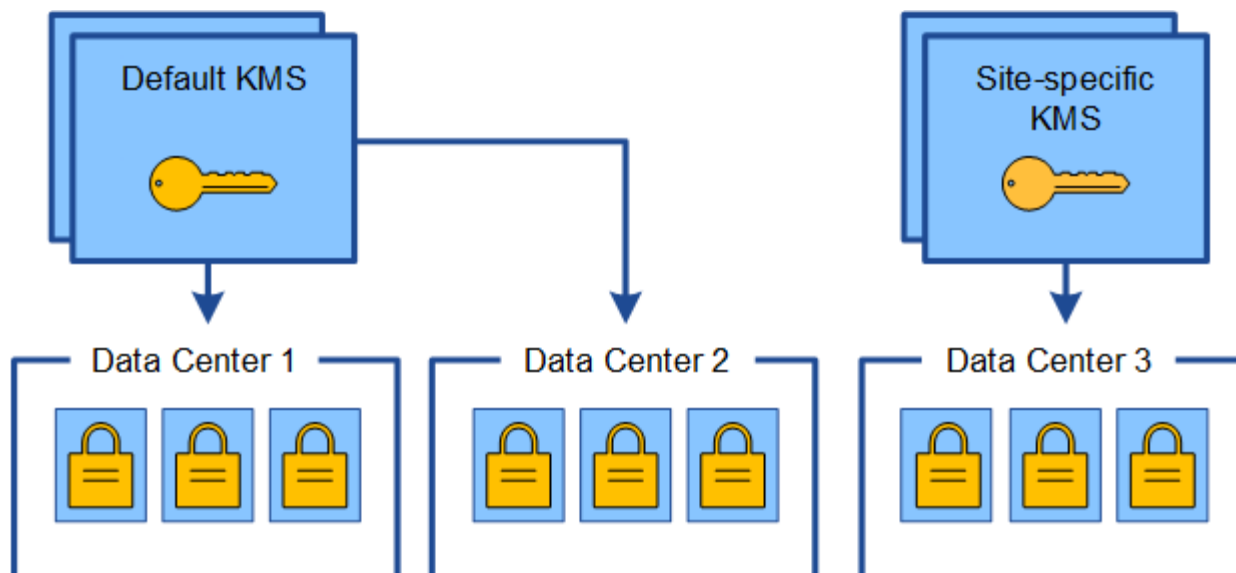
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar esos dispositivos.



3. 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.



4. 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 <b>administra claves para</b>, seleccione <b>Sitios no administrados por otro KMS (KMS predeterminado)</b>. El KMS específico del sitio se utilizará ahora como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado.</p> <p><a href="#">Editar un servidor de gestión de claves (KMS)</a></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"> <li>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.</li> <li>2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio.</li> </ol> <p><a href="#">Añadir un servidor de gestión de claves (KMS)</a></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"> <li>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.</li> <li>2. Con el Administrador de cuadrícula, edite la configuración de KMS existente e introduzca el nuevo nombre de host o la dirección IP.</li> </ol> <p><a href="#">Añadir un servidor de gestión de claves (KMS)</a></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"> <li>• Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos en un sitio específico.</li> <li>• Seleccione <b>Sitios no administrados por otro KMS (KMS predeterminado)</b> 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.</li> </ul> <p><b>Nota:</b> 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><b>Nota:</b> 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 <b>Sitios no administrados por otro KMS (KMS predeterminado)</b>.</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 <b>Editar</b>.</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><b>Nota:</b> 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](#).

<a href="#">+ Create</a>	<a href="#">Edit</a>	<a href="#">Remove</a>			
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. 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><a href="#">Añadir un servidor de gestión de claves (KMS)</a></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><b>Nota:</b> 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> <span>+ Create</span> <span>Edit</span> <span>Remove</span> </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**.

3. 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><a href="#">Consideraciones y requisitos para usar un servidor de gestión de claves</a></p> </div>
Administra claves para	<p>Si va a editar un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione <b>Sitios no administrados por otro KMS (KMS predeterminado)</b>. 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><b>Nota:</b> 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><b>Nota:</b> 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 configurar un clúster KMS, seleccione el signo más **+** para agregar un nombre de host para cada servidor del clúster.
5. 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](#).

<a href="#">+ Create</a>	<a href="#">✎ Edit</a>	<a href="#">🗑 Remove</a>			
KMS Display Name <a href="#">?</a>	Key Name <a href="#">?</a>	Manages keys for <a href="#">?</a>	Hostname <a href="#">?</a>	Certificate Status <a href="#">?</a>	
<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.



## 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 INTERRUPTIÓN 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.