Configuración de servidores de gestión de claves

StorageGRID 11.7

NetApp
April 12, 2024

Tabla de contenidos

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).

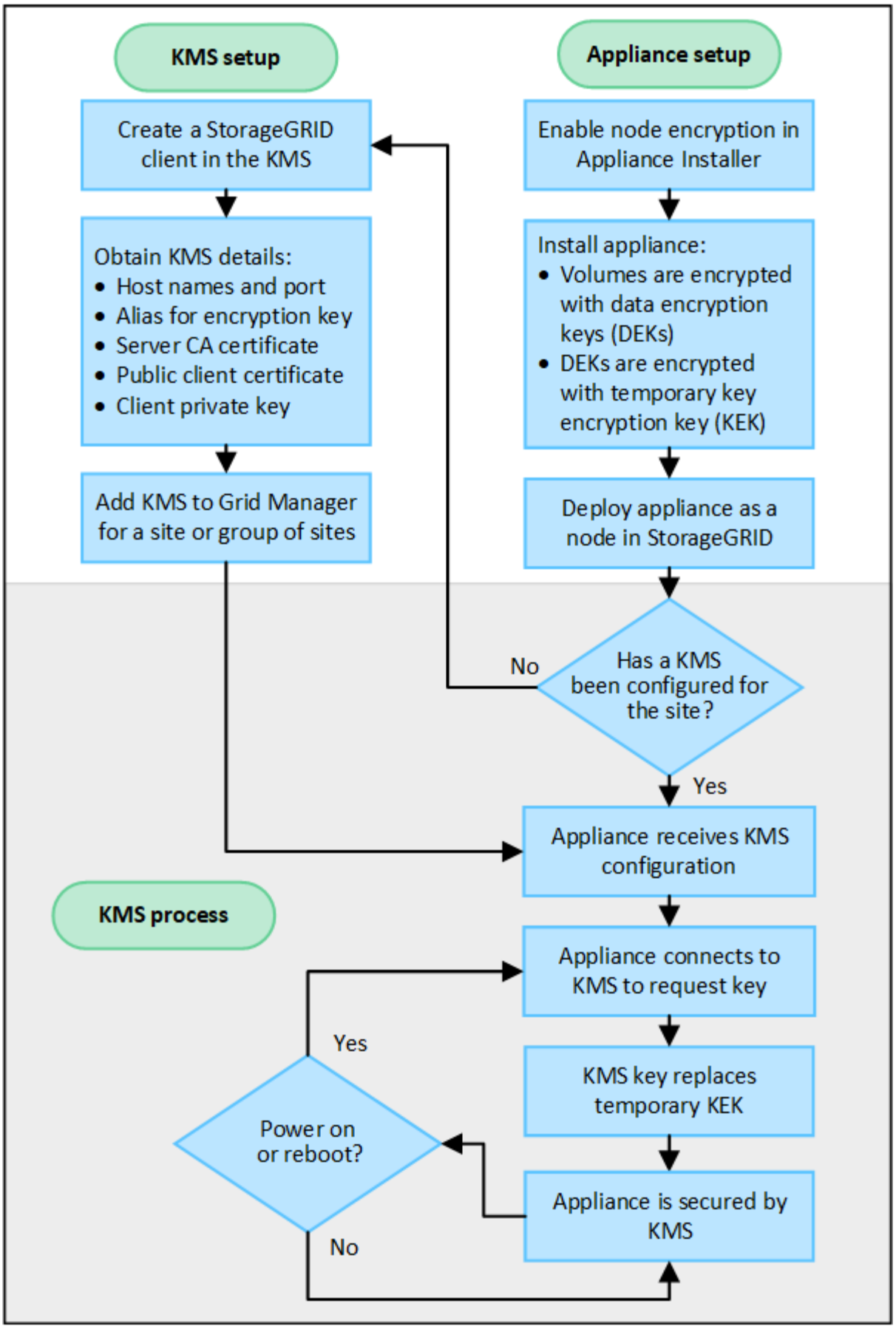
Puede utilizar uno o varios servidores de gestión de claves para administrar las claves de cifrado de nodos para los nodos de dispositivo StorageGRID que tengan activada la configuración * cifrado de nodos* durante la instalación. El uso de servidores de gestión de claves con estos nodos de dispositivos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

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 habilitar la configuración **Node Encryption** después de agregar un dispositivo a la cuadrícula, y no puede usar 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 mediante el cifrado de disco de Linux Unified Key Setup (LUKS) en el SO 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.

Consulte "Habilite el cifrado del nodo" para obtener más detalles.

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

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

1. 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 encriptado 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 clave, 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 comunique 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 nodo después de añadir un dispositivo al grid, y no se puede usar la gestión de claves externa para dispositivos que no tienen el cifrado de nodo habilitado.

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

No puede usar el KMS configurado para nodos basados en software (no en dispositivos), 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.

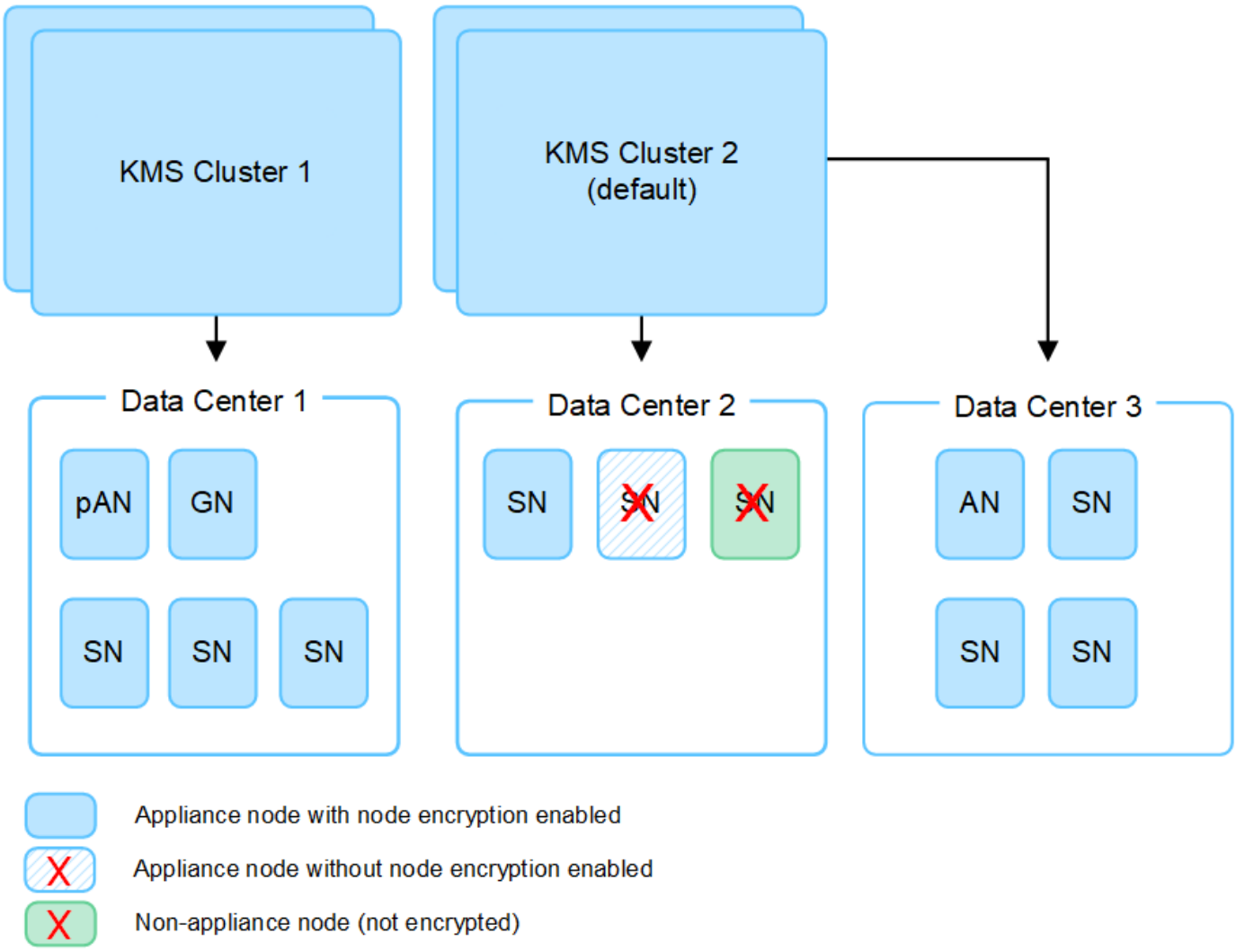
¿Cuántos servidores de gestión de claves necesito?

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 usar un KMS para nodos que no sean del dispositivo ni para ningún nodo del dispositivo que no tenga habilitada la configuración **Node Encryption** 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 **KMS encryption key rotation failed** 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 utilizar el instalador de dispositivos de StorageGRID para "Borre 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.

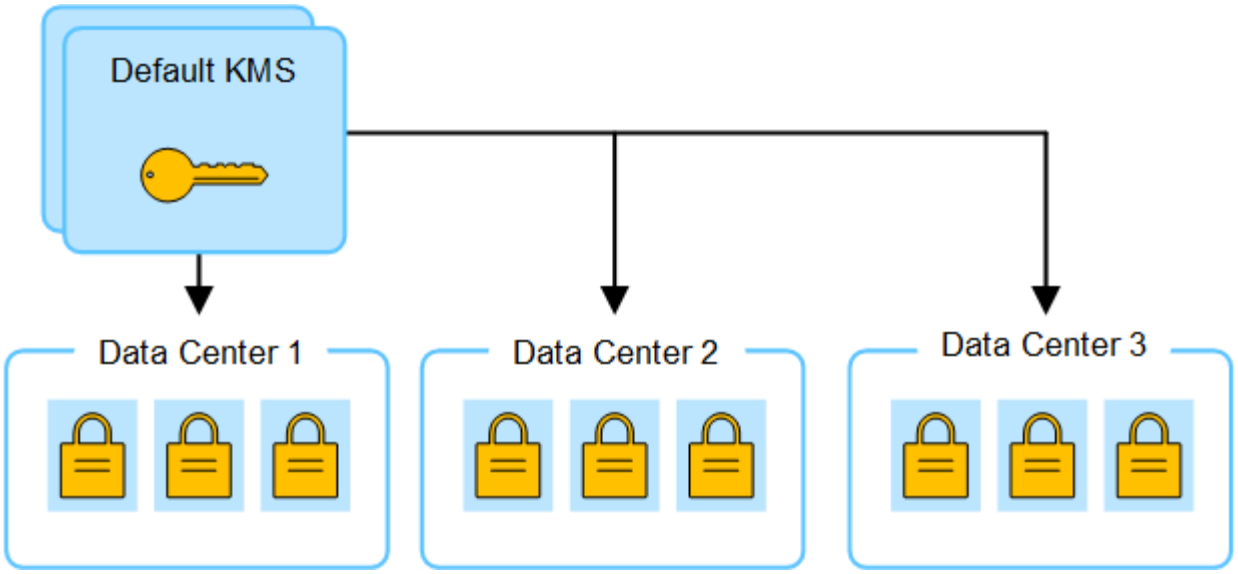
Consideraciones para cambiar el KMS de un sitio

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.

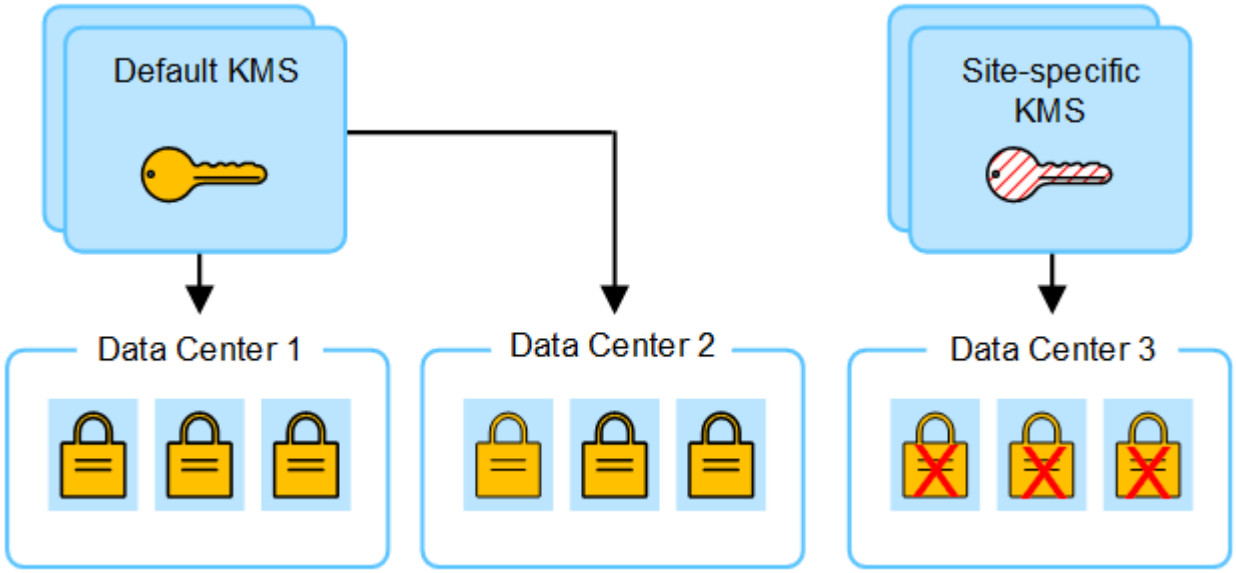
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original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

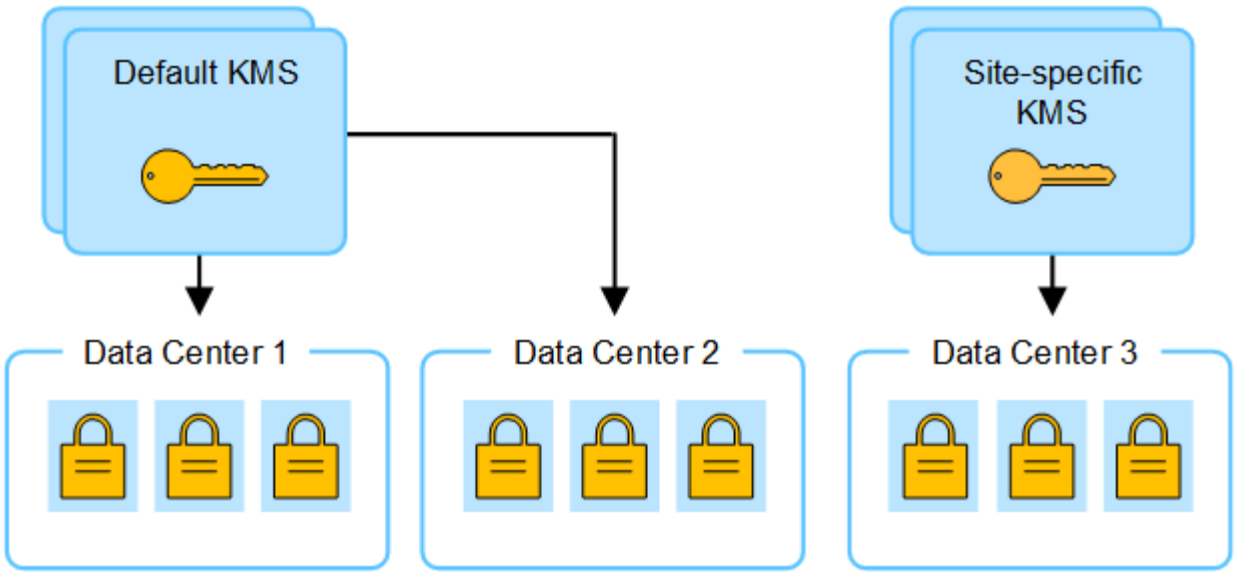
1. Inicialmente configuras un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa 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.	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. "Editar un servidor de gestión de claves (KMS)"
Tiene un KMS predeterminado y agrega un sitio nuevo en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	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. "Añadir un servidor de gestión de claves (KMS)"
Desea que el KMS para un sitio utilice un servidor diferente.	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. "Añadir un servidor de gestión de claves (KMS)"

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. Para obtener una lista de versiones compatibles, utilice "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

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 de 2.048 bits o más, y 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.

Antes de empezar

- 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.

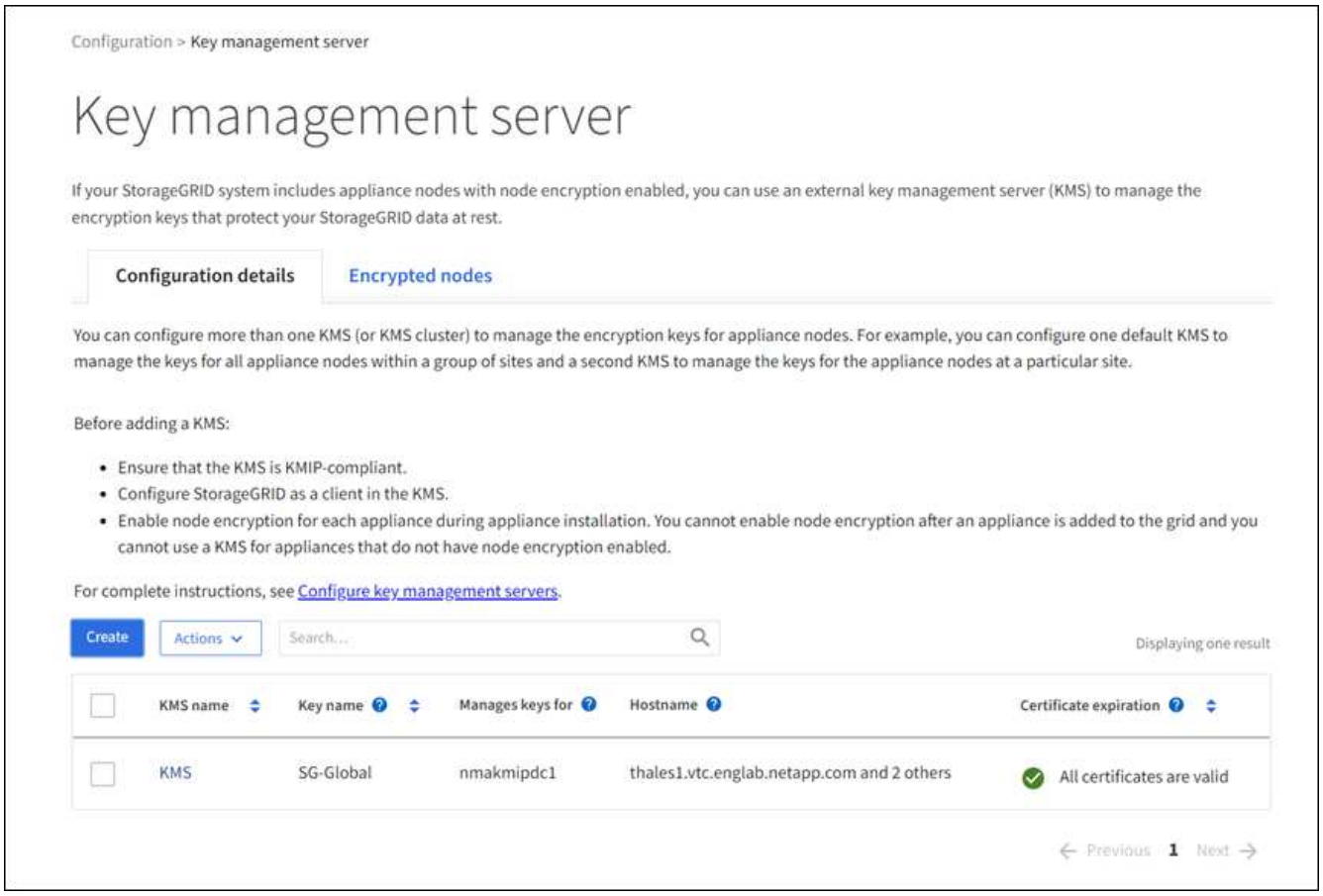
Paso 1: Detalles de KM

En el Paso 1 (detalles de KMS) del Asistente para agregar un servidor de gestión de claves, proporciona detalles sobre el clúster de KMS o KMS.

Pasos

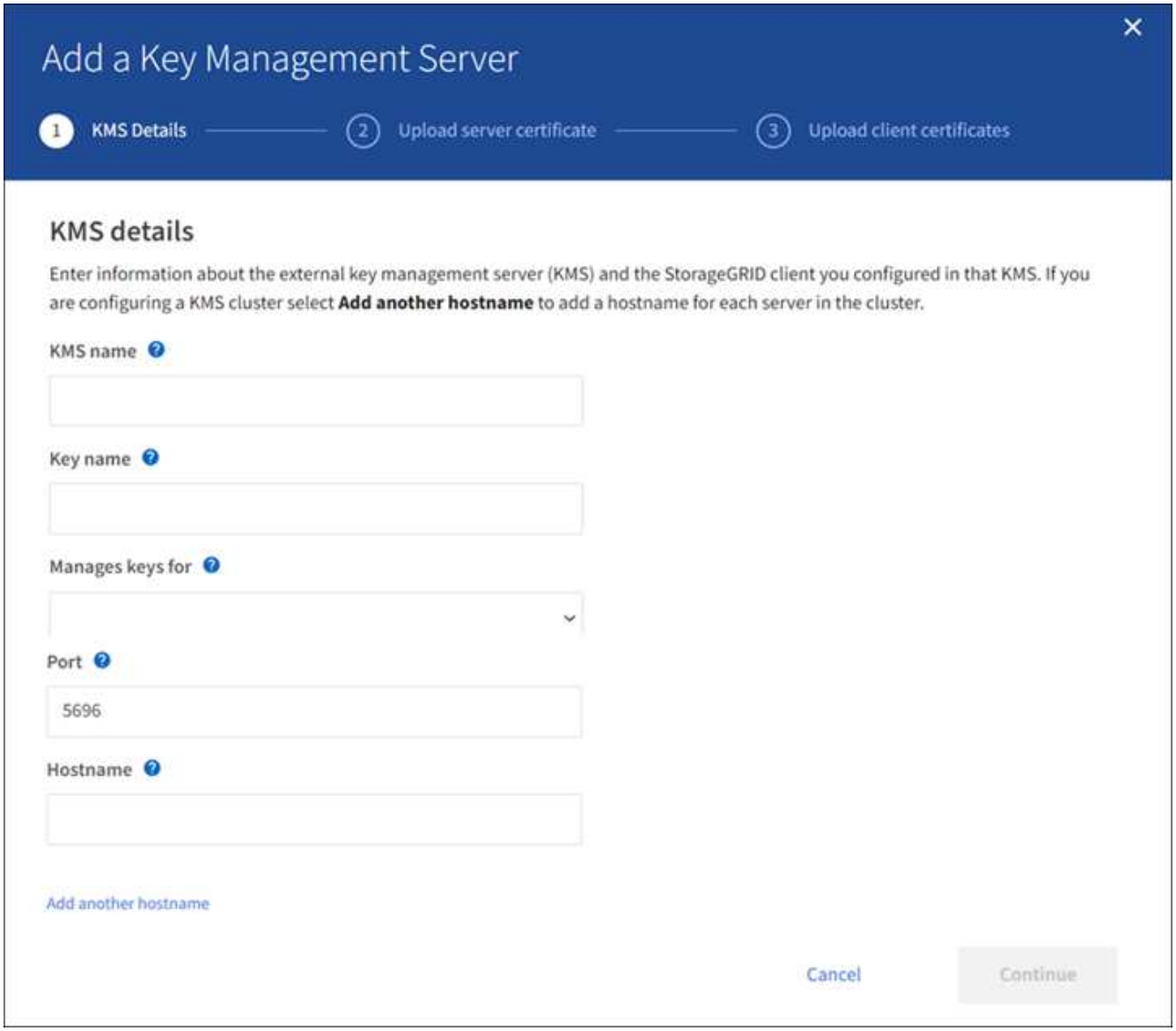
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

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



2. Seleccione **Crear**.

   Paso 1 (detalles de KMS) del asistente Add a Key Management Server.



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

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres.

Campo	Descripción
Administra claves para	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. • Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos en un sitio específico. • Seleccione **Sitios no gestionados por otro KMS (por defecto KMS)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que agregue en expansiones posteriores. **Nota:** se producirá Un error de validación 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.
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 hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del 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.

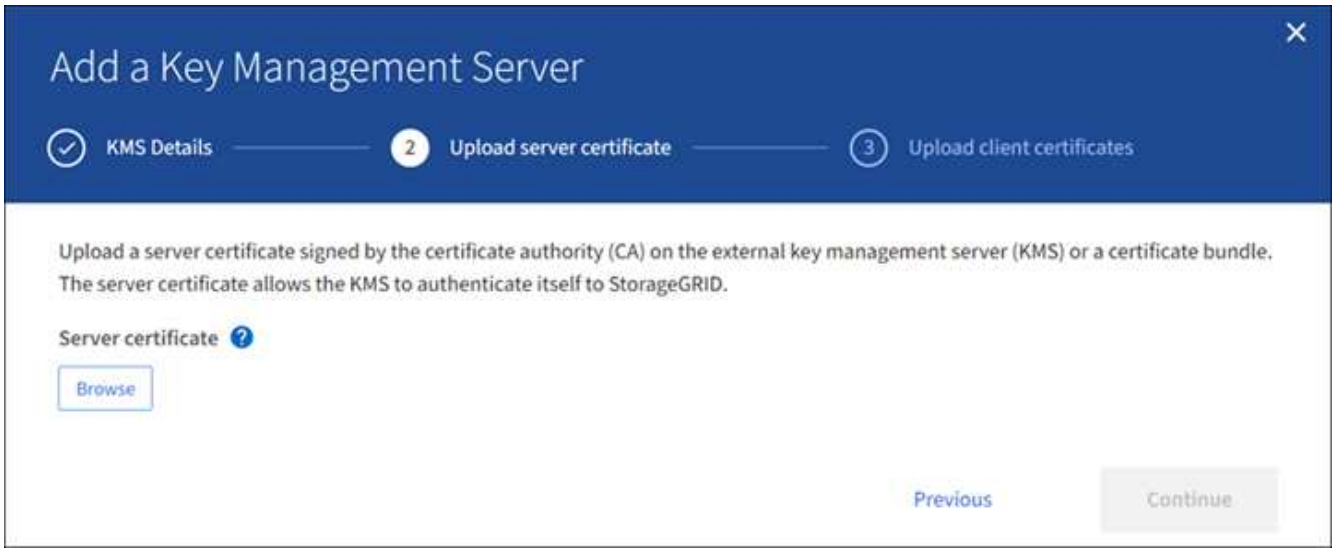
4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

Paso 2: Cargar certificado de servidor

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

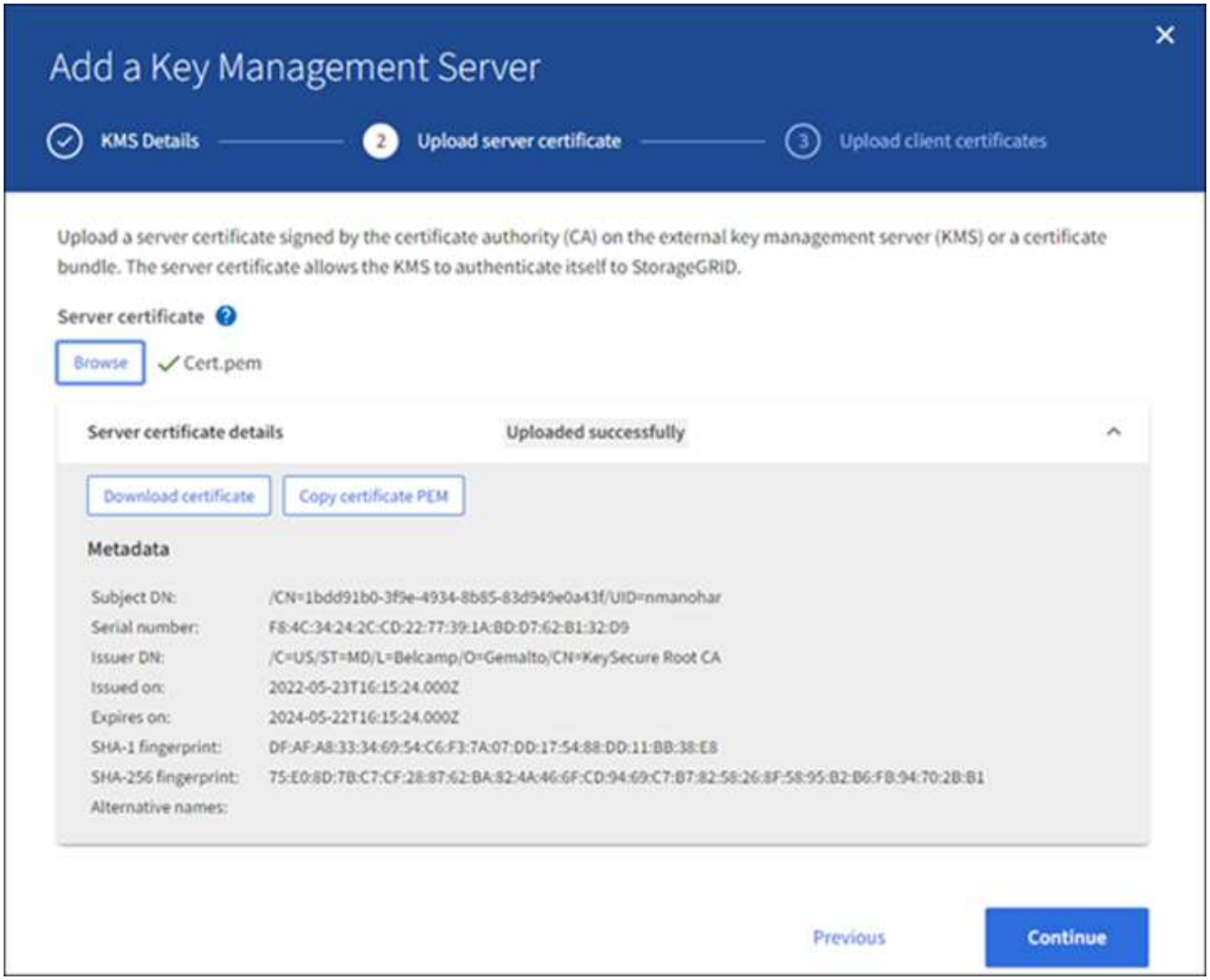
Pasos

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



2. Cargue el archivo de certificado.

   Se muestran los metadatos del certificado del servidor.



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

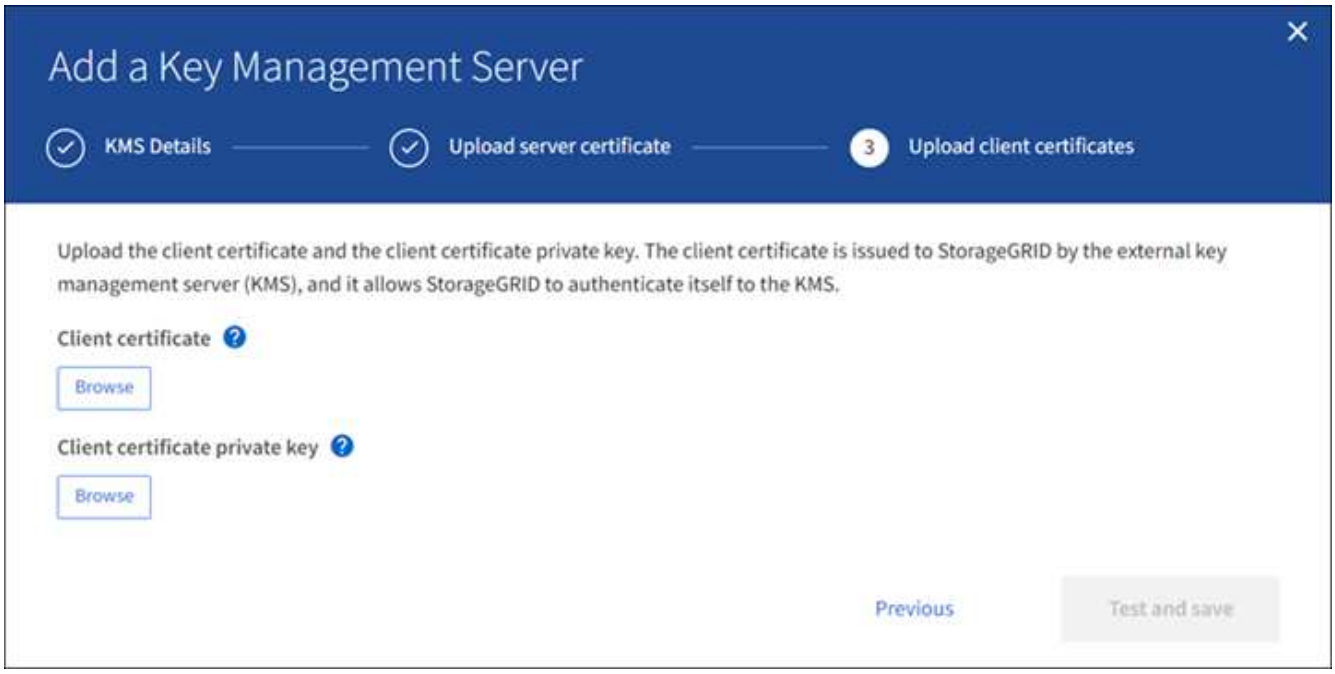
3. Seleccione **continuar**.

Paso 3: Cargar certificados de cliente

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

Pasos

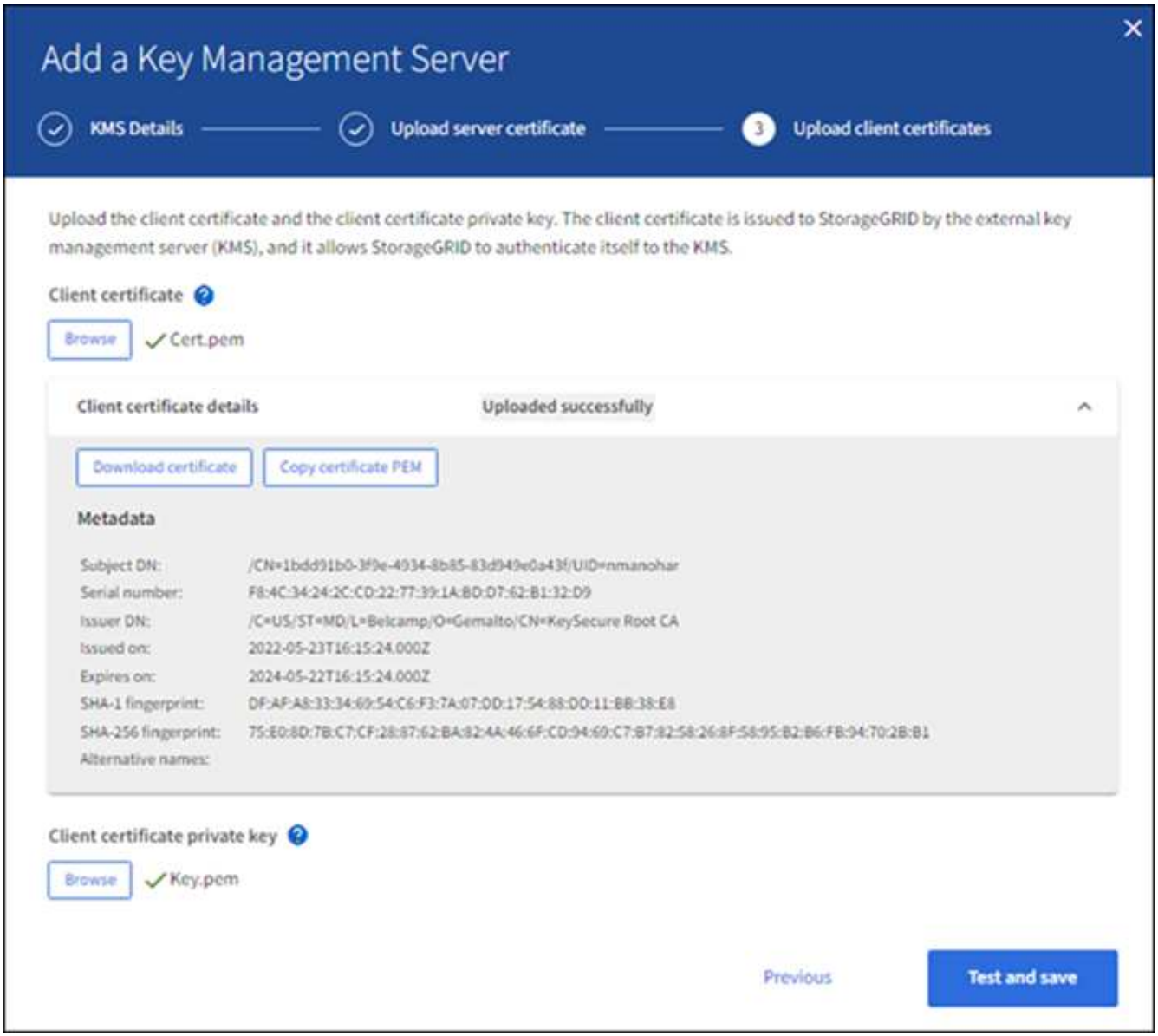
1. Desde **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.



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.



5. Selecciona **Probar y 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 **Probar y guardar**, revise los detalles del mensaje y luego 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 **Forzar guardar**.

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.

   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**.

   Aparece la página del servidor de gestión de claves. La pestaña Detalles de configuración muestra todos los servidores de gestión de claves configurados.

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

Campo	Descripción
Nombre de KM	Nombre descriptivo del KMS.
Nombre de clave	El alias clave del cliente StorageGRID en el KMS.
Administra claves para	El sitio StorageGRID asociado con el KMS. Este campo muestra el nombre de un sitio StorageGRID específico o **Sitios no administrados por otro KMS (KMS predeterminado).**
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. 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. Por ejemplo: `10.10.10.10 and 10.10.10.11` o. `10.10.10.10 and 2 others`. Para ver todos los nombres de host de un clúster, abra un KMS y seleccione **Editar** o **Acciones** > **Editar**.

Campo	Descripción
Caducidad del certificado	Estado actual del certificado de servidor, del certificado de CA opcional y del certificado de cliente: Válido, caducado, casi espirado o desconocido. **Nota:** StorageGRID puede tardar hasta 30 minutos en recibir actualizaciones del vencimiento del certificado. Debe actualizar el navegador web para ver los valores actuales.

3. Si la caducidad del certificado es Desconocido, espere hasta 30 minutos y actualice el explorador web.

> Inmediatamente después de agregar un KMS, el vencimiento 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.

4. Si la columna Caducidad del certificado indica que un certificado ha caducado o está a punto de caducar, solucione el problema lo antes posible.

   Cuando se activan las alertas **KMS CA CERTIFICATION**, **KMS client certificate expiration** y **KMS server certificate expiration**, anote la descripción de cada alerta y realice las acciones recomendadas.

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

5. Para ver los detalles del certificado de este KMS, seleccione el nombre del KMS en la tabla.
6. En la página de resumen de KMS, revise los metadatos y el certificado PEM tanto para el certificado de servidor como para el certificado de cliente. Según sea necesario, seleccione **Editar certificado** para reemplazar un certificado por uno nuevo.

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.

2. En la parte superior de la página, seleccione la pestaña **Nodos encriptados**.

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

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 KM	Nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Añadir un servidor de gestión de claves (KMS)"
UID de clave	El ID único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver una UID de clave completa, coloque el cursor sobre la celda. 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.
Estado	El estado de la conexión entre el KMS y el nodo del dispositivo. Si el nodo está conectado, la Marca de tiempo se actualiza cada 30 minutos. El estado de la conexión puede tardar varios minutos en actualizarse después de que cambie la configuración de KMS. **Nota:** debe actualizar el explorador Web para ver los nuevos valores.

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

   Realice las acciones recomendadas para estas alertas.

   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.

Antes de empezar

- 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**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas editar y selecciona **Acciones** > **Editar**.

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

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

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de 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. 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. "Consideraciones y requisitos para usar un servidor de gestión de claves"

Campo	Descripción
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente **Sitios no gestionados 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. **Nota:** Si está editando un KMS específico del sitio, no puede seleccionar otro sitio. Si está editando el KMS predeterminado, no puede seleccionar un sitio específico.
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 hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del 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.

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

   Paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de gestión de claves.

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

   El paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de gestión de claves aparece.

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

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.

    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.

Antes de empezar

- 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**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas eliminar y selecciona **Acciones** > **Eliminar**.

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

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

La configuración de KMS se elimina.