Configurar servidores de administración de claves

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Configurar servidores de administración de claves

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

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

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

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

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

Configuración de KMS y dispositivos

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

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

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

Configurar el servidor de administración de claves (KMS)

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

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

Configurar el aparato

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

1. Durante la etapa de configuración de hardware de la instalación del dispositivo, utilice el instalador de dispositivos StorageGRID para habilitar la configuración **Cifrado de nodo** para el dispositivo.

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

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

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

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

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

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

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

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

Consideraciones y requisitos para utilizar un servidor de administración de claves

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

¿Qué versión de KMIP es compatible?

StorageGRID es compatible con KMIP versión 1.4.

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

¿Cuáles son las consideraciones de la red?

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

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

¿Qué versiones de TLS son compatibles?

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

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

¿Qué dispositivos son compatibles?

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

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

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

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

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

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

¿Cuándo debo configurar los servidores de administración de claves?

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

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

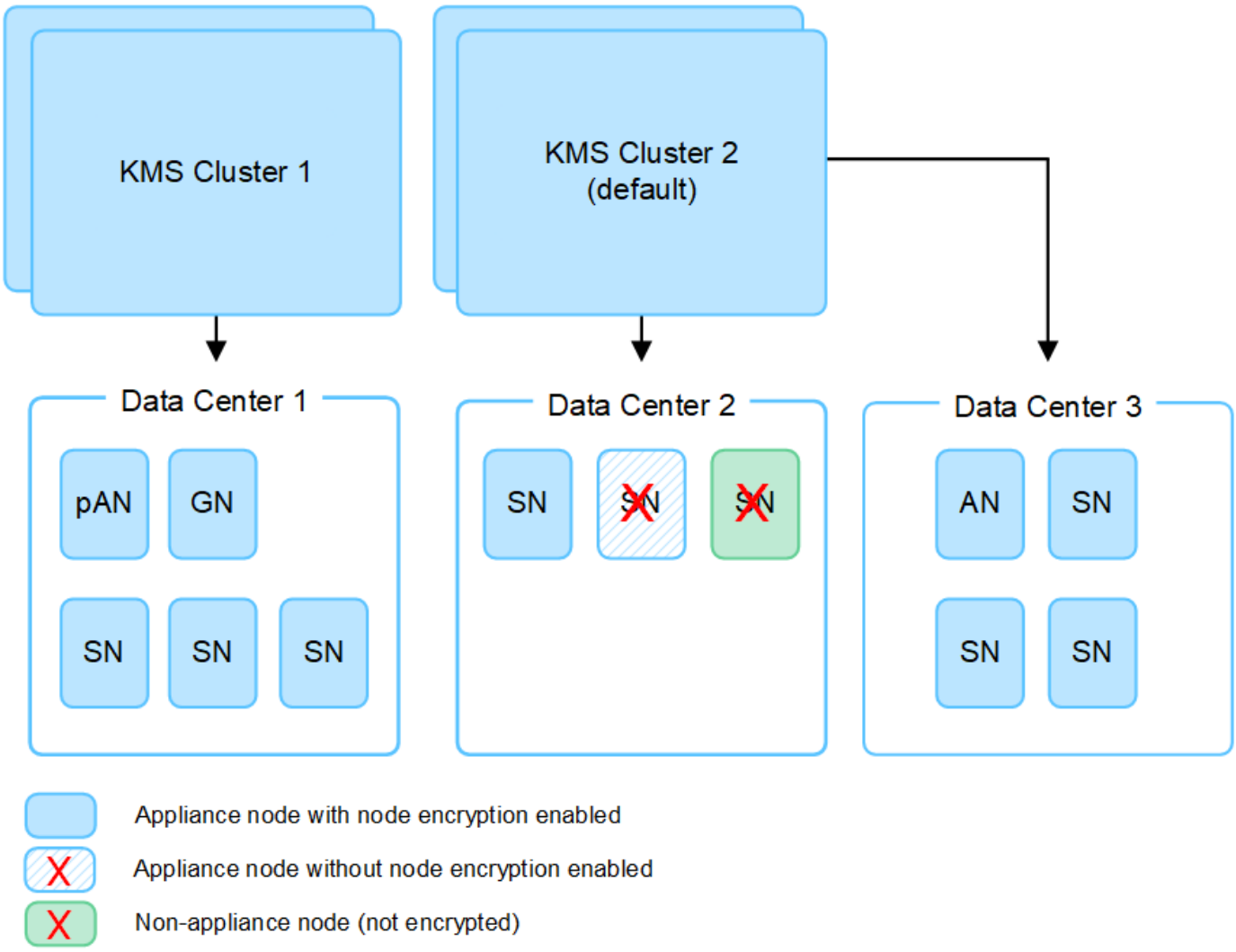
¿Cuántos servidores de gestión de claves necesito?

Puede configurar uno o más servidores de administración de claves externos para proporcionar claves de cifrado a los nodos del dispositivo en su sistema StorageGRID . Cada KMS proporciona una única clave de cifrado a los nodos del dispositivo StorageGRID en un solo sitio o en un grupo de sitios.

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

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

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



¿Qué sucede cuando se gira una llave?

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

Cuando la nueva versión de la clave esté disponible:

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

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

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

configuración de **Cifrado de nodo** y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS para el sitio StorageGRID .

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

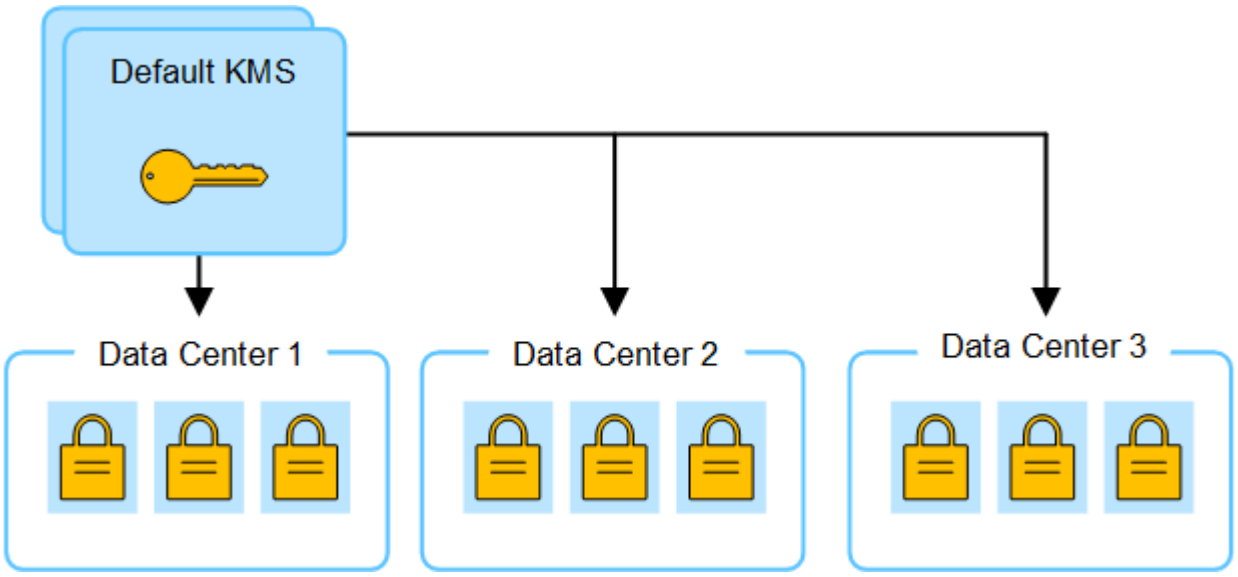
Consideraciones para cambiar el KMS de un sitio

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

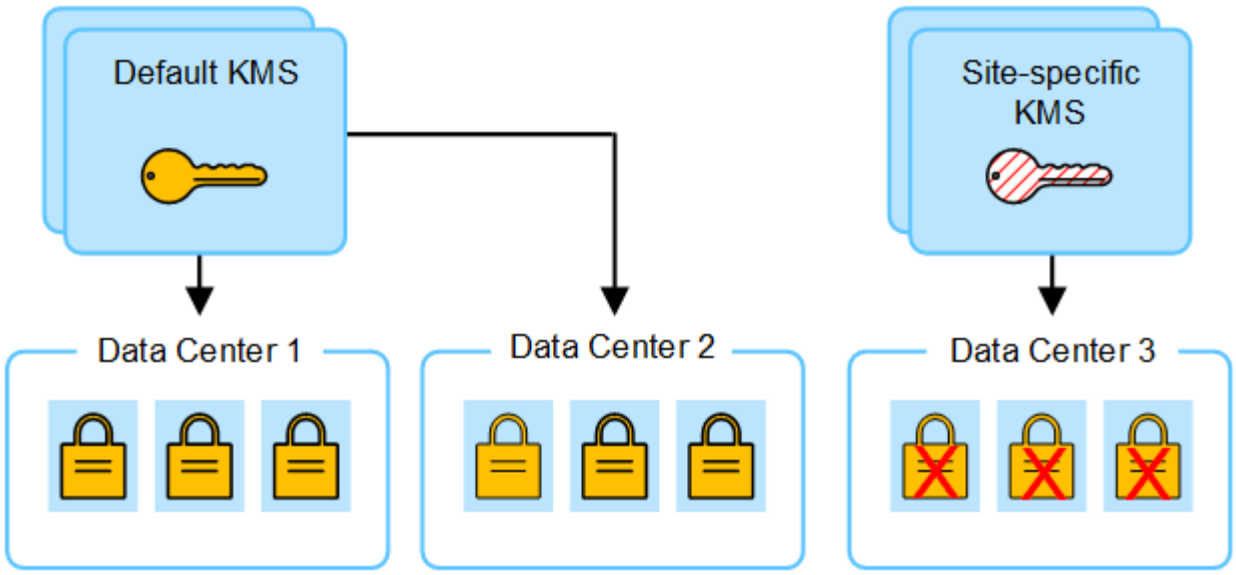
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo previamente cifrados en ese sitio se puedan descifrar usando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesites copiar la versión actual de la clave de cifrado del KMS original al nuevo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

Por ejemplo:

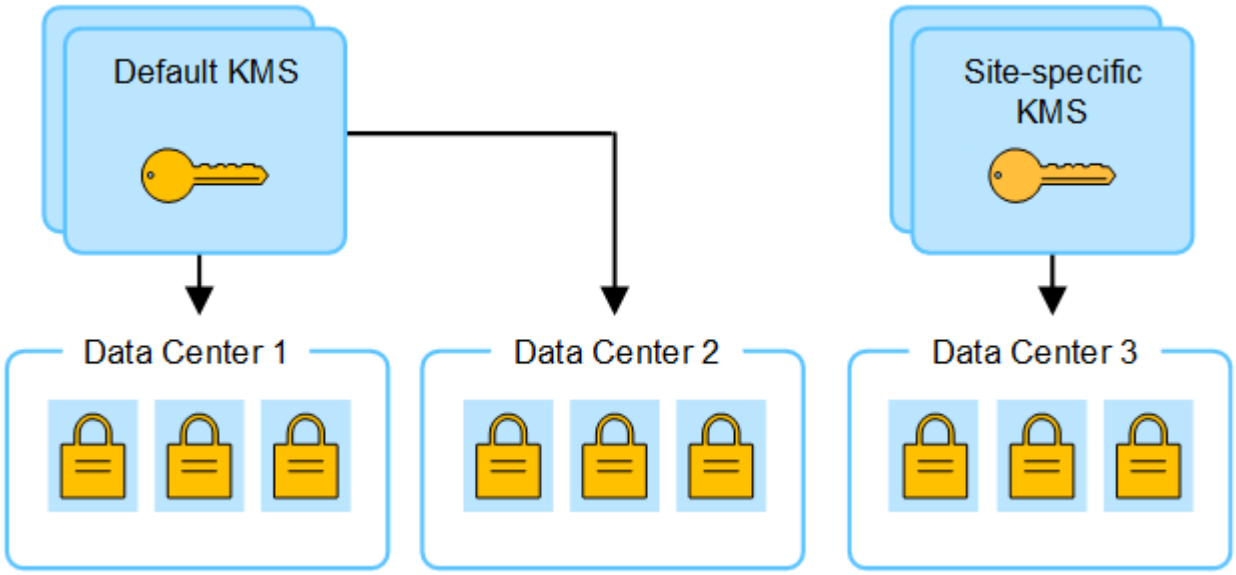
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos del dispositivo que tienen habilitada la configuración **Cifrado de nodo** se conectan al KMS y solicitan la clave de cifrado. Esta clave se utiliza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



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



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



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

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

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

Configurar StorageGRID como cliente en el KMS

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

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

Pasos

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

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

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

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

   - Haga que StorageGRID cree la clave. Se le avisará cuando realice la prueba y guarde

después"cargando certificados de cliente" .

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

   Necesita esta información cuando agrega el KMS a StorageGRID:

   - Nombre de host o dirección IP para cada servidor.
   - Puerto KMIP utilizado por el KMS.
   - Alias de clave para la clave de cifrado en el KMS.

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

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

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

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

   - El certificado del servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que normalmente utiliza el puerto 5696.

5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada para el certificado de cliente.

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

Agregar un servidor de administración de claves (KMS)

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

Antes de empezar

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

Acerca de esta tarea

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

Paso 1: Detalles del KMS

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

Pasos

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

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

2. Seleccione **Crear**.

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

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

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarle a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. **Nota**: Si no ha creado una clave con su producto KMS, se le solicitará que StorageGRID cree la clave.
Administra claves para	El sitio StorageGRID que se asociará con este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no administrados por otro KMS. • Seleccione un sitio si este KMS administrará claves de cifrado para los nodos del dispositivo en un sitio específico. • Seleccione **Sitios no administrados por otro KMS (KMS predeterminado)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que agregue en expansiones posteriores. **Nota:** Se producirá un error de validación cuando guarde la configuración de KMS si selecciona un sitio que anteriormente fue cifrado por el KMS predeterminado pero no proporcionó la versión actual de la clave de cifrado original al nuevo KMS.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.

Campo	Descripción
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. **Nota:** El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

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

Paso 2: Cargar el certificado del servidor

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

Pasos

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

   Aparecen los metadatos del certificado del servidor.

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

3. Seleccione **Continuar**.

Paso 3: Cargar certificados de cliente

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

Pasos

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

   Aparecen los metadatos del certificado del cliente.

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

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

   Se prueban las conexiones entre el servidor de administración de claves y los nodos del dispositivo. Si

todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el nuevo servidor de administración de claves se agrega a la tabla en la página Servidor de administración de claves.

> Inmediatamente después de agregar un KMS, el estado del certificado en la página del Servidor de administración de claves aparece como Desconocido. StorageGRID podría tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar su navegador web para ver el estado actual.

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

   Por ejemplo, es posible que reciba un error 422: Entidad no procesable si falla una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Forzar guardado**.

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

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

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

Administrar un KMS

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

Antes de empezar

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

Ver detalles de KMS

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

Pasos

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

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

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

2. Para ver los detalles de un KMS específico y realizar operaciones en ese KMS, seleccione el nombre del

KMS. La página de detalles del KMS enumera la siguiente información:

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

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

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

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

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

Si rota la clave de cifrado utilizando el software KMS, rótela desde la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.

Nunca intente rotar una clave cambiando el nombre de la clave (alias) para el KMS. StorageGRID requiere que todas las versiones de clave utilizadas anteriormente (así como cualquier versión futura) sean accesibles desde el KMS con el mismo alias de clave. Si cambia el alias de clave de un KMS configurado, es posible que StorageGRID no pueda descifrar sus datos.

Administrar certificados

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

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Servidor de administración de claves**.
2. En la tabla, observe el valor de vencimiento del certificado para cada KMS.
3. Si la expiración del certificado para cualquier KMS es desconocida, espere hasta 30 minutos y luego actualice su navegador web.
4. Si la columna Vencimiento del certificado indica que un certificado ha vencido o está próximo a vencer, seleccione el KMS para ir a la página de detalles del KMS.
   a. Seleccione **Certificado de servidor** y verifique el valor del campo "Vence el".
   b. Para reemplazar el certificado, seleccione **Editar certificado** para cargar un nuevo certificado.
   c. Repita estos subpasos y seleccione **Certificado de cliente** en lugar de Certificado de servidor.
5. Cuando se activan las alertas **Expiración del certificado de CA de KMS**, **Expiración del certificado de cliente de KMS** y **Expiración del certificado de servidor de KMS**, tenga en cuenta la descripción de cada alerta y realice las acciones recomendadas.

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

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

Ver nodos cifrados

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

Pasos

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

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

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

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

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

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, Administración o Puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde está instalado el nodo.
Nombre KMS	El nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Agregar un servidor de administración de claves (KMS)"
UID de clave	El identificador único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, seleccione el texto. Un guion (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo y el KMS.
Estado	El estado de la conexión entre el KMS y el nodo del dispositivo. Si el nodo está conectado, la marca de tiempo se actualiza cada 30 minutos. El estado de la conexión puede tardar varios minutos en actualizarse después de los cambios de configuración de KMS. **Nota:** Actualice su navegador web para ver los nuevos valores.

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

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

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

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

Realice las acciones recomendadas para estas alertas.

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

Editar un KMS

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

Antes de empezar

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

Pasos

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

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

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

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

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

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarle a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de la clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.

Campo	Descripción
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente **Sitios no administrados por otro KMS (KMS predeterminado)**. Esta selección convierte un KMS específico del sitio en el KMS predeterminado, que se aplicará a todos los sitios que no tengan un KMS dedicado y a cualquier sitio agregado en una expansión. **Nota:** Si está editando un KMS específico del sitio, no podrá seleccionar otro sitio. Si está editando el KMS predeterminado, no podrá seleccionar un sitio específico.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. **Nota:** El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

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

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

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

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

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

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

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

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

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

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

Se guarda la configuración de KMS.

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

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

Eliminar un servidor de administración de claves (KMS)

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

Antes de empezar

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

Acerca de esta tarea

Puedes eliminar un KMS en estos casos:

- Puede eliminar un KMS específico del sitio si el sitio se ha dado de baja o si no incluye nodos de dispositivos con cifrado de nodos habilitado.
- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tenga nodos de dispositivo con cifrado de nodo habilitado.

Pasos

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

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

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

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

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

   Se elimina la configuración de KMS.