



# **Configurando servidores de gerenciamento de chaves**

## **StorageGRID**

NetApp  
March 10, 2025

# Índice

Configurando servidores de gerenciamento de chaves	1
O que é um servidor de gerenciamento de chaves (KMS)?	1
Rever os métodos de encriptação StorageGRID	1
Usando vários métodos de criptografia	4
Visão geral do KMS e da configuração do appliance	4
Configurando o servidor de gerenciamento de chaves (KMS)	6
Configurar o aparelho	6
Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)	7
Considerações e requisitos para usar um servidor de gerenciamento de chaves	7
Quais são os requisitos do KMIP?	7
Quais aparelhos são suportados?	8
Quando devo configurar servidores de gerenciamento de chaves?	8
Quantos servidores de gerenciamento de chaves eu preciso?	8
O que acontece quando uma chave é girada?	9
Posso reutilizar um nó de appliance depois que ele foi criptografado?	10
Considerações para alterar o KMS para um site	10
Casos de uso para alterar qual KMS é usado para um site	12
Configurando o StorageGRID como um cliente no KMS	13
Adicionar um servidor de gerenciamento de chaves (KMS)	14
Passo 1: Insira os detalhes do KMS	14
Passo 2: Carregar certificado de servidor	17
Passo 3: Faça o upload de certificados de cliente	19
Visualizar detalhes do KMS	23
Exibindo nós criptografados	25
Editar um servidor de gerenciamento de chaves (KMS)	27
Remover um servidor de gerenciamento de chaves (KMS)	30

# Configurando servidores de gerenciamento de chaves

Você pode configurar um ou mais servidores de gerenciamento de chaves externos (KMS) para proteger os dados em nós de dispositivo especialmente configurados.

## O que é um servidor de gerenciamento de chaves (KMS)?

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiros que fornece chaves de criptografia para nós de dispositivos StorageGRID no site associado do StorageGRID usando o Protocolo de interoperabilidade de Gerenciamento de chaves (KMIP).

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó de dispositivo StorageGRID que tenha a configuração **criptografia de nó** ativada durante a instalação. O uso de servidores de gerenciamento de chaves com esses nós de dispositivo permite que você proteja seus dados mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.



O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do dispositivo. Se você pretende usar um servidor de gerenciamento de chaves externo para proteger dados do StorageGRID, você deve entender como configurar esse servidor e entender como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo dessas instruções. Se precisar de ajuda, consulte a documentação do servidor de gerenciamento de chaves ou entre em Contato com o suporte técnico.

## Rever os métodos de encriptação StorageGRID

O StorageGRID fornece várias opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais métodos atendem aos requisitos de proteção de dados.

A tabela fornece um resumo de alto nível dos métodos de criptografia disponíveis no StorageGRID.

Opção de criptografia	Como funciona	Aplica-se a
Servidor de gerenciamento de chaves (KMS) no Grid Manager	Configure um servidor de gerenciamento de chaves para o site StorageGRID ( <b>Configuração &gt; Configurações do sistema &gt; servidor de gerenciamento de chaves</b> ) e habilite a criptografia de nó para o dispositivo. Em seguida, um nó de dispositivo se conecta ao KMS para solicitar uma chave de criptografia de chave (KEK). Essa chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivo que têm <b>Node Encryption</b> ativado durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. Pode ser usado com alguns dispositivos de armazenamento e serviços StorageGRID.
Conduza a segurança no Gerenciador de sistemas do SANtricity	Se o recurso Segurança da unidade estiver habilitado para um dispositivo de armazenamento, você poderá usar o Gerenciador de sistema do SANtricity para criar e gerenciar a chave de segurança. A chave é necessária para acessar aos dados nas unidades seguras.	Dispositivos de storage com unidades Full Disk Encryption (FDE) ou unidades FIPS (Federal Information Processing Standard). Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de armazenamento ou com qualquer dispositivo de serviço.  <a href="#">"SG6000 dispositivos de armazenamento"</a>  <a href="#">"SG5700 dispositivos de armazenamento"</a>  <a href="#">"SG5600 dispositivos de armazenamento"</a>
Opção de grade de criptografia de objetos armazenados	A opção <b>Stored Object Encryption</b> pode ser ativada no Grid Manager ( <b>Configuration &gt; System Settings &gt; Grid Options</b> ). Quando ativado, todos os novos objetos que não são criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objeto S3 e Swift recém-ingeridos. Os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.  <a href="#">"Configurando a criptografia de objeto armazenado"</a>

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de bucket do S3	Você emite uma solicitação de criptografia PUT Bucket para habilitar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão.	Apenas dados de objetos S3 recém-ingeridos. a encriptação tem de ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.  "Use S3"
Criptografia do lado do servidor de objetos S3 (SSE)	Você emite uma solicitação S3 para armazenar um objeto e incluir o <code>x-amz-server-side-encryption</code> cabeçalho da solicitação.	Somente dados de objeto S3 recém-ingeridos. a criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.  StorageGRID gerencia as chaves.  "Use S3"
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e incluir três cabeçalhos de solicitação. <ul style="list-style-type: none"> <li>• <code>x-amz-server-side-encryption-customer-algorithm</code></li> <li>• <code>x-amz-server-side-encryption-customer-key</code></li> <li>• <code>x-amz-server-side-encryption-customer-key-MD5</code></li> </ul>	Somente dados de objeto S3 recém-ingeridos. a criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.  As chaves são gerenciadas fora do StorageGRID.  "Use S3"
Criptografia de volume externo ou datastore	Você usa um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação o suportar.	Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado.  Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de objetos fora do StorageGRID	Você usa um método de criptografia fora do StorageGRID para criptografar dados e metadados de objetos antes que eles sejam ingeridos no StorageGRID.	<p>Somente dados e metadados de objetos (os dados de configuração do sistema não são criptografados).</p> <p>Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.</p> <p><a href="#">"Amazon Simple Storage Service - Guia do desenvolvedor: Protegendo dados usando criptografia do lado do cliente"</a></p>

## Usando vários métodos de criptografia

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia de cada vez. Por exemplo:

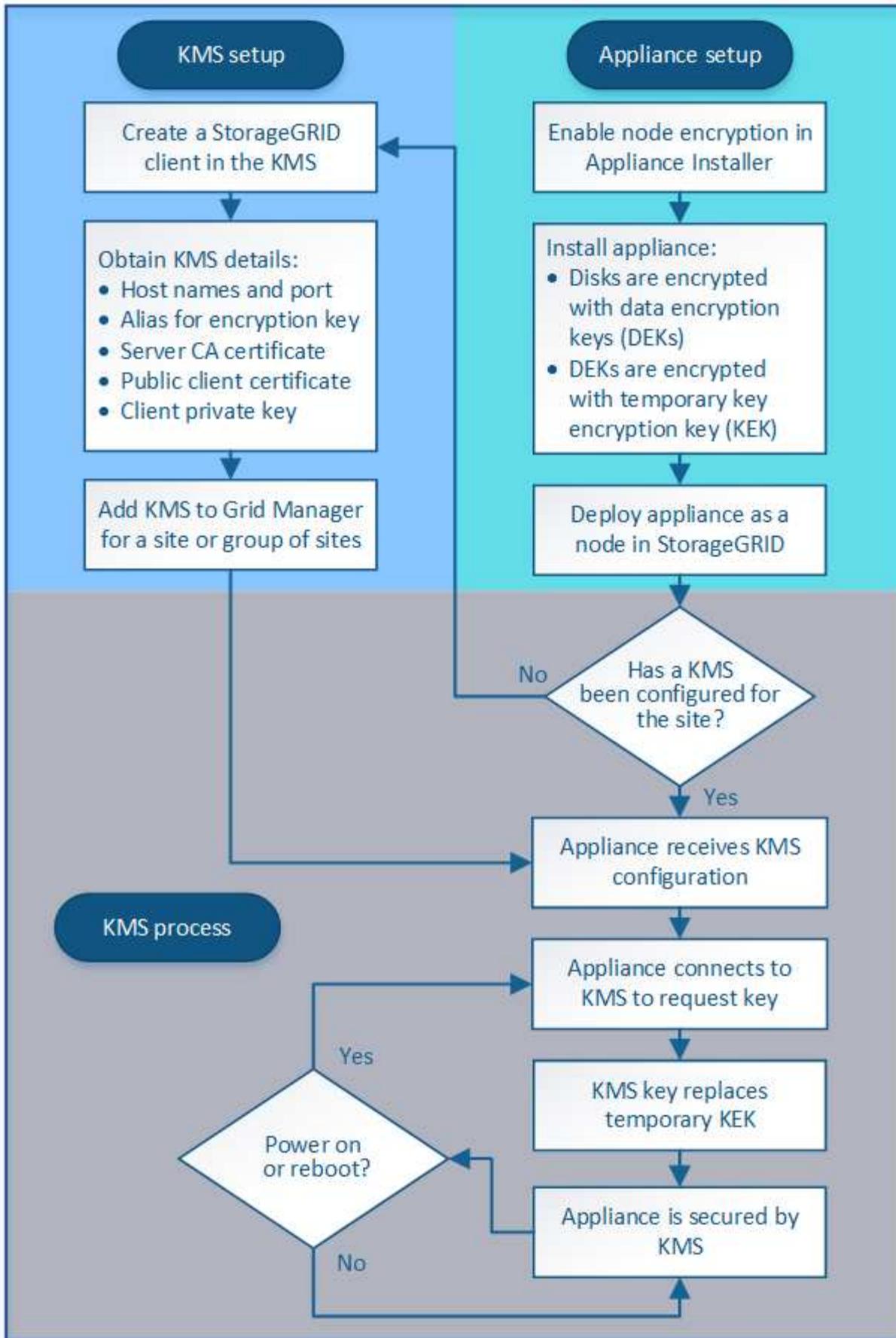
- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança da unidade no Gerenciador de sistema do SANtricity para "criptografar" os dados nas unidades de autcriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados nos nós do dispositivo e também usar a opção de grade criptografia de objetos armazenados para criptografar todos os objetos quando eles são ingeridos.

Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

## Visão geral do KMS e da configuração do appliance

Antes de usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID nos nós do dispositivo, você deve concluir duas tarefas de configuração: Configurar um ou mais servidores KMS e habilitar a criptografia de nós para os nós do dispositivo. Quando essas duas tarefas de configuração são concluídas, o processo de gerenciamento de chaves ocorre automaticamente.

O fluxograma mostra as etapas de alto nível para usar um KMS para proteger os dados do StorageGRID em nós do dispositivo.



O fluxograma mostra a configuração do KMS e a configuração do appliance ocorrendo em paralelo; no

entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nó para novos nós de dispositivo, com base em seus requisitos.

## Configurando o servidor de gerenciamento de chaves (KMS)

A configuração de um servidor de gerenciamento de chaves inclui as seguintes etapas de alto nível.

Passo	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada cluster KMS ou KMS.	<a href="#">"Configurando o StorageGRID como um cliente no KMS"</a>
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	<a href="#">"Configurando o StorageGRID como um cliente no KMS"</a>
Adicione o KMS ao Gerenciador de Grade, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS.	<a href="#">"Adicionar um servidor de gerenciamento de chaves (KMS)"</a>

## Configurar o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui os seguintes passos de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o Instalador de dispositivos StorageGRID para ativar a configuração **criptografia de nó** para o dispositivo.



Não é possível ativar a configuração **criptografia de nó** depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm criptografia de nó ativada.

2. Execute o Instalador de dispositivos StorageGRID. Durante a instalação, uma chave de criptografia de dados aleatórios (DEK) é atribuída a cada volume de dispositivo, da seguinte forma:
  - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco LUKS (Unified Key Setup) do Linux no sistema operacional do dispositivo e não podem ser alteradas.
  - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). O KEK inicial é uma chave temporária que criptografa os DEKs até que o dispositivo possa se conectar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

Para obter detalhes, consulte o seguinte:

- ["Aparelhos de serviços SG100 SG1000"](#)
- ["SG6000 dispositivos de armazenamento"](#)
- ["SG5700 dispositivos de armazenamento"](#)
- ["SG5600 dispositivos de armazenamento"](#)

## Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)

A criptografia de gerenciamento de chaves inclui as seguintes etapas de alto nível que são executadas automaticamente.

1. Quando você instala um dispositivo que tem criptografia de nó ativada na grade, o StorageGRID determina se existe uma configuração de KMS para o site que contém o novo nó.
  - Se um KMS já tiver sido configurado para o site, o appliance receberá a configuração do KMS.
  - Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão a ser criptografados pelo KEK temporário até que você configure um KMS para o site e o appliance receba a configuração do KMS.
2. O dispositivo usa a configuração KMS para se conectar ao KMS e solicitar uma chave de criptografia.
3. O KMS envia uma chave de criptografia para o dispositivo. A nova chave do KMS substitui o KEK temporário e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.



Todos os dados existentes antes do nó de dispositivo criptografado se conectarem ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo não devem ser considerados protegidos contra a remoção do data center até que a chave temporária seja substituída pela chave de criptografia KMS.

4. Se o aparelho estiver ligado ou reinicializado, ele se reconecta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não pode sobreviver a uma perda de energia ou a uma reinicialização.

## Considerações e requisitos para usar um servidor de gerenciamento de chaves

Antes de configurar um servidor de gerenciamento de chaves externo (KMS), você deve entender as considerações e os requisitos.

### Quais são os requisitos do KMIP?

O StorageGRID é compatível com KMIP versão 1,4.

["Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"](#)

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID é compatível com as seguintes cifras TLS v1,2 para KMIP:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

Você deve garantir que cada nó de dispositivo que usa criptografia de nó tenha acesso de rede ao cluster KMS ou KMS configurado para o site.

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique através da porta usada para comunicações KMIP (Key Management Interoperability Protocol). A porta KMIP padrão é 5696.

## Quais aparelhos são suportados?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar chaves de criptografia para qualquer dispositivo StorageGRID em sua grade que tenha a configuração **criptografia de nó** ativada. Esta definição só pode ser ativada durante a fase de configuração de hardware da instalação do dispositivo utilizando o Instalador de dispositivos StorageGRID.



Não é possível ativar a criptografia de nó depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm a criptografia de nó ativada.

Você pode usar o KMS configurado para os seguintes dispositivos e nós de dispositivo StorageGRID:

Aparelho	Tipo de nó
Dispositivo de serviços SG1000	Nó de administração ou nó de gateway
Dispositivo de serviços SG100	Nó de administração ou nó de gateway
SG6000 dispositivo de armazenamento	Nó de storage
SG5700 dispositivo de armazenamento	Nó de storage
SG5600 dispositivo de armazenamento	Nó de storage

Você não pode usar o KMS configurado para nós baseados em software (não-dispositivo), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em contentores do Docker em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no armazenamento de dados ou no nível de disco.

## Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, você normalmente deve configurar um ou mais servidores de gerenciamento de chaves no Gerenciador de Grade antes de criar locatários. Essa ordem garante que os nós sejam protegidos antes que quaisquer dados de objeto sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Gerenciador de Grade antes ou depois de instalar os nós do dispositivo.

## Quanto servidores de gerenciamento de chaves eu preciso?

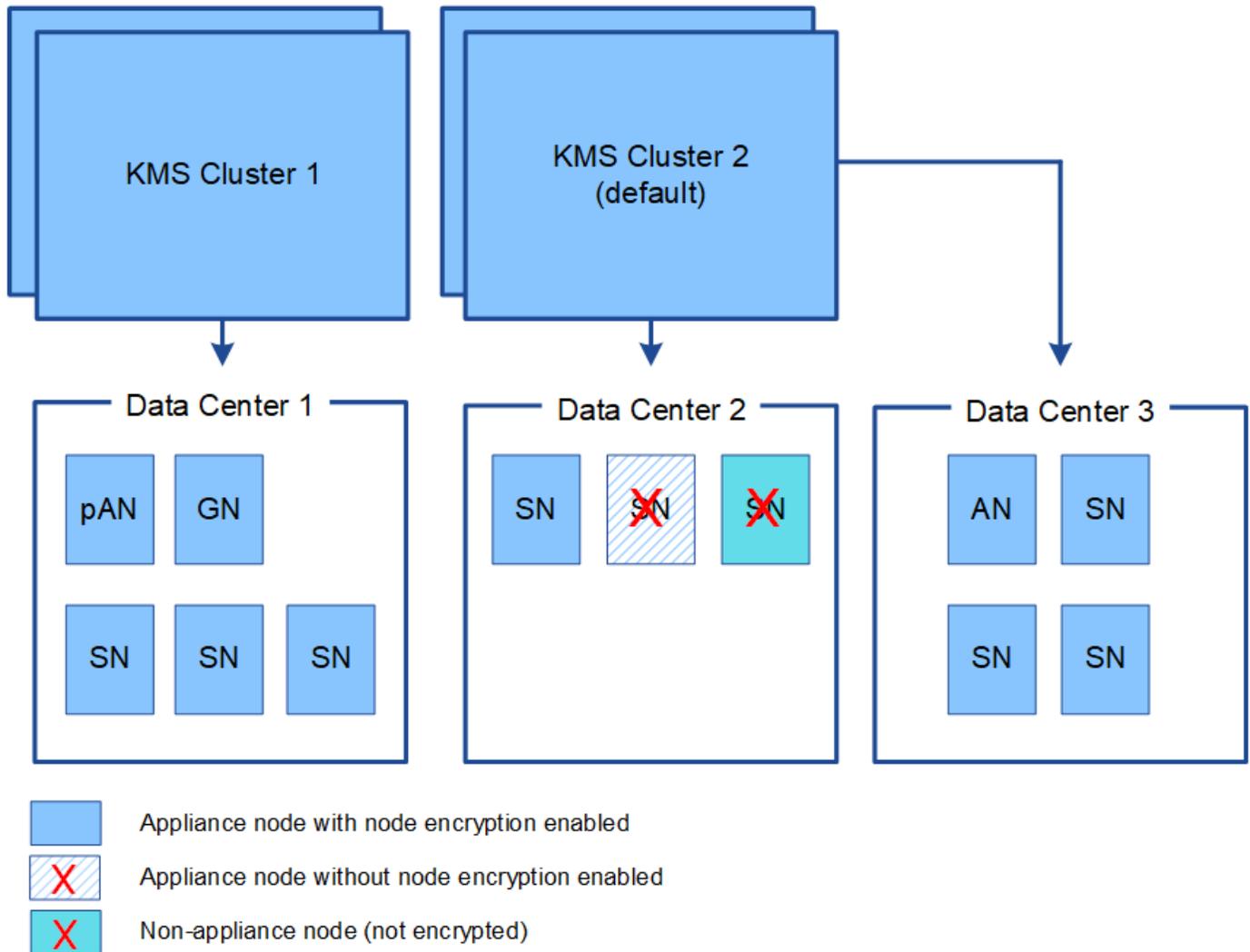
Você pode configurar um ou mais servidores de gerenciamento de chaves externos para fornecer chaves de criptografia aos nós do dispositivo em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único local ou em um grupo de sites.

O StorageGRID é compatível com o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham configurações e chaves de criptografia. O uso de

clusters KMS para gerenciamento de chaves é recomendado porque melhora os recursos de failover de uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três locais de data center. Você pode configurar um cluster KMS para fornecer uma chave para todos os nós do dispositivo no Data Center 1 e um segundo cluster KMS para fornecer uma chave para todos os nós do dispositivo em todos os outros locais. Ao adicionar o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que você não pode usar um KMS para nós que não sejam do dispositivo ou para nenhum nó de dispositivo que não tenha a configuração **criptografia do nó** ativada durante a instalação.



## O que acontece quando uma chave é girada?

Como prática recomendada de segurança, você deve girar periodicamente a chave de criptografia usada por cada KMS configurado.

Ao girar a chave de criptografia, use o software KMS para girar da última versão usada da chave para uma nova versão da mesma chave. Não rode para uma chave totalmente diferente.



Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS no Gerenciador de Grade. Em vez disso, gire a chave atualizando a versão da chave no software KMS. Use o mesmo alias de chave para novas chaves que foi usado para chaves anteriores. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós de dispositivos criptografados no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora de quando a chave é girada.
- Se o nó do dispositivo criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reinicializada.
- Se a nova versão de chave não puder ser usada para criptografar volumes de appliance por qualquer motivo, o alerta **rotação da chave de criptografia KMS falhou** será acionado para o nó do appliance. Talvez seja necessário entrar em Contato com o suporte técnico para obter ajuda na resolução desse alerta.

## Posso reutilizar um nó de appliance depois que ele foi criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID, primeiro será necessário desativar o nó da grade para mover dados de objeto para outro nó. Em seguida, você pode usar o Instalador de dispositivos StorageGRID para limpar a configuração do KMS. A limpeza da configuração KMS desativa a configuração **criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração KMS para o site StorageGRID.



Sem acesso à chave de criptografia KMS, todos os dados que permanecem no dispositivo não podem mais ser acessados e ficam permanentemente bloqueados.

["Aparelhos de serviços SG100 SG1000"](#)

["SG6000 dispositivos de armazenamento"](#)

["SG5700 dispositivos de armazenamento"](#)

["SG5600 dispositivos de armazenamento"](#)

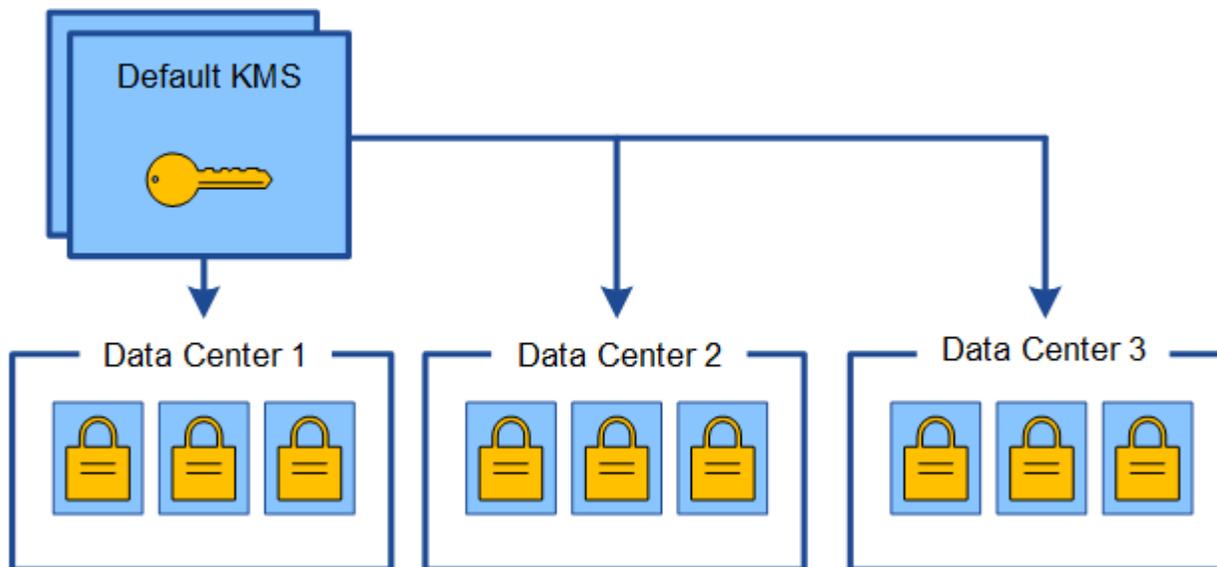
## Considerações para alterar o KMS para um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único local ou em um grupo de sites. Se você precisar alterar qual KMS é usado para um site, talvez seja necessário copiar a chave de criptografia de um KMS para outro.

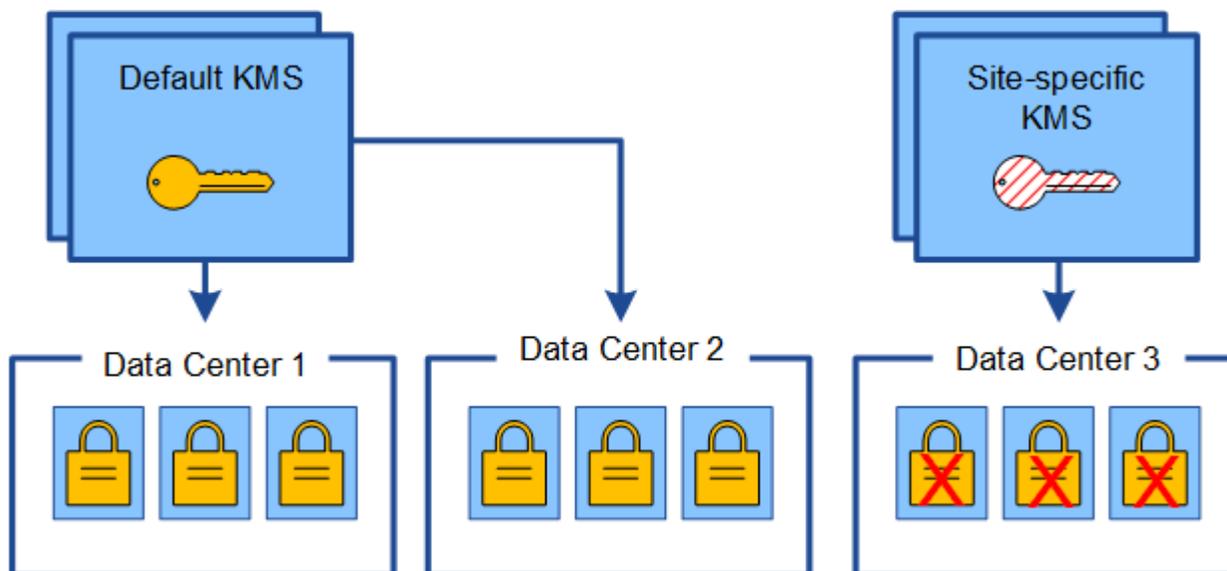
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de dispositivo criptografado no local.

Por exemplo:

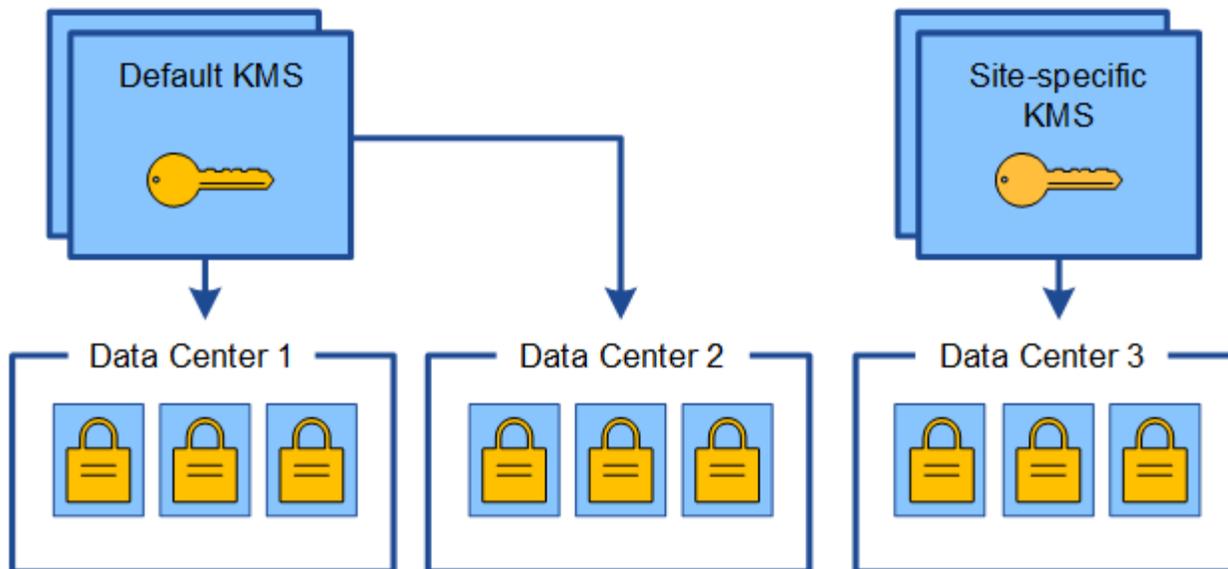
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós do dispositivo em todos os locais. Esta mesma chave também deve ser usada para descriptografar esses aparelhos.



3. Você decide adicionar um KMS específico para um site (Data Center 3 na figura). No entanto, como os nós do appliance já estão criptografados, um erro de validação ocorre quando você tenta salvar a configuração para o KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós nesse site.



4. Para resolver o problema, copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original torna-se uma versão anterior da nova chave.) O KMS específico do local agora tem a chave correta para descriptografar os nós do appliance no Data Center 3, para que ele possa ser salvo no StorageGRID.



## Casos de uso para alterar qual KMS é usado para um site

A tabela resume as etapas necessárias para os casos mais comuns para alterar o KMS de um site.

Caso de uso para alterar o KMS de um site	Passos necessários
<p>Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como KMS padrão.</p>	<p>Edite o KMS específico do site. No campo <b>gerencia chaves para</b>, selecione <b>Sites não gerenciados por outro KMS (KMS padrão)</b>. O KMS específico do site agora será usado como o KMS padrão. Ele se aplicará a quaisquer sites que não tenham um KMS dedicado.</p> <p><a href="#">"Editar um servidor de gerenciamento de chaves (KMS)"</a></p>
<p>Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não deseja usar o KMS padrão para o novo site.</p>	<ol style="list-style-type: none"> <li>1. Se os nós de appliance no novo site já tiverem sido criptografados pelo KMS padrão, use o software KMS para copiar a versão atual da chave de criptografia do KMS padrão para um novo KMS.</li> <li>2. Usando o Gerenciador de Grade, adicione o novo KMS e selecione o site.</li> </ol> <p><a href="#">"Adicionar um servidor de gerenciamento de chaves (KMS)"</a></p>

Caso de uso para alterar o KMS de um site	Passos necessários
<p>Você quer que o KMS para um site use um servidor diferente.</p>	<ol style="list-style-type: none"> <li>1. Se os nós do dispositivo no local já tiverem sido criptografados pelo KMS existente, use o software KMS para copiar a versão atual da chave de criptografia do KMS existente para o novo KMS.</li> <li>2. Usando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP.</li> </ol> <p><a href="#">"Adicionar um servidor de gerenciamento de chaves (KMS)"</a></p>

## Configurando o StorageGRID como um cliente no KMS

Você deve configurar o StorageGRID como um cliente para cada servidor de gerenciamento de chaves externo ou cluster KMS antes de poder adicionar o KMS ao StorageGRID.

### Sobre esta tarefa

Estas instruções aplicam-se ao Thales CipherTrust Manager k170v, versões 2,0, 2,1 e 2,2. Se tiver dúvidas sobre o uso de um servidor de gerenciamento de chaves diferente com o StorageGRID, entre em Contato com o suporte técnico.

### ["Thales CipherTrust Manager"](#)

#### Passos

1. A partir do software KMS, crie um cliente StorageGRID para cada cluster KMS ou KMS que você pretende usar.

Cada KMS gerencia uma única chave de criptografia para os nós do StorageGRID Appliances em um único local ou em um grupo de sites.

2. A partir do software KMS, crie uma chave de criptografia AES para cada cluster KMS ou KMS.

A chave de criptografia precisa ser exportável.

3. Registre as seguintes informações para cada cluster KMS ou KMS.

Você precisa dessas informações quando você adiciona o KMS ao StorageGRID.

- Nome do host ou endereço IP para cada servidor.
- Porta KMIP usada pelo KMS.
- Alias de chave para a chave de criptografia no KMS.



A chave de criptografia já deve existir no KMS. O StorageGRID não cria nem gerencia chaves KMS.

4. Para cada cluster KMS ou KMS, obtenha um certificado de servidor assinado por uma autoridade de

certificação (CA) ou um pacote de certificados que contém cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

- O certificado deve usar o formato X.509 codificado base-64 de Email Avançado de Privacidade (PEM).
- O campo Nome alternativo do assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou o endereço IP ao qual o StorageGRID se conetará.



Ao configurar o KMS no StorageGRID, você deve inserir os mesmos FQDNs ou endereços IP no campo **Nome do host**.

- O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.

5. Obtenha o certificado de cliente público emitido para o StorageGRID pelo KMS externo e a chave privada para o certificado de cliente.

O certificado de cliente permite que o StorageGRID se autentique no KMS.

## Adicionar um servidor de gerenciamento de chaves (KMS)

Você usa o assistente do servidor de gerenciamento de chaves do StorageGRID para adicionar cada cluster KMS ou KMS.

### O que você vai precisar

- Tem de ter revisto a "[considerações e requisitos para usar um servidor de gerenciamento de chaves](#)".
- Você deve ter "[Configurado o StorageGRID como um cliente no KMS](#)", e você deve ter as informações necessárias para cada cluster KMS ou KMS
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

### Sobre esta tarefa

Se possível, configure qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. Se você criar o KMS padrão primeiro, todos os dispositivos criptografados por nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site mais tarde, primeiro copie a versão atual da chave de criptografia do KMS padrão para o novo KMS.

["Considerações para alterar o KMS para um site"](#)

### Passos

1. "[Passo 1: Insira os detalhes do KMS](#)"
2. "[Passo 2: Carregar certificado de servidor](#)"
3. "[Passo 3: Faça o upload de certificados de cliente](#)"

## Passo 1: Insira os detalhes do KMS

Na Etapa 1 (Inserir detalhes do KMS) do assistente Adicionar um servidor de

gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

## Passos

1. Selecione **Configuração > Configurações do sistema > servidor de gerenciamento de chaves**.

A página Key Management Server (servidor de gerenciamento de chaves) é exibida com a guia Configuration Details (Detalhes da configuração) selecionada.

### 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](#).

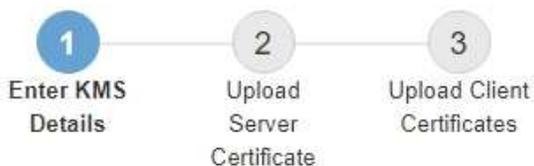
+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
<i>No key management servers have been configured. Select Create.</i>				

2. Selecione **criar**.

O passo 1 (Digite os detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibido.

## 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 

Key Name 

Manages keys for  -- Choose One -- 

Port 

Hostname   

Cancel

Next

3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

Campo	Descrição
Nome de exibição de KMS	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres.

Campo	Descrição
Gere as chaves para	<p>O site StorageGRID que será associado a este KMS. Se possível, você deve configurar qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplica a todos os sites não gerenciados por outro KMS.</p> <ul style="list-style-type: none"> <li>• Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um local específico.</li> <li>• Selecione <b>Sites não gerenciados por outro KMS (KMS padrão)</b> para configurar um KMS padrão que se aplicará a quaisquer sites que não tenham um KMS dedicado e a quaisquer sites que você adicionar em expansões subsequentes.</li> </ul> <p><b>Nota:</b> Um erro de validação ocorrerá quando você salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas você não forneceu a versão atual da chave de criptografia original para o novo KMS.</p>
Porta	<p>A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.</p>
Nome do anfitrião	<p>O nome de domínio ou endereço IP totalmente qualificado para o KMS.</p> <p><b>Observação:</b> o campo SAN do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conectar ao KMS ou a todos os servidores em um cluster KMS.</p>

4. Se você estiver usando um cluster KMS, selecione o sinal de mais **+** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **seguinte**.

A etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

## Passo 2: Carregar certificado de servidor

Na Etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado do servidor (ou pacote de

certificados) para o KMS. O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

**Passos**

1. A partir de **passo 2 (carregar certificado do servidor)**, navegue até a localização do certificado ou pacote de certificados do servidor guardado.

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

2. Carregue o ficheiro de certificado.

Os metadados do certificado do servidor são exibidos.

## 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 ⓘ  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



Se você carregou um pacote de certificados, os metadados de cada certificado serão exibidos em sua própria guia.

### 3. Selecione **seguinte**.

A etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

## Passo 3: Faça o upload de certificados de cliente

Na Etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado de cliente e a chave privada do certificado de cliente. O certificado de cliente permite que o StorageGRID se autentique no KMS.

### Passos

1. A partir do **passo 3 (carregar certificados de cliente)**, navegue até a localização do 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 

Client Certificate Private Key 

Cancel

Back

Save

2. Carregue o ficheiro de certificado do cliente.

Os metadados do certificado do cliente são exibidos.

3. Navegue até a localização da chave privada para o certificado do cliente.

4. Carregue o ficheiro de chave privada.

Os metadados do certificado de cliente e da chave privada do certificado de cliente são exibidos.

## 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 ⓘ  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 ⓘ  k170vClientKey.pem

### 5. Selecione **Guardar**.

As conexões entre o servidor de gerenciamento de chaves e os nós do dispositivo são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.



Imediatamente após adicionar um KMS, o status do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status atual.

### 6. Se uma mensagem de erro for exibida quando você selecionar **Salvar**, revise os detalhes da mensagem e selecione **OK**.

Por exemplo, você pode receber um erro de entidade 422: Não processável se um teste de conexão falhar.

### 7. Se você precisar salvar a configuração atual sem testar a conexão externa, selecione **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 ⓘ  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 ⓘ  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



Selecionar **Force Save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

## 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

A configuração do KMS é salva, mas a conexão com o KMS não é testada.

## Visualizar detalhes do KMS

Você pode exibir informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo o status atual do servidor e dos certificados de cliente.

### Passos

1. Selecione **Configuração > Configurações do sistema > servidor de gerenciamento de chaves**.

A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves 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](#).

+ 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. Reveja as informações na tabela para cada KMS.

Campo	Descrição
Nome de exibição de KMS	O nome descritivo do KMS.

Campo	Descrição
Nome da chave	O alias de chave para o cliente StorageGRID no KMS.
Gere as chaves para	<p>O site StorageGRID associado ao KMS.</p> <p>Este campo exibe o nome de um site StorageGRID específico ou <b>sites não gerenciados por outro KMS (KMS padrão)</b>.</p>
Nome do anfitrião	<p>O nome de domínio totalmente qualificado ou endereço IP do KMS.</p> <p>Se houver um cluster de dois servidores de gerenciamento de chaves, o nome de domínio totalmente qualificado ou o endereço IP de ambos os servidores serão listados. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o nome de domínio totalmente qualificado ou o endereço IP do primeiro KMS são listados juntamente com o número de servidores de gerenciamento de chaves adicionais no cluster.</p> <p>Por exemplo: 10.10.10.10 and 10.10.10.11 Ou 10.10.10.10 and 2 others.</p> <p>Para exibir todos os nomes de host em um cluster, selecione um KMS e, em seguida, selecione <b>Editar</b>.</p>
Estado do certificado	<p>Estado atual do certificado do servidor, do certificado da CA opcional e do certificado do cliente: Válido, expirado, próximo da expiração ou desconhecido.</p> <p><b>Nota:</b> pode demorar StorageGRID até 30 minutos para obter atualizações do status do certificado. Você deve atualizar o navegador da Web para ver os valores atuais.</p>

- Se o Status do certificado for desconhecido, aguarde até 30 minutos e, em seguida, atualize o navegador da Web.



Imediatamente após adicionar um KMS, o status do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status real.

- Se a coluna Status do certificado indicar que um certificado expirou ou está prestes a expirar, solucione o problema o mais rápido possível.

Consulte as ações recomendadas para os alertas **expiração do certificado KMS CA**, **expiração do**

**certificado do cliente KMS e expiração do certificado do servidor KMS** nas instruções para monitoramento e solução de problemas do StorageGRID.



Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

### Informações relacionadas

["Monitorizar Resolução de problemas"](#)

## Exibindo nós criptografados

Você pode exibir informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

### Passos

1. Selecione **Configuração > Configurações do sistema > servidor de gerenciamento de chaves**.

A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram 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](#).

+ 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. Na parte superior da página, selecione a guia **nós criptografados**.

#### 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.

A guia nós criptografados lista os nós do dispositivo no sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

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 as informações na tabela para cada nó de dispositivo.

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo nó	O tipo de nó: Storage, Admin ou Gateway.
Local	O nome do site do StorageGRID onde o nó está instalado.
Nome de exibição de KMS	O nome descritivo do KMS usado para o nó.  Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS.  <a href="#">"Adicionar um servidor de gerenciamento de chaves (KMS)"</a>
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para exibir um UID de chave inteiro, passe o cursor sobre a célula.  Um traço (--) indica que a chave UID é desconhecida, possivelmente por causa de um problema de conexão entre o nó do aparelho e o KMS.
Estado	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conectado, o carimbo de data/hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações de configuração do KMS.  <b>Observação:</b> você deve atualizar seu navegador para ver os novos valores.

### 4. Se a coluna Status indicar um problema KMS, solucione o problema imediatamente.

Durante as operações normais de KMS, o status será **conectado ao KMS**. Se um nó for desconectado da grade, o estado de conexão do nó é mostrado (administrativamente para baixo ou desconhecido).

Outras mensagens de status correspondem a alertas StorageGRID com os mesmos nomes:

- Falha ao carregar a configuração DE KMS

- Erro de conectividade DE KMS
- Nome da chave de encriptação KMS não encontrado
- Falha na rotação da chave de CRIPTOGRAFIA KMS
- A chave KMS falhou ao descriptar um volume de aparelho
- O KMS não está configurado consulte as ações recomendadas para esses alertas nas instruções para monitoramento e solução de problemas do StorageGRID.



Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

## Informações relacionadas

["Monitorizar Resolução de problemas"](#)

# Editar um servidor de gerenciamento de chaves (KMS)

Talvez seja necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

## O que você vai precisar

- Tem de ter revisto a ["considerações e requisitos para usar um servidor de gerenciamento de chaves"](#).
- Se pretende atualizar o local selecionado para um KMS, tem de ter revisto o ["Considerações para alterar o KMS para um site"](#).
- Você deve ter a permissão de acesso root.
- Você deve estar conectado ao Gerenciador de Grade usando um navegador compatível.

## Passos

1. Selecione **Configuração > Configurações do sistema > servidor de gerenciamento de chaves**.

A página Key Management Server (servidor de gerenciamento de chaves) é exibida e mostra todos os servidores de gerenciamento de chaves que foram 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](#).

<span>+ Create</span> <span>Edit</span> <span>Remove</span>				
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. Selecione o KMS que deseja editar e selecione **Editar**.
3. Opcionalmente, atualize os detalhes em **Etapa 1 (Inserir detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
Nome de exibição de KMS	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	<p>O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres.</p> <p>Você só precisa editar o nome da chave em casos raros. Por exemplo, você deve editar o nome da chave se o alias for renomeado no KMS ou se todas as versões da chave anterior tiverem sido copiadas para o histórico de versões do novo alias.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS. Em vez disso, gire a chave atualizando a versão da chave no software KMS. O StorageGRID requer que todas as versões de chave usadas anteriormente (bem como quaisquer versões futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.</p> <p><a href="#">"Considerações e requisitos para usar um servidor de gerenciamento de chaves"</a></p> </div>
Gere as chaves para	<p>Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione <b>Sites não gerenciados por outro KMS (KMS padrão)</b>. Esta seleção converte um KMS específico do site para o KMS padrão, que se aplicará a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão.</p> <p><b>Observação:</b> se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não poderá selecionar um site específico.</p>
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.

Campo	Descrição
Nome do anfitrião	<p>O nome de domínio ou endereço IP totalmente qualificado para o KMS.</p> <p><b>Observação:</b> o campo SAN do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conectar ao KMS ou a todos os servidores em um cluster KMS.</p>

4. Se você estiver configurando um cluster KMS, selecione o sinal de mais **+** para adicionar um nome de host para cada servidor no cluster.

5. Selecione **seguinte**.

A etapa 2 (carregar certificado do servidor) do assistente Editar um servidor de gerenciamento de chaves é exibida.

6. Se precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.

7. Selecione **seguinte**.

A etapa 3 (carregar certificados de cliente) do assistente Editar um servidor de gerenciamento de chaves é exibida.

8. Se precisar substituir o certificado de cliente e a chave privada do certificado de cliente, selecione **Procurar** e carregue os novos arquivos.

9. Selecione **Guardar**.

As conexões entre o servidor de gerenciamento de chaves e todos os nós de dispositivos criptografados por nós nos locais afetados são testadas. Se todas as conexões de nó forem válidas e a chave correta for encontrada no KMS, o servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

10. Se for apresentada uma mensagem de erro, reveja os detalhes da mensagem e selecione **OK**.

Por exemplo, você pode receber um erro de entidade 422: Não processável se o site selecionado para este KMS já for gerenciado por outro KMS, ou se um teste de conexão falhou.

11. Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Force Save**.



Selecionar **Force Save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

A configuração do KMS é salva.

12. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

## ⚠ 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

A configuração do KMS é salva, mas a conexão com o KMS não é testada.

## Remover um servidor de gerenciamento de chaves (KMS)

Em alguns casos, você pode querer remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se você tiver desativado o site.

### O que você vai precisar

- Tem de ter revisto a ["considerações e requisitos para usar um servidor de gerenciamento de chaves"](#).
- Você deve ter a permissão de acesso root.
- Você deve estar conectado ao Gerenciador de Grade usando um navegador compatível.

### Sobre esta tarefa

Você pode remover um KMS nestes casos:

- Você pode remover um KMS específico do site se o site tiver sido desativado ou se o site não incluir nós de dispositivo com criptografia de nó ativada.
- Você pode remover o KMS padrão se um KMS específico do site já existir para cada site que tenha nós de dispositivo com criptografia de nó ativada.

### Passos

1. Selecione **Configuração > Configurações do sistema > servidor de gerenciamento de chaves**.

A página Key Management Server (servidor de gerenciamento de chaves) é exibida e mostra todos os servidores de gerenciamento de chaves que foram 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. Selecione o botão de opção para o KMS que deseja remover e selecione **Remove**.
3. Reveja as considerações na caixa de diálogo de aviso.

**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. Selecione **OK**.

A configuração do KMS é removida.

## **Informações sobre direitos autorais**

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.