Configurar servidores de gerenciamento de chaves

StorageGRID software

NetApp
December 03, 2025

Índice

Configurar servidores de gerenciamento de chaves

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 do dispositivo StorageGRID no site StorageGRID associado usando o Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP).

O StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista de produtos e versões suportados, use o "Ferramenta de Matriz de Interoperabilidade NetApp (IMT)" .

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó do 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 dispositivos permite que você proteja seus dados mesmo se um dispositivo for removido do data center. Depois que os volumes do dispositivo forem criptografados, você não poderá 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 nós do dispositivo. Se você planeja usar um servidor externo de gerenciamento de chaves para proteger os dados do StorageGRID , você deve entender como configurar esse servidor e como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo destas instruções. Se precisar de ajuda, consulte a documentação do seu servidor de gerenciamento de chaves ou entre em contato com o suporte técnico.

Configuração do KMS e do dispositivo

Antes de poder usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID em 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 dados do StorageGRID em nós do dispositivo.

O fluxograma mostra a configuração do KMS e a configuração do dispositivo ocorrendo em paralelo; no entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nós para novos nós do dispositivo, com base em seus requisitos.

Configurar o servidor de gerenciamento de chaves (KMS)

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

Etapa	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada KMS ou cluster KMS.	"Configurar o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configurar o StorageGRID como um cliente no KMS"
Adicione o KMS ao Grid Manager, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS.	"Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui as seguintes etapas de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o StorageGRID Appliance Installer para habilitar a configuração **Criptografia de nó** para o dispositivo.

   > Não é possível habilitar 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 tenham a criptografia de nó habilitada.

2. Execute o instalador do dispositivo StorageGRID . Durante a instalação, uma chave de criptografia de dados aleatória (DEK) é atribuída a cada volume do dispositivo, da seguinte forma:
   - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco Linux Unified Key Setup (LUKS) no sistema operacional do dispositivo e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). A 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.

Ver "Habilitar criptografia de nó" para mais detalhes.

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 com criptografia de nó habilitada na grade, o StorageGRID determina se existe uma configuração KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o dispositivo receberá a configuração do KMS.
   - Se um KMS ainda não tiver sido configurado para o site, os dados no dispositivo continuarão sendo criptografados pela KEK temporária até que você configure um KMS para o site e o dispositivo receba a configuração do KMS.
2. O dispositivo usa a configuração do 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 a KEK temporária e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.

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

4. Se o dispositivo for ligado ou reiniciado, ele se reconectará ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não sobrevive a uma queda 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.

Qual versão do KMIP é suportada?

O StorageGRID suporta o KMIP versão 1.4.

"Especificação do Protocolo de Interoperabilidade de Gerenciamento de Chaves Versão 1.4"

Quais são as considerações sobre a rede?

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

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

Quais versões do TLS são suportadas?

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID pode oferecer suporte ao protocolo TLS 1.2 ou TLS 1.3 ao fazer conexões KMIP com um cluster KMS ou KMS, com base no que o KMS oferece suporte e em quais"Política de TLS e SSH" você está usando.

O StorageGRID negocia o protocolo e a cifra (TLS 1.2) ou conjunto de cifras (TLS 1.3) com o KMS quando faz a conexão. Para ver quais versões de protocolo e cifras/conjuntos de cifras estão disponíveis, revise o `tlsOutbound` seção da política TLS e SSH ativa da grade (**CONFIGURAÇÃO** > **Segurança Configurações de segurança**).

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** habilitada. Esta configuração só pode ser ativada durante o estágio de configuração de hardware da instalação do dispositivo usando o StorageGRID Appliance Installer.

Não é possível habilitar a criptografia de nós depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não tenham a criptografia de nós habilitada.

Você pode usar o KMS configurado para dispositivos e nós de dispositivos StorageGRID .

Não é possível usar o KMS configurado para nós baseados em software (não dispositivos), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em mecanismos de contêiner em hosts Linux

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

Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, normalmente você deve configurar um ou mais servidores de gerenciamento de chaves no Grid Manager 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 Grid Manager antes ou depois de instalar os nós do dispositivo.

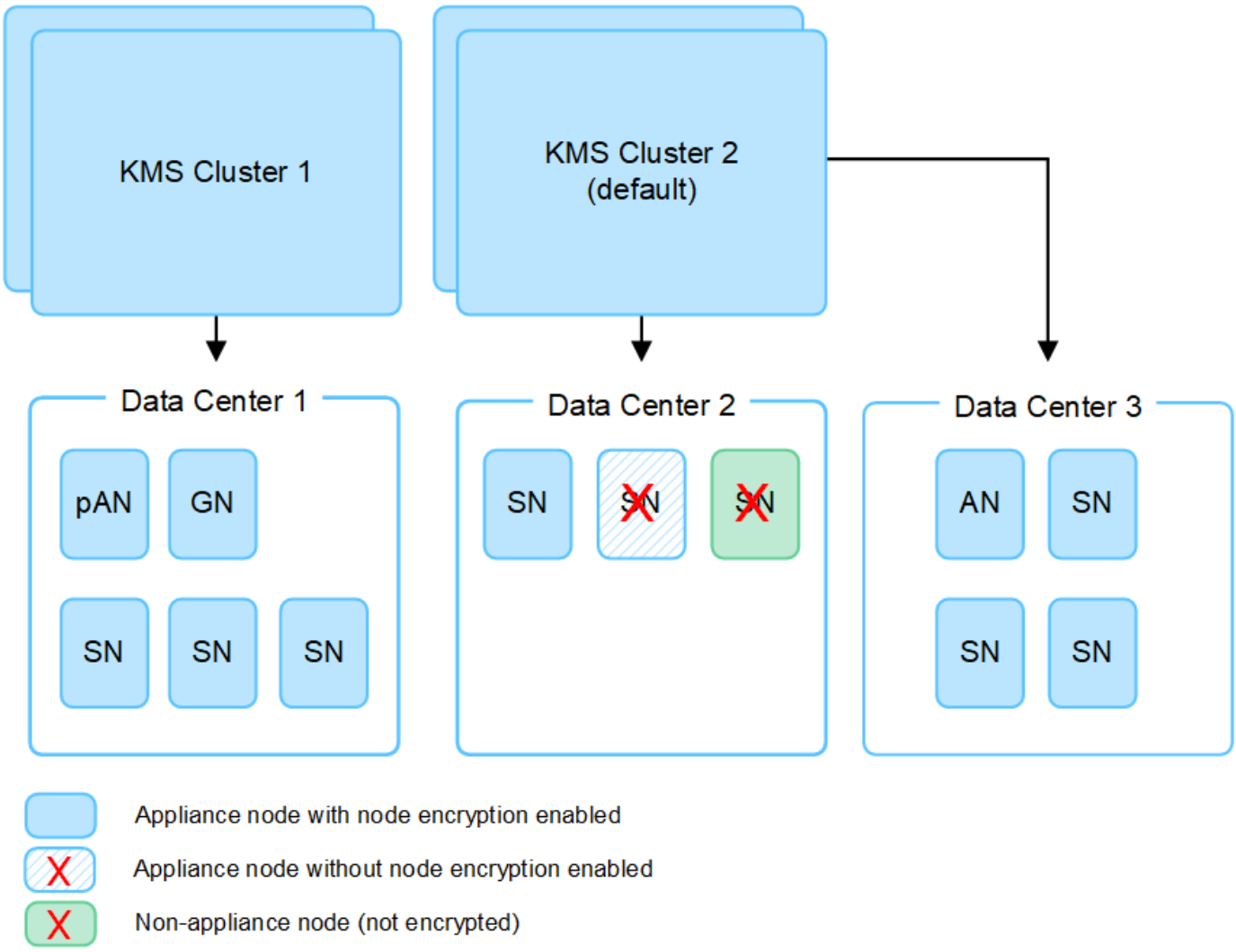
Quantos servidores de gerenciamento de chaves eu preciso?

Você pode configurar um ou mais servidores externos de gerenciamento de chaves para fornecer chaves de criptografia aos nós do dispositivo no seu sistema StorageGRID . Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único site ou em um grupo de sites.

O StorageGRID suporta o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham definições de configuração 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 sites. 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 de dispositivo ou para nós de dispositivo que não tenham a configuração **Criptografia de nó** ativada durante a instalação.



O que acontece quando uma chave é girada?

Como prática recomendada de segurança, você deve periodicamente"gire a chave de criptografia" usado por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós do dispositivo criptografado no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora após a rotação da chave.
- 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 reinicializado.
- Se a nova versão da chave não puder ser usada para criptografar volumes do dispositivo por qualquer motivo, o alerta **Falha na rotação da chave de criptografia KMS** será acionado para o nó do dispositivo. Talvez seja necessário entrar em contato com o suporte técnico para obter ajuda para resolver este alerta.

Posso reutilizar um nó de dispositivo depois que ele for criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID , primeiro desative o nó da grade para mover os dados do objeto para outro nó. Em seguida, você pode usar o StorageGRID Appliance Installer para "limpar a configuração do KMS" . Limpar a configuração do KMS desabilita a configuração **Criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração do KMS

para o site StorageGRID .

> Sem acesso à chave de criptografia do KMS, todos os dados que permanecerem no dispositivo não poderão mais ser acessados e serão bloqueados permanentemente.

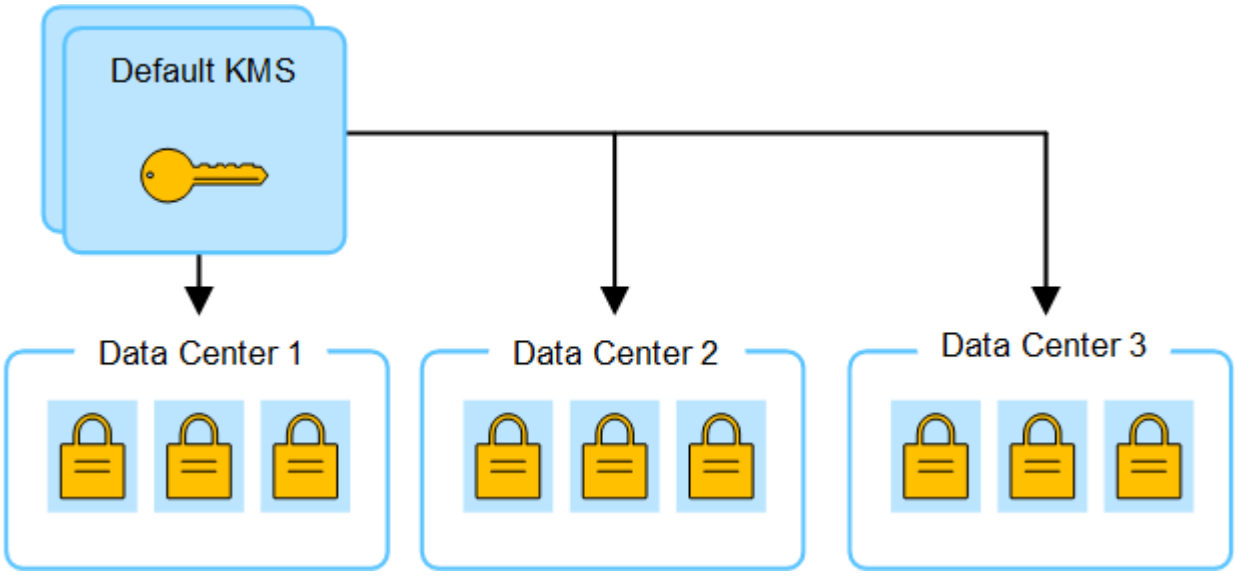
Considerações para alterar o KMS de um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único site 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.

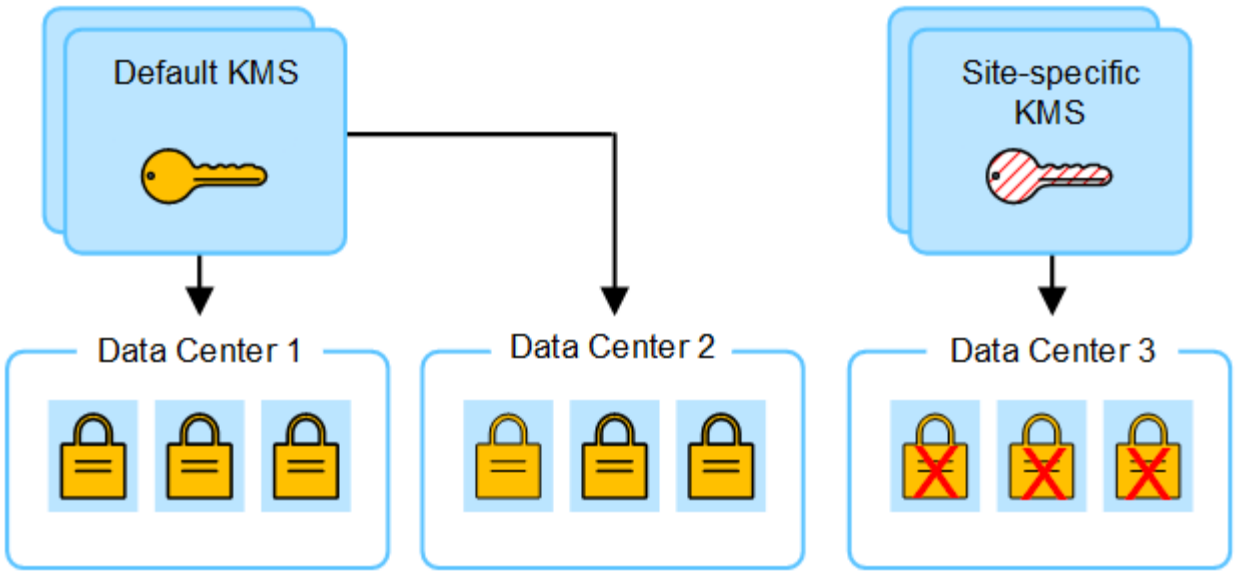
Se você alterar o KMS usado para um site, deverá garantir que os nós do dispositivo criptografados anteriormente naquele site possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, pode ser necessário copiar a versão atual da chave de criptografia do KMS original para o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

Por exemplo:

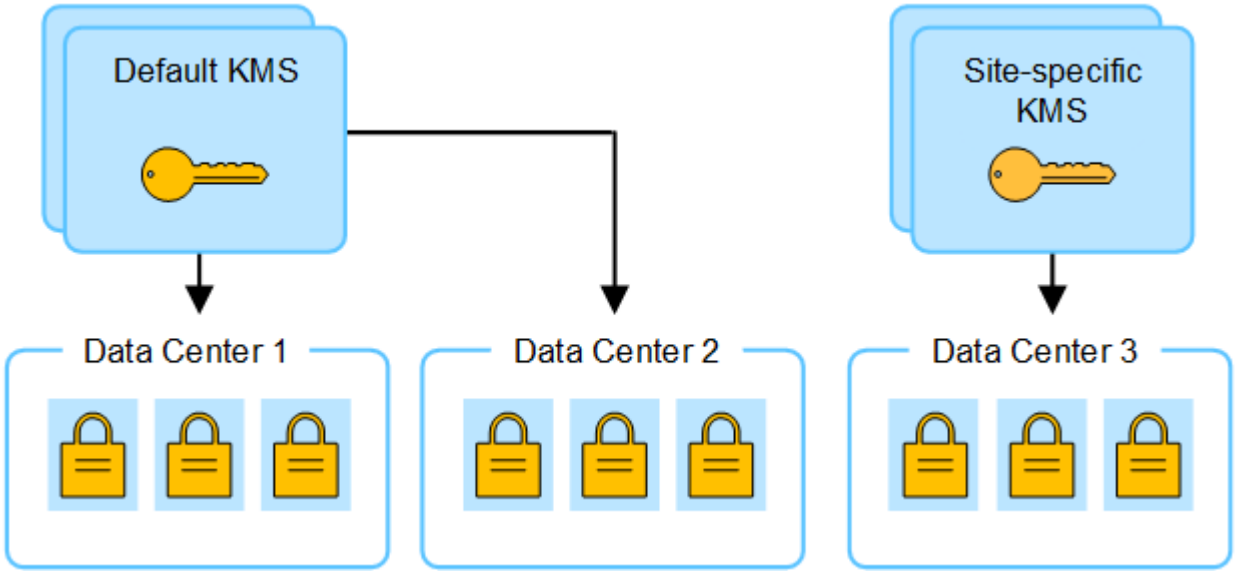
1. Inicialmente, você configura um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós do dispositivo que têm a configuração **Criptografia de nó** ativada se conectam ao KMS e solicitam a chave de criptografia. Esta chave é usada para criptografar os nós do dispositivo em todos os sites. Essa 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 dispositivo já estão criptografados, ocorre um erro de validação quando você tenta salvar a configuração do KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós naquele 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 se torna uma versão anterior da nova chave.) O KMS específico do site agora tem a chave correta para descriptografar os nós do dispositivo no Data Center 3, para que ela possa ser salva 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 de alteração do KMS de um site.

Caso de uso para alterar o KMS de um site	Etapas necessárias
Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como o KMS padrão.	Edite o KMS específico do site. No campo **Gerencia chaves para**, selecione **Sites não gerenciados por outro KMS (KMS padrão)**. O KMS específico do site agora será usado como o KMS padrão. Ele será aplicado a qualquer site que não tenha um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"

Caso de uso para alterar o KMS de um site	Etapas necessárias
Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não quer usar o KMS padrão para o novo site.	1. Se os nós do dispositivo 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. 2. Usando o Grid Manager, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS de um site use um servidor diferente.	1. Se os nós do dispositivo no site 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. 2. Usando o Grid Manager, edite a configuração do KMS existente e insira o novo nome do host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar 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.

Estas instruções se aplicam ao Thales CipherTrust Manager e ao Hashicorp Vault. Para obter uma lista de produtos e versões suportados, use o "Ferramenta de Matriz de Interoperabilidade NetApp (IMT)" .

Passos

1. No software KMS, crie um cliente StorageGRID para cada KMS ou cluster KMS que você planeja usar.

   Cada KMS gerencia uma única chave de criptografia para os nós dos dispositivos StorageGRID em um único site ou em um grupo de sites.

2. Crie uma chave usando um dos dois métodos a seguir:
   - Use a página de gerenciamento de chaves do seu produto KMS. Crie uma chave de criptografia AES para cada KMS ou cluster KMS.

     A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

   - Faça com que o StorageGRID crie a chave. Você será avisado quando testar e salvar depois"carregando certificados de cliente" .
3. Registre as seguintes informações para cada KMS ou cluster KMS.

   Você precisa dessas informações ao adicionar 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.

4. Para cada KMS ou cluster KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contenha cada um dos arquivos de certificado de CA codificados em PEM, concatenados na ordem da 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 em Base 64 do Privacy Enhanced Mail (PEM).
   - O campo Nome Alternativo do Assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou endereço IP ao qual o StorageGRID se conectará.

     > 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 do cliente permite que o StorageGRID se autentique no KMS.

Adicionar um servidor de gerenciamento de chaves (KMS)

Use o assistente do StorageGRID Key Management Server para adicionar cada KMS ou cluster KMS.

Antes de começar

- Você revisou o"considerações e requisitos para usar um servidor de gerenciamento de chaves" .
- Você tem"configurou o StorageGRID como um cliente no KMS" , e você terá as informações necessárias para cada KMS ou cluster KMS.
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

Se possível, configure quaisquer servidores de gerenciamento de chaves específicos 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 deverá copiar a versão atual da chave de criptografia do KMS padrão para o novo KMS. Ver"Considerações para alterar o KMS de um site" para mais detalhes.

Etapa 1: detalhes do KMS

Na Etapa 1 (Detalhes do KMS) do assistente Adicionar um Servidor de Gerenciamento de Chaves, você fornece detalhes sobre o KMS ou cluster KMS.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

A página do servidor de gerenciamento de chaves é exibida com a guia Detalhes da configuração selecionada.

2. Selecione **Criar**.

   A etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

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

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. **Observação**: se você não criou uma chave usando seu produto KMS, será solicitado que o StorageGRID crie a chave.
Gerencia chaves para	O site StorageGRID que será associado a este KMS. Se possível, você deve configurar quaisquer servidores de gerenciamento de chaves específicos do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. • Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um site específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que será aplicado a todos os sites que não tenham um KMS dedicado e a todos os sites que você adicionar em expansões subsequentes. **Observação:** 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 não tiver fornecido a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP para o KMS. **Observação:** O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o FQDN ou endereço IP que você inserir aqui. Caso contrário, o StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.

5. Selecione **Continuar**.

Etapa 2: Carregar certificado do 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. Na **Etapa 2 (Carregar certificado do servidor)**, navegue até o local do certificado do servidor ou pacote de certificados salvo.
2. Carregue o arquivo do certificado.

   Os metadados do certificado do servidor são exibidos.

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

3. Selecione **Continuar**.

Etapa 3: Carregar 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 do cliente permite que o StorageGRID se autentique no KMS.

Passos

1. Na **Etapa 3 (Carregar certificados do cliente)**, navegue até o local do certificado do cliente.
2. Carregue o arquivo de certificado do cliente.

   Os metadados do certificado do cliente são exibidos.

3. Navegue até o local da chave privada do certificado do cliente.
4. Carregue o arquivo da chave privada.
5. Selecione **Testar e salvar**.

   Se uma chave não existir, você será solicitado a solicitar que o StorageGRID crie uma.

   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 Servidor de Gerenciamento de Chaves aparece como Desconhecido. O StorageGRID pode levar até 30 minutos para obter o status real de cada certificado. Você deve atualizar seu navegador para ver o status atual.

6. Se uma mensagem de erro aparecer quando você selecionar **Testar e salvar**, revise os detalhes da mensagem e selecione **OK**.

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

7. Se precisar salvar a configuração atual sem testar a conexão externa, selecione **Forçar salvamento**.

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

8. Revise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

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

Gerenciar um KMS

Gerenciar um servidor de gerenciamento de chaves (KMS) envolve visualizar ou editar detalhes, gerenciar certificados, visualizar nós criptografados e remover um KMS quando ele não for mais necessário.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissão de acesso necessária" .

Ver detalhes do KMS

Você pode visualizar informações sobre cada servidor de gerenciamento de chaves (KMS) no seu sistema StorageGRID , incluindo detalhes da chave e o status atual dos certificados do servidor e do cliente.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida e mostra as seguintes informações:

   - A guia Detalhes da configuração lista todos os servidores de gerenciamento de chaves que estão configurados.
   - A guia Nós criptografados lista todos os nós que têm a criptografia de nós habilitada.

2. Para visualizar os detalhes de um KMS específico e executar operações nesse KMS, selecione o nome do KMS. A página de detalhes do KMS lista as seguintes informações:

Campo	Descrição
Gerencia chaves para	O site StorageGRID associado ao KMS. Este campo exibe o nome de um site StorageGRID específico ou **Sites não gerenciados por outro KMS (KMS padrão).**

Campo	Descrição
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. 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 será listado junto com o número de servidores de gerenciamento de chaves adicionais no cluster. Por exemplo: `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others`. Para visualizar todos os nomes de host em um cluster, selecione um KMS e selecione **Editar** ou **Ações** > **Editar**.

3. Selecione uma guia na página de detalhes do KMS para visualizar as seguintes informações:

Aba	Campo	Descrição
Detalhes importantes	Nome da chave	O alias da chave para o cliente StorageGRID no KMS.
UID da chave	O identificador exclusivo da versão mais recente da chave.	Última modificação
Data e hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (privacy enhanced mail) do certificado.
Certificado de cliente	Metadados	Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.

4. Sempre que exigido pelas práticas de segurança da sua organização, selecione **Girar chave** ou use o software KMS para criar uma nova versão da chave.

   Quando a rotação da chave é bem-sucedida, os campos UID da chave e Última modificação são atualizados.

Se você girar a chave de criptografia usando o software KMS, gire-a da última versão usada da chave para uma nova versão da mesma chave. Não gire para uma chave totalmente diferente.

Nunca tente rotacionar uma chave alterando o nome da chave (alias) para o KMS. O StorageGRID exige que todas as versões de chaves usadas anteriormente (bem como quaisquer futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias da chave de um KMS configurado, o StorageGRID poderá não conseguir descriptografar seus dados.

Gerenciar certificados

Resolva imediatamente quaisquer problemas de certificado de servidor ou cliente. Se possível, substitua os certificados antes que eles expirem.

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.
2. Na tabela, observe o valor de Expiração do certificado para cada KMS.
3. Se a expiração do certificado para qualquer KMS for Desconhecida, aguarde até 30 minutos e atualize seu navegador.
4. Se a coluna Expiração do certificado indicar que um certificado expirou ou está próximo da expiração, selecione o KMS para acessar a página de detalhes do KMS.
   a. Selecione **Certificado do servidor** e verifique o valor do campo "Expira em".
   b. Para substituir o certificado, selecione **Editar certificado** para carregar um novo certificado.
   c. Repita essas subetapas e selecione **Certificado do cliente** em vez de Certificado do servidor.
5. Quando os alertas **Expiração do certificado da CA KMS**, **Expiração do certificado do cliente KMS** e **Expiração do certificado do servidor KMS** forem acionados, observe a descrição de cada alerta e execute as ações recomendadas.

   Pode levar até 30 minutos para o StorageGRID receber atualizações sobre a expiração do certificado. Atualize seu navegador para ver os valores atuais.

Se você receber o status **Status do certificado do servidor desconhecido**, certifique-se de que seu KMS permite obter um certificado de servidor sem exigir um certificado de cliente.

Exibir nós criptografados

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página Servidor de Gerenciamento de Chaves é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. No topo da página, selecione a aba **Nós criptografados**.

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

3. Revise as informações na tabela para cada nó do dispositivo.

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Armazenamento, Administração ou Gateway.
Site	O nome do site StorageGRID onde o nó está instalado.
Nome da 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. "Adicionar um servidor de gerenciamento de chaves (KMS)"
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para visualizar um UID de chave inteiro, selecione o texto. Um traço (--) indica que o UID da chave é desconhecido, possivelmente devido a um problema de conexão entre o nó do dispositivo e o KMS.
Status	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conectado, o registro de data e hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações na configuração do KMS. **Observação:** Atualize seu navegador para ver os novos valores.

4. Se a coluna Status indicar um problema do KMS, resolva o problema imediatamente.

   Durante as operações normais do KMS, o status será **Conectado ao KMS**. Se um nó for desconectado da rede, o estado da conexão do nó será exibido (Administrativamente inativo ou Desconhecido).

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

   - Falha ao carregar a configuração do KMS
   - Erro de conectividade do KMS
   - Nome da chave de criptografia KMS não encontrado
   - Falha na rotação da chave de criptografia do KMS
   - A chave KMS falhou ao descriptografar um volume do dispositivo
   - O KMS não está configurado

Execute as ações recomendadas para esses alertas.

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

Editar um KMS

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

Antes de começar

- Se você planeja atualizar o site selecionado para um KMS, você revisou o"considerações para alterar o KMS de um site" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página Servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja editar e selecione **Ações** > **Editar**.

   Você também pode editar um KMS selecionando o nome do KMS na tabela e selecionando **Editar** na página de detalhes do KMS.

3. Opcionalmente, atualize os detalhes na **Etapa 1 (Detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

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

Campo	Descrição
Gerencia chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione **Sites não gerenciados por outro KMS (KMS padrão)**. Esta seleção converte um KMS específico do site no KMS padrão, que será aplicado a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão. **Observação:** 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.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP para o KMS. **Observação:** O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o FQDN ou endereço IP que você inserir aqui. Caso contrário, o StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **Continuar**.

   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 **Continuar**.

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

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

   As conexões entre o servidor de gerenciamento de chaves e todos os nós do dispositivo criptografados nos sites afetados são testadas. Se todas as conexões de nós 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 uma mensagem de erro for exibida, revise os detalhes da mensagem e selecione **OK**.

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

11. Se precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Forçar salvamento**.

Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo com esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós do dispositivo que tenham 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. Revise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

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

Antes de começar

- Você revisou o"considerações e requisitos para usar um servidor de gerenciamento de chaves" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

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 habilitada.
- Você pode remover o KMS padrão se já existir um KMS específico do site para cada site que tenha nós de dispositivo com criptografia de nó habilitada.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página Servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja remover e selecione **Ações** > **Remover**.

   Você também pode remover um KMS selecionando o nome do KMS na tabela e selecionando **Remover** na página de detalhes do KMS.

3. Confirme se o seguinte é verdadeiro:
   - Você está removendo um KMS específico de um site que não tem nenhum nó de dispositivo com criptografia de nó habilitada.
   - Você está removendo o KMS padrão, mas já existe um KMS específico do site para cada site com criptografia de nó.
4. Selecione **Sim**.

   A configuração do KMS foi removida.

Informações sobre direitos autorais

Informações sobre marcas comerciais