Configurar servidores de gerenciamento de chaves

StorageGRID

NetApp
March 12, 2025

Índice

Configurar servidores de gerenciamento de chaves

Configurar servidores de gerenciamento de chaves: Visão geral

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

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

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.

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.

Configurar 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.	"Configure o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configure o StorageGRID como um cliente no KMS"
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.	"Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure 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 conetar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

```
https://docs.netapp.com/us-en/storagegrid-
appliances/installconfig/optional-enabling-node-
encryption.html["Habilite a criptografia do nó"^]Consulte para obter
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 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 conetar 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 conetarem 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 reconeta 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.

Qual versão do KMIP é suportada?

O StorageGRID é compatível com KMIP versão 1,4.

"Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"

Quais são as considerações de rede?

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.

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.

Quais versões do TLS são suportadas?

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID pode dar suporte ao protocolo TLS 1,2 ou TLS 1,3 quando faz conexões KMIP a um cluster KMS ou KMS, com base no suporte do KMS e no qual "Política TLS e SSH" você está usando.

O StorageGRID negocia o protocolo e a cifra (TLS 1,2) ou conjunto de cifra (TLS 1,3) com o KMS quando faz a conexão. Para ver quais versões de protocolo e conjuntos de cifras/cifras estão disponíveis, consulte `tlsOutbound` a seção da política TLS e SSH ativa da grade (**CONFIGURATION** > **Security Security Security Security settings**).

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 dispositivos StorageGRID e nós de dispositivo.

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

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados nos mecanismos de contêiner 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.

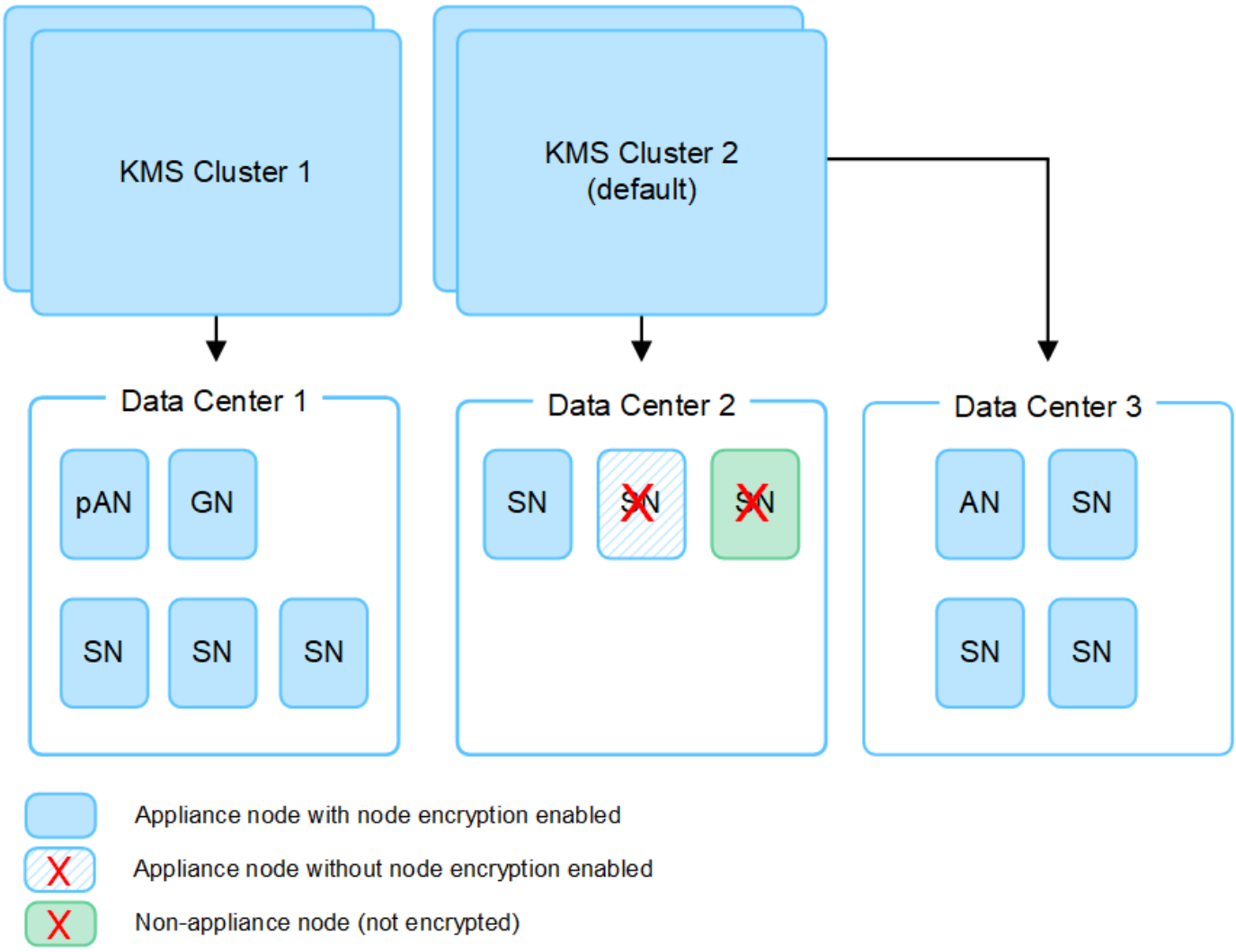
Quantos servidores de gerenciamento de chaves eu preciso?

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 não é possível 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 uma prática recomendada de segurança, você deve ser usado periodicamente "rode a chave de encriptação"por cada KMS configurado.

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** é 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 "Limpe 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.

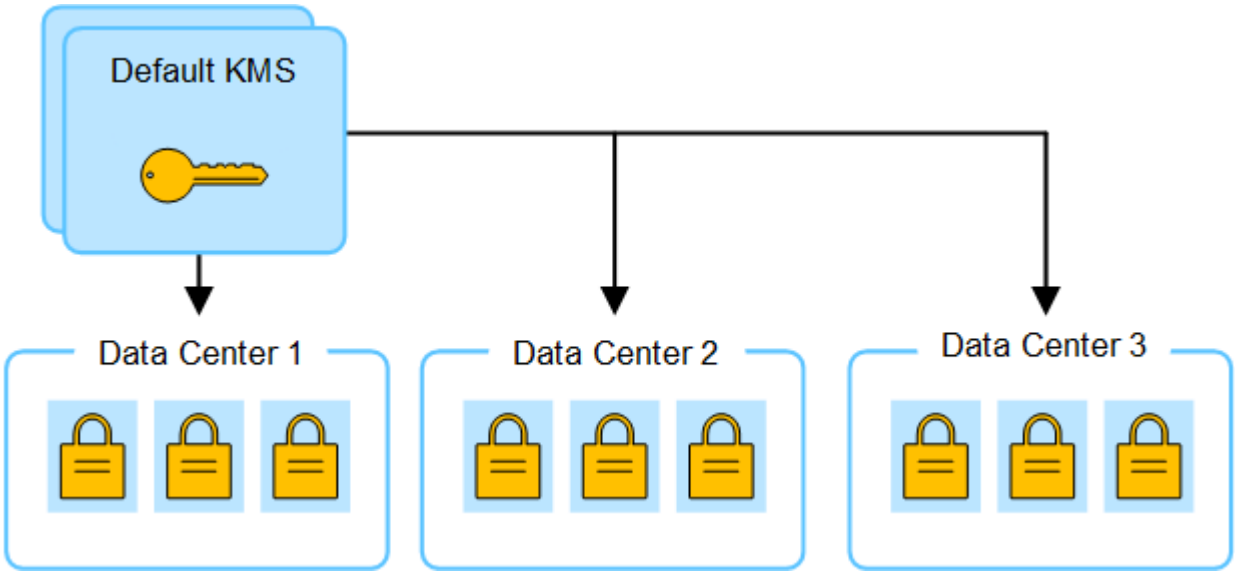
Considerações para alterar o KMS para um site

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.

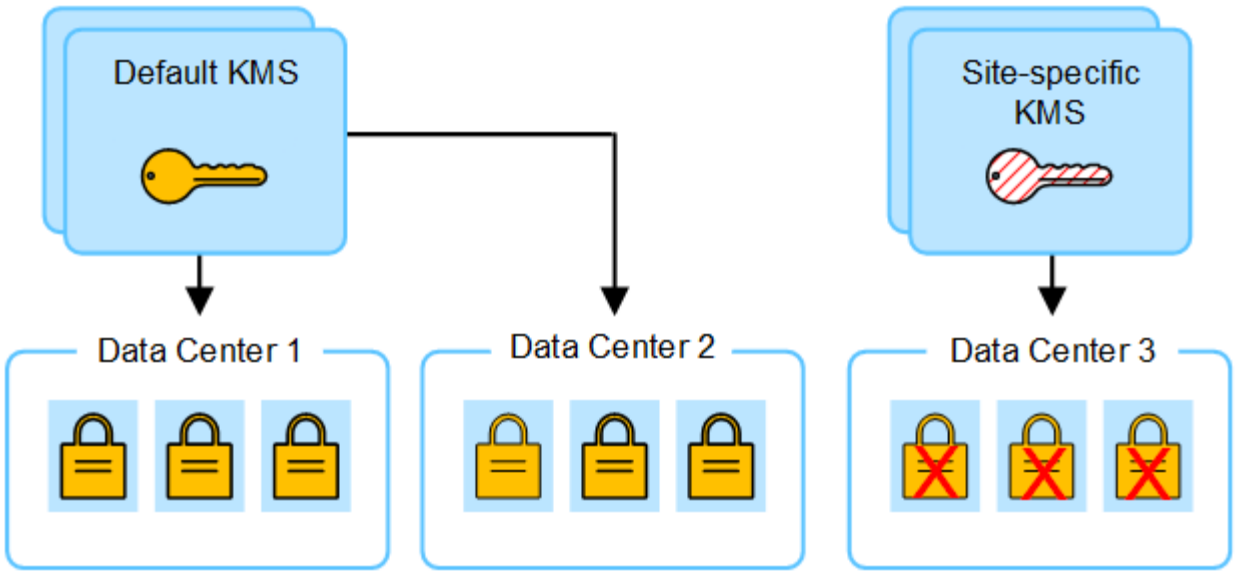
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para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

Por exemplo:

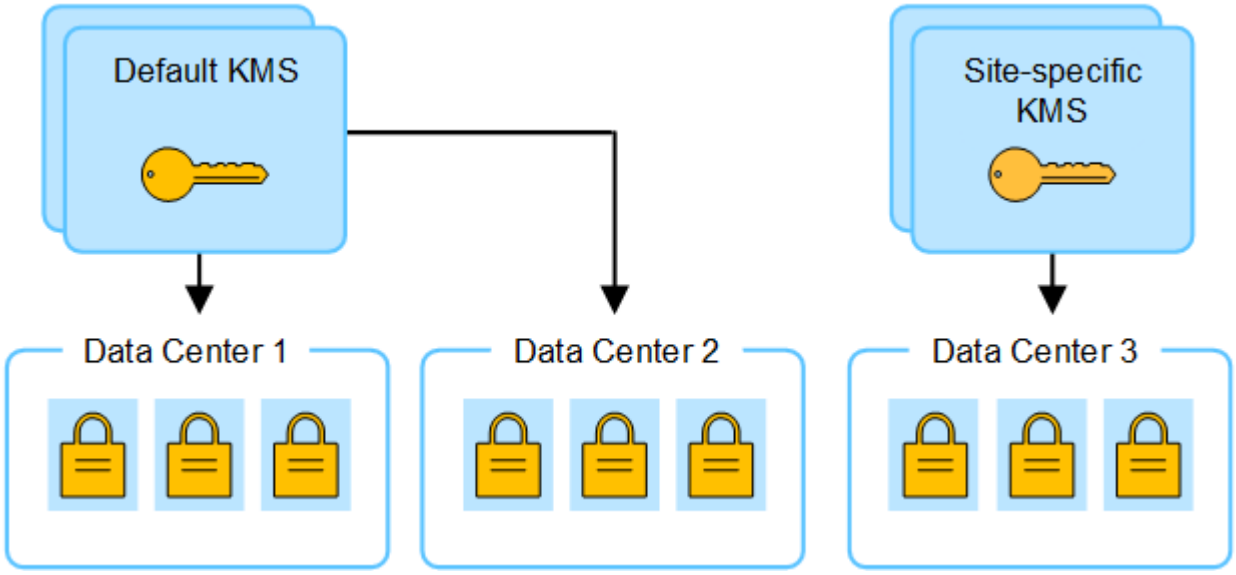
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar 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
Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como 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 se aplicará a quaisquer sites que não tenham um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"

Caso de uso para alterar o KMS de um site	Passos necessários
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 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. 2. Usando o Gerenciador de Grade, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS para um site use um servidor diferente.	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. 2. Usando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure 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 Hashicorp Vault. Para obter uma lista de produtos e versões compatíveis, use o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

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

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

   - Peça ao StorageGRID que crie a chave. Você será solicitado quando testar e salvar após "carregar certificados de cliente".
3. Registre as seguintes informações para cada cluster KMS ou KMS.

   Você precisa dessas informações quando 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 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.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você tem "Configurado o StorageGRID como um cliente no KMS", e você tem as informações necessárias para cada cluster KMS ou KMS.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

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"Consulte para obter detalhes.

Passo 1: KMS detalhes

Na Etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

A página 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
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. **Nota**: Se você não criou uma chave usando seu produto KMS, será solicitado que o StorageGRID crie a chave.
Gere as chaves para	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. • Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um local específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** 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. **Nota:** 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.
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.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar 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**.

Passo 2: Faça upload do 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. A partir de **passo 2 (carregar certificado do servidor)**, navegue até a localização do certificado ou pacote de certificados do servidor guardado.
2. Carregue o ficheiro de certificado.

   Os metadados do certificado do servidor são exibidos.

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

3. Selecione **continuar**.

Passo 3: Faça 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 de **passo 3 (carregar certificados de cliente)**, navegue até a localização do certificado de cliente.
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.
5. Selecione **testar e salvar**.

   Se uma chave não existir, você será solicitado a 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 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 **Test and save**, 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**.

> 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.

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

Gerenciar um KMS

O gerenciamento de um servidor de gerenciamento de chaves (KMS) envolve a visualização ou edição de detalhes, o gerenciamento de certificados, a visualização de nós criptografados e a remoção de um KMS quando não for mais necessário.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "permissão de acesso necessária".

Ver detalhes do KMS

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

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página 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 configurados.
   - A guia nós criptografados lista todos os nós que têm criptografia de nó ativada.

2. Para exibir 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
Gere as 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 anfitrião	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 são listados juntamente 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 exibir as seguintes informações:

Separador	Campo	Descrição
Principais detalhes	Nome da chave	O alias de chave para o cliente StorageGRID no KMS.
UID da chave	O identificador exclusivo da versão mais recente da chave.	Modificado pela última vez
A data e a 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) para o 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 **Rotate key** 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 Last modified 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 rode para uma chave totalmente diferente.

Nunca tente girar uma chave alterando o nome da chave (alias) para o 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.

Gerenciar certificados

Resolver imediatamente quaisquer problemas de certificado de servidor ou cliente. Se possível, substitua os certificados antes de expirarem.

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

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.
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, em seguida, atualize seu navegador da Web.
4. Se a coluna expiração do certificado indicar que um certificado expirou ou está prestes a expirar, selecione o KMS para ir para 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 KMS CA**, **expiração do certificado do cliente KMS** e **expiração do certificado do servidor KMS** forem acionados, anote a descrição de cada alerta e execute as ações recomendadas.

Pode demorar StorageGRID até 30 minutos para obter atualizações para a expiração do certificado. Atualize seu navegador da Web para ver os valores atuais.

Exibir 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 **CONFIGURATION** > **Security** > **Key Management Server**.

   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.

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

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

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

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Storage, Admin ou Gateway.
Local	O nome do site do StorageGRID onde o nó está instalado.
KMS nome	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 ver um UID de chave inteiro, selecione o texto. 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 conetado, 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. **Observação:** Atualize 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 desconetado 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 conetividade DE KMS
   - Nome da chave de encriptação KMS não encontrado
   - Falha na rotação da chave de CRIPTOGRAFIA KMS
   - A chave KMS falhou ao desencriptar um volume de aparelho
   - 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.

Edite um KMS

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

Antes de começar

- Se pretende atualizar o site selecionado para um KMS, analisou o "Considerações para alterar o KMS para um site".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   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 em **Etapa 1 (detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. 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.
Gere as 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 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. **Observação:** se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não será possível selecionar um site específico.

Campo	Descrição
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.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar 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 de cliente e a chave privada do certificado de 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 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.

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.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

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 **CONFIGURATION** > **Security** > **Key Management Server**.

   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 do site para um site que não tem nó de dispositivo com criptografia de nó ativada.
   - Você está removendo o KMS padrão, mas um KMS específico do site já existe para cada site com criptografia de nó.
4. Selecione **Sim**.

   A configuração do KMS é removida.

Informações sobre direitos autorais

Informações sobre marcas comerciais