



# **Gerir as definições de segurança**

## **StorageGRID**

NetApp  
March 12, 2025

# Índice

Gerir as definições de segurança .....	1
Gerenciar certificados .....	1
Sobre certificados de segurança .....	1
Configurar certificados de servidor .....	12
Configurar certificados de cliente .....	23
Configurar servidores de gerenciamento de chaves .....	32
Configurar servidores de gerenciamento de chaves: Visão geral .....	32
Reveja os métodos de encriptação StorageGRID .....	32
Visão geral do KMS e da configuração do appliance .....	35
Considerações e requisitos para usar um servidor de gerenciamento de chaves .....	39
Considerações para alterar o KMS para um site .....	42
Configure o StorageGRID como um cliente no KMS .....	45
Adicionar um servidor de gerenciamento de chaves (KMS) .....	46
Ver detalhes do KMS .....	54
Exibir nós criptografados .....	56
Editar um servidor de gerenciamento de chaves (KMS) .....	58
Remover um servidor de gerenciamento de chaves (KMS) .....	61
Gerenciar configurações de proxy .....	62
Configure as configurações de proxy de armazenamento .....	62
Configure as configurações do proxy Admin .....	63
Gerenciar redes de clientes não confiáveis .....	65
Gerenciar redes de clientes não confiáveis: Visão geral .....	65
Especificar rede cliente do nó não é confiável .....	65

# Gerir as definições de segurança

## Gerenciar certificados

### Sobre certificados de segurança

Certificados de segurança são pequenos arquivos de dados usados para criar conexões seguras e confiáveis entre componentes do StorageGRID e entre componentes do StorageGRID e sistemas externos.

O StorageGRID usa dois tipos de certificados de segurança:

- **Certificados de servidor** são necessários quando você usa conexões HTTPS. Os certificados de servidor são usados para estabelecer conexões seguras entre clientes e servidores, autenticando a identidade de um servidor para seus clientes e fornecendo um caminho de comunicação seguro para os dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam uma identidade de cliente ou usuário no servidor, fornecendo autenticação mais segura do que senhas sozinhas. Os certificados de cliente não encriptam dados.

Quando um cliente se conecta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

O StorageGRID funciona como o servidor para algumas conexões (como o endpoint do balanceador de carga) ou como o cliente para outras conexões (como o serviço de replicação do CloudMirror).

- Certificado padrão de CA de grade\*

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado interno da CA de grade durante a instalação do sistema. O certificado de CA de grade é usado, por padrão, para proteger o tráfego interno do StorageGRID. Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora seja possível usar o certificado da CA de Grade para um ambiente que não seja de produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não protegidas sem certificado também são suportadas, mas não são recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser os especificados para verificar conexões de servidor.
- Todos os certificados personalizados devem atender aos [diretrizes de endurecimento do sistema](#) certificados do servidor para.
- O StorageGRID oferece suporte ao agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados da CA).



O StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todas as grades. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa em vez do certificado CA do sistema operacional.

Variantes dos tipos de certificado de servidor e cliente são implementadas de várias maneiras. Você deve ter

todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

## Acesse certificados de segurança

Você pode acessar informações sobre todos os certificados do StorageGRID em um único local, juntamente com links para o fluxo de trabalho de configuração de cada certificado.

1. No Gerenciador de Grade, selecione **CONFIGURATON > Segurança > certificados**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global Grid CA Client Load balancer endpoints Tenants Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type	Expiration date
<a href="#">Management interface certificate</a>	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
<a href="#">S3 and Swift API certificate</a>	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Selecione uma guia na página certificados para obter informações sobre cada categoria de certificado e para acessar as configurações de certificado. Você só pode acessar uma guia se tiver a permissão apropriada.

- \* **Global\***: Protege o acesso à StorageGRID de navegadores da web e clientes de API externos.
- \* **Grade CA\***: Protege o tráfego interno do StorageGRID.
- **Cliente**: Protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
- \* **Terminais de balanceador de carga\***: Protege conexões entre clientes S3 e Swift e o balanceador de carga StorageGRID.
- \* **Inquilinos\***: Protege conexões com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de armazenamento S3.
- **Outros**: Protege conexões StorageGRID que exigem certificados específicos.

Cada guia é descrito abaixo com links para detalhes adicionais do certificado.

## Global

Os certificados globais protegem o acesso à StorageGRID a partir de navegadores da Web e clientes externos da API S3 e Swift. Dois certificados globais são inicialmente gerados pela autoridade de certificação StorageGRID durante a instalação. A prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

- [Certificado de interface de gerenciamento](#): Protege as conexões do navegador da Web do cliente às interfaces de gerenciamento do StorageGRID.
- [Certificado API S3 e Swift](#): Protege as conexões da API do cliente aos nós de storage, nós de administração e nós de gateway, que os aplicativos clientes S3 e Swift usam para carregar e baixar dados de objetos.

As informações sobre os certificados globais instalados incluem:

- **Nome**: Nome do certificado com link para gerenciar o certificado.
- **Descrição**
- **Tipo**: Personalizado ou padrão. Você deve sempre usar um certificado personalizado para melhorar a segurança da grade.
- **Data de expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
  - [Substitua o certificado padrão da interface de gerenciamento gerado pelo StorageGRID](#) Usado para conexões do Grid Manager e do Tenant Manager.
  - [Substitua o certificado API S3 e Swift](#) Usado para conexões de nó de armazenamento, serviço CLB (obsoleto) e terminais de balanceador de carga (opcional).
- [Restaure o certificado padrão da interface de gerenciamento](#).
- [Restaure o certificado padrão da API S3 e Swift](#).
- [Use um script para gerar um novo certificado de interface de gerenciamento autoassinado](#).
- Copie ou transfira a [certificado de interface de gerenciamento](#) ou [Certificado API S3 e Swift](#).

## CA da grelha

O [Certificado CA de grade](#), gerado pela autoridade de certificação StorageGRID durante a instalação do StorageGRID, protege todo o tráfego interno do StorageGRID.

As informações do certificado incluem a data de validade do certificado e o conteúdo do certificado.

Você pode [Copie ou baixe o certificado da CA de Grade](#), mas não pode alterá-lo.

## Cliente

[Certificados de cliente](#), Gerado por uma autoridade de certificação externa, proteja as conexões entre ferramentas de monitoramento externas e o banco de dados do StorageGRID Prometheus.

A tabela de certificados tem uma linha para cada certificado de cliente configurado e indica se o certificado pode ser usado para acesso ao banco de dados Prometheus, juntamente com a data de validade do certificado.

Você pode:

- [Carregue ou gere um novo certificado de cliente.](#)
- Selecione um nome de certificado para exibir os detalhes do certificado onde você pode:
  - [Altere o nome do certificado do cliente.](#)
  - [Defina a permissão de acesso Prometheus.](#)
  - [Carregue e substitua o certificado do cliente.](#)
  - [Copie ou baixe o certificado do cliente.](#)
  - [Remova o certificado do cliente.](#)
- Selecione **ações** para rapidamente [editar](#), [fixe](#), ou [retire](#) um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los ao mesmo tempo usando **ações** > **Remover**.

### Pontos de extremidade do balanceador de carga

[Certificados de terminais do balanceador de carga](#), Que você carrega ou gera, proteja as conexões entre clientes S3 e Swift e o serviço de balanceamento de carga StorageGRID em nós de gateway e nós de administração.

A tabela de endpoint do balanceador de carga tem uma linha para cada endpoint do balanceador de carga configurado e indica se o certificado global S3 e Swift API ou um certificado de endpoint do balanceador de carga personalizado está sendo usado para o endpoint. A data de validade de cada certificado também é exibida.



As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- [Selecione um nome de endpoint para abrir uma guia do navegador com informações sobre o endpoint do balanceador de carga, incluindo os detalhes do certificado.](#)
- [Especifique um certificado de endpoint do balanceador de carga para o FabricPool.](#)
- [Use o certificado global S3 e Swift API](#) em vez de gerar um novo certificado de endpoint do balanceador de carga.

### Inquilinos

Os locatários podem usar [certificados de servidor de federação de identidade](#) ou [certificados de endpoint de serviço de plataforma](#) proteger suas conexões com o StorageGRID.

A tabela de locatário tem uma linha para cada locatário e indica se cada locatário tem permissão para usar sua própria fonte de identidade ou serviços de plataforma.

Você pode:

- [Selecione um nome de locatário para iniciar sessão no Gestor de inquilinos](#)
- [Selecione um nome de locatário para exibir os detalhes da federação de identidade do locatário](#)
- [Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma do locatário](#)
- [Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint](#)

### Outros

O StorageGRID usa outros certificados de segurança para fins específicos. Estes certificados são listados pelo seu nome funcional. Outros certificados de segurança incluem:

- [Certificados de federação de identidade](#)
- [Certificados do Cloud Storage Pool](#)
- [Certificados de servidor de gerenciamento de chaves \(KMS\)](#)
- [Certificados de logon único](#)
- [Certificados de notificação de alerta por e-mail](#)
- [Certificados de servidor syslog externos](#)

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração do certificado do servidor e do cliente, conforme aplicável. A seleção de um nome de função abre uma guia do navegador onde você pode exibir e editar os detalhes do certificado.



Você só pode exibir e acessar informações de outros certificados se tiver a permissão apropriada.

Você pode:

- [Exibir e editar um certificado de federação de identidade](#)
- [Carregar certificados de servidor de gerenciamento de chaves \(KMS\) e cliente](#)
- [Especifique um certificado do Cloud Storage Pool para S3, C2S S3 ou Azure](#)
- [Especifique manualmente um certificado SSO para confiança de parte confiável](#)
- [Especifique um certificado para notificações por e-mail de alerta](#)
- [Especifique um certificado de servidor syslog externo](#)

## Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para artigos que contêm instruções de implementação.

### Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	<p>Autentica a conexão entre navegadores da Web cliente e a interface de gerenciamento do StorageGRID, permitindo que os usuários acessem o Gerenciador de Grade e o Gerenciador de locatário sem avisos de segurança.</p> <p>Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário.</p> <p>Pode utilizar o certificado predefinido criado durante a instalação ou carregar um certificado personalizado.</p>	<b>CONFIGURATION &gt; Security &gt; Certificates</b> , selecione a guia <b>Global</b> e, em seguida, selecione <b>Management interface certificate</b>	<a href="#">Configurar certificados de interface de gerenciamento</a>

#### Certificado API S3 e Swift

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 ou Swift a um nó de armazenamento, ao serviço CLB (Connection Load Balancer) obsoleto em um nó de gateway e terminais de balanceador de carga (opcional).	<b>CONFIGURATION &gt; Security &gt; Certificates</b> , selecione a guia <b>Global</b> e, em seguida, selecione <b>S3 e Swift API certificate</b>	<a href="#">Configure os certificados API S3 e Swift</a>

#### Certificado CA de grade

Consulte [Descrição do certificado da CA de Grade padrão](#).

#### Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	<p>Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de cliente externo.</p> <ul style="list-style-type: none"> <li>• Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus.</li> <li>• Permite o monitoramento seguro do StorageGRID usando ferramentas externas.</li> </ul>	<p><b>CONFIGURATION &gt; Security &gt; Certificates</b> e selecione a guia <b>Client</b></p>	<p><a href="#">Configurar certificados de cliente</a></p>

**Certificado de ponto final do balanceador de carga**

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	<p>Autentica a conexão entre clientes S3 ou Swift e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração. Você pode fazer upload ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos clientes usam o certificado do balanceador de carga ao se conectar ao StorageGRID para salvar e recuperar dados de objeto.</p> <p>Você também pode usar uma versão personalizada do certificado global <a href="#">Certificado API S3 e Swift</a> para autenticar conexões com o serviço Load Balancer. Se o certificado global for usado para autenticar conexões do balanceador de carga, você não precisará carregar ou gerar um certificado separado para cada ponto de extremidade do balanceador de carga.</p> <p><b>Nota:</b> o certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID.</p>	<b>CONFIGURATION &gt; Network &gt; Load balancer endpoints</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configurar pontos de extremidade do balanceador de carga</a></li> <li>• <a href="#">Crie um ponto de extremidade do balanceador de carga para o FabricPool</a></li> </ul>

#### Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre o StorageGRID e um provedor de identidade externo, como ative Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, que permite que grupos de administração e usuários sejam gerenciados por um sistema externo.	<b>CONFIGURATION &gt; Access Control &gt; Identity Federation</b>	<a href="#">Use a federação de identidade</a>

#### Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID a um recurso de storage S3.	<b>Gerenciador do Locatário &gt; ARMAZENAMENTO (S3) &gt; terminais de serviços da plataforma</b>	<a href="#">Criar endpoint de serviços de plataforma</a> <a href="#">Editar endpoint de serviços de plataforma</a>

#### Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de storage de nuvem do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	<b>ILM &gt; conjuntos de armazenamento</b>	<a href="#">Crie um pool de storage em nuvem</a>

#### Certificado de servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre o StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID.	<b>CONFIGURATION &gt; Security &gt; Key Management Server</b>	<a href="#">Adicionar servidor de gerenciamento de chaves (KMS)</a>

#### Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como AD FS (Serviços de Federação do Active Directory) e StorageGRID usados para solicitações de logon único (SSO).	<b>CONFIGURATION &gt; access control &gt; Single sign-on</b>	<a href="#">Configurar o logon único</a>

#### Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	<p>Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta.</p> <ul style="list-style-type: none"> <li>• Se as comunicações com o servidor SMTP exigirem TLS (Transport Layer Security), você deverá especificar o certificado CA do servidor de e-mail.</li> <li>• Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.</li> </ul>	<b>ALERTAS &gt; Configuração do e-mail</b>	<a href="#">Configurar notificações por e-mail para alertas</a>

#### Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	<p>Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que Registra eventos no StorageGRID.</p> <p><b>Nota:</b> não é necessário um certificado de servidor syslog externo para conexões TCP, RELP/TCP e UDP a um servidor syslog externo.</p>	<b>CONFIGURATION &gt; Monitoring &gt; Audit and syslog Server</b> e selecione <b>Configure External syslog Server</b>	<a href="#">Configurar um servidor syslog externo</a>

#### Exemplos de certificados

##### Exemplo 1: Serviço do Load Balancer

Neste exemplo, o StorageGRID atua como servidor.

1. Você configura um ponto de extremidade do balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.
2. Você configura uma conexão de cliente S3 ou Swift para o endpoint do balanceador de carga e carrega o mesmo certificado para o cliente.

3. Quando o cliente deseja salvar ou recuperar dados, ele se conecta ao endpoint do balanceador de carga usando HTTPS.
4. O StorageGRID responde com o certificado do servidor, que contém uma chave pública e com uma assinatura baseada na chave privada.
5. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados de objeto para o StorageGRID.

### **Exemplo 2: Servidor de gerenciamento de chaves externas (KMS)**

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software servidor de gerenciamento de chaves externo, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado pela CA, um certificado de cliente público e a chave privada para o certificado de cliente.
2. Usando o Gerenciador de Grade, você configura um servidor KMS e carrega os certificados de servidor e cliente e a chave privada do cliente.
3. Quando um nó StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura com base na chave privada.
4. O servidor KMS valida a assinatura do certificado e decide que pode confiar no StorageGRID.
5. O servidor KMS responde usando a conexão validada.

## **Configurar certificados de servidor**

### **Tipos de certificado de servidor suportados**

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (algoritmo de assinatura digital de curva elítica).

Para obter mais informações sobre como o StorageGRID protege conexões de clientes para a API REST, [Use S3](#) consulte ou [Use Swift](#).

### **Configurar certificados de interface de gerenciamento**

Você pode substituir o certificado de interface de gerenciamento padrão por um único certificado personalizado que permite que os usuários acessem o Gerenciador de Grade e o Gerenciador do locatário sem encontrar avisos de segurança. Você também pode reverter para o certificado de interface de gerenciamento padrão ou gerar um novo.

#### **Sobre esta tarefa**

Por padrão, cada nó de administrador é emitido um certificado assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento personalizado comum e uma chave privada correspondente.

Como um único certificado de interface de gerenciamento personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conectar ao Gerenciador de Grade e ao Gerenciador de locatário. Defina o certificado personalizado de modo que corresponda a todos os nós de administração na grade.

Você precisa concluir a configuração no servidor e, dependendo da autoridade de certificação raiz (CA) que você está usando, os usuários também podem precisar instalar o certificado de CA de grade no navegador da Web que eles usarão para acessar o Gerenciador de Grade e o Gerenciador de locatário.



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Management Interface** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION > Security > Certificates** e observando a data de validade do certificado da interface de gerenciamento na guia Global.



Se você estiver acessando o Gerenciador de Grade ou o Gerenciador de locatário usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se uma das seguintes situações ocorrer:

- O certificado de interface de gerenciamento personalizado expira.
- [reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão](#) Você .

#### **Adicione um certificado de interface de gerenciamento personalizado**

Para adicionar um certificado de interface de gerenciamento personalizado, você pode fornecer seu próprio certificado ou gerar um usando o Gerenciador de Grade.

#### **Passos**

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

## Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor:** O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado:** O arquivo de chave privada de certificado de servidor personalizado (.key).



As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

## Gerar certificado

Gere os ficheiros de certificado do servidor.



A prática recomendada para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado assinado por uma autoridade de certificação externa.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

- **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um \* como um curinga para representar vários nomes de domínio.
- **IP:** Um ou mais endereços IP a incluir no certificado.
- **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
- **Dias válidos:** Número de dias após a criação em que o certificado expira.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

5. Atualize a página para garantir que o navegador da Web seja atualizado.



Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página de certificado de interface de gerenciamento exibe informações detalhadas de certificado para os certificados que estão em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

#### Restaure o certificado padrão da interface de gerenciamento

Você pode reverter para o uso do certificado de interface de gerenciamento padrão para conexões do Gerenciador de Grade e do Gerenciador de Tenant.

#### Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **Use default certificate** (usar certificado padrão).

Quando você restaura o certificado de interface de gerenciamento padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado de interface de gerenciamento padrão é usado para todas as novas conexões de cliente subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

#### Use um script para gerar um novo certificado de interface de gerenciamento autoassinado

Se for necessária uma validação estrita do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

#### O que você vai precisar

- Você tem permissões de acesso específicas.
- Você tem o `Passwords.txt` arquivo.

#### Sobre esta tarefa

A melhor prática para um ambiente de produção é usar um certificado assinado por uma autoridade de certificação externa.

## Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó Admin.
2. Faça login no nó de administração principal:
  - a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
  - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
  - c. Digite o seguinte comando para mudar para root: `su -`
  - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

3. Configure o StorageGRID com um novo certificado autoassinado.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Para `--domains`, use curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração. Por exemplo, `*.ui.storagegrid.example.com` usa o caractere curinga `*` para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Defina `--type` como `management` para configurar o certificado da interface de gerenciamento, que é usado pelo Gerenciador de Grade e pelo Gerenciador de Locatário.
- Por padrão, os certificados gerados são válidos por um ano (365 dias) e devem ser recriados antes de expirarem. Você pode usar o `--days` argumento para substituir o período de validade padrão.



O período de validade de um certificado começa quando `make-certificate` é executado. Você deve garantir que o cliente de gerenciamento esteja sincronizado com a mesma fonte de tempo que o StorageGRID; caso contrário, o cliente poderá rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

A saída resultante contém o certificado público necessário pelo cliente da API de gerenciamento.

4. Selecione e copie o certificado.

Inclua as tags DE INÍCIO e FIM em sua seleção.

5. Faça logout do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
  - a. Acesse o Gerenciador de Grade.
  - b. Selecione **CONFIGURATION > Security > Certificates**
  - c. Na guia **Global**, selecione **certificado de interface de gerenciamento**.

7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

#### Transfira ou copie o certificado da interface de gestão

Você pode salvar ou copiar o conteúdo do certificado da interface de gerenciamento para uso em outro lugar.

#### Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

#### Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA .pem. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

#### Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

#### Configure os certificados API S3 e Swift

Você pode substituir ou restaurar o certificado do servidor usado para conexões de cliente S3 ou Swift para nós de armazenamento, o serviço CLB (Connection Load Balancer) obsoleto em nós de Gateway ou para carregar pontos de extremidade do balanceador. O certificado de servidor personalizado de substituição é específico para a sua organização.

## Sobre esta tarefa

Por padrão, cada nó de armazenamento é emitido um certificado de servidor X,509 assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os nós de armazenamento, portanto, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conectar ao endpoint de armazenamento. Defina o certificado personalizado de modo que corresponda a todos os nós de storage na grade.

Depois de concluir a configuração no servidor, você também pode precisar instalar o certificado de CA de Grade no cliente API S3 ou Swift que você usará para acessar o sistema, dependendo da autoridade de certificação raiz (CA) que você estiver usando.



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of global Server certificate for S3 and Swift API** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION > Security > Certificates** e observando a data de expiração do certificado API S3 e Swift na guia Global.

Você pode fazer upload ou gerar um certificado personalizado de API S3 e Swift.

### Adicione um certificado personalizado de API S3 e Swift

#### Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

## Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

- a. Selecione **carregar certificado**.
- b. Carregue os ficheiros de certificado do servidor necessários:
  - **Certificado de servidor:** O arquivo de certificado de servidor personalizado (codificado PEM).
  - **Chave privada de certificado:** O arquivo de chave privada de certificado de servidor personalizado (.key).



As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.
- c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado personalizado da API S3 e Swift que foi carregado. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

- d. Selecione **Guardar**.

O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

## Gerar certificado

Gere os ficheiros de certificado do servidor.

- a. Selecione **Generate certificate** (gerar certificado).
- b. Especifique as informações do certificado:
  - **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um \* como um curinga para representar vários nomes de domínio.
  - **IP:** Um ou mais endereços IP a incluir no certificado.
  - **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
  - **Dias válidos:** Número de dias após a criação em que o certificado expira.
- c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para exibir os metadados e o PEM para o certificado personalizado da API S3 e Swift que foi gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**.

O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

5. Selecione uma guia para exibir metadados para o certificado padrão do servidor StorageGRID, um certificado assinado pela CA que foi carregado ou um certificado personalizado que foi gerado.



Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Atualize a página para garantir que o navegador da Web seja atualizado.

7. Depois de adicionar um certificado personalizado de API S3 e Swift, a página de certificado de API S3 e Swift exibe informações detalhadas de certificado para o certificado personalizado de API S3 e Swift que está em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

### Restaure o certificado padrão da API S3 e Swift

Você pode reverter para o uso do certificado padrão S3 e Swift API para conexões de clientes S3 e Swift para nós de armazenamento e para o serviço CLB obsoleto em nós de Gateway. No entanto, você não pode usar o certificado padrão S3 e Swift API para um endpoint de balanceador de carga.

### Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **Use default certificate** (usar certificado padrão).

Quando você restaura a versão padrão do certificado global S3 e Swift API, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 e Swift será usado para novas conexões de cliente S3 e Swift subsequentes para nós de armazenamento e para o serviço CLB obsoleto em nós de Gateway.

4. Selecione **OK** para confirmar o aviso e restaurar o certificado padrão da API S3 e Swift.

Se você tiver permissão de acesso root e o certificado personalizado S3 e Swift API foi usado para conexões de endpoint do balanceador de carga, uma lista será exibida de endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado padrão S3 e Swift API. Acesse a [Configurar pontos de extremidade do balanceador de carga](#) para editar ou remover os endpoints afetados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

#### Faça o download ou copie o certificado API S3 e Swift

Você pode salvar ou copiar o conteúdo do certificado S3 e Swift API para uso em outro lugar.

#### Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

#### Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA .pem. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

#### Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

#### Informações relacionadas

- [Use S3](#)
- [Use Swift](#)
- [Configure os nomes de domínio de endpoint da API S3](#)

#### Copie o certificado da CA de Grade

O StorageGRID usa uma autoridade de certificação interna (CA) para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

## O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

## Sobre esta tarefa

Se um certificado de servidor personalizado tiver sido configurado, os aplicativos cliente devem verificar o servidor usando o certificado de servidor personalizado. Eles não devem copiar o certificado da CA do sistema StorageGRID.

## Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Grid CA**.
2. Na seção **Certificate PEM**, baixe ou copie o certificado.

### Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

- a. Selecione **Baixar certificado**.
- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

### Copiar certificado PEM

Copie o texto do certificado para colar em outro lugar.

- a. Selecione **Copiar certificado PEM**.
- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

## Configurar certificados StorageGRID para FabricPool

Para clientes S3 que executam validação estrita de nome de host e não suportam a desativação estrita de validação de nome de host, como clientes ONTAP que usam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o ponto de extremidade do balanceador de carga.

## O que você vai precisar

- Você tem permissões de acesso específicas.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

## Sobre esta tarefa

Ao criar um endpoint de balanceador de carga, você pode gerar um certificado de servidor autoassinado ou carregar um certificado assinado por uma autoridade de certificação (CA) conhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA conhecida. Os certificados assinados por uma

CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam FabricPool. Para obter informações e procedimentos mais detalhados, [Configurar o StorageGRID para FabricPool](#) consulte .



O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é recomendado para uso com o FabricPool.

## Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso do FabricPool.
2. Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

Quando você cria um endpoint do balanceador de carga HTTPS, é solicitado que você carregue o certificado do servidor, a chave privada do certificado e o pacote opcional da CA.

3. Anexar o StorageGRID como uma categoria de nuvem no ONTAP.

Especifique a porta de endpoint do balanceador de carga e o nome de domínio totalmente qualificado usado no certificado da CA que você carregou. Em seguida, forneça o certificado CA.



Se uma CA intermediária tiver emitido o certificado StorageGRID, você deverá fornecer o certificado de CA intermediário. Se o certificado StorageGRID tiver sido emitido diretamente pela CA raiz, você deverá fornecer o certificado CA raiz.

## Configurar certificados de cliente

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus, fornecendo uma maneira segura para que ferramentas externas monitorem o StorageGRID.

Se você precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deve carregar ou gerar um certificado de cliente usando o Gerenciador de Grade e copiar as informações do certificado para a ferramenta externa.

Consulte as informações sobre [uso geral do certificado de segurança](#) e [configurando certificados de servidor personalizados](#).



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **expiração de certificados de cliente configurados na página certificados** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION > Security > Certificates** e observando a data de validade do certificado do cliente na guia Client.



Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivo especialmente configurados, consulte as informações específicas sobre [Carregar um certificado de cliente KMS](#)o .

## O que você vai precisar

- Você tem permissão de acesso root.

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Para configurar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.
  - Se tiver configurado o certificado da interface de gerenciamento do StorageGRID, você terá a CA, o certificado do cliente e a chave privada usadas para configurar o certificado da interface de gerenciamento.
  - Para carregar o seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
  - A chave privada deve ter sido salva ou gravada no momento em que foi criada. Se você não tiver a chave privada original, você deve criar uma nova.
- Para editar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.
  - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no computador local.

### Adicionar certificados de cliente

Siga o procedimento para o seu cenário para adicionar um certificado de cliente:

- [Certificado de interface de gerenciamento já configurado](#)
- [Certificado de cliente emitido pela CA](#)
- [Certificado gerado pelo Grid Manager](#)

#### Certificado de interface de gerenciamento já configurado

Use este procedimento para adicionar um certificado de cliente se um certificado de interface de gerenciamento já estiver configurado usando uma CA fornecida pelo cliente, um certificado de cliente e uma chave privada.

#### Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
5. Na seção **tipo de certificado**, carregue o arquivo de certificado da interface de gerenciamento `.pem`.
  - a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
  - b. Carregar o ficheiro de certificado da interface de gestão (`.pem`).
    - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
    - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
  - c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

6. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.

a. **Nome:** Insira um nome para a conexão.

O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

b. **URL:** Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

Por exemplo: `https://admin-node.example.com:9091`

c. Ative **TLS Client Auth** e **com CA Cert**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole

- A interface de gerenciamento certificado CA para **CA Cert**
- O certificado de cliente para **Cert de cliente**
- A chave privada para **chave do cliente**

e. **ServerName:** Insira o nome de domínio do nó Admin.

Servername deve corresponder ao nome de domínio como aparece no certificado da interface de gerenciamento.

f. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

Agora você pode acessar as métricas Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

Para obter informações sobre as métricas, consulte o [Instruções para monitorar o StorageGRID](#).

### Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use um certificado de cliente emitido pela CA e uma chave privada.

### Passos

1. Execute as etapas para [configurar um certificado de interface de gerenciamento](#).
2. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
3. Selecione **Adicionar**.
4. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
6. Na seção **tipo de certificado**, carregue o certificado do cliente, a chave privada e os arquivos do pacote CA `.pem`:
  - a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
  - b. Carregar ficheiros de certificado de cliente, chave privada e pacote CA (`.pem`).
    - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

Os novos certificados aparecem na guia Cliente.

7. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.

- a. **Nome:** Insira um nome para a conexão.

O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

- b. **URL:** Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

Por exemplo: `https://admin-node.example.com:9091`

- c. Ative **TLS Client Auth** e **com CA Cert**.

- d. Em Detalhes de autenticação TLS/SSL, copie e cole

- A interface de gerenciamento certificado CA para **CA Cert**
- O certificado de cliente para **Cert de cliente**
- A chave privada para **chave do cliente**

- e. **ServerName:** Insira o nome de domínio do nó Admin.

Servername deve corresponder ao nome de domínio como aparece no certificado da interface de gerenciamento.

- f. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

Agora você pode acessar as métricas Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

Para obter informações sobre as métricas, consulte o [Instruções para monitorar o StorageGRID](#).

### Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use a função gerar certificado no Gerenciador de Grade.

### Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
5. Na seção **tipo de certificado**, selecione **gerar certificado**.
6. Especifique as informações do certificado:
  - **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados do nó de administrador a

incluir no certificado. Use um \* como um curinga para representar vários nomes de domínio.

- **IP:** Um ou mais endereços IP de nó de administrador a incluir no certificado.
- **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.

7. Selecione **Generate**.

8. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.



Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

Especifique o nome do arquivo de chave privada e o local de download.

9. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

10. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Global**.

11. Selecione **certificado de interface de gestão**.

12. Selecione **usar certificado personalizado**.

13. Carregue os arquivos `certificate.pem` e `private_key.pem` da [detalhes do certificado do cliente](#) etapa. Não há necessidade de carregar o pacote CA.

- Selecione **carregar certificado** e, em seguida, selecione **continuar**.
- Carregar cada ficheiro de certificado (`.pem`).
- Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

14. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.

a. **Nome:** Insira um nome para a conexão.

O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

b. **URL:** Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

Por exemplo: `https://admin-node.example.com:9091`

c. Ative **TLS Client Auth** e com **CA Cert**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole

- O certificado de cliente de interface de gerenciamento para **CA Cert** e **Client Cert**
- A chave privada para **chave do cliente**

e. **ServerName**: Insira o nome de domínio do nó Admin.

Servername deve corresponder ao nome de domínio como aparece no certificado da interface de gerenciamento.

f. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

Agora você pode acessar as métricas Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

Para obter informações sobre as métricas, consulte o [Instruções para monitorar o StorageGRID](#).

## Editar certificados de cliente

Você pode editar um certificado de cliente administrador para alterar seu nome, ativar ou desativar o acesso Prometheus ou carregar um novo certificado quando o atual expirar.

### Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.

As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.

3. Selecione **Editar** e, em seguida, selecione **Editar nome e permissão**

4. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.

5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.

6. Selecione **continuar** para salvar o certificado no Gerenciador de Grade.

O certificado atualizado é exibido na guia Cliente.

## Anexar novo certificado de cliente

Você pode carregar um novo certificado quando o atual expirar.

### Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.

As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.

3. Selecione **Editar** e, em seguida, selecione uma opção de edição.

## Carregar certificado

Copie o texto do certificado para colar em outro lugar.

- a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
- b. Carregue o nome do certificado do cliente (.pem).

Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: storagegrid\_certificate.pem

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O certificado atualizado é exibido na guia Cliente.

## Gerar certificado

Gere o texto do certificado para colar em outro lugar.

- a. Selecione **Generate certificate** (gerar certificado).
- b. Especifique as informações do certificado:

- **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um \* como um curinga para representar vários nomes de domínio.
- **IP:** Um ou mais endereços IP a incluir no certificado.
- **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
- **Dias válidos:** Número de dias após a criação em que o certificado expira.

- c. Selecione **Generate**.

- d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.



Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: storagegrid\_certificate.pem

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

Especifique o nome do arquivo de chave privada e o local de download.

e. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

## Baixar ou copie certificados de cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro lugar.

### Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende copiar ou transferir.
3. Baixe ou copie o certificado.

#### Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

- a. Selecione **Baixar certificado**.
- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

#### Copiar certificado

Copie o texto do certificado para colar em outro lugar.

- a. Selecione **Copiar certificado PEM**.
- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

## Remover certificados de cliente

Se você não precisar mais de um certificado de cliente administrador, poderá removê-lo.

### Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende remover.

3. Selecione **Delete** e confirme.



Para remover até 10 certificados, selecione cada certificado a ser removido na guia Cliente e selecione **ações > Excluir**.

Depois que um certificado é removido, os clientes que usaram o certificado devem especificar um novo certificado de cliente para acessar o banco de dados do StorageGRID Prometheus.

## 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 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.

### Reveja 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	<p>Você configura um servidor de gerenciamento de chaves para o site StorageGRID (<b>CONFIGURATION &gt; Security &gt; Key Management Server</b>) e habilita 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.</p>	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>O gerenciamento de chaves de criptografia com um KMS só é compatível com nós de storage e dispositivos de serviços.</p> </div>
Conduza a segurança no Gerenciador de sistemas do SANtricity	<p>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.</p>	<p>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.</p> <ul style="list-style-type: none"> <li>• <a href="#">SG6000 dispositivos de armazenamento</a></li> <li>• <a href="#">SG5700 dispositivos de armazenamento</a></li> <li>• <a href="#">SG5600 dispositivos de armazenamento</a></li> </ul>
Opção de grade de criptografia de objetos armazenados	<p>A opção <b>Stored Object Encryption</b> pode ser ativada no Grid Manager (<b>CONFIGURATION &gt; System &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.</p>	<p>Dados de objeto S3 e Swift recém-ingeridos.</p> <p>Os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <ul style="list-style-type: none"> <li>• <a href="#">Configurar a criptografia de objeto armazenado</a></li> </ul>

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de bucket do S3	<p>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.</p>	<p>Somente dados de objeto S3 recém-ingeridos.</p> <p>A criptografia deve ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <ul style="list-style-type: none"> <li>• <a href="#">Use S3</a></li> </ul>
Criptografia do lado do servidor de objetos S3 (SSE)	<p>Você emite uma solicitação S3 para armazenar um objeto e incluir o <code>x-amz-server-side-encryption</code> cabeçalho da solicitação.</p>	<p>Somente dados de objeto S3 recém-ingeridos.</p> <p>A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <p>StorageGRID gerencia as chaves.</p> <ul style="list-style-type: none"> <li>• <a href="#">Use S3</a></li> </ul>
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	<p>Você emite uma solicitação S3 para armazenar um objeto e incluir três cabeçalhos de solicitação.</p> <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>	<p>Somente dados de objeto S3 recém-ingeridos.</p> <p>A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <p>As chaves são gerenciadas fora do StorageGRID.</p> <ul style="list-style-type: none"> <li>• <a href="#">Use S3</a></li> </ul>

Opção de criptografia	Como funciona	Aplica-se a
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.	<p>Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado.</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>
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> <ul style="list-style-type: none"> <li>• <a href="#">"Amazon Simple Storage Service - Guia do desenvolvedor: Protegendo dados usando criptografia do lado do cliente"</a></li> </ul>

### Use 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.

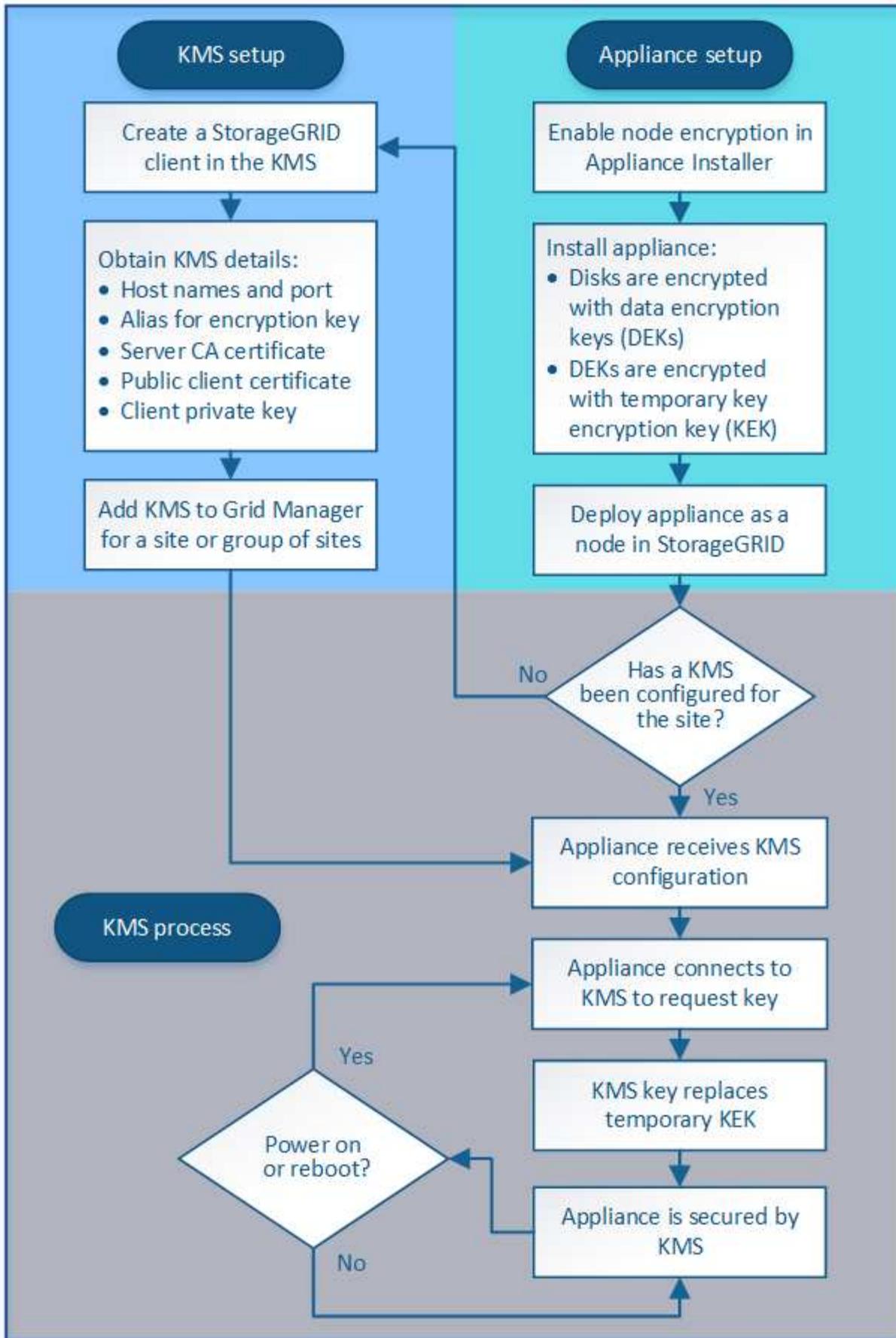
Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

### 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.

## 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.	<a href="#">Configure o StorageGRID como um cliente no KMS</a>
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	<a href="#">Configure 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>

## 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 conectar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

Para obter detalhes, consulte o seguinte:

- [Aparelhos de serviços SG100 e 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 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 localários. 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?

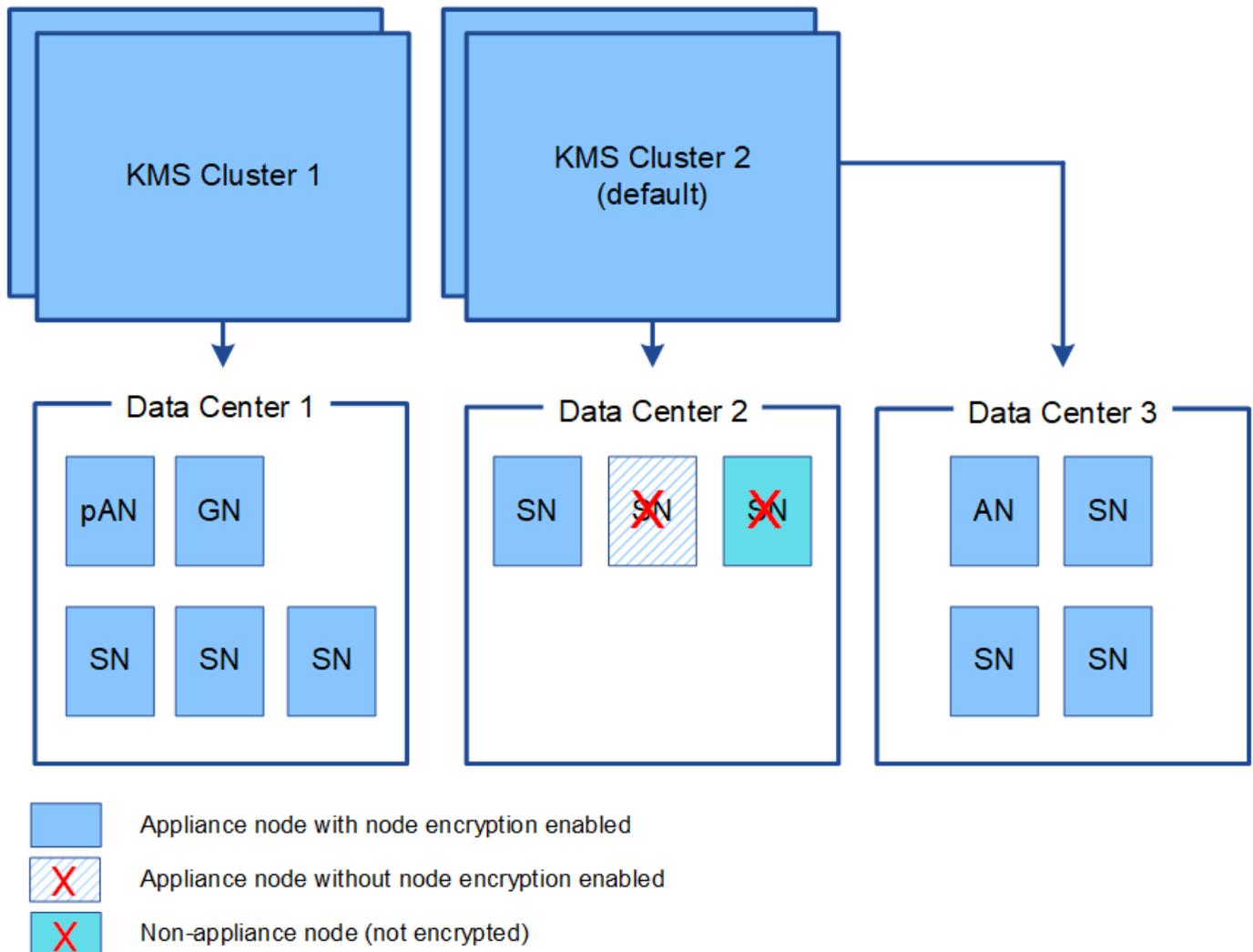
Você pode configurar um ou mais servidores de gerenciamento de chaves externos para fornecer chaves de criptografia aos nós do dispositivo em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único local ou em um grupo de sites.

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.

#### Informações relacionadas

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

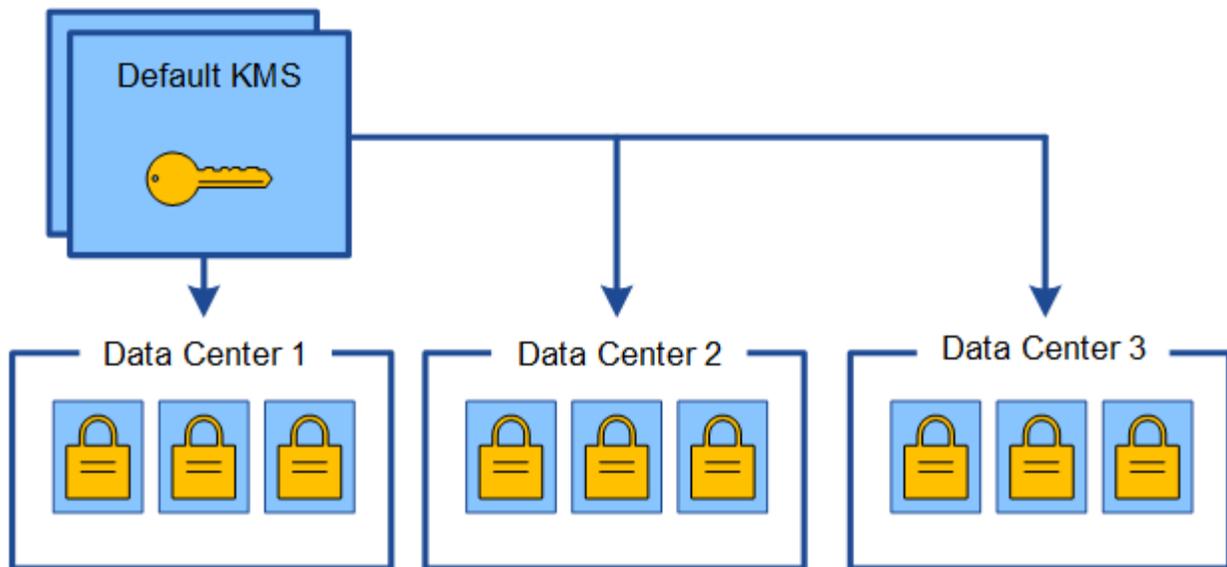
### Considerações para alterar o KMS para um site

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.

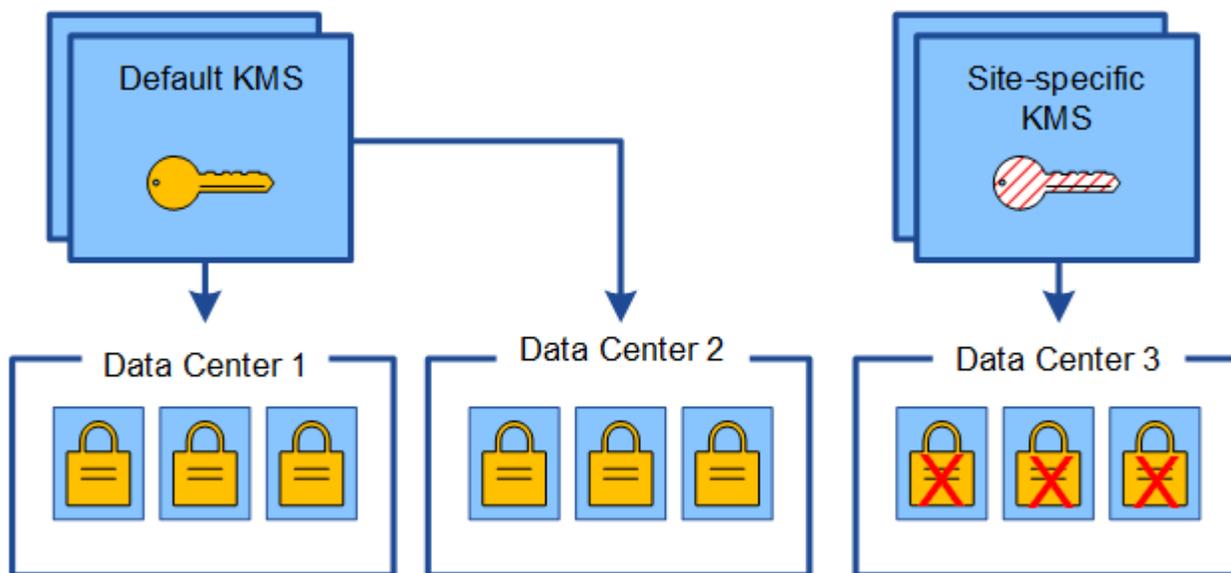
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para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

Por exemplo:

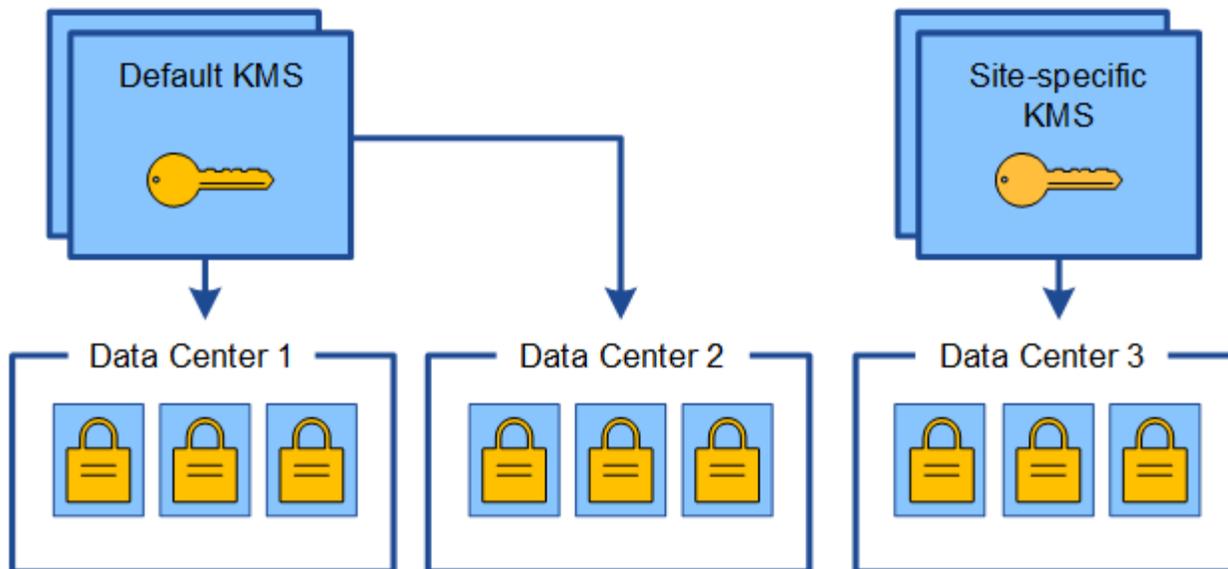
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar 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>

## 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.

### 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

- 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 a permissão de acesso root.

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

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](#).

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

## 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

1 Enter KMS Details      2 Upload Server Certificate      3 Upload Client Certificates

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

Port

Hostname

## 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.

Campo	Descrição
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres.
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	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	<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**.

## 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**.

### 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

Cancel

Back

Save

### 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.

## Ver 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 **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 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.

## 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.

#### 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
- KMS não está configurado

Consulte as ações recomendadas para esses alertas nas instruções do [Monitoramento e solução de problemas do StorageGRID](#).



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

## 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

- Você revisou o [considerações e requisitos para usar um servidor de gerenciamento de chaves](#).
- Se pretende atualizar o site selecionado para um KMS, analisou o [Considerações para alterar o KMS para um site](#).
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

### Passos

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

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
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	<span>✓</span> 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.
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

- Você revisou o [considerações e requisitos para usar um servidor de gerenciamento de chaves](#).
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a 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 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 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](#).

+ Create    Edit    Remove				
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
<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.

## Gerenciar configurações de proxy

### Configure as configurações de proxy de armazenamento

Se você estiver usando serviços de plataforma ou pools de storage em nuvem, poderá configurar um proxy não transparente entre nós de storage e os pontos de extremidade externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens de serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na Internet.

#### O que você vai precisar

- Você tem permissões de acesso específicas.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

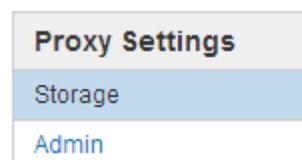
#### Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

#### Passos

1. Selecione **CONFIGURATION > Security > Proxy settings**.

A página Configurações do proxy de armazenamento é exibida. Por padrão, **Storage** está selecionado no menu da barra lateral.



2. Marque a caixa de seleção **Enable Storage Proxy** (Ativar proxy de armazenamento\*).

Os campos para configurar um proxy de armazenamento são exibidos.

#### Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy

Protocol  HTTP  SOCKS5

Hostname

Port (optional)

3. Selecione o protocolo para o proxy de armazenamento não transparente.
4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para se conectar ao servidor proxy.

Você pode deixar este campo em branco se usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Guardar**.

Depois que o proxy Storage for salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem podem ser configurados e testados.



As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma do StorageGRID não sejam bloqueadas.

#### Depois de terminar

Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção **Ativar proxy de armazenamento** e selecione **Salvar**.

#### Informações relacionadas

- [Rede e portas para serviços de plataforma](#)
- [Gerenciar objetos com ILM](#)

## Configure as configurações do proxy Admin

Se você enviar mensagens AutoSupport usando HTTP ou HTTPS ([Configurar o AutoSupport](#) consulte ), poderá configurar um servidor proxy não transparente entre nós de administração e o suporte técnico (AutoSupport).

#### O que você vai precisar

- Você tem permissões de acesso específicas.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

### Sobre esta tarefa

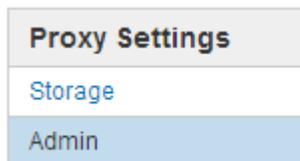
Você pode configurar as configurações para um único proxy Admin.

### Passos

1. Selecione **CONFIGURATION > Security > Proxy settings**.

É apresentada a página Admin Proxy Settings (Definições de proxy de administração). Por padrão, **Storage** está selecionado no menu da barra lateral.

2. No menu da barra lateral, selecione **Admin**.



3. Marque a caixa de seleção **Enable Admin Proxy** (Ativar proxy de administrador).

#### Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy

Hostname

Port

Username (optional)

Password (optional)

4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Introduza a porta utilizada para ligar ao servidor proxy.
6. Opcionalmente, insira o nome de usuário do proxy.

Deixe este campo em branco se o servidor proxy não exigir um nome de usuário.

7. Opcionalmente, insira a senha do proxy.

Deixe este campo em branco se o servidor proxy não exigir uma senha.

8. Selecione **Guardar**.

Depois que o proxy Admin é salvo, o servidor proxy entre nós Admin e o suporte técnico é configurado.



As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se você precisar desativar o proxy, desmarque a caixa de seleção **Ativar proxy Admin** e selecione **Salvar**.

## Gerenciar redes de clientes não confiáveis

### Gerenciar redes de clientes não confiáveis: Visão geral

Se você estiver usando uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis aceitando tráfego de clientes de entrada apenas em endpoints configurados explicitamente.

Por padrão, a rede do cliente em cada nó de grade é *confiável*. Ou seja, por padrão, o StorageGRID confia em conexões de entrada para cada nó de grade em todas as portas externas disponíveis (consulte as informações sobre comunicações externas no [Diretrizes de rede](#)).

Você pode reduzir a ameaça de ataques hostis em seu sistema StorageGRID especificando que a rede de clientes em cada nó seja *não confiável*. Se a rede de cliente de um nó não for confiável, o nó só aceita conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga. [Configurar pontos de extremidade do balanceador de carga](#) Consulte .

#### Exemplo 1: O Gateway Node aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway recuse todo o tráfego de entrada na rede do cliente, exceto para solicitações HTTPS S3. Você executaria estes passos gerais:

1. Na página Load Balancer Endpoints, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página redes de clientes não confiáveis, especifique que a rede de cliente no nó de gateway não é confiável.

Depois de salvar sua configuração, todo o tráfego de entrada na rede de clientes do nó de Gateway será descartado, exceto para solicitações HTTPS S3 na porta 443 e ICMP echo (ping).

#### Exemplo 2: O nó de storage envia S3 solicitações de serviços de plataforma

Suponha que você queira ativar o tráfego de serviço de plataforma S3 de saída de um nó de armazenamento, mas você deseja impedir quaisquer conexões de entrada para esse nó de armazenamento na rede cliente. Você executaria este passo geral:

- Na página redes de clientes não confiáveis, indique que a rede de cliente no nó de armazenamento não é confiável.

Depois de salvar sua configuração, o nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua a permitir solicitações de saída para a Amazon Web Services.

### Especificar rede cliente do nó não é confiável

Se você estiver usando uma rede de cliente, poderá especificar se a rede de cliente de cada nó é confiável ou não confiável. Você também pode especificar a configuração

padrão para novos nós adicionados em uma expansão.

### O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Se você quiser que um nó de administrador ou nó de gateway aceite o tráfego de entrada somente em endpoints configurados explicitamente, você definiu os endpoints do balanceador de carga.



As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

### Passos

1. Selecione **CONFIGURATION > Security > UnTrusted Client Networks**.

A página redes de clientes não confiáveis lista todos os nós do seu sistema StorageGRID. A coluna motivo indisponível inclui uma entrada se a rede do cliente no nó tiver de ser fidedigna.

#### Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

#### Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Default  Trusted  Untrusted

#### Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

2. Na seção **Definir novo padrão de nó**, especifique qual deve ser a configuração padrão quando novos nós forem adicionados à grade em um procedimento de expansão.

- **Trusted**: Quando um nó é adicionado em uma expansão, sua rede de clientes é confiável.
- **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede cliente não é confiável. Conforme necessário, você pode retornar a esta página para alterar a configuração de um novo nó

específico.



Esta configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Na seção **Selecione nós de rede de cliente não confiáveis**, selecione os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente.

Você pode selecionar ou desmarcar a caixa de seleção no título para selecionar ou desmarcar todos os nós.

4. Selecione **Guardar**.

As novas regras de firewall são imediatamente adicionadas e aplicadas. As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

## 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 INTERRUPTÃO 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.