



# **Configurar certificados de servidor**

## **StorageGRID**

NetApp  
March 12, 2025

# Índice

Configurar certificados de servidor .....	1
Tipos de certificado de servidor suportados .....	1
Configurar certificados de interface de gerenciamento .....	1
Adicione um certificado de interface de gerenciamento personalizado .....	2
Restaure o certificado padrão da interface de gerenciamento .....	4
Use um script para gerar um novo certificado de interface de gerenciamento autoassinado .....	5
Transfira ou copie o certificado da interface de gestão .....	6
Configure os certificados API S3 e Swift .....	7
Adicione um certificado personalizado de API S3 e Swift .....	8
Restaure o certificado padrão da API S3 e Swift .....	11
Faça o download ou copie o certificado API S3 e Swift .....	11
Copie o certificado da CA de Grade .....	12
Configurar certificados StorageGRID para FabricPool .....	13

# 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).



O tipo de codificação da diretiva de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, as cifras RSA exigem certificados RSA e as cifras ECDSA exigem certificados ECDSA. ["Gerenciar certificados de segurança"](#) Consulte . Se configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, pode ["reverter temporariamente para a política de segurança padrão"](#).

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, ["Segurança para clientes S3 e Swift"](#) consulte .

## 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:

Campo	Descrição
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.

<b>Campo</b>	<b>Descrição</b>
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado.  Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado.  Essas extensões definem a finalidade da chave contida no certificado.  <b>Nota:</b> Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

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.

### Antes de começar

- Você "[permissões de acesso específicas](#)"tem .
- 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 de servidor usado para conexões de cliente S3 ou Swift para nós de armazenamento ou para terminais de balanceador de carga. 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:

Campo	Descrição
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.

<b>Campo</b>	<b>Descrição</b>
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado.  Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado.  Essas extensões definem a finalidade da chave contida no certificado.  <b>Nota:</b> Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

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.

## Restaurar 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 storage. 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 que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão S3 e Swift API será usado para novas conexões de clientes S3 e Swift subsequentes aos nós de armazenamento.

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 A API REST DO S3"](#)
- ["Use a API Swift REST"](#)
- ["Configurar nomes de domínio de endpoint 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.

### Antes de começar

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

### 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.

### Antes de começar

- Você "[permissões de acesso específicas](#)"tem .
- 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 .

## 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.



## **Informações sobre direitos autorais**

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

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

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

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

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

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

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

## **Informações sobre marcas comerciais**

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