# Configurando certificados de servidor

StorageGRID

NetApp
March 10, 2025

# Índice

# Configurando certificados de servidor

Você pode personalizar os certificados de servidor usados pelo sistema StorageGRID.

O sistema StorageGRID usa certificados de segurança para vários fins distintos:

- Certificados de servidor de interface de gerenciamento: Usado para proteger o acesso ao Gerenciador de grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento de locatário.
- Certificados de servidor de API de storage: Usado para proteger o acesso aos nós de armazenamento e nós de Gateway, que os aplicativos de cliente de API usam para carregar e baixar dados de objeto.

Você pode usar os certificados padrão criados durante a instalação, ou pode substituir qualquer um desses tipos padrão de certificados por seus próprios certificados personalizados.

## Tipos suportados de certificado de servidor personalizado

O sistema StorageGRID suporta certificados de servidor 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, consulte os guias de implementação S3 ou Swift.

## Certificados para pontos de extremidade do balanceador de carga

O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, consulte as instruções para configurar os pontos de extremidade do balanceador de carga.

**Informações relacionadas**

"Use S3"

"Use Swift"

"Configuração dos pontos de extremidade do balanceador de carga"

## Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário

Você pode substituir o certificado de servidor StorageGRID padrão por um único certificado de servidor personalizado que permite aos usuários acessar o Gerenciador de Grade e o Gerenciador de locatário sem encontrar avisos de segurança.

**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 servidor personalizado comum e uma chave privada correspondente.

Como um único certificado de servidor personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado de curinga ou de vários domínios se os clientes precisarem verificar o nome do host ao se conetar 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 raiz 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** e o alarme legado de expiração de certificado de Interface de Gerenciamento (MCEP) são acionados quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

> 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 do servidor de interface de gerenciamento personalizado expira.
> - Você reverte de um certificado de servidor de interface de gerenciamento personalizado para o certificado de servidor padrão.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção certificado do servidor de interface de gerenciamento, clique em **Instalar certificado personalizado**.
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

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

   - **CA Bundle**: Um único arquivo 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.
4. Clique em **Salvar**.

   Os certificados de servidor personalizados são usados para todas as novas conexões de cliente subsequentes.

   Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   > Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

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

# Restaurando os certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário

Você pode reverter para o uso dos certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Gerenciar certificado do servidor de interface, clique em **usar certificados padrão**.
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente subsequentes.

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

# Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB

Você pode substituir o certificado do servidor usado para conexões de cliente S3 ou Swift ao nó de armazenamento ou ao serviço CLB (obsoleto) no nó de gateway. 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 conetar 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, os usuários também podem precisar instalar o certificado CA raiz no cliente API S3 ou Swift que eles usarão 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 Server certificate for Storage API Endpoints** e o alarme legacy Storage API Service Endpoints Certificate Expiration (SCEP) são acionados quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

Os certificados personalizados só são usados se os clientes se conetarem ao StorageGRID usando o serviço CLB obsoleto nos nós do gateway ou se eles se conetarem diretamente aos nós de armazenamento. Os

clientes S3 ou Swift que se conetam ao StorageGRID usando o serviço de balanceador de carga em nós de administração ou nós de gateway usam o certificado configurado para o ponto de extremidade do balanceador de carga.

> O alerta **Expiration of load balancer endpoint certificate** é acionado para os pontos de extremidade do balanceador de carga que expirarão em breve.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate, clique em **Install Custom Certificate** (Instalar certificado personalizado).
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

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

   - **CA Bundle**: Um único arquivo 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.
4. Clique em **Salvar**.

   O certificado de servidor personalizado é usado para todas as novas conexões de cliente API subsequentes.

   Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   > Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

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

**Informações relacionadas**

"Use S3"

"Use Swift"

"Configurando nomes de domínio de endpoint da API S3"

# Restaurando os certificados de servidor padrão para os endpoints S3 e Swift REST API

Você pode reverter para o uso dos certificados de servidor padrão para os endpoints da API REST S3 e Swift.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate (certificado do servidor de Endpoints), clique em **Use Default Certificates** (usar certificados padrão).
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão para os endpoints da API de armazenamento de objetos, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente API subsequentes.

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

# Copiar o certificado CA do sistema StorageGRID

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

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

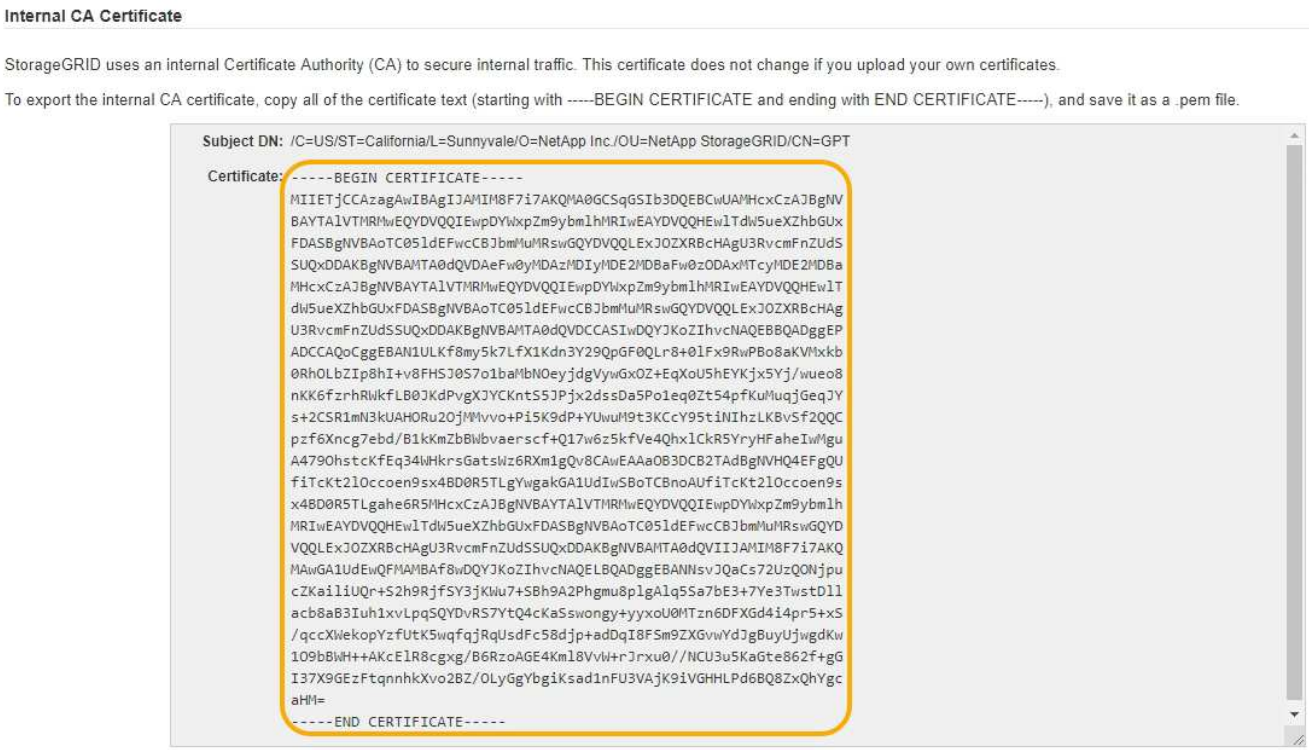
**Sobre esta tarefa**

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 **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção **certificado de CA interno**, selecione todo o texto do certificado.

   Você deve incluir `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` em sua seleção.




3. Clique com o botão direito do rato no texto selecionado e selecione **Copiar**.
4. Cole o certificado copiado em um editor de texto.
5. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

# Configurando 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 deve ter permissões de acesso específicas.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Sobre esta tarefa**

Quando você cria um ponto de extremidade do 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, consulte as instruções de configuração do StorageGRID for FabricPool.

O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é mais 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 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 relacionadas**

"Configurar o StorageGRID para FabricPool"

# Gerando um certificado de servidor autoassinado para a interface de gerenciamento

Você pode usar um script para gerar um certificado de servidor auto-assinado para clientes de API de gerenciamento que exigem validação estrita do nome de host.

**O que você vai precisar**

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

**Sobre esta tarefa**

Em ambientes de produção, você deve usar um certificado assinado por uma autoridade de certificação (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.

**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 usado pelo Gerenciador de Grade e pelo Gerenciador de Tenant.
   - 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 da API 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 365
     ```

     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 **Configuração** > **certificados de servidor** > **certificado de servidor de interface de gerenciamento**.
7. Configure seu cliente de API de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais