Gerenciar certificados

StorageGRID software

NetApp
December 03, 2025

Índice

Gerenciar certificados

Gerenciar 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 dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam a identidade de um cliente ou usuário no servidor, fornecendo autenticação mais segura do que apenas senhas. Os certificados do cliente não criptografam 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 este 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 servidor para algumas conexões (como o ponto de extremidade do balanceador de carga) ou como cliente para outras conexões (como o serviço de replicação do CloudMirror).

Certificado Grid CA padrão

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

- Os certificados CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser aqueles especificados para verificar as conexões do servidor.
- Todos os certificados personalizados devem atender aos"diretrizes de reforço do sistema para certificados de servidor" .
- O StorageGRID oferece suporte ao agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados de 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 no lugar do certificado de CA do sistema operacional.

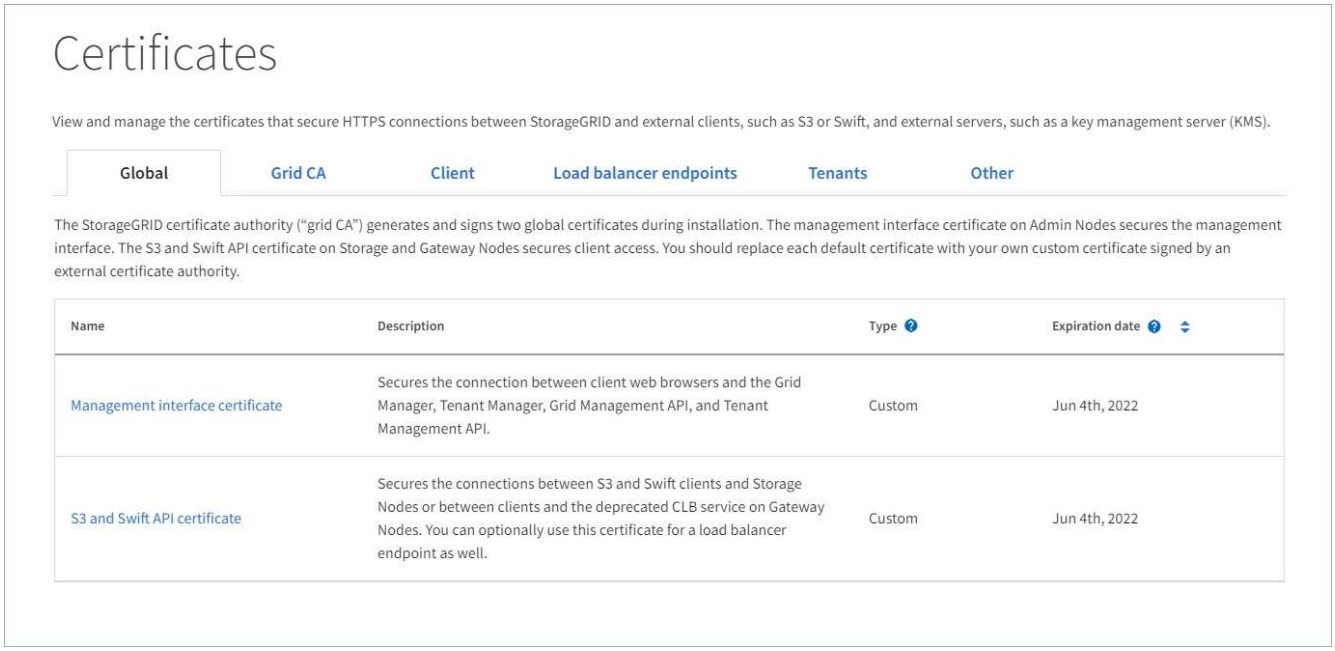
Variantes dos tipos de certificados de servidor e cliente são implementadas de diversas maneiras. Você deve ter todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Certificados de segurança de acesso

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

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.



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

   - **Global**: Protege o acesso ao StorageGRID de navegadores da web e clientes de API externos.
   - **Grid CA**: protege o tráfego interno do StorageGRID .
   - **Cliente**: protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
   - **Pontos de extremidade do balanceador de carga**: protege conexões entre clientes S3 e o balanceador de carga StorageGRID .
   - **Inquilinos**: protege conexões com servidores de federação de identidade ou de pontos de extremidade de serviço de plataforma para recursos de armazenamento S3.
   - **Outro**: Protege conexões StorageGRID que exigem certificados específicos.

     Cada aba é descrita abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso ao StorageGRID de navegadores da web e clientes externos da API S3. Dois certificados globais são gerados inicialmente pela autoridade de certificação StorageGRID durante a instalação. A melhor prática 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 com as interfaces de gerenciamento do StorageGRID .
- Certificado S3 API: Protege conexões de API do cliente com nós de armazenamento, nós de administração e nós de gateway, que os aplicativos cliente S3 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 validade**: Se estiver usando o certificado padrão, nenhuma data de validade será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
  - "Substituir o certificado de interface de gerenciamento gerado pelo StorageGRID padrão"usado para conexões do Grid Manager e do Tenant Manager.
  - "Substituir o certificado da API S3"usado para conexões de nó de armazenamento e ponto de extremidade do balanceador de carga (opcional).
- "Restaurar o certificado da interface de gerenciamento padrão" .
- "Restaurar o certificado padrão da API S3" .
- "Use um script para gerar um novo certificado de interface de gerenciamento autoassinado" .
- Copie ou baixe o"certificado de interface de gerenciamento" ou"Certificado S3 API" .

Grade CA

OCertificado Grid CA , gerado pela autoridade de certificação do 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 Grid CA" , mas você não pode alterá-lo.

Cliente

Certificados de cliente, gerado por uma autoridade de certificação externa, protege as conexões entre ferramentas de monitoramento externo e o banco de dados 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 do Prometheus, juntamente com a data de expiração 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:
  - "Alterar o nome do certificado do cliente."
  - "Defina a permissão de acesso do 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" ,"anexar" , ou"remover" um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los de uma só vez usando **Ações** > **Remover**.

Pontos de extremidade do balanceador de carga

Certificados de ponto de extremidade do balanceador de cargaproteger as conexões entre clientes S3 e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração.

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

> Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- "Exibir um ponto de extremidade do balanceador de carga", incluindo os detalhes do seu certificado.
- "Especifique um certificado de ponto de extremidade do balanceador de carga para FabricPool."
- "Use o certificado global da API S3"em vez de gerar um novo certificado de ponto de extremidade do balanceador de carga.

Inquilinos

Os inquilinos podem usarcertificados de servidor de federação de identidade oucertificados de ponto de extremidade de serviço de plataforma para proteger suas conexões com o StorageGRID.

A tabela de locatários 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 inquilino para fazer login no Gerenciador de Inquilinos"
- "Selecione um nome de locatário para visualizar os detalhes da federação de identidade do locatário"
- "Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma de locatários"
- "Especifique um certificado de ponto de extremidade de serviço de plataforma durante a criação

do ponto de extremidade"

Outro

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

- Certificados de pool de armazenamento em nuvem
- Certificados de notificação de alerta por e-mail
- Certificados de servidor syslog externo
- Certificados de conexão de federação de rede
- Certificados de federação de identidade
- Certificados do servidor de gerenciamento de chaves (KMS)
- Certificados de logon único

As informações indicam o tipo de certificado que uma função usa e as datas de expiração dos certificados de servidor e cliente, conforme aplicável. Selecionar um nome de função abre uma aba do navegador onde você pode visualizar e editar os detalhes do certificado.

> Você só pode visualizar e acessar informações de outros certificados se tiver a permissão"permissão apropriada" .

Você pode:

- "Especifique um certificado de pool de armazenamento em nuvem para S3, C2S S3 ou Azure"
- "Especificar um certificado para notificações de alerta por e-mail"
- "Use um certificado para um servidor syslog externo"
- "Girar certificados de conexão de federação de rede"
- "Visualizar e editar um certificado de federação de identidade"
- "Carregar certificados de servidor e cliente do servidor de gerenciamento de chaves (KMS)"
- "Especificar manualmente um certificado SSO para uma parte confiável"

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre os navegadores da Web do cliente e a interface de gerenciamento do StorageGRID , permitindo que os usuários acessem o Grid Manager e o Tenant Manager sem avisos de segurança. Este certificado também autentica conexões da API de gerenciamento de grade e da API de gerenciamento de locatários. Você pode usar o certificado padrão criado durante a instalação ou carregar um certificado personalizado.	**CONFIGURAÇÃO** > **Segurança** > **Certificados**, selecione a aba **Global** e então selecione **Certificado de interface de gerenciamento**	"Configurar certificados de interface de gerenciamento"

Certificado S3 API

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras do cliente S3 com um nó de armazenamento e com pontos de extremidade do balanceador de carga (opcional).	**CONFIGURAÇÃO** > **Segurança** > **Certificados**, selecione a aba **Global** e então selecione **Certificado S3 API**	"Configurar certificados da API S3"

Certificado Grid CA

Veja oDescrição do certificado CA de grade padrão .

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de clientes externos. • Permite que clientes externos autorizados acessem o banco de dados StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**	"Configurar certificados de cliente"

Certificado de ponto de extremidade do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração. Você pode carregar ou gerar um certificado do balanceador de carga ao configurar um ponto de extremidade do balanceador de carga. Os aplicativos cliente usam o certificado do balanceador de carga ao se conectar ao StorageGRID para salvar e recuperar dados de objetos. Você também pode usar uma versão personalizada do globalCertificado S3 API certificado 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. **Observação:** O certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID .	**CONFIGURAÇÃO** > **Rede** > **Pontos de extremidade do balanceador de carga**	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade do balanceador de carga para o FabricPool"

Certificado de ponto de extremidade do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de armazenamento em nuvem do StorageGRID com um local de armazenamento externo, como o S3 Glacier ou o armazenamento de Blobs do Microsoft Azure. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **Pools de armazenamento**	"Criar um pool de armazenamento em nuvem"

Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta. • Se as comunicações com o servidor SMTP exigirem o Transport Layer Security (TLS), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	**ALERTAS** > **Configuração de e-mail**	"Configurar notificações por e-mail para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que registra eventos no StorageGRID. **Observação:** Um certificado de servidor syslog externo não é necessário para conexões TCP, RELP/TCP e UDP com um servidor syslog externo.	**CONFIGURAÇÃO** > **Monitoramento** > **Servidor de auditoria e syslog**	"Use um servidor syslog externo"

Certificado de conexão de federação de rede

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentique e criptografe as informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grade.	**CONFIGURAÇÃO** > **Sistema** > **Federação de grade**	• "Criar conexões de federação de grade" • "Girar certificados de conexão"

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 Active Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, o que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	**CONFIGURAÇÃO** > **Controle de Acesso** > **Federação de Identidade**	"Usar federação de identidade"

Certificado do 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 .	**CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de ponto de extremidade de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID com um recurso de armazenamento S3.	**Gerenciador de inquilinos** > **ARMAZENAMENTO (S3)** > **Pontos de extremidade de serviços de plataforma**	"Criar ponto de extremidade de serviços de plataforma" "Editar ponto de extremidade dos serviços da plataforma"

Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como os Serviços de Federação do Active Directory (AD FS) e o StorageGRID , que são usados para solicitações de logon único (SSO).	**CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**	"Configurar logon único"

Exemplos de certificados

Exemplo 1: serviço de balanceador de carga

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 com o ponto de extremidade 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 ponto de extremidade 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 este 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 do objeto para StorageGRID.

Exemplo 2: Servidor de gerenciamento de chaves externo (KMS)

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software externo Key Management Server, 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 Grid Manager, você configura um servidor KMS e carrega os certificados do servidor e do 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 baseada 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.

Tipos de certificados de servidor suportados

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (Algoritmo de Assinatura Digital de Curva Elíptica).

> O tipo de cifra da política de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, cifras RSA exigem certificados RSA, e cifras ECDSA exigem certificados ECDSA. Ver "Gerenciar certificados de segurança" . Se você configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, você poderá"reverter temporariamente para a política de segurança padrão" .

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, consulte"Segurança para clientes S3" .

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 Grid Manager e o Tenant Manager 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 administração recebe um certificado assinado pela CA da grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento personalizado comum e pela 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 multidomínio se os clientes precisarem verificar o nome do host ao se conectar ao Grid Manager e ao Tenant Manager. Defina o certificado personalizado de forma que ele 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 estiver usando, os usuários também podem precisar instalar o certificado Grid CA no navegador da Web que usarão para acessar o Grid Manager e o Tenant Manager.

Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado do servidor para a Interface de Gerenciamento** é acionado quando este certificado do servidor está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO** > **Segurança** > **Certificados** e verificando a data de expiração do certificado da interface de gerenciamento na guia Global.

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

- Seu certificado de interface de gerenciamento personalizado expira.
- Vocêreverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão .

Adicionar 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 Grid Manager.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
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 arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

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

> As chaves privadas da 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 certificadora intermediária emissora (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, 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 certificados.

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

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

d. Selecione **Salvar**. + O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

Gerar certificado

Gere os arquivos de certificado do servidor.

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

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP a serem incluídos no certificado.
Assunto (opcional)	Assunto X.509 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.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Observação**: deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Salvar**. + O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

5. Atualize a página para garantir que o navegador da web esteja atualizado.

> Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página Certificado da interface de gerenciamento exibe informações detalhadas do certificado que está em uso. + Você pode baixar ou copiar o certificado PEM conforme necessário.

Restaurar o certificado da interface de gerenciamento padrão

Você pode voltar a usar o certificado de interface de gerenciamento padrão para conexões do Grid Manager e do Tenant Manager.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
3. Selecione **Usar certificado padrão**.

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

4. Atualize a página para garantir que o navegador da web esteja atualizado.

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

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

Antes de começar

- 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 de administração.
2. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

      Quando você está logado como root, o prompt muda 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 curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com` .
   - Definir `--type` para `management` para configurar o certificado da interface de gerenciamento, que é usado pelo Grid Manager e pelo Tenant Manager.
   - 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 para seu cliente de API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags BEGIN e END na sua seleção.

5. Saia do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Grid Manager.
   b. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**
   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 BEGIN e END.

Baixe ou copie o certificado da interface de gerenciamento

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
3. Selecione a aba **Servidor** ou **Pacote de CA** e então baixe ou copie o certificado.

Baixar arquivo de certificado ou pacote de CA

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

a. Selecione **Baixar certificado** ou **Baixar pacote de 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 do certificado e o local do 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 de 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`

Configurar certificados da API S3

Você pode substituir ou restaurar o certificado do servidor usado para conexões do cliente S3 com nós de armazenamento ou com pontos de extremidade do balanceador de carga. O certificado de servidor personalizado de substituição é específico para sua organização.

Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "StorageGRID 11.8: Configurar certificados S3 e Swift API" .

Sobre esta tarefa

Por padrão, cada nó de armazenamento recebe um certificado de servidor X.509 assinado pela CA da grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e pela 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 multidomínio se os clientes precisarem verificar o nome do host ao se conectar ao ponto de extremidade de armazenamento. Defina o certificado personalizado de forma que ele corresponda a todos os nós de armazenamento na grade.

Após concluir a configuração no servidor, talvez você também precise instalar o certificado Grid CA no cliente S3 API que você usará para acessar o sistema, dependendo da autoridade de certificação raiz (CA) que estiver usando.

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado de servidor global para API S3** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO** > **Segurança** > **Certificados** e verificando a data de expiração do certificado da API S3 na guia Global.

Você pode carregar ou gerar um certificado de API S3 personalizado.

Adicionar um certificado de API S3 personalizado

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione **Usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

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

> As chaves privadas da 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 certificadora emissora intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado de API S3 personalizado que foi carregado. Se você carregou um pacote de CA opcional, 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 certificados.

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

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

d. Selecione **Salvar**.

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

Gerar certificado

Gere os arquivos de certificado do servidor.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a serem incluídos no certificado.

Campo	Descrição
Assunto (opcional)	Assunto X.509 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.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Observação**: deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

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

   - Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Salvar**.

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

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

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

6. Atualize a página para garantir que o navegador da web esteja atualizado.

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

Restaurar o certificado padrão da API S3

Você pode voltar a usar o certificado padrão da API S3 para conexões de cliente S3 com nós de armazenamento. No entanto, você não pode usar o certificado padrão da API S3 para um ponto de extremidade do balanceador de carga.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione **Usar certificado padrão**.

   Quando você restaura a versão padrão do certificado global da API S3, os arquivos de certificado de servidor personalizados que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 será usado para novas conexões de cliente S3 subsequentes com os nós de armazenamento.

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

   Se você tiver permissão de acesso Root e o certificado de API S3 personalizado tiver sido usado para conexões de ponto de extremidade do balanceador de carga, será exibida uma lista de pontos de extremidade do balanceador de carga que não estarão mais acessíveis usando o certificado de API S3 padrão. Vá para"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 esteja atualizado.

Baixe ou copie o certificado da API S3

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione a aba **Servidor** ou **Pacote de CA** e então baixe ou copie o certificado.

Baixar arquivo de certificado ou pacote de CA

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

a. Selecione **Baixar certificado** ou **Baixar pacote de 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 do certificado e o local do 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 de 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

- "Usar API REST do S3"
- "Configurar nomes de domínio de endpoint S3"

Copie o certificado Grid CA

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 Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Grid CA**.
2. Na seção **Certificado PEM**, baixe ou copie o certificado.

Baixar arquivo de certificado

Baixe o certificado `.pem` arquivo.

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

   Por exemplo: `storagegrid_certificate.pem`

Certificado de cópia 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 realizam validação estrita de nome de host e não oferecem suporte à desabilitação da validação estrita 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 tem"permissões de acesso específicas" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Ao criar 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. Certificados assinados por uma CA podem ser rotacionados sem interrupções. Eles também são mais seguros porque oferecem melhor proteção contra ataques do tipo man-in-the-middle.

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

Passos

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

Ao criar um ponto de extremidade do balanceador de carga HTTPS, você será solicitado a carregar seu certificado de servidor, a chave privada do certificado e o pacote de CA opcional.

3. Anexe o StorageGRID como uma camada de nuvem no ONTAP.

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

> Se uma CA intermediária emitiu o certificado StorageGRID , você deverá fornecer o certificado da CA intermediária. Se o certificado StorageGRID foi emitido diretamente pela CA raiz, você deve fornecer o certificado da CA raiz.

Configurar certificados de cliente

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

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

Ver"Gerenciar certificados de segurança" e"Configurar 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 visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO** > **Segurança** > **Certificados** e verificando a data de expiração do certificado do cliente na guia Cliente.

> Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivos especialmente configurados, consulte as informações específicas sobre"carregando um certificado de cliente KMS" .

Antes de começar

- Você tem permissão de acesso Root.
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Para configurar um certificado de cliente:
  - Você tem o endereço IP ou nome de domínio do nó de administração.
  - Se você configurou o certificado da interface de gerenciamento do StorageGRID , terá a CA, o certificado do cliente e a chave privada usados para configurar o certificado da interface de gerenciamento.
  - Para carregar seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
  - A chave privada deve ter sido salva ou registrada no momento em que foi criada. Se você não tiver a chave privada original, será necessário criar uma nova.
- Para editar um certificado de cliente:

- Você tem o endereço IP ou nome de domínio do nó de administração.
- Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no seu computador local.

Adicionar certificados de cliente

Para adicionar o certificado do cliente, use um destes procedimentos:

- 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 Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Adicionar**.
3. Digite um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
5. Selecione **Continuar**.
6. Para a etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
   a. Selecione **Carregar certificado**.
   b. Selecione **Navegar** e selecione o arquivo de certificado da interface de gerenciamento(`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
   c. Selecione **Criar** para salvar o certificado no Grid Manager.

      O novo certificado aparece na aba Cliente.
7. Configurar uma ferramenta de monitoramento externa, como Grafana.

Certificado de cliente emitido pela CA

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

Passos

1. Execute os passos para"configurar um certificado de interface de gerenciamento" .
2. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a

guia **Cliente**.

3. Selecione **Adicionar**.
4. Digite um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
6. Selecione **Continuar**.
7. Para a etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote da CA:
   a. Selecione **Carregar certificado**.
   b. Selecione **Navegar** e selecione o certificado do cliente, a chave privada e os arquivos do pacote CA(`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
   c. Selecione **Criar** para salvar o certificado no Grid Manager.

      Os novos certificados aparecem na aba Cliente.
8. Configurar uma ferramenta de monitoramento externa, como Grafana.

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente de administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para o Prometheus que use a função de geração de certificado no Grid Manager.

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Adicionar**.
3. Digite um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
5. Selecione **Continuar**.
6. Para a etapa **Anexar certificados**, selecione **Gerar certificado**.
7. Especifique as informações do certificado:
   - **Assunto** (opcional): Assunto X.509 ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que ele é gerado.
   - **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendida são adicionadas ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

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

Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado e colá-la em outro lugar.
- Selecione **Baixar chave privada** para salvar a chave privada como um arquivo.

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

10. Selecione **Criar** para salvar o certificado no Grid Manager.

    O novo certificado aparece na aba Cliente.

11. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Global**.
12. Selecione **Certificado de interface de gerenciamento**.
13. Selecione **Usar certificado personalizado**.
14. Carregue os arquivos certificate.pem e private_key.pem dodetalhes do certificado do cliente etapa. Não há necessidade de fazer upload do pacote CA.
    a. Selecione **Carregar certificado** e depois selecione **Continuar**.
    b. Carregar cada arquivo de certificado(`.pem`).
    c. Selecione **Salvar** para salvar o certificado no Grid Manager.

       O novo certificado aparece na página de certificados da Interface de Gerenciamento.

15. Configurar uma ferramenta de monitoramento externa, como Grafana.

Configurar uma ferramenta de monitoramento externa

Passos

1. Configure as seguintes configurações na sua ferramenta de monitoramento externa, como o Grafana.
   a. **Nome**: Digite um nome para a conexão.

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

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

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

c. Habilite **Autenticação de cliente TLS** e **Com certificado CA**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole:
   - Certificado CA da interface de gerenciamento para **CA Cert**
   - O certificado do cliente para **Client Cert**
   - A chave privada para **Chave do Cliente**

e. **ServerName**: Digite o nome de domínio do nó de administração.

   ServerName deve corresponder ao nome de domínio conforme aparece no certificado da interface de gerenciamento.

2. 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 do Prometheus do StorageGRID com sua ferramenta de monitoramento externa.

   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, habilitar ou desabilitar o acesso ao Prometheus ou carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.

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

2. Selecione o certificado que você deseja editar.
3. Selecione **Editar** e depois selecione **Editar nome e permissão**
4. Digite um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
6. Selecione **Continuar** para salvar o certificado no Grid Manager.

   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 **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.

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

2. Selecione o certificado que você deseja editar.
3. Selecione **Editar** e depois selecione uma opção de edição.

Carregar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Carregar certificado** e depois selecione **Continuar**.

b. Carregar 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 **Baixar certificado** para salvar o arquivo de certificado.

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

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

c. Selecione **Criar** para salvar o certificado no Grid Manager.

   O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

   - **Assunto** (opcional): Assunto X.509 ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que ele é gerado.
   - **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendida são adicionadas ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

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

   Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro

lugar.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado e colá-la em outro lugar.
- Selecione **Baixar chave privada** para salvar a chave privada como um arquivo.

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

e. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na aba Cliente.

Baixar ou copiar certificados de cliente

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.
2. Selecione o certificado que você deseja copiar ou baixar.
3. Baixe ou copie o certificado.

Baixar arquivo de certificado

Baixe o certificado `.pem` arquivo.

a. Selecione **Baixar certificado**.

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

Por exemplo: `storagegrid_certificate.pem`

Certificado de cópia

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 **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.
2. Selecione o certificado que você deseja remover.
3. Selecione **Excluir** e depois confirme.

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

Após a remoção de um certificado, os clientes que o utilizaram devem especificar um novo certificado de cliente para acessar o banco de dados StorageGRID Prometheus.

Informações sobre direitos autorais

Informações sobre marcas comerciais