Controlar o acesso do administrador ao StorageGRID

StorageGRID

NetApp
October 03, 2025

Índice

Controlar o acesso do administrador ao StorageGRID

Você pode controlar o acesso do administrador ao sistema StorageGRID abrindo ou fechando portas de firewall, gerenciando grupos de administração e usuários, configurando logon único (SSO) e fornecendo certificados de cliente para permitir acesso externo seguro às métricas do StorageGRID.

- "Controlar o acesso através de firewalls"
- "Usando a federação de identidade"
- "Gerenciando grupos de administradores"
- "Gerenciamento de usuários locais"
- "Usando logon único (SSO) para StorageGRID"
- "Configurando certificados de cliente de administrador"

Controlar o acesso através de firewalls

Quando quiser controlar o acesso através de firewalls, abra ou feche portas específicas no firewall externo.

Controlar o acesso no firewall externo

Você pode controlar o acesso às interfaces de usuário e APIs nos nós de administração do StorageGRID abrindo ou fechando portas específicas no firewall externo. Por exemplo, você pode evitar que os locatários sejam capazes de se conetar ao Gerenciador de Grade no firewall, além de usar outros métodos para controlar o acesso ao sistema.

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para nós de administração	Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade, a API de gerenciamento de grade, o Gerenciador de locatário e a API de gerenciamento do locatário. **Nota:** a porta 443 também é usada para algum tráfego interno.

Porta	Descrição	Se a porta estiver aberta…
8443	Porta restrita do Gerenciador de Grade em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade e a API de Gerenciamento de Grade usando HTTPS. • Os navegadores da Web e os clientes da API de gerenciamento não podem acessar o Gerenciador do locatário ou a API de gerenciamento do locatário. • As solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Gerenciador de inquilinos em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador do locatário e a API de gerenciamento do locatário usando HTTPS. • Navegadores da Web e clientes de API de gerenciamento não podem acessar o Gerenciador de Grade ou a API de Gerenciamento de Grade. • As solicitações de conteúdo interno serão rejeitadas.

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

"Iniciar sessão no Grid Manager"

"Criando uma conta de locatário se o StorageGRID não estiver usando SSO"

"Resumo: Endereços IP e portas para conexões de clientes"

"Gerenciando redes de clientes não confiáveis"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

Usando a federação de identidade

O uso da federação de identidade torna a configuração de grupos e usuários mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configurando a federação de identidade

Você pode configurar a federação de identidade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como ative Directory, OpenLDAP ou Oracle Directory Server.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Se você pretende ativar o logon único (SSO), você deve usar o ative Directory como a origem de identidade federada e o AD FS como o provedor de identidade. Consulte ""requisitos para utilizar o início de sessão único.""
- Você deve estar usando o ative Directory, OpenLDAP ou Oracle Directory Server como o provedor de identidade.

> Se pretender utilizar um serviço LDAP v3 que não esteja listado, tem de contactar o suporte técnico.

- Se você pretende usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade deve estar usando TLS 1,2 ou 1,3.

Sobre esta tarefa

Você deve configurar uma origem de identidade para o Gerenciador de Grade se quiser importar os seguintes tipos de grupos federados:

- Grupos de administração. Os usuários nos grupos de administração podem entrar no Gerenciador de Grade e executar tarefas, com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários de locatários que não usam sua própria origem de identidade. Os usuários em grupos de inquilinos podem entrar no Gerenciador de inquilinos e executar tarefas, com base nas permissões atribuídas ao grupo no Gerenciador de inquilinos.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.
2. Selecione **Ativar federação de identidade**.

   São apresentados os campos para configurar o servidor LDAP.

3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.

   Você pode selecionar **ative Directory**, **OpenLDAP** ou **Other**.

   > Se selecionar **OpenLDAP**, tem de configurar o servidor OpenLDAP. Consulte as diretrizes para configurar um servidor OpenLDAP.

   > Selecione **Other** para configurar valores para um servidor LDAP que use o Oracle Directory Server.

4. Se você selecionou **Other**, preencha os campos na seção atributos LDAP.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.

- **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
- **Group unique name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
- **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.

5. Na secção Configurar servidor LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias.
   - **Nome do host**: O nome do host do servidor ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar ao servidor LDAP.

     A porta padrão para STARTTLS é 389 e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta desde que seu firewall esteja configurado corretamente.

   - **Nome de usuário**: O caminho completo do nome distinto (DN) para o usuário que se conetará ao servidor LDAP.

     No ative Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

     O usuário especificado deve ter permissão para listar grupos e usuários e para acessar os seguintes atributos:

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`

   - **Senha**: A senha associada ao nome de usuário.
   - **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

     Os valores **Group unique name** devem ser exclusivos dentro do **Group base DN** a que pertencem.

   - **DN da base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP que você deseja pesquisar por usuários.

     Os valores **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN base do usuário** a que pertencem.

6. Na seção **Transport Layer Security (TLS)**, selecione uma configuração de segurança.
   - **Use STARTTLS (recomendado)**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada.
   - **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Esta opção é suportada por razões de compatibilidade.
   - **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido.

   > O uso da opção **não usar TLS** não é suportado se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

7. Se você selecionou STARTTLS ou LDAPS, escolha o certificado usado para proteger a conexão.
   - **Use o certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger conexões.
   - **Use certificado CA personalizado**: Use um certificado de segurança personalizado.

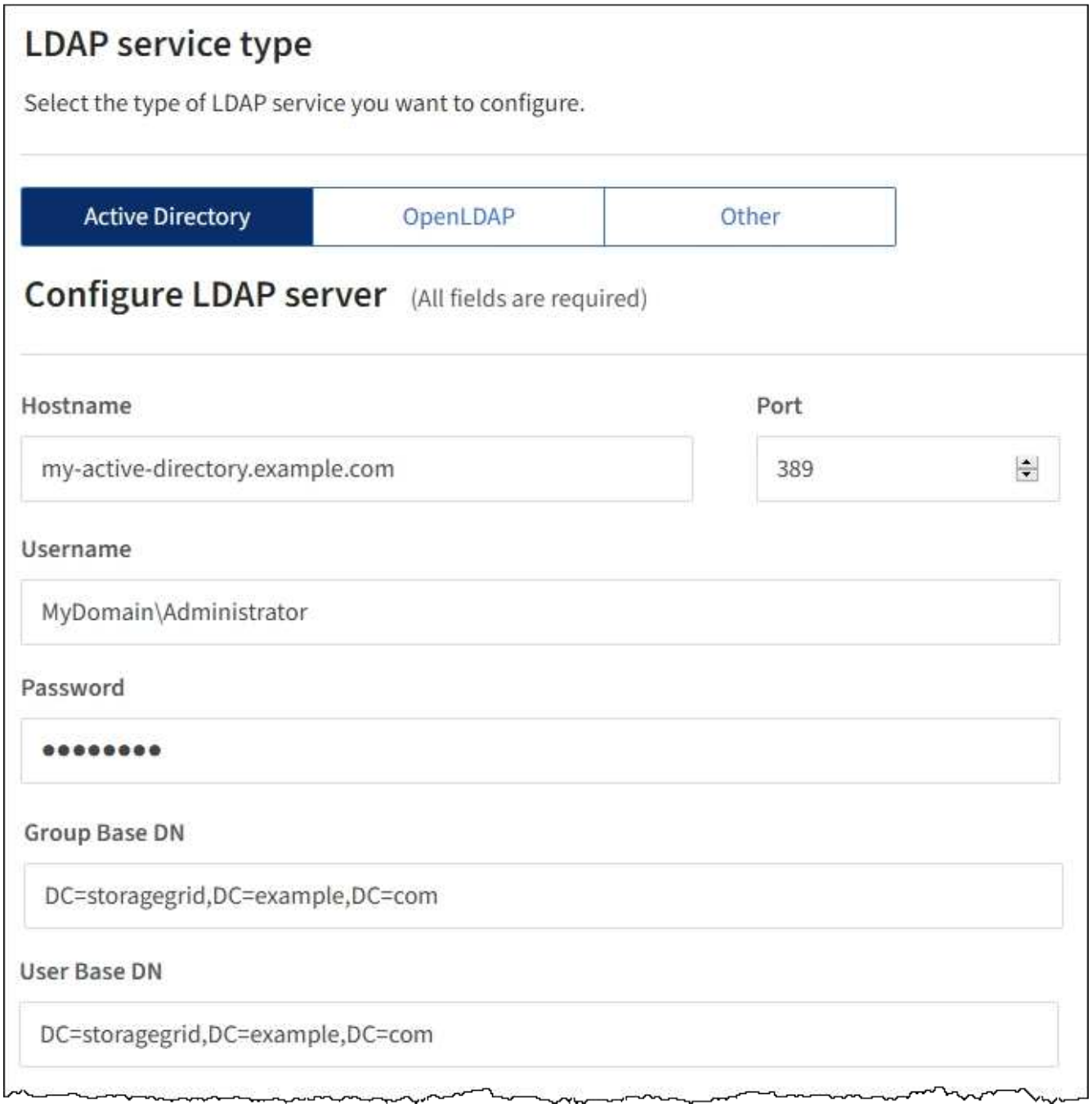
     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

8. Opcionalmente, selecione **testar conexão** para validar suas configurações de conexão para o servidor LDAP.

   Uma mensagem de confirmação aparece no canto superior direito da página se a conexão for válida.

9. Se a conexão for válida, selecione **Salvar**.

   A captura de tela a seguir mostra valores de configuração de exemplo para um servidor LDAP que usa o ative Directory.



Informações relacionadas

"Cifras suportadas para conexões TLS de saída"

"Requisitos para o uso de logon único"

"Criando uma conta de locatário"

"Use uma conta de locatário"

Diretrizes para configurar um servidor OpenLDAP

Se você quiser usar um servidor OpenLDAP para federação de identidade, você deve configurar configurações específicas no servidor OpenLDAP.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para manutenção de associação reversa em grupo no Guia do Administrador para OpenLDAP.

Indexação

Você deve configurar os seguintes atributos OpenLDAP com as palavras-chave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Além disso, certifique-se de que os campos mencionados na ajuda do Nome de usuário sejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção da associação de grupo reverso no Guia do Administrador para OpenLDAP.

Informações relacionadas

"Documentação do OpenLDAP: Guia do administrador da versão 2,4"

Forçando a sincronização com a fonte de identidade

O sistema StorageGRID sincroniza periodicamente grupos federados e usuários da origem da identidade. Você pode forçar o início da sincronização se quiser ativar ou restringir as permissões de usuário o mais rápido possível.

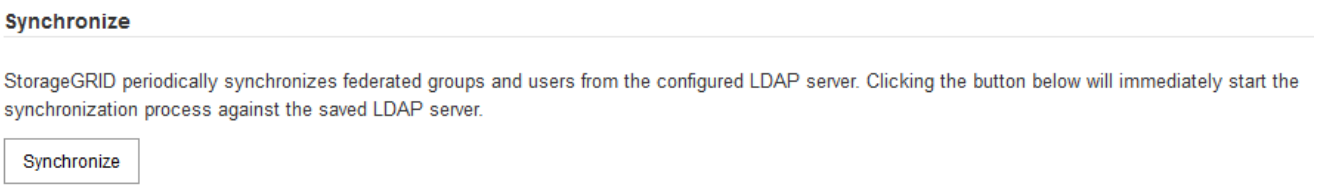
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- A origem da identidade deve estar ativada.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.

   A página Federação de identidade é exibida. O botão **Sincronizar** está na parte inferior da página.

2. Clique em **Sincronizar**.

   Uma mensagem de confirmação indica que a sincronização foi iniciada com êxito. O processo de sincronização pode demorar algum tempo, dependendo do ambiente.

O alerta **Falha na sincronização da federação de identidade** é acionado se houver um problema na sincronização de grupos federados e usuários da origem da identidade.

Desativando a federação de identidade

Você pode desativar temporariamente ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desativada, não há comunicação entre o StorageGRID e a fonte de identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

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

Antes de desativar a federação de identidade, você deve estar ciente do seguinte:

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a origem da identidade não ocorrerá e os alertas ou alarmes não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Ativar Federação de identidade** será desativada se o logon único (SSO) estiver definido como **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.
2. Desmarque a caixa de seleção **Ativar Federação de identidade**.
3. Clique em **Salvar**.

Informações relacionadas

"Desativação do logon único"

Gerenciando grupos de administradores

Você pode criar grupos de administração para gerenciar as permissões de segurança para um ou mais usuários de administração. Os usuários devem pertencer a um grupo para ter acesso ao sistema StorageGRID.

Criando grupos de administração

Os grupos de administração permitem determinar quais usuários podem acessar quais recursos e operações no Gerenciador de Grade e na API de Gerenciamento de Grade.

O que você vai precisar

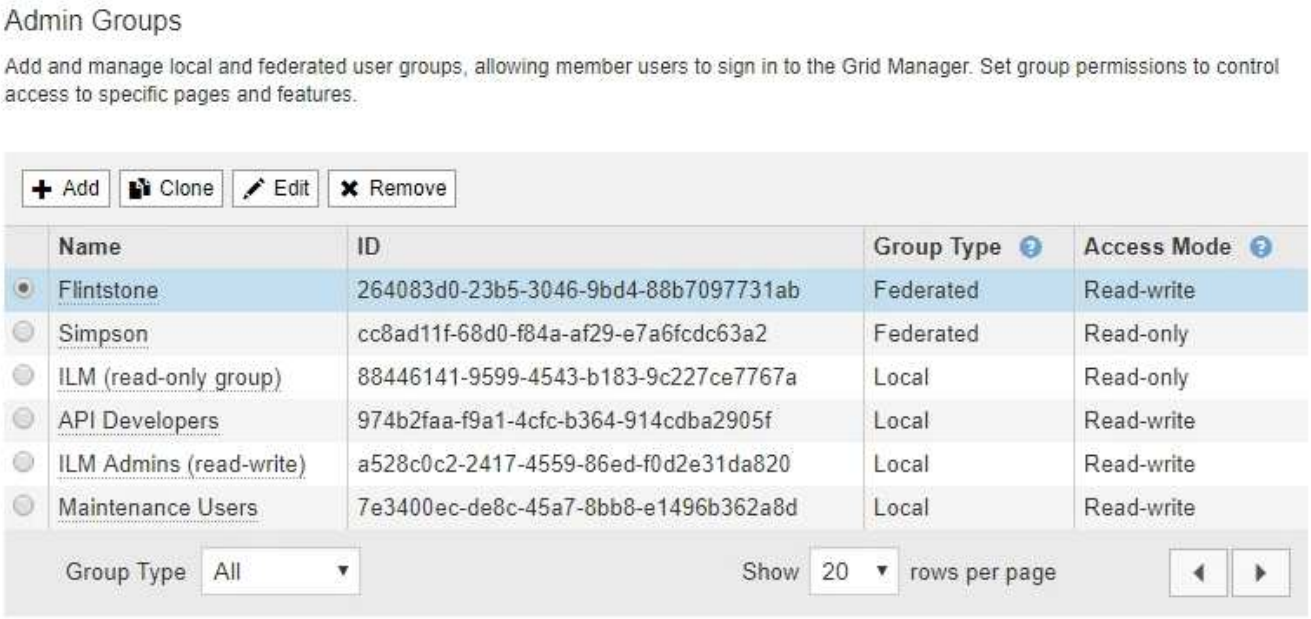
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.
- Se você pretende importar um grupo federado, você deve ter a federação de identidade configurada e o grupo federado já deve existir na origem de identidade configurada.

Passos

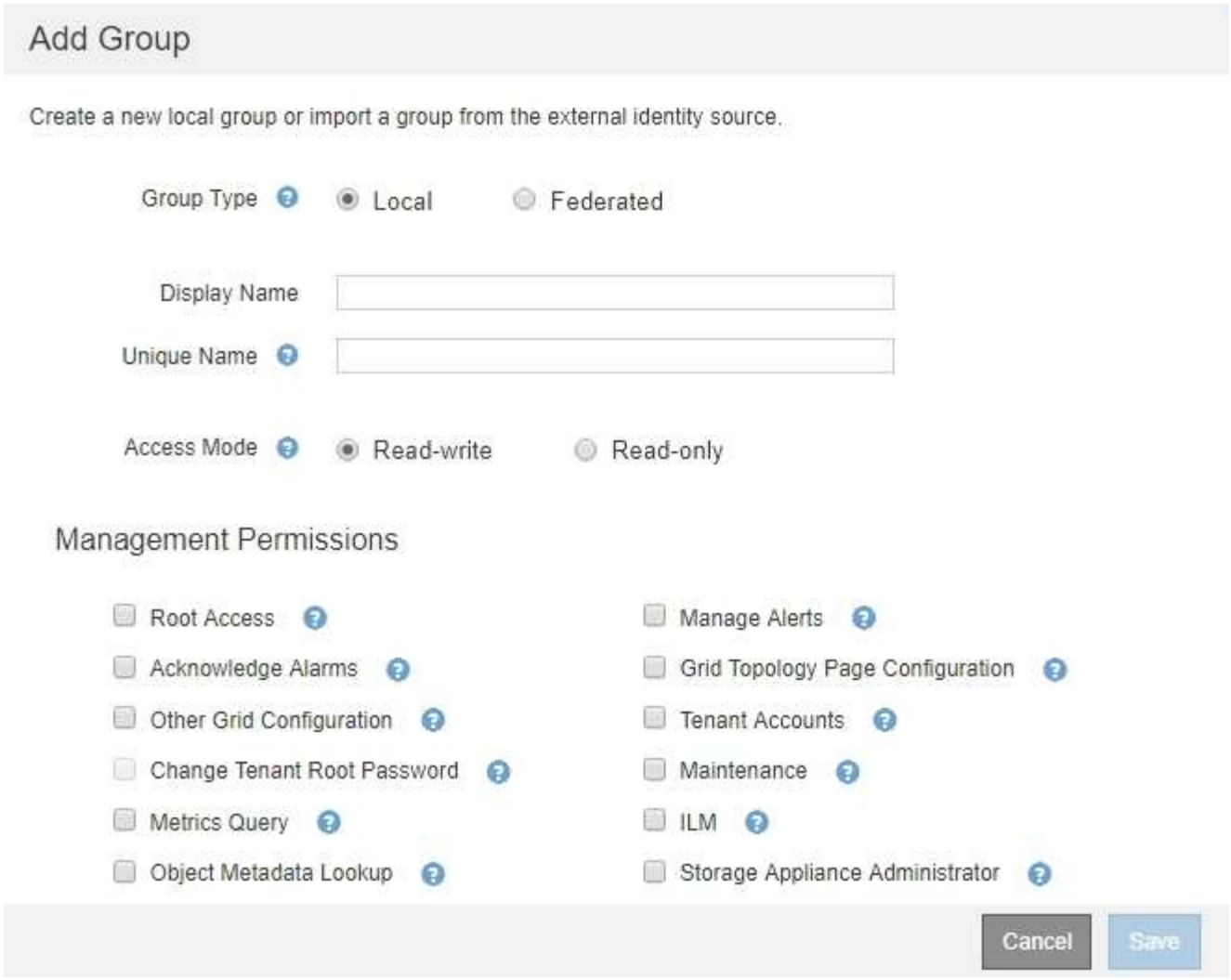
1. Selecione **Configuration** > **Access Control** > **Admin Groups**.

   A página grupos de administração é exibida e lista todos os grupos de administração existentes.



2. Selecione **Adicionar**.

   A caixa de diálogo Adicionar grupo é exibida.



3. Para tipo de grupo, selecione **local** se quiser criar um grupo que será usado somente no StorageGRID ou selecione **federado** se quiser importar um grupo da origem de identidade.
4. Se você selecionou **local**, digite um nome de exibição para o grupo. O nome de exibição é o nome que aparece no Gerenciador de Grade. Por exemplo, "'usuários de Manutenção'" ou "'Administradores de ILM.'"
5. Introduza um nome exclusivo para o grupo.
   - **Local**: Digite o nome exclusivo que você deseja. Por exemplo, "'Administradores ILM.'"
   - **Federated**: Insira o nome do grupo exatamente como ele aparece na origem de identidade configurada.
6. Para **modo de Acesso**, selecione se os usuários do grupo podem alterar as configurações e executar operações no Gerenciador de Grade e na API de Gerenciamento de Grade ou se eles só podem exibir configurações e recursos.
   - **Leitura-escrita** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade. Os usuários locais só de leitura podem alterar suas próprias senhas.

Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

7. Selecione uma ou mais permissões de gerenciamento.

   Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes ao grupo não poderão entrar no StorageGRID.

8. Selecione **Guardar**.

   O novo grupo é criado. Se este for um grupo local, agora você pode adicionar um ou mais usuários. Se este for um grupo federado, a fonte de identidade gerencia quais usuários pertencem ao grupo.

Informações relacionadas

"Gerenciamento de usuários locais"

Permissões do grupo de administração

Ao criar grupos de usuários admin, você seleciona uma ou mais permissões para controlar o acesso a recursos específicos do Gerenciador de Grade. Em seguida, você pode atribuir cada usuário a um ou mais desses grupos de administração para determinar quais tarefas o usuário pode executar.

Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes a esse grupo não poderão entrar no Gerenciador de Grade.

Por padrão, qualquer usuário que pertença a um grupo que tenha pelo menos uma permissão pode executar as seguintes tarefas:

- Faça login no Gerenciador de Grade
- Veja o Dashboard
- Exibir as páginas de nós
- Monitore a topologia da grade
- Ver alertas atuais e resolvidos
- Visualizar alarmes atuais e históricos (sistema legado)
- Alterar sua própria senha (somente usuários locais)
- Visualize determinadas informações nas páginas Configuração e Manutenção

As seções a seguir descrevem as permissões que você pode atribuir ao criar ou editar um grupo de administradores. Qualquer funcionalidade não mencionada explicitamente requer a permissão de acesso root.

Acesso à raiz

Essa permissão fornece acesso a todos os recursos de administração de grade.

Gerenciar alertas

Essa permissão fornece acesso a opções de gerenciamento de alertas. Os usuários devem ter essa permissão para gerenciar silêncios, notificações de alerta e regras de alerta.

Reconhecer alarmes (sistema legado)

Esta permissão fornece acesso para reconhecer e responder a alarmes (sistema legado). Todos os usuários conetados podem visualizar alarmes atuais e históricos.

Se você quiser que um usuário monitore a topologia da grade e reconheça somente alarmes, você deve atribuir essa permissão.

Configuração da página de topologia da grelha

Esta permissão fornece acesso às seguintes opções de menu:

- Guias de configuração disponíveis nas páginas em **suporte** > **Ferramentas** > **topologia de grade**.
- **Redefinir contagens de eventos** na guia **nós** > **Eventos**.

Outra Configuração de Grade

Esta permissão fornece acesso a opções de configuração de grade adicionais.

> Para ver essas opções adicionais, os usuários também devem ter a permissão de Configuração de Página de topologia de Grade.

- **Alarmes** (sistema legado):
  - Alarmes globais
  - Configuração de e-mail legado
- **ILM**:
  - Pools de armazenamento
  - Classes de armazenamento
- **Configuração** > **Configurações de rede**
  - Custo da ligação
- **Configuração** > **Configurações do sistema**:
  - Opções de exibição
  - Opções de grelha
  - Opções de armazenamento
- **Configuração** > **Monitoramento**:
  - Eventos
- **Suporte**:
  - AutoSupport

Contas de inquilino

Esta permissão fornece acesso à página **tenants** > **Tenant Accounts**.

> A versão 1 da API Grid Management (que foi obsoleta) usa essa permissão para gerenciar políticas de grupo de locatários, redefinir senhas de administrador Swift e gerenciar chaves de acesso S3 do usuário raiz.

Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página Contas de locatário, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.

> Você deve atribuir a permissão Contas do locatário ao grupo antes de poder atribuir essa permissão.

Manutenção

Esta permissão fornece acesso às seguintes opções de menu:

- **Configuração** > **Configurações do sistema**:
  - Nomes de domínio*
  - Certificados de servidor*
- **Configuração** > **Monitoramento**:
  - Auditoria*
- **Configuração** > **Controle de Acesso**:
  - Senhas de grade
- **Manutenção** > **tarefas de manutenção**
  - Descomissionar
  - Expansão
  - Recuperação
- **Manutenção** > **rede**:
  - Servidores DNS*
  - Rede de rede*
  - Servidores NTP*
- **Manutenção** > **sistema**:
  - Licença*
  - Pacote de recuperação
  - Atualização de software
- **Suporte** > **Ferramentas**:
  - Registos
- Os usuários que não têm a permissão Manutenção podem exibir, mas não editar, as páginas marcadas com um asterisco.

Consulta de métricas

Esta permissão fornece acesso à página **suporte** > **Ferramentas** > **métricas**. Essa permissão também fornece acesso a consultas de métricas personalizadas do Prometheus usando a seção **Metrics** da API Grid Management.

ILM

Esta permissão fornece acesso às seguintes opções de menu **ILM**:

- **Codificação de apagamento**
- **Regras**
- **Políticas**
- **Regiões**

> O acesso às opções de menu **ILM** > **Storage Pools** e **ILM** > **Storage grades** é controlado pelas outras permissões de Configuração de Grade e topologia de Grade Page Configuration.

Pesquisa de metadados de objetos

Esta permissão fornece acesso à opção de menu **ILM** > **Object Metadata Lookup**.

Administrador do dispositivo de armazenamento

Essa permissão fornece acesso ao Gerenciador de sistemas do e-Series SANtricity em dispositivos de storage por meio do Gerenciador de Grade.

Interação entre permissões e modo de acesso

Para todas as permissões, a configuração modo de acesso do grupo determina se os usuários podem alterar configurações e executar operações ou se eles podem exibir somente as configurações e recursos relacionados. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

Desativando recursos da API de Gerenciamento de Grade

Você pode usar a API de gerenciamento de grade para desativar completamente certos recursos no sistema StorageGRID. Quando um recurso é desativado, ninguém pode receber permissões para executar as tarefas relacionadas a esse recurso.

Sobre esta tarefa

O sistema de funcionalidades desativadas permite-lhe impedir o acesso a determinadas funcionalidades no sistema StorageGRID. A desativação de um recurso é a única maneira de impedir que o usuário raiz ou os usuários que pertencem a grupos de administração com a permissão de acesso root possam usar esse recurso.

Para entender como essa funcionalidade pode ser útil, considere o seguinte cenário:

A empresa A é um provedor de serviços que aluga a capacidade de armazenamento de seu sistema StorageGRID criando contas de inquilino. Para proteger a segurança dos objetos de seus arrendatários, a empresa A quer garantir que seus próprios funcionários nunca possam acessar qualquer conta de locatário depois que a conta tiver sido implantada.

*A empresa A pode atingir esse objetivo usando o sistema Deactivate Features na API Grid Management. Ao desativar completamente o recurso **Change Tenant Root Password** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A pode garantir que nenhum usuário Admin - incluindo o usuário root e usuários pertencentes a grupos com a permissão de acesso root - pode alterar a senha para o usuário root de qualquer conta de locatário.*

Reativando as funcionalidades desativadas

Por padrão, você pode usar a API de Gerenciamento de Grade para reativar um recurso que foi desativado. No entanto, se você quiser impedir que os recursos desativados sejam reativados, você pode desativar o próprio recurso **activateFeatures**.

> O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar esse recurso, esteja ciente de que você perderá permanentemente a capacidade de reativar quaisquer outros recursos desativados. Você deve entrar em Contato com o suporte técnico para restaurar qualquer funcionalidade perdida.

Para obter detalhes, consulte as instruções para a implementação de aplicativos cliente S3 ou Swift.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o endpoint Deactivate Features
3. Para desativar um recurso, como **alterar senha de root do locatário**, envie um corpo para a API assim:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Quando a solicitação estiver concluída, o recurso alterar senha raiz do locatário é desativado. A permissão de gerenciamento de senha raiz do locatário de alteração não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário falhará com "'403 Forbidden.'"

4. Para reativar todos os recursos, envie um corpo para a API assim:

```
{ "grid": null }
```

Quando esta solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento de senha de raiz do locatário de alteração agora aparece na interface do usuário e qualquer solicitação de API que tente alterar a senha de raiz de um locatário será bem-sucedida, assumindo que o usuário tenha a permissão de gerenciamento de senha de raiz do locatário ou altere a permissão de gerenciamento de senha de raiz do locatário.

> O exemplo anterior faz com que os recursos *All* desativados sejam reativados. Se outros recursos tiverem sido desativados que devem permanecer desativados, você deverá especificá-los explicitamente na SOLICITAÇÃO PUT. Por exemplo, para reativar o recurso alterar senha de raiz do locatário e continuar a desativar o recurso de reconhecimento de alarme, envie esta SOLICITAÇÃO DE COMPRA:

```
{ "grid": { "alarmAcknowledgment": true } }
```

Informações relacionadas

"Usando a API de gerenciamento de grade"

Modificando um grupo de administração

Você pode modificar um grupo de administração para alterar as permissões associadas ao grupo. Para grupos de administração locais, também é possível atualizar o nome de exibição.

O que você vai precisar

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

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Groups**.
2. Selecione o grupo.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Editar**.
4. Opcionalmente, para grupos locais, digite o nome do grupo que aparecerá para os usuários, por exemplo, "'usuários de Manutenção.'"

   Não é possível alterar o nome exclusivo, que é o nome do grupo interno.

5. Opcionalmente, altere o modo de acesso do grupo.
   - **Leitura-escrita** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade. Os usuários locais só de leitura podem alterar suas próprias senhas.

   > Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

6. Opcionalmente, adicione ou remova permissões de grupo.

   Consulte informações sobre as permissões do grupo de administração.

7. Selecione **Guardar**.

Informações relacionadas

Permissões do grupo de administração

Eliminar um grupo de administração

Você pode excluir um grupo de administração quando quiser remover o grupo do sistema e remover todas as permissões associadas ao grupo. A exclusão de um grupo de administração remove quaisquer usuários de administrador do grupo, mas não exclui os usuários de administrador.

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

Quando você exclui um grupo, os usuários atribuídos a esse grupo perderão todos os Privileges de Acesso ao Gerenciador de Grade, a menos que sejam concedidos Privileges por um grupo diferente.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Groups**.
2. Selecione o nome do grupo.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Selecione **Remover**.
4. Selecione **OK**.

Gerenciamento de usuários locais

Você pode criar usuários locais e atribuí-los a grupos de administração locais para determinar quais recursos do Gerenciador de Grade esses usuários podem acessar.

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, não é possível remover o usuário root.

Se o logon único (SSO) tiver sido ativado, os usuários locais não poderão fazer login no StorageGRID.

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

Criando um usuário local

Se tiver criado grupos de administração locais, pode criar um ou mais utilizadores locais e atribuir cada utilizador a um ou mais grupos. As permissões do grupo controlam quais recursos do Gerenciador de Grade o usuário pode acessar.

Sobre esta tarefa

Você só pode criar usuários locais e só pode atribuir esses usuários a grupos de administração locais. Usuários federados e grupos federados são gerenciados usando a fonte de identidade externa.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Clique em **criar**.
3. Introduza o nome de apresentação do utilizador, o nome exclusivo e a palavra-passe.
4. Atribua o usuário a um ou mais grupos que governam as permissões de acesso.

   A lista de nomes de grupos é gerada a partir da tabela grupos.

5. Clique em **Salvar**.

Informações relacionadas

"Gerenciando grupos de administradores"

Modificando a conta de um usuário local

Você pode modificar a conta de um usuário de administrador local para atualizar o nome de exibição do usuário ou a associação de grupo. Você também pode impedir temporariamente que um usuário acesse o sistema.

Sobre esta tarefa

Só pode editar utilizadores locais. Os detalhes do usuário federados são sincronizados automaticamente com a fonte de identidade externa.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Selecione o utilizador que pretende editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Editar**.
4. Opcionalmente, faça alterações no nome ou na associação ao grupo.
5. Opcionalmente, para impedir que o usuário acesse o sistema temporariamente, marque **Negar acesso**.
6. Clique em **Salvar**.

   As novas configurações são aplicadas da próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.

Eliminar a conta de um utilizador local

Você pode excluir contas de usuários locais que não precisam mais de acesso ao Gerenciador de Grade.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Selecione o utilizador local que pretende eliminar.

   Não é possível eliminar o utilizador local raiz predefinido.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Remover**.
4. Clique em **OK**.

Alterar a palavra-passe de um utilizador local

Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade. Além disso, os usuários que têm acesso à página usuários administradores podem alterar senhas para outros usuários locais.

Sobre esta tarefa

Você pode alterar senhas apenas para usuários locais. Os usuários federados devem alterar suas próprias senhas na fonte de identidade externa.

Passos

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Na página usuários, selecione o usuário.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **alterar senha**.
4. Introduza e confirme a palavra-passe e clique em **Guardar**.

Usando logon único (SSO) para StorageGRID

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0). Quando o SSO está ativado, todos os usuários devem ser autenticados por um provedor de identidade externo antes que possam acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatário. Os utilizadores locais não podem iniciar sessão no StorageGRID.

- "Como o single sign-on funciona"
- "Requisitos para o uso de logon único"
- "Configurando logon único"

Como o single sign-on funciona

Antes de ativar o SSO (logon único), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está ativado.

Iniciar sessão quando o SSO está ativado

Quando o SSO está ativado e você entra no StorageGRID, você é redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

1. Insira o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó de administrador do StorageGRID em um navegador da Web.

   É apresentada a página de início de sessão do StorageGRID.

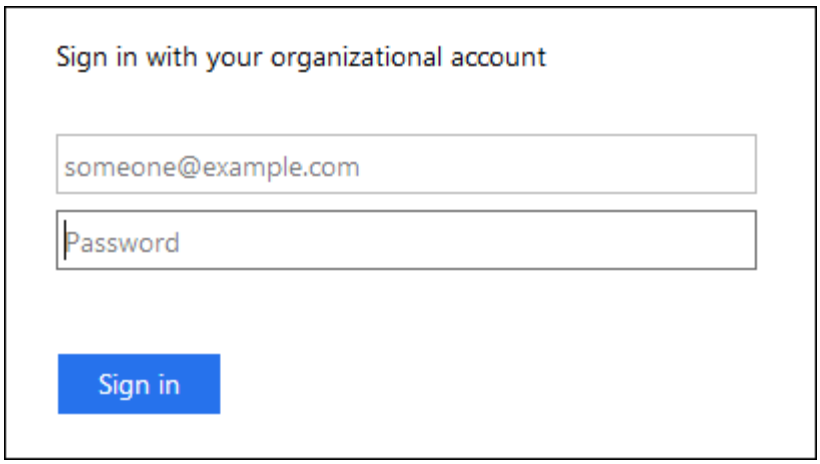
- Se esta for a primeira vez que você acessou o URL neste navegador, será solicitado um ID de conta:

- Se você acessou anteriormente o Gerenciador de Grade ou o Gerente do Locatário, será solicitado que você selecione uma conta recente ou insira um ID de conta:

A página de login do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido de `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da sua organização, onde você pode Inicie sessão com as suas credenciais SSO.

2. Indique se deseja acessar o Gerenciador de Grade ou o Gerenciador de Locatário:
   - Para acessar o Gerenciador de Grade, deixe o campo **ID de conta** em branco, digite **0** como ID de conta ou selecione **Gerenciador de Grade** se ele aparecer na lista de contas recentes.
   - Para acessar o Gerenciador do Locatário, insira o ID da conta do locatário de 20 dígitos ou selecione um locatário pelo nome se ele aparecer na lista de contas recentes.
3. Clique em **entrar**

O StorageGRID redireciona você para a página de login SSO da sua organização. Por exemplo:



4. Faça login com suas credenciais SSO.

   Se suas credenciais SSO estiverem corretas:

   a. O provedor de identidade (IDP) fornece uma resposta de autenticação ao StorageGRID.
   b. O StorageGRID valida a resposta de autenticação.
   c. Se a resposta for válida e você pertencer a um grupo federado que tenha permissão de acesso adequada, você será conetado ao Gerenciador de Grade ou ao Gerente do locatário, dependendo da conta selecionada.

5. Opcionalmente, acesse outros nós de administração ou acesse o Gerenciador de grade ou o Gerenciador de locatário, se você tiver permissões adequadas.

   Você não precisa reinserir suas credenciais SSO.

Terminar sessão quando o SSO está ativado

Quando o SSO está ativado para o StorageGRID, o que acontece quando você sai depende do que você está conetado e de onde você está se saindo.

Passos

1. Localize o link **Sair** no canto superior direito da interface do usuário.
2. Clique em **Sair**.

   É apresentada a página de início de sessão do StorageGRID. A lista suspensa **Recent Accounts** (Contas recentes) é atualizada para incluir o **Grid Manager** ou o nome do locatário, para que você possa acessar essas interfaces de usuário mais rapidamente no futuro.

Se você estiver conetado a…	E você sai de…	Você está logado fora de…
Grid Manager em um ou mais nós de administração	Grid Manager em qualquer nó de administração	Grid Manager em todos os nós de administração
Gerenciador de locatários em um ou mais nós de administração	Gerente de locatário em qualquer nó de administrador	Gerenciador de locatários em todos os nós de administração

Se você estiver conetado a…	E você sai de…	Você está logado fora de…
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Apenas o Grid Manager. Você também deve sair do Gerenciador do Locatário para sair do SSO.

A tabela resume o que acontece quando você sai se estiver usando uma única sessão do navegador. Se você estiver conetado ao StorageGRID em várias sessões do navegador, será necessário sair de todas as sessões do navegador separadamente.

Requisitos para o uso de logon único

Antes de ativar o logon único (SSO) para um sistema StorageGRID, revise os requisitos nesta seção.

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Requisitos do provedor de identidade

O provedor de identidade (IDP) para SSO deve atender aos seguintes requisitos:

- Uma das seguintes versões do ative Directory Federation Service (AD FS):
  - AD FS 4,0, incluído no Windows Server 2016

    O Windows Server 2016 deve estar usando o "Atualização do KB3201845", ou superior.

  - AD FS 3,0, incluído na atualização do Windows Server 2012 R2 ou superior.
- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Requisitos de certificado do servidor

O StorageGRID usa um certificado de servidor de interface de gerenciamento em cada nó de administrador 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. Quando você configura as confianças de parte confiáveis SSO para o StorageGRID no AD FS, você usa o certificado do servidor como o certificado de assinatura para solicitações do StorageGRID para o AD FS.

Se você ainda não tiver instalado um certificado de servidor personalizado para a interface de gerenciamento, você deve fazê-lo agora. Quando você instala um certificado de servidor personalizado, ele é usado para todos os nós de administração e você pode usá-lo em todos os trusts de terceiros dependentes do StorageGRID.

O uso do certificado de servidor padrão de um nó Admin na confiança de parte dependente do AD FS não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de poder iniciar sessão no nó recuperado, tem de atualizar a confiança da parte dependente no AD FS com o novo certificado.

Você pode acessar o certificado de servidor de um nó de administrador fazendo login no shell de comando do nó e indo para `/var/local/mgmt-api` o diretório. Um certificado de servidor personalizado é `custom-server.crt` nomeado . O certificado de servidor padrão do nó é `server.crt` nomeado .

Informações relacionadas

"Controlar o acesso através de firewalls"

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

Configurando logon único

Quando o logon único (SSO) está ativado, os usuários só podem acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de gerenciamento de grade ou a API de gerenciamento de locatário se suas credenciais forem autorizadas usando o processo de login SSO implementado pela sua organização.

- "Confirmar que usuários federados podem entrar"
- "Usando o modo sandbox"
- "Criando confianças de parte confiáveis no AD FS"
- "Testando confianças de parte de confiança"
- "Ativar o início de sessão único"
- "Desativação do logon único"
- "Desativando e rehabilitando temporariamente o logon único para um nó de administração"

Confirmar que usuários federados podem entrar

Antes de ativar o logon único (SSO), você deve confirmar que pelo menos um usuário federado pode entrar no Gerenciador de Grade e entrar no Gerenciador de locatários para quaisquer contas de locatário existentes.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você está usando o ative Directory como fonte de identidade federada e o AD FS como provedor de identidade.

  "Requisitos para o uso de logon único"

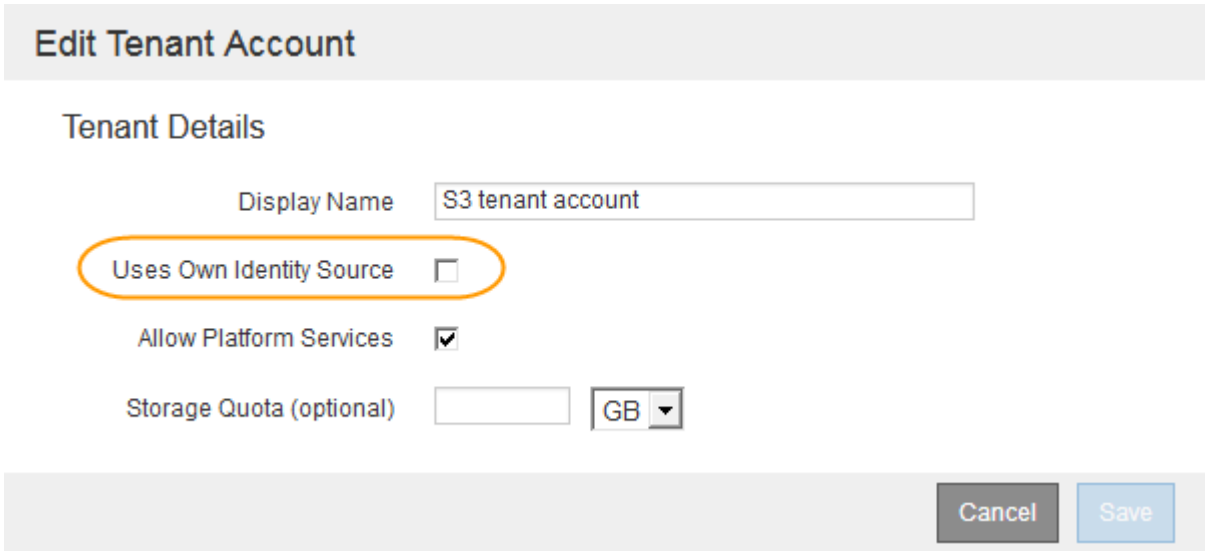
Passos

1. Se houver contas de inquilino existentes, confirme que nenhum dos inquilinos está usando sua própria fonte de identidade.

   Quando você ativa o SSO, uma fonte de identidade configurada no Gerenciador de locatário é substituída pela origem de identidade configurada no Gerenciador de Grade. Os usuários pertencentes à fonte de identidade do locatário não poderão mais entrar a menos que tenham uma conta com a fonte de identidade do Gerenciador de Grade.

a. Inicie sessão no Gestor do Locatário para cada conta de inquilino.
b. Selecione **Access Control** > **Identity Federation**.
c. Confirme se a caixa de verificação **Ativar Federação de identidade** não está selecionada.
d. Se estiver, confirme se os grupos federados que possam estar em uso para essa conta de locatário não são mais necessários, desmarque a caixa de seleção e clique em **Salvar**.

2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
   a. No Gerenciador de Grade, selecione **Configuração** > **Controle de Acesso** > **grupos de administradores**.
   b. Certifique-se de que pelo menos um grupo federado tenha sido importado da origem de identidade do ative Directory e de que tenha sido atribuída a permissão de acesso raiz.
   c. Terminar sessão.
   d. Confirme que você pode fazer login novamente no Gerenciador de Grade como um usuário no grupo federado.
3. Se houver contas de locatário existentes, confirme se um usuário federado que tenha permissão de acesso root pode entrar:
   a. No Gerenciador de Grade, selecione **tenants**.
   b. Selecione a conta de locatário e clique em **Editar conta**.
   c. Se a caixa de seleção **usa origem de identidade própria** estiver selecionada, desmarque a caixa e clique em **Salvar**.



   A página Contas do locatário é exibida.
   a. Selecione a conta de locatário, clique em **entrar** e faça login na conta de locatário como usuário raiz local.
   b. No Gerenciador do Locatário, clique em **Controle de Acesso** > **grupos**.
   c. Certifique-se de que pelo menos um grupo federado do Gerenciador de Grade recebeu a permissão de acesso raiz para esse locatário.
   d. Terminar sessão.
   e. Confirme que você pode fazer login novamente no locatário como um usuário no grupo federado.

Informações relacionadas

"Requisitos para o uso de logon único"

"Gerenciando grupos de administradores"

"Use uma conta de locatário"

Usando o modo sandbox

Você pode usar o modo sandbox para configurar e testar as confianças de parte dependentes dos Serviços de Federação do ative Directory (AD FS) antes de aplicar o logon único (SSO) para usuários do StorageGRID. Depois que o SSO estiver ativado, você poderá reativar o modo sandbox para configurar ou testar novos e existentes trusts de terceiros. A reativação do modo sandbox desativa temporariamente o SSO para usuários do StorageGRID.

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

Quando o SSO está ativado e um usuário tenta entrar em um nó de administrador, o StorageGRID envia uma solicitação de autenticação para o AD FS. Por sua vez, o AD FS envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autorização foi bem-sucedida. Para solicitações bem-sucedidas, a resposta inclui um identificador universal exclusivo (UUID) para o usuário.

Para permitir que o StorageGRID (o provedor de serviços) e o AD FS (o provedor de identidade) se comuniquem com segurança sobre solicitações de autenticação de usuário, você deve configurar determinadas configurações no StorageGRID. Em seguida, você deve usar o AD FS para criar uma confiança de parte confiável para cada nó Admin. Finalmente, você deve retornar ao StorageGRID para ativar o SSO.

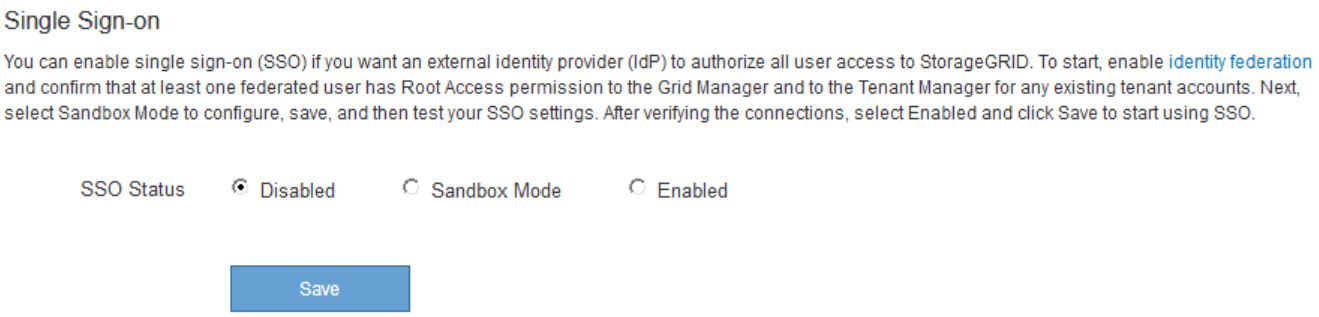
O modo Sandbox facilita a execução desta configuração de back-and-forth e testar todas as suas configurações antes de ativar o SSO.

> O uso do modo sandbox é altamente recomendado, mas não é estritamente necessário. Se você estiver preparado para criar confianças de parte dependentes do AD FS imediatamente após configurar o SSO no StorageGRID e não precisar testar os processos de SSO e logout único (SLO) para cada nó de administrador, clique em **habilitado**, insira as configurações do StorageGRID, crie uma confiança de parte confiável para cada nó de administrador no AD FS e clique em **Salvar** para ativar o SSO.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   A página Single Sign-On (Início de sessão único) é exibida, com a opção **Disabled** selecionada.



Se as opções de Status SSO não forem exibidas, confirme se você configurou o ative Directory como a origem de identidade federada. Consulte ""requisitos para utilizar o início de sessão único.""

2. Selecione a opção **Sandbox Mode**.

   As configurações Provedor de identidade e parte dependente aparecem. Na seção Provedor de identidade, o campo **tipo de serviço** é somente leitura. Ele mostra o tipo de serviço de federação de identidade que você está usando (por exemplo, ative Directory).

3. Na seção Provedor de identidade:

   a. Insira o nome do Serviço de Federação, exatamente como aparece no AD FS.

      Para localizar o Nome do Serviço de Federação, vá para Windows Server Manager. Selecione **Ferramentas** > **Gerenciamento do AD FS**. No menu Ação, selecione **Editar Propriedades do Serviço de Federação**. O Nome do Serviço de Federação é apresentado no segundo campo.

   b. Especifique se deseja usar a Segurança da camada de Transporte (TLS) para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.

      - **Use o certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
      - **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

        Se você selecionar essa configuração, copie e cole o certificado na caixa de texto **certificado CA**.

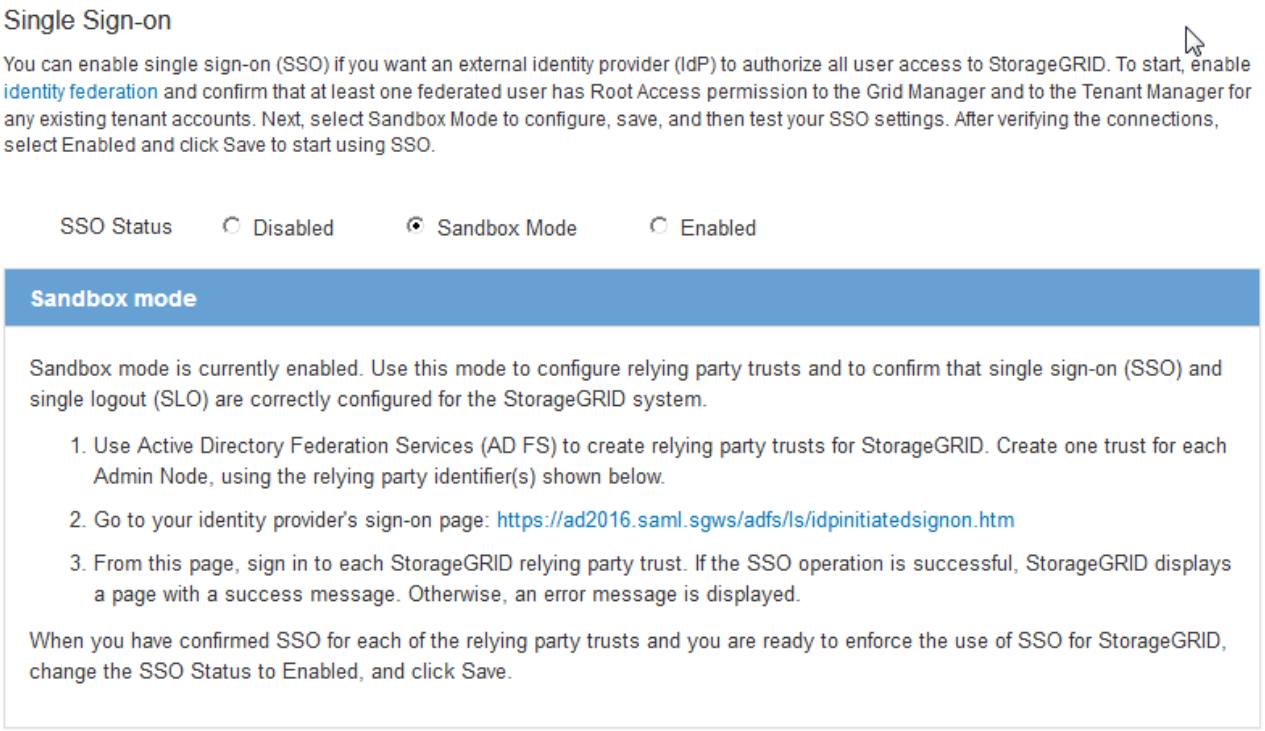
      - **Não use TLS**: Não use um certificado TLS para proteger a conexão.

4. Na seção parte dependente, especifique o identificador de parte dependente que você usará para nós de administrador do StorageGRID quando você configurar confianças de parte dependentes.

   - Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
   - Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que inclui um identificador de parte confiável para cada nó Admin, com base no nome do host do nó. Observação: Você deve criar uma confiança de parte confiável para cada nó de administrador em seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

5. Clique em **Salvar**.
   - Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

   - O aviso de confirmação do modo Sandbox aparece, confirmando que o modo sandbox está agora ativado. Você pode usar esse modo enquanto usa o AD FS para configurar uma confiança de parte confiável para cada nó Admin e testar os processos de login único (SSO) e logout único (SLO).



Informações relacionadas

"Requisitos para o uso de logon único"

Criando confianças de parte confiáveis no AD FS

Você deve usar os Serviços de Federação do ative Directory (AD FS) para criar uma confiança de parte confiável para cada nó de administração em seu sistema. Você pode criar trusts confiáveis de parte usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Criando uma confiança de parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais trusts de parte confiáveis.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.

Você deve criar uma confiança de parte confiável para cada nó de administrador no seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

- Você tem experiência em criar confiança de parte confiável no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No menu Iniciar do Windows, clique com o botão direito do Mouse no ícone do PowerShell e selecione **Executar como Administrador**.
2. No prompt de comando do PowerShell, digite o seguinte comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para *Admin_Node_Identifier*, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão único. Por exemplo, `SG-DC1-ADM1`.
   - Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)
3. No Gerenciador do Windows Server, selecione **Ferramentas** > **Gerenciamento do AD FS**.

   A ferramenta de gerenciamento do AD FS é exibida.
4. Selecione **AD FS** > **confiar em parts**.

   É apresentada a lista de confianças de partes dependentes.
5. Adicione uma Política de Controle de Acesso à confiança da entidade dependente recém-criada:
   a. Localize a confiança de quem confia que você acabou de criar.
   b. Clique com o botão direito do rato na fidedignidade e selecione **Editar política de controlo de acesso**.
   c. Selecione uma política de controlo de acesso.
   d. Clique em **Apply** e clique em **OK**
6. Adicione uma Política de emissão de reclamação à recém-criada confiança da parte dependente:
   a. Localize a confiança de quem confia que você acabou de criar.
   b. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.
   c. Clique em **Adicionar regra**.

d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.

e. Na página Configurar regra, insira um nome de exibição para essa regra.

   Por exemplo, **ObjectGUID to Name ID**.

f. Para o Attribute Store, selecione **ative Directory**.

g. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.

h. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.

i. Clique em **Finish** e clique em **OK**.

7. Confirme se os metadados foram importados com sucesso.

   a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.

   b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** estão preenchidos.

      Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou simplesmente insira os valores manualmente.

8. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.

9. Quando terminar, regresse ao StorageGRID e "teste todos os trusts de confiança"confirme que estão configurados corretamente.

Criando uma confiança de parte confiável importando metadados de federação

Você pode importar os valores de cada confiança de parte confiável acessando os metadados SAML para cada nó de administração.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.

  > Você deve criar uma confiança de parte confiável para cada nó de administrador no seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

- Você tem experiência em criar confiança de parte confiável no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No Gerenciador do Windows Server, clique em **Ferramentas** e selecione **Gerenciamento do AD FS**.
2. Em ações, clique em **Adicionar confiança de parte dependente**.

3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e clique em **Iniciar**.
4. Selecione **Importar dados sobre a parte dependente publicada on-line ou em uma rede local**.
5. Em **Endereço de metadados de Federação (nome do host ou URL)**, digite o local dos metadados SAML para este nó de administração:

   `https://Admin_Node_FQDN/api/saml-metadata`

   Para *`Admin_Node_FQDN`*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

6. Conclua o assistente confiar na parte confiável, salve a confiança da parte confiável e feche o assistente.

   Ao inserir o nome de exibição, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. Por exemplo, `SG-DC1-ADM1`.

7. Adicionar uma regra de reclamação:
   a. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.
   b. Clique em **Adicionar regra**:
   c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
   d. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID to Name ID**.

   e. Para o Attribute Store, selecione **ative Directory**.
   f. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
   g. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   h. Clique em **Finish** e clique em **OK**.
8. Confirme se os metadados foram importados com sucesso.
   a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
   b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** estão preenchidos.

      Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou simplesmente insira os valores manualmente.

9. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.
10. Quando terminar, regresse ao StorageGRID e "teste todos os trusts de confiança"confirme que estão configurados corretamente.

Criando uma confiança de parte confiável manualmente

Se você optar por não importar os dados para as partes confiáveis, você poderá inserir os valores

manualmente.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.

> Você deve criar uma confiança de parte confiável para cada nó de administrador no seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

- Você tem o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID ou sabe como fazer login em um nó de administrador a partir do shell de comando.
- Você tem experiência em criar confiança de parte confiável no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No Gerenciador do Windows Server, clique em **Ferramentas** e selecione **Gerenciamento do AD FS**.
2. Em ações, clique em **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e clique em **Iniciar**.
4. Selecione **Digite os dados sobre a parte confiável manualmente** e clique em **Avançar**.
5. Conclua o assistente confiança da parte dependente:

   a. Introduza um nome de apresentação para este nó de administração.

      Para obter consistência, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. Por exemplo, `SG-DC1-ADM1`.

   b. Ignore a etapa para configurar um certificado de criptografia de token opcional.

   c. Na página Configurar URL, marque a caixa de seleção **Ativar suporte para o protocolo SAML 2,0 WebSSO**.

   d. Digite o URL do endpoint do serviço SAML para o nó Admin:

      `https://Admin_Node_FQDN/api/saml-response`

      Para *`Admin_Node_FQDN`*, introduza o nome de domínio totalmente qualificado para o nó Admin. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

   e. Na página Configurar Identificadores, especifique o Identificador da parte de dependência para o mesmo nó de administração:

      `Admin_Node_Identifier`

Para *Admin_Node_Identifier*, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão único. Por exemplo, `SG-DC1-ADM1`.

f. Revise as configurações, salve a confiança da parte confiável e feche o assistente.

A caixa de diálogo Editar política de emissão de reclamação é exibida.

> Se a caixa de diálogo não for exibida, clique com o botão direito do Mouse no Trust e selecione **Editar política de emissão de reclamação**.

6. Para iniciar o assistente de regra de reclamação, clique em **Adicionar regra**:
   a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
   b. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID to Name ID**.

   c. Para o Attribute Store, selecione **ative Directory**.
   d. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
   e. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   f. Clique em **Finish** e clique em **OK**.
7. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):
   a. Clique em **Add SAML**.
   b. Selecione **Endpoint Type** > **SAML Logout**.
   c. Selecione **Binding** > **Redirect**.
   d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó Admin:

      `https://Admin_Node_FQDN/api/saml-logout`

   Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado do nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

   a. Clique em **OK**.
9. Na guia **assinatura**, especifique o certificado de assinatura para essa confiança de parte confiável:
   a. Adicione o certificado personalizado:
      - Se tiver o certificado de gestão personalizado que carregou no StorageGRID, selecione esse certificado.
      - Se você não tiver o certificado personalizado, faça login no Admin Node, vá para `/var/local/mgmt-api` o diretório do Admin Node e adicione o `custom-server.crt` arquivo de certificado.

        Observação: usando o certificado padrão do Admin Node (`server.crt`) não é recomendado. Se

o nó Admin falhar, o certificado padrão será regenerado quando você recuperar o nó e você precisará atualizar a confiança da parte confiável.

b. Clique em **Apply** e clique em **OK**.

As propriedades da parte dependente são salvas e fechadas.

10. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.
11. Quando terminar, regresse ao StorageGRID e "teste todos os trusts de confiança"confirme que estão configurados corretamente.

Testando confianças de parte de confiança

Antes de aplicar o uso de logon único (SSO) para StorageGRID, confirme se o logon único e o logout único (SLO) estão configurados corretamente. Se você criou uma confiança de parte confiável para cada nó Admin, confirme que você pode usar SSO e SLO para cada nó Admin.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você configurou uma ou mais confianças de parte confiáveis no AD FS.

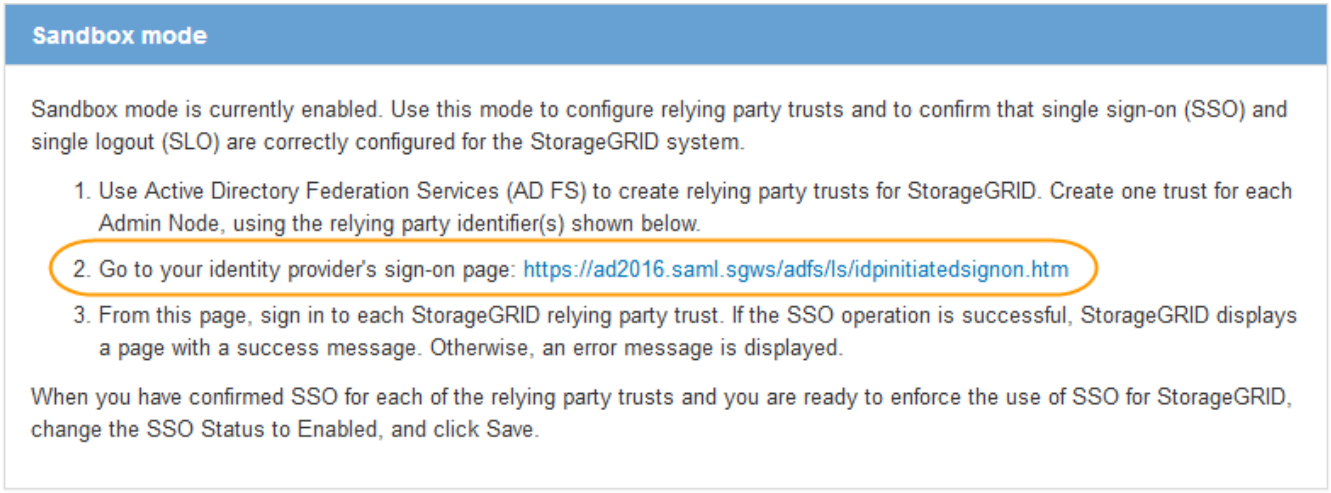
Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   A página Single Sign-On (Início de sessão único) é exibida, com a opção **Sandbox Mode** selecionada.

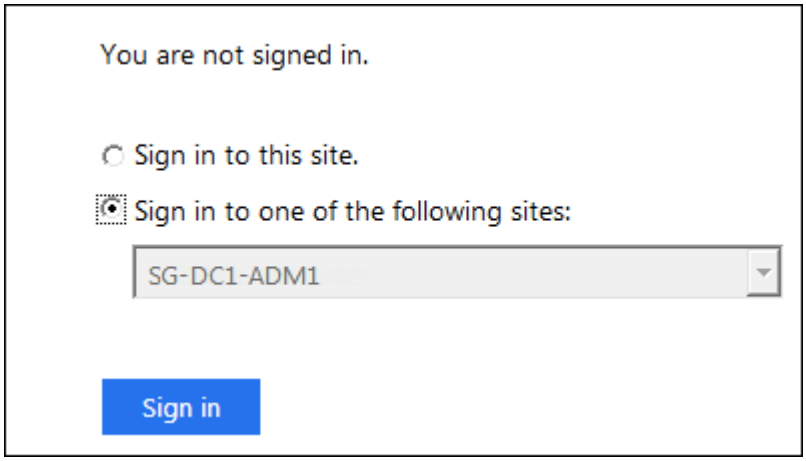
2. Nas instruções para o modo sandbox, localize o link para a página de logon do provedor de identidade.

   O URL é derivado do valor inserido no campo **Nome do serviço federado**.



3. Clique no link ou copie e cole o URL em um navegador para acessar a página de logon do provedor de identidade.
4. Para confirmar que você pode usar o SSO para entrar no StorageGRID, selecione **entrar em um dos seguintes sites**, selecione o identificador de parte confiável para seu nó de administrador principal e

clique em **entrar**.



Você é solicitado a digitar seu nome de usuário e senha.

5. Introduza o seu nome de utilizador federado e a palavra-passe.
   - Se as operações de login e logout SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se a operação SSO não for bem-sucedida, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
6. Repita as etapas anteriores para confirmar que você pode entrar em qualquer outro nó Admin.

   Se todas as operações de login e logout SSO forem bem-sucedidas, você estará pronto para ativar o SSO.

Ativar o início de sessão único

Depois de usar o modo sandbox para testar todas as suas trusts de terceiros dependentes do StorageGRID, você está pronto para ativar o logon único (SSO).

O que você vai precisar

- Você deve ter importado pelo menos um grupo federado da origem da identidade e atribuído permissões de gerenciamento de acesso raiz ao grupo. Você deve confirmar que pelo menos um usuário federado tem permissão de acesso root ao Gerenciador de Grade e ao Gerente do locatário para quaisquer contas de locatário existentes.
- Você deve ter testado todas as confianças de parte que dependem usando o modo sandbox.

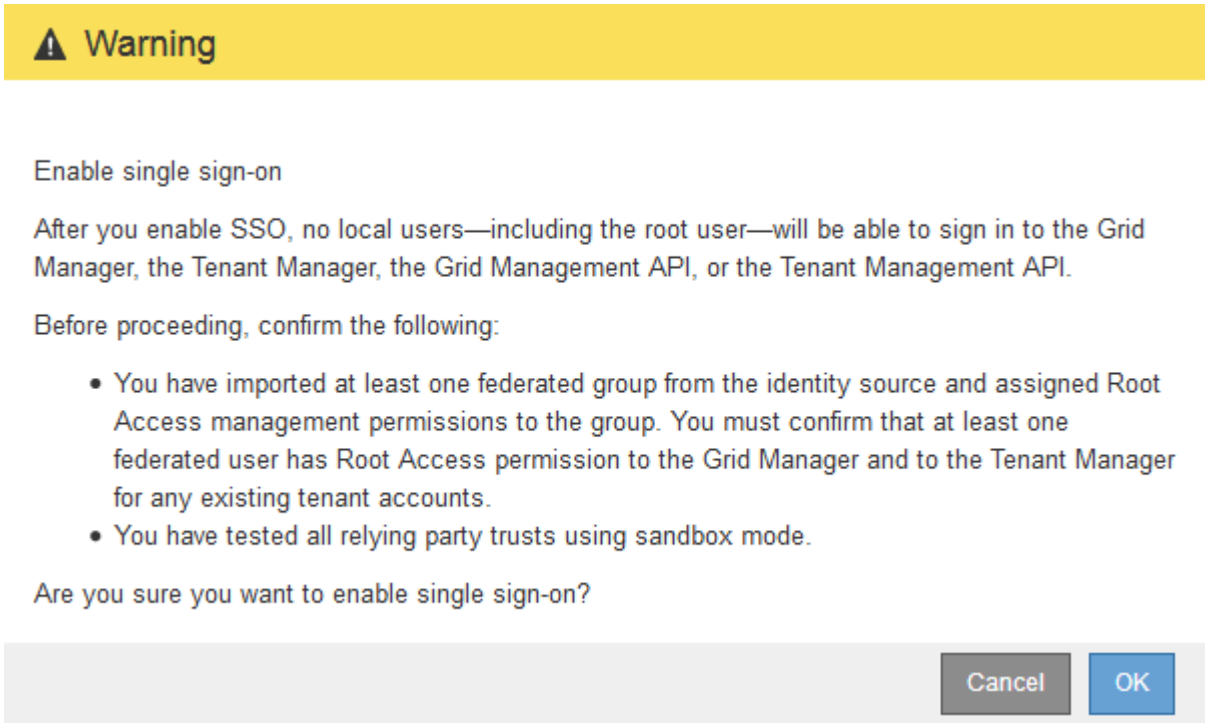
Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   A página Single Sign-On (Início de sessão único) aparece com **Sandbox Mode** selecionado.

2. Altere o Status SSO para **Enabled**.
3. Clique em **Salvar**.

É apresentada uma mensagem de aviso.



4. Reveja o aviso e clique em **OK**.

   O início de sessão único está agora ativado.

> Todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Tenant, a API de gerenciamento de grade e a API de gerenciamento de locatário. Os usuários locais não podem mais acessar o StorageGRID.

Desativação do logon único

Você pode desativar o logon único (SSO) se não quiser mais usar essa funcionalidade. Você deve desativar o logon único antes de desativar a federação de identidade.

O que você vai precisar

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

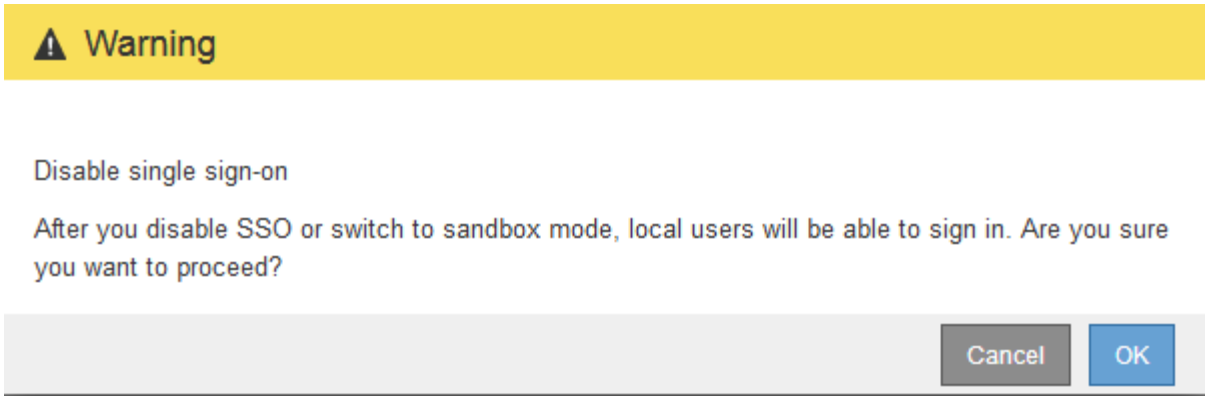
Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.

   É apresentada a página Single Sign-on (Início de sessão único).

2. Selecione a opção **Disabled** (Desativado).
3. Clique em **Salvar**.

   É apresentada uma mensagem de aviso indicando que os utilizadores locais poderão iniciar sessão.



4. Clique em **OK**.

   Na próxima vez que você entrar no StorageGRID, a página de login do StorageGRID será exibida e você deverá inserir o nome de usuário e a senha de um usuário do StorageGRID local ou federado.

Desativando e rehabilitando temporariamente o logon único para um nó de administração

Talvez você não consiga entrar no Gerenciador de Grade se o sistema de logon único (SSO) estiver inativo. Nesse caso, você pode desativar e reativar temporariamente o SSO para um nó de administrador. Para desativar e reativar o SSO, você deve acessar o shell de comando do nó.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber a senha para o usuário raiz local.

Sobre esta tarefa

Depois de desativar o SSO para um nó Admin, você pode entrar no Gerenciador de Grade como o usuário raiz local. Para proteger seu sistema StorageGRID, você deve usar o shell de comando do nó para reativar o SSO no nó Admin assim que você sair.

> ⓘ A desativação do SSO para um nó Admin não afeta as configurações de SSO para quaisquer outros nós Admin na grade. A caixa de seleção **Ativar SSO** na página de logon único no Gerenciador de Grade permanece selecionada e todas as configurações SSO existentes são mantidas, a menos que você as atualize.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@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 `#`.

2. Execute o seguinte comando:`disable-saml`

   Uma mensagem indica que o comando se aplica somente a esse nó Admin.

3. Confirme que você deseja desativar o SSO.

   Uma mensagem indica que o logon único está desativado no nó.

4. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.

   A página de login do Gerenciador de Grade agora é exibida porque o SSO foi desativado.

5. Inicie sessão com a raiz do nome de utilizador e a palavra-passe do utilizador raiz local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração SSO:
   a. Selecione **Configuração** > **Controle de Acesso** > **Início de sessão único**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.
   c. Clique em **Salvar**.

      Clicar em **Salvar** na página de logon único reativa automaticamente o SSO para toda a grade.

7. Se você desativou o SSO temporariamente porque precisava acessar o Gerenciador de Grade por algum outro motivo:

   a. Execute qualquer tarefa ou tarefas que você precisa executar.
   b. Clique em **Sair** e feche o Gerenciador de Grade.
   c. Reative o SSO no nó Admin. Você pode executar uma das seguintes etapas:

      - Execute o seguinte comando: `enable-saml`

        Uma mensagem indica que o comando se aplica somente a esse nó Admin.

      Confirme se você deseja ativar o SSO.

   Uma mensagem indica que o logon único está ativado no nó.

      - Reinicie o nó da grade: `reboot`

8. A partir de um navegador da Web, acesse o Gerenciador de Grade a partir do mesmo nó Admin.
9. Confirme se a página de login do StorageGRID é exibida e que você deve inserir suas credenciais SSO para acessar o Gerenciador de Grade.

Informações relacionadas

"Configurando logon único"

Configurando certificados de cliente de administrador

Você pode usar certificados de cliente para permitir que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. Os certificados de cliente fornecem uma maneira segura de usar ferramentas externas para monitorar o StorageGRID.

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

Adicionando certificados de cliente administrador

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

O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve saber o endereço IP ou o nome de domínio do nó Admin.
- Você deve ter configurado o certificado do servidor de interface de gerenciamento do StorageGRID e ter o pacote de CA correspondente
- Se você quiser carregar seu próprio certificado, a chave pública e a chave privada do certificado devem estar disponíveis no computador local.

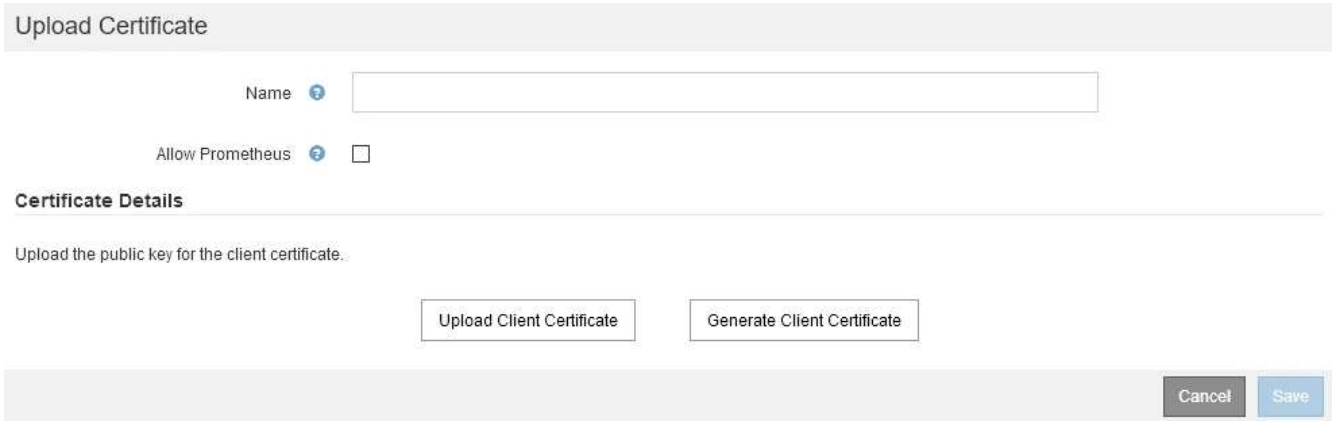
Passos

1. No Gerenciador de Grade, selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

   A página certificados de cliente é exibida.

2. Selecione **Adicionar**.

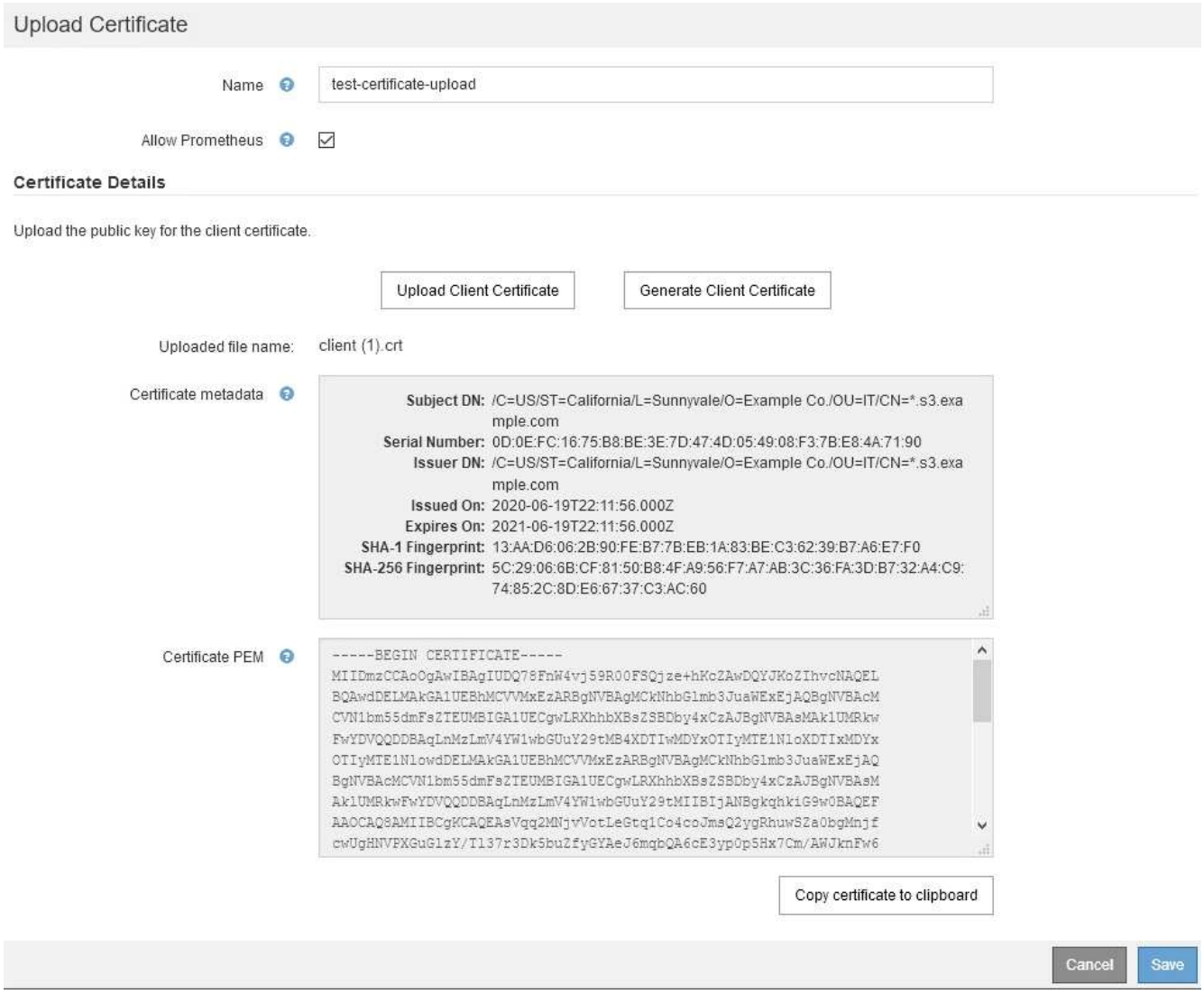
   A página carregar certificado é exibida.



3. Digite um nome entre 1 e 32 carateres para o certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, marque a caixa de seleção **Allow Prometheus**.

5. Carregar ou gerar um certificado:
   a. Para carregar um certificado, vá aqui.
   b. Para gerar um certificado, vá aqui.
6. para carregar um certificado:
   a. Selecione **carregar certificado de cliente**.
   b. Procure a chave pública do certificado.

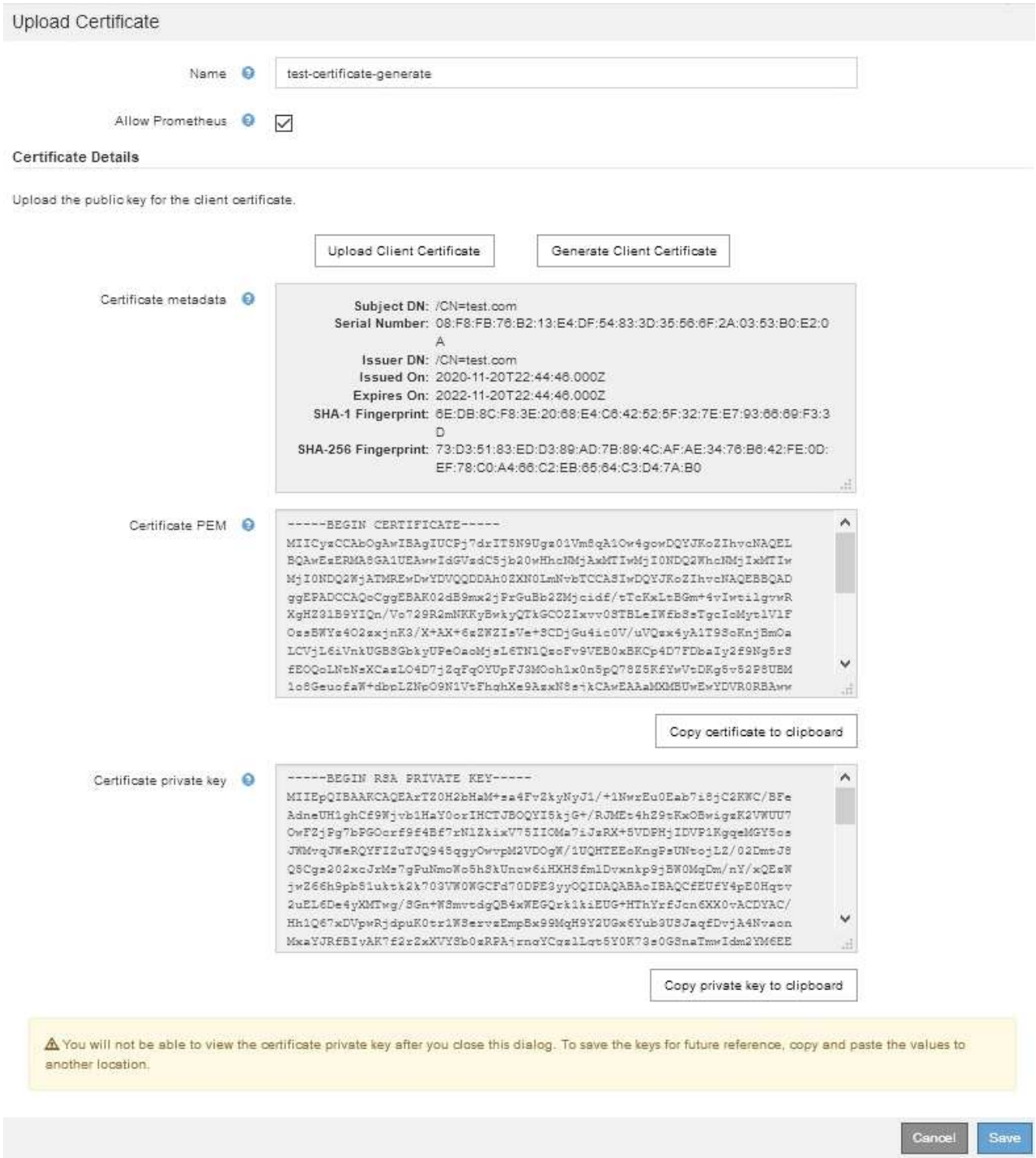
      Depois de carregar a chave pública para o certificado, os campos **metadados do certificado** e **PEM** do certificado são preenchidos.



   a. Selecione **Copiar certificado para a área de transferência** e cole o certificado na ferramenta de monitoramento externa.
   b. Use uma ferramenta de edição para copiar e colar a chave privada na sua ferramenta de monitoramento externo.
   c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.
7. para gerar um certificado:

a. Selecione **Generate Client Certificate**.
b. Introduza o nome de domínio ou o endereço IP do nó de administração.
c. Opcionalmente, insira um assunto X,509, também chamado de Nome distinto (DN), para identificar o administrador que possui o certificado.
d. Opcionalmente, selecione o número de dias em que o certificado é válido. O padrão é de 730 dias.
e. Selecione **Generate**.

   Os campos **metadados do certificado**, **PEM** do certificado e **chave privada do certificado** são preenchidos.



a. Selecione **Copiar certificado para a área de transferência** e cole o certificado na ferramenta de monitoramento externa.

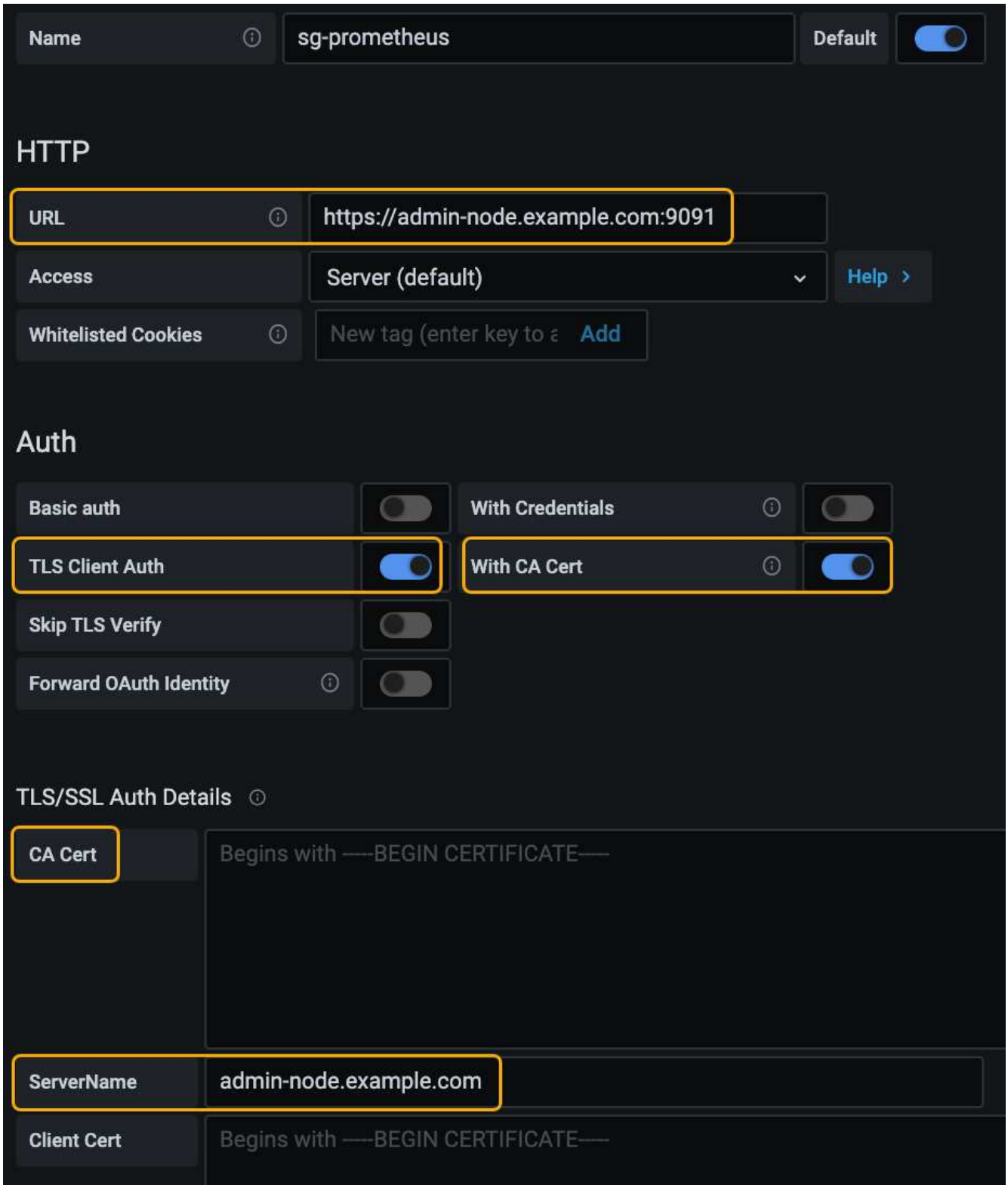
b. Selecione **Copie a chave privada para a área de transferência** e cole a chave na ferramenta de monitoramento externa.

> Não será possível visualizar a chave privada depois de fechar a caixa de diálogo. Copie a chave para um local seguro.

c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.

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

   Um exemplo de Grafana é mostrado na seguinte captura de tela:



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

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

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

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

c. Ative **TLS Client Authorization** e **with CA Cert**.

d. Copie e cole o certificado do servidor de interface de gerenciamento ou o pacote CA para **CA Cert** em Detalhes de autenticação TLS/SSL.

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

   O nome do servidor deve corresponder ao nome de domínio como aparece no certificado do servidor de interface de gerenciamento.

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

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

Para obter informações sobre as métricas, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

Informações relacionadas

"Usando certificados de segurança do StorageGRID"

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

"Monitorizar Resolução de problemas"

Editando certificados de cliente do administrador

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

O que você vai precisar

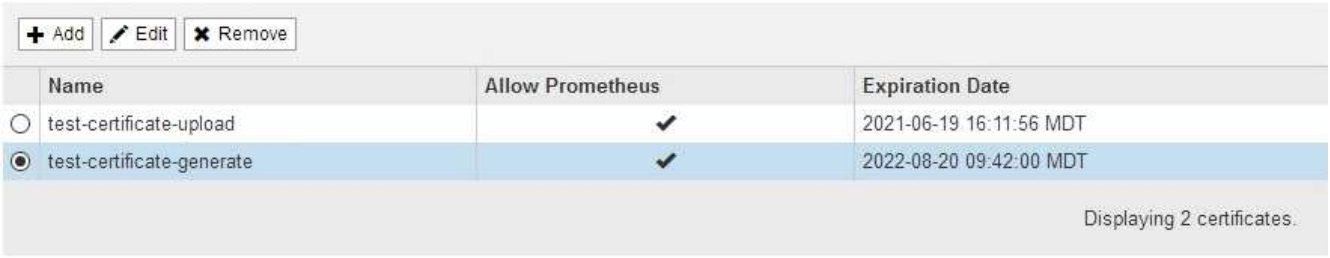
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve saber o endereço IP ou o nome de domínio do nó Admin.
- Se você quiser carregar um novo certificado e uma chave privada, eles devem estar disponíveis no computador local.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

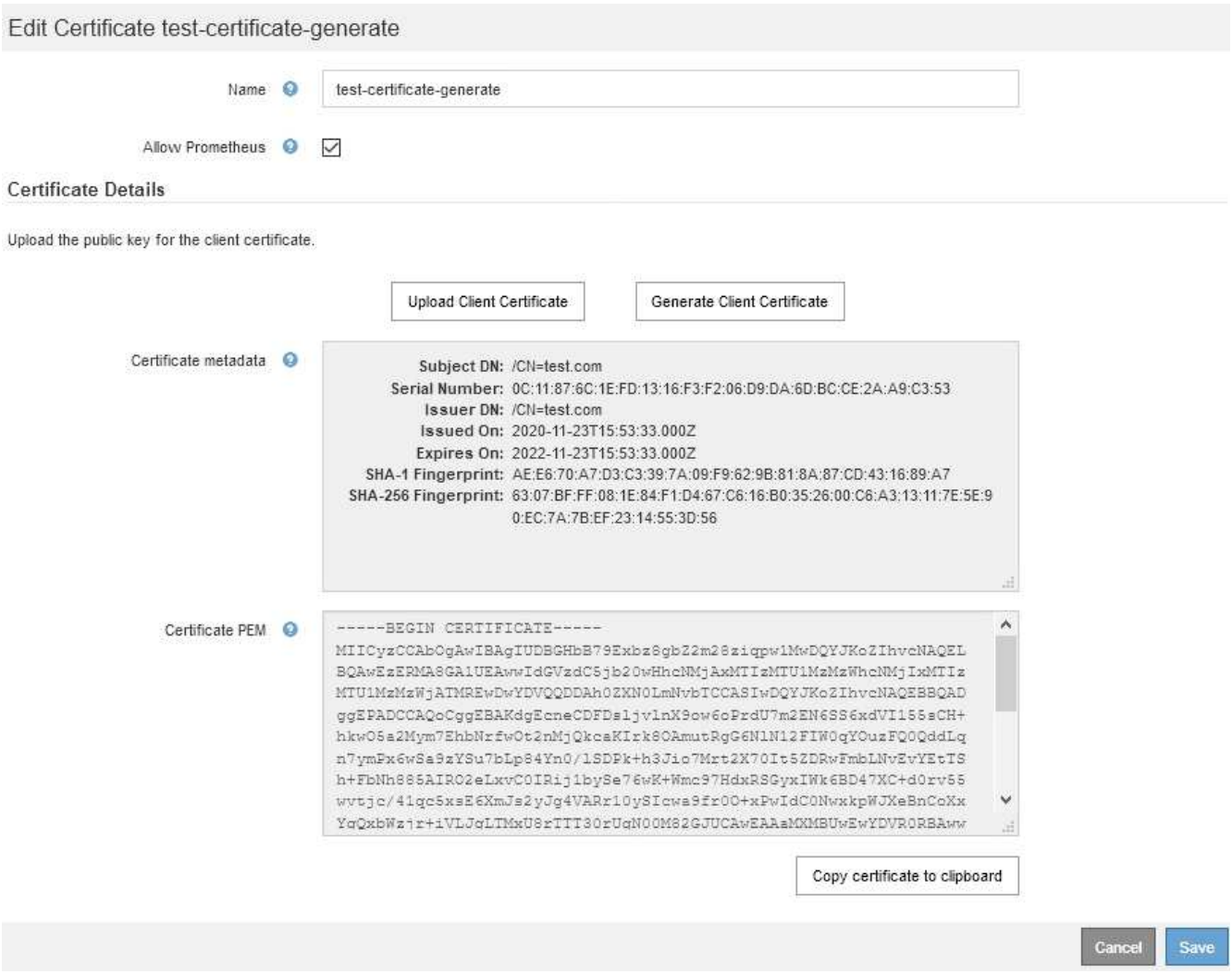
   A página certificados de cliente é exibida. Os certificados existentes são listados.

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



2. Selecione o botão de opção à esquerda do certificado que deseja editar.
3. Selecione **Editar**.

   A caixa de diálogo Editar certificado é exibida.



4. Faça as alterações desejadas no certificado.
5. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.
6. Se você carregou um novo certificado:
   a. Selecione **Copiar certificado para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.
   b. Use uma ferramenta de edição para copiar e colar a nova chave privada na sua ferramenta de monitoramento externo.

c. Salve e teste o certificado e a chave privada em sua ferramenta de monitoramento externa.

7. Se você gerou um novo certificado:
   a. Selecione **Copiar certificado para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.
   b. Selecione **Copiar chave privada para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.

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

   c. Salve e teste o certificado e a chave privada em sua ferramenta de monitoramento externa.

Removendo certificados de cliente de administrador

Se você não precisar mais de um certificado, você pode removê-lo.

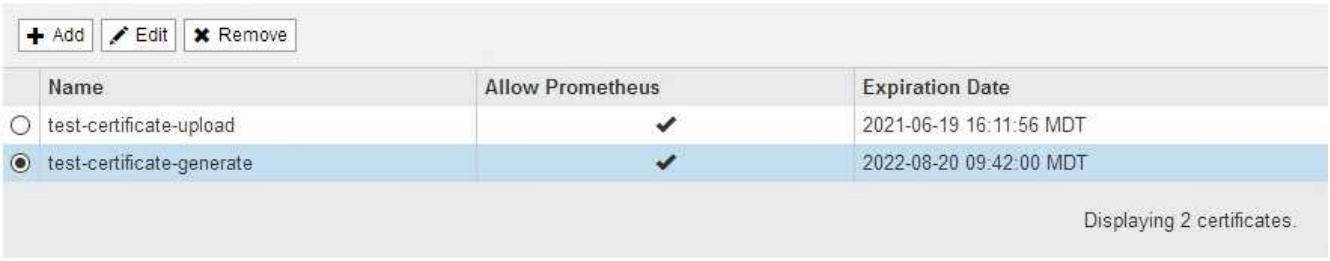
O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

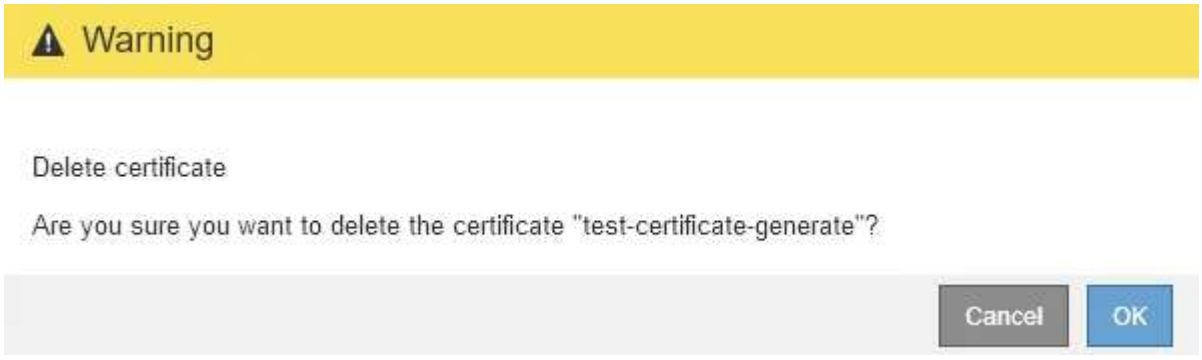
1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

   A página certificados de cliente é exibida. Os certificados existentes são listados.



2. Selecione o botão de opção à esquerda do certificado que deseja remover.
3. Selecione **Remover**.

   É apresentada uma caixa de diálogo de confirmação.



4. Selecione **OK**.

O certificado é removido.

Informações sobre direitos autorais

Informações sobre marcas comerciais