Controle o acesso ao StorageGRID

StorageGRID

NetApp
October 03, 2025

Índice

Controle o acesso ao StorageGRID

Altere a frase-passe de aprovisionamento

Use este procedimento para alterar a senha de provisionamento do StorageGRID. A frase-passe é necessária para procedimentos de recuperação, expansão e manutenção. A senha também é necessária para baixar backups do pacote de recuperação que incluem informações de topologia de grade, senhas de console de nó de grade e chaves de criptografia para o sistema StorageGRID.

O que você vai precisar

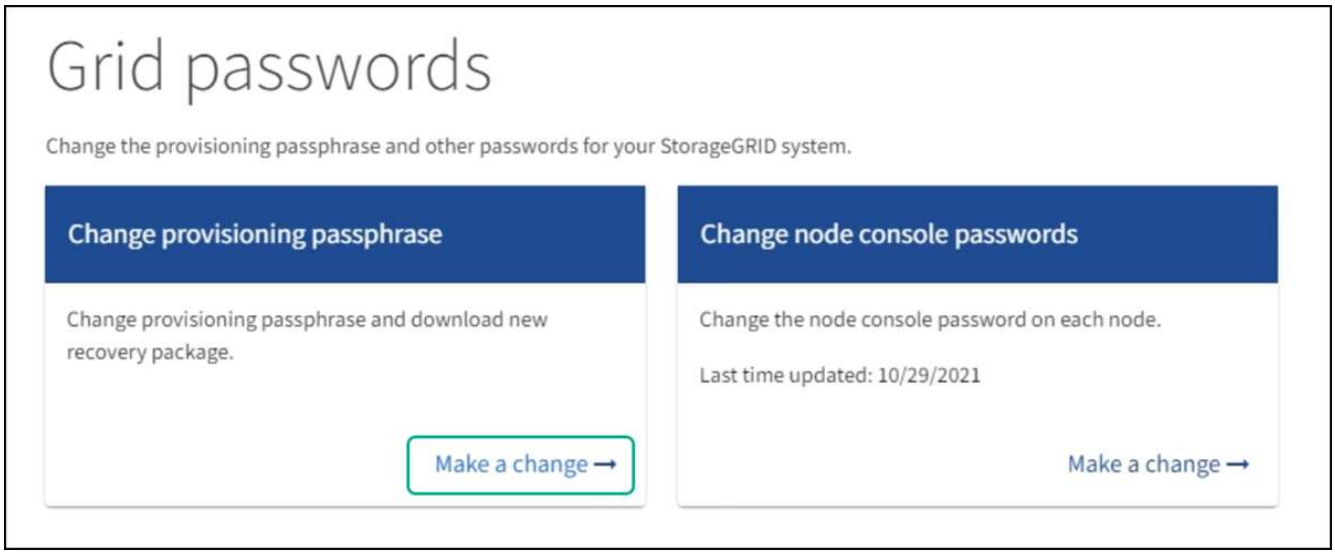
- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

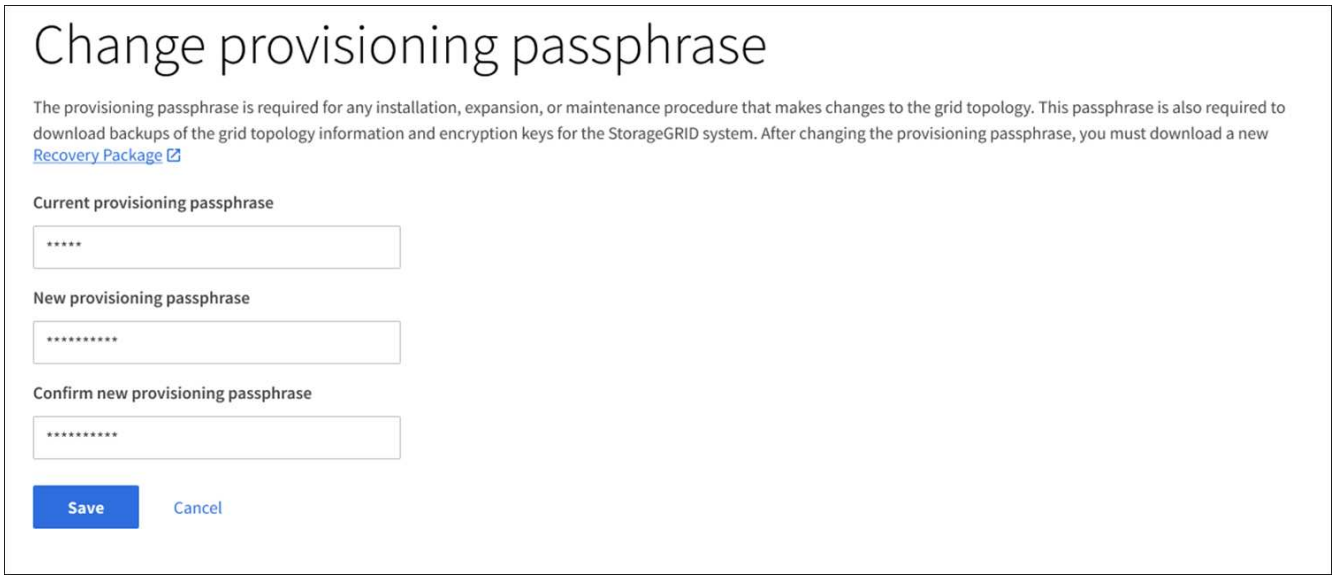
A frase-passe de aprovisionamento é necessária para muitos procedimentos de instalação e manutenção, e para Transferir o pacote de recuperaçãoo . A senha de provisionamento não está listada no `Passwords.txt` arquivo. Certifique-se de documentar a senha de provisionamento e mantê-la em um local seguro e seguro.

Passos

1. Selecione **CONFIGURATION** > **access control**> **Grid passwords**.

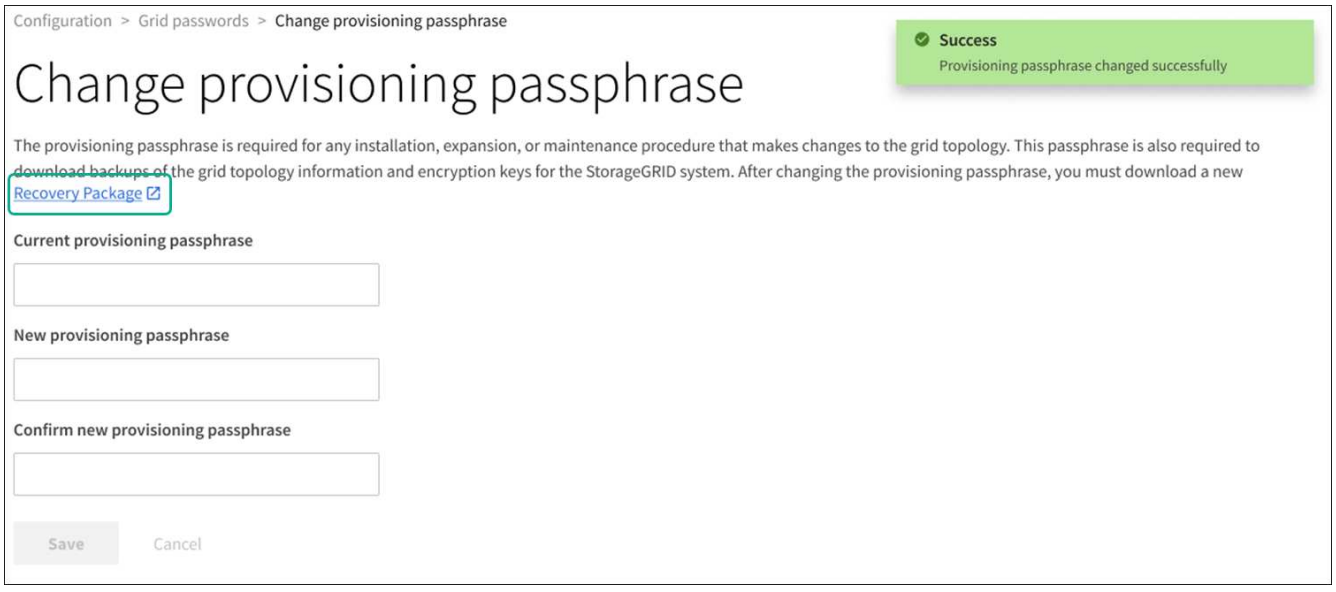


2. Selecione **Faça uma alteração** em **Change Provisioning passphrase**.



3. Introduza a sua frase-passe de aprovisionamento atual.
4. Introduza a nova frase-passe. A frase-passe deve conter pelo menos 8 e não mais de 32 carateres. As senhas são sensíveis a maiúsculas e minúsculas.
5. Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.
6. Digite novamente a nova senha e selecione **Salvar**.

   O sistema exibe um banner verde de sucesso quando a alteração da senha de provisionamento estiver concluída.



7. Selecione **Pacote de recuperação**.
8. Insira a nova senha de provisionamento para baixar o novo Pacote de recuperação.

> Depois de alterar a senha de provisionamento, você deve baixar imediatamente um novo Pacote de recuperação. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

Altere as senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console de nó, que você precisa fazer login no nó. Use estas etapas para alterar cada senha exclusiva do console de nó para cada nó na grade.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

Use a senha do console do nó para fazer login em um nó como "admin" usando SSH, ou para o usuário raiz em uma conexão VM/console físico. O processo de alteração de senha do console do nó cria novas senhas para cada nó na grade e armazena as senhas em um arquivo atualizado `Passwords.txt` no Pacote de recuperação. As senhas são listadas na coluna Senha no `Passwords.txt` arquivo.

Existem senhas de acesso SSH separadas para as chaves SSH usadas para comunicação entre nós. As senhas de acesso SSH não são alteradas por este procedimento.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access control** > **Grid passwords**.
2. Em **alterar senhas de console de nó**, selecione **fazer uma alteração**.

Introduza a frase-passe de aprovisionamento

Passos

1. Introduza a frase-passe de aprovisionamento da grelha.
2. Selecione **continuar**.

Faça o download do pacote de recuperação atual

Antes de alterar as senhas do console do nó, baixe o Pacote de recuperação atual. Você pode usar as senhas neste arquivo se o processo de alteração de senha falhar em qualquer nó.

Passos

1. Selecione **Baixar pacote de recuperação**.
2. Copie o arquivo do pacote de recuperação (`.zip`) para dois locais seguros, seguros e separados.

O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

3. Selecione **continuar**.
4. Quando a caixa de diálogo de confirmação for exibida, selecione **Sim** se estiver pronto para começar a alterar as senhas do console do nó.

Não é possível cancelar este processo após o início.

Altere as senhas do console do nó

Quando o processo de senha do console do nó é iniciado, um novo Pacote de recuperação é gerado que inclui as novas senhas. Em seguida, as senhas são atualizadas em cada nó.

Passos

1. Aguarde que o novo pacote de recuperação seja gerado, o que pode levar alguns minutos.
2. Selecione **Transferir novo pacote de recuperação**.
3. Quando o download for concluído:

   a. Abra o `.zip` ficheiro.

   b. Confirme se você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas senhas do console do nó.

   c. Copie o novo arquivo do pacote de recuperação (`.zip`) para dois locais seguros, seguros e separados.

   > Não substituir o pacote de recuperação antigo.

   O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

4. Marque a caixa de seleção para indicar que você baixou o novo Pacote de recuperação e verificou o conteúdo.
5. Selecione **alterar senhas do console de nós** e aguarde que todos os nós sejam atualizados com as novas senhas. Isso pode levar alguns minutos.

   Se as senhas forem alteradas para todos os nós, um banner verde de sucesso será exibido. Vá para a próxima etapa.

   Se houver um erro durante o processo de atualização, uma mensagem de banner lista o número de nós que não conseguiram alterar suas senhas. O sistema irá tentar novamente automaticamente o processo em qualquer nó que não tenha a sua palavra-passe alterada. Se o processo terminar com alguns nós ainda não tendo uma senha alterada, o botão **Repetir** será exibido.

   Se a atualização da palavra-passe tiver falhado para um ou mais nós:

   a. Reveja as mensagens de erro listadas na tabela.

   b. Resolva os problemas.

   c. Selecione **Repetir**.

   > A tentativa de novo altera apenas as senhas do console do nó nos nós que falharam durante tentativas anteriores de alteração de senha.

6. Depois que as senhas do console do nó tiverem sido alteradas para todos os nós, exclua o Primeiro pacote de recuperação que você baixou.
7. Opcionalmente, use o link **Recovery package** para baixar uma cópia adicional do novo Recovery Package.

Controle o acesso através de firewalls

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

Controle 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.
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

- Faça login no Gerenciador de Grade
- Crie uma conta de locatário
- Comunicações externas

Use 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.

Configure a federação de identidade para o Grid Manager

Você pode configurar a federação de identidade no Gerenciador de Grade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como ative Directory, Azure ative Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de acesso específicas.
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

  Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

- Se você pretende usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Diretrizes para configurar um servidor OpenLDAPConsulte .
- Se você planeja habilitar o logon único (SSO), revisou o requisitos para o uso de logon único.
- Se você planeja usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade está usando TLS 1,2 ou 1,3. Cifras suportadas para conexões TLS de saídaConsulte .

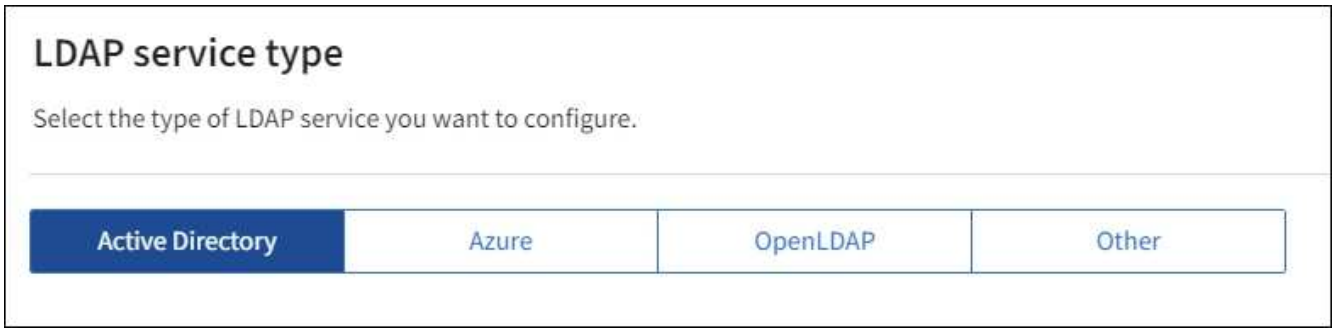
Sobre esta tarefa

Você pode configurar uma fonte de identidade para o Gerenciador de Grade se quiser importar grupos de outro sistema, como ative Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Você pode importar os seguintes tipos de grupos:

- 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. Crie uma conta de locatárioConsulte e Use uma conta de locatário para obter detalhes.

Introduza a configuração

1. Selecione **CONFIGURATION** > **access control** > **Identity Federation**.
2. Selecione **Ativar federação de identidade**.
3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.



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. Caso contrário, vá para a próxima etapa.
   - **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. Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na secção Configurar servidor LDAP.
   - **Nome de host**: O nome de domínio totalmente qualificado (FQDN) 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`
- **Ative Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
- **Azure**: `accountEnabled` E. `userPrincipalName`

◦ **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 da base de usuários** a que pertencem.

◦ **Bind username format** (opcional): O padrão de username padrão StorageGRID deve ser usado se o padrão não puder ser determinado automaticamente.

É recomendado fornecer **Bind username format** porque pode permitir que os usuários façam login se o StorageGRID não conseguir vincular-se à conta de serviço.

Introduza um destes padrões:

- **Padrão UserPrincipalName (ative Directory e Azure)**: `[USERNAME]@*example*.com`
- * Padrão de nome de logon de nível inferior (ative Directory e Azure)*: `*example*\[USERNAME]`
- * Padrão de nome distinto *: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

Inclua **[USERNAME]** exatamente como escrito.

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.
   ◦ **Use STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para ative Directory, OpenLDAP ou outro, mas esta opção não é suportada para o Azure.
   ◦ **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar essa opção para o Azure.
   ◦ **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada para o Azure.

> 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 de grade padrão instalado no

sistema operacional para proteger conexões.

- **Use certificado CA personalizado**: Use um certificado de segurança personalizado.

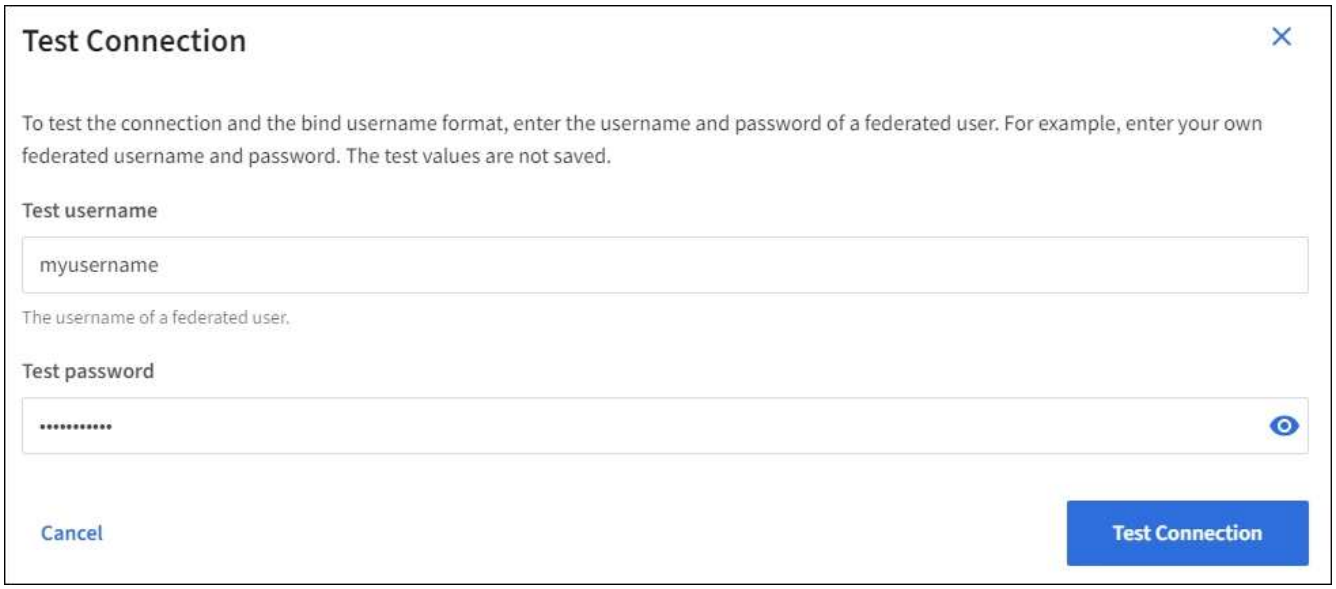
  Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

Teste a conexão e salve a configuração

Depois de introduzir todos os valores, tem de testar a ligação antes de poder guardar a configuração. O StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato de nome de usuário de vinculação, se você tiver fornecido uma.

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem "'test Connection could not be established'" (não foi possível estabelecer ligação) é apresentada se as definições de ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você tiver fornecido um formato de nome de usuário do BIND, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, insira seu próprio nome de usuário e senha. Não inclua carateres especiais no nome de usuário, como em ou /.



   - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem de erro é exibida se as configurações de conexão, o formato de nome de usuário de ligação ou o nome de usuário de teste e a senha forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar 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.

Passos

1. Vá para a página de federação de identidade.
2. Selecione **servidor de sincronização** na parte superior da página.

   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.

Desativar 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.

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 **habilitado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. Desative o logon únicoConsulte .

Passos

1. Vá para a página de federação de identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

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.

> ⓘ Para fontes de identidade que não são ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso S3 aos usuários que estão desativados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 para o usuário e remova o usuário de todos os grupos.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

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

Gerenciar 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.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de acesso específicas.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Crie um grupo 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.

Acesse o assistente

1. Selecione **CONFIGURATION** > **Access Control** > **Admin Groups**.
2. Selecione **criar grupo**.

Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

- Crie um grupo local se quiser atribuir permissões a usuários locais.
- Crie um grupo federado para importar usuários da origem da identidade.

Grupo local

1. Selecione **local group**.
2. Introduza um nome de apresentação para o grupo, que pode atualizar posteriormente, conforme necessário. Por exemplo, "'usuários de Manutenção'" ou "'Administradores de ILM.'"
3. Introduza um nome exclusivo para o grupo, que não pode atualizar mais tarde.
4. Selecione **continuar**.

Grupo federado

1. Selecione **Federated Group**.
2. Introduza o nome do grupo que pretende importar, exatamente como aparece na origem de identidade configurada.
   - Para o ative Directory e Azure, use o sAMAccountName.
   - Para OpenLDAP, use o CN (Nome Comum).
   - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **continuar**.

Gerenciar permissões de grupo

1. 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.

2. Selecione um ou mais Permissões de grupo.

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

3. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

Adicionar utilizadores (apenas grupos locais)

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.

   Se ainda não tiver criado utilizadores locais, pode guardar o grupo sem adicionar utilizadores. Pode adicionar este grupo ao utilizador na página utilizadores. Gerenciar usuáriosConsulte para obter detalhes.

2. Selecione **criar grupo** e **concluir**.

Exibir e editar grupos de administração

Você pode exibir detalhes de grupos existentes, modificar um grupo ou duplicar um grupo.

- Para exibir informações básicas de todos os grupos, revise a tabela na página grupos.
- Para exibir todos os detalhes de um grupo específico ou editar um grupo, use o menu **ações** ou a página de detalhes.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do grupo	a. Marque a caixa de seleção do grupo. b. Selecione **ações** > **Exibir detalhes do grupo**.	Selecione o nome do grupo na tabela.
Editar nome de exibição (apenas grupos locais)	a. Marque a caixa de seleção do grupo. b. Selecione **ações** > **Editar nome do grupo**. c. Introduza o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Salvar alterações**.
Editar o modo de acesso ou permissões	a. Marque a caixa de seleção do grupo. b. Selecione **ações** > **Exibir detalhes do grupo**. c. Opcionalmente, altere o modo de acesso do grupo. d. Opcionalmente, selecione ou Permissões de grupodesmarque . e. Selecione **Salvar alterações**.	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o modo de acesso do grupo. c. Opcionalmente, selecione ou Permissões de grupodesmarque . d. Selecione **Salvar alterações**.

Duplicar um grupo

1. Marque a caixa de seleção do grupo.
2. Selecione **ações** > **grupo duplicado**.
3. Conclua o assistente de grupo duplicado.

Eliminar um grupo

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 todos os usuários do grupo, mas não exclui os usuários.

1. Na página grupos, marque a caixa de seleção para cada grupo que deseja remover.
2. Selecione **ações** > **Excluir grupo**.
3. Selecione **Excluir grupos**.

Permissões de grupo

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 ou na API de Gerenciamento 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

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.

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 **Root Access**.

Acesso à raiz

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

Reconhecer alarmes (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.

Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página de locatários, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Essa permissão também é usada para migrar chaves S3 quando o recurso de importação de chaves S3 estiver ativado. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.

Para conceder acesso à página de locatários, que contém a opção **alterar senha de root**, atribua também a permissão **Contas de locatário**.

Configuração da página de topologia de grade

Esta permissão fornece acesso às guias Configuração na página **SUPPORT** > **Tools** > **Grid topology**.

ILM

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

- Regras
- Políticas
- Codificação de apagamento
- Regiões
- Pools de armazenamento

Os usuários devem ter as permissões **outras configurações de grade** e **Configuração de página de topologia de grade** para gerenciar as notas de armazenamento.

Manutenção

Os usuários devem ter a permissão Manutenção para usar estas opções:

- **CONFIGURAÇÃO** > **controlo de acesso**:
  - Senhas de grade
- **MANUTENÇÃO** > **tarefas**:
  - Descomissionar
  - Expansão
  - Verificação de existência do objeto
  - Recuperação
- **MANUTENÇÃO** > **sistema**:
  - Pacote de recuperação
  - Atualização de software
- **SUPORTE** > **Ferramentas**:
  - Registos

Os utilizadores que não têm a permissão Manutenção podem ver, mas não editar, estas páginas:

- **MANUTENÇÃO** > **rede**:
  - Servidores DNS
  - Rede de rede
  - Servidores NTP
- **MANUTENÇÃO** > **sistema**:

    - Licença
- **CONFIGURAÇÃO** > **Segurança**:
    - Certificados
    - Nomes de domínio
- **CONFIGURAÇÃO** > **Monitoramento**:
    - Servidor de auditoria e syslog

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.

Consulta de métricas

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

Pesquisa de metadados de objetos

Esta permissão fornece acesso à página **ILM** > **Object metadata lookup**.

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 **Grid topology page Configuration**.

- **ILM**:
    - Classes de armazenamento
- **CONFIGURAÇÃO** > **rede**:
    - Custo da ligação
- **CONFIGURAÇÃO** > **sistema**:
    - Opções de visualização
    - Opções de grelha
    - Opções de armazenamento
- **SUPORTE** > **Alarmes (legado)**:
    - Eventos personalizados
    - Alarmes globais
    - Configuração de e-mail legado

Administrador do dispositivo de storage

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

Contas de inquilino

Essa permissão fornece acesso à página de locatários, onde você pode criar, editar e remover contas de locatários. Essa permissão também permite que os usuários visualizem as políticas de classificação de tráfego existentes.

Desative recursos com a API

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. Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administração com permissão **root Access** 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 **alterar senha de root do locatário** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A pode garantir que nenhum usuário Admin - incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **acesso root** - pode alterar a senha para o usuário raiz de qualquer conta de locatário.*

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. Use a API de gerenciamento de gradeConsulte .
2. Localize o endpoint Deactivate Features
3. Para desativar um recurso, como alterar a 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 * alterar senha de root do locatário * não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha de raiz de um locatário falhará com "'403 Forbidden.'"

Reativar 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.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o endpoint Deactivate Features
3. Para reativar todos os recursos, envie um corpo para a API assim:

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

Quando essa solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento **alterar senha de root do locatário** agora aparece na interface do usuário, e qualquer solicitação de API que tente alterar a senha de root de um locatário terá êxito, assumindo que o usuário tenha a permissão de gerenciamento **acesso root** ou **alterar senha de root 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 raiz do locatário e continuar a desativar o recurso de reconhecimento de alarme, envie esta SOLICITAÇÃO PUT:

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

Gerenciar usuários

Você pode exibir usuários locais e federados. Você também 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 que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de acesso específicas.

Crie um usuário local

Você pode criar um ou mais usuários locais e atribuir cada usuário a um ou mais grupos locais. As permissões do grupo controlam quais recursos do Gerenciador de Grade e da API de Gerenciamento de Grade o usuário pode acessar.

Você pode criar somente usuários locais. Use a fonte de identidade externa para gerenciar usuários e grupos federados.

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Você não pode remover o usuário raiz.

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

Acesse o assistente

1. Selecione **CONFIGURATION** > **Access Control** > **Admin Users**.
2. Selecione **criar usuário**.

Introduza as credenciais do utilizador

1. Introduza o nome completo do utilizador, um nome de utilizador exclusivo e uma palavra-passe.
2. Opcionalmente, selecione **Sim** se esse usuário não tiver acesso ao Gerenciador de Grade ou à API de Gerenciamento de Grade.
3. Selecione **continuar**.

Atribuir a grupos

1. Opcionalmente, atribua o usuário a um ou mais grupos para determinar as permissões do usuário.

   Se ainda não tiver criado grupos, pode guardar o utilizador sem selecionar grupos. Você pode adicionar esse usuário a um grupo na página grupos.

   Se um usuário pertencer a vários grupos, as permissões serão cumulativas. Gerenciar grupos de administradoresConsulte para obter detalhes.

2. Selecione **Create user** e selecione **Finish**.

Ver e editar utilizadores locais

Você pode exibir detalhes de usuários locais e federados existentes. Você pode modificar um usuário local para alterar o nome completo, a senha ou a associação de grupo do usuário. Você também pode impedir temporariamente que um usuário acesse o Gerenciador de Grade e a API de Gerenciamento de Grade.

Só pode editar utilizadores locais. Use a fonte de identidade externa para gerenciar usuários federados.

- Para exibir informações básicas para todos os usuários locais e federados, revise a tabela na página usuários.
- Para visualizar todos os detalhes de um usuário específico, editar um usuário local ou alterar a senha de um usuário local, use o menu **ações** ou a página de detalhes.

  Todas as edições são aplicadas na próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.

  Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do utilizador	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**.	Selecione o nome do usuário na tabela.
Editar nome completo (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Editar nome completo**. c. Introduza o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Salvar alterações**.
Negar ou permitir acesso à StorageGRID	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia Acesso. d. Selecione **Sim** para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione **não** para permitir que o usuário faça login. e. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Acesso. c. Selecione **Sim** para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione **não** para permitir que o usuário faça login. d. Selecione **Salvar alterações**.
Alterar palavra-passe (apenas utilizadores locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia Senha. d. Introduza uma nova palavra-passe. e. Selecione **alterar palavra-passe**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Senha. c. Introduza uma nova palavra-passe. d. Selecione **alterar palavra-passe**.

Tarefa	Menu ações	Página de detalhes
Alterar grupos (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia grupos. d. Opcionalmente, selecione o link após um nome de grupo para exibir os detalhes do grupo em uma nova guia do navegador. e. Selecione **Editar grupos** para selecionar grupos diferentes. f. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia grupos. c. Opcionalmente, selecione o link após um nome de grupo para exibir os detalhes do grupo em uma nova guia do navegador. d. Selecione **Editar grupos** para selecionar grupos diferentes. e. Selecione **Salvar alterações**.

Duplicar um usuário

Você pode duplicar um usuário existente para criar um novo usuário com as mesmas permissões.

1. Selecione a caixa de verificação para o utilizador.
2. Selecione **ações** > **usuário duplicado**.
3. Conclua o assistente de usuário duplicado.

Eliminar um utilizador

Você pode excluir um usuário local para remover permanentemente esse usuário do sistema.

Não é possível eliminar o utilizador raiz.

1. Na página usuários, marque a caixa de seleção para cada usuário que deseja remover.
2. Selecione **ações** > **Excluir usuário**.
3. Selecione **Eliminar utilizador**.

Usar logon único (SSO)

Configurar o 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. Os utilizadores locais não podem iniciar sessão no StorageGRID.

Como o single sign-on funciona

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0).

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

Inicie sessão quando o SSO estiver 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.

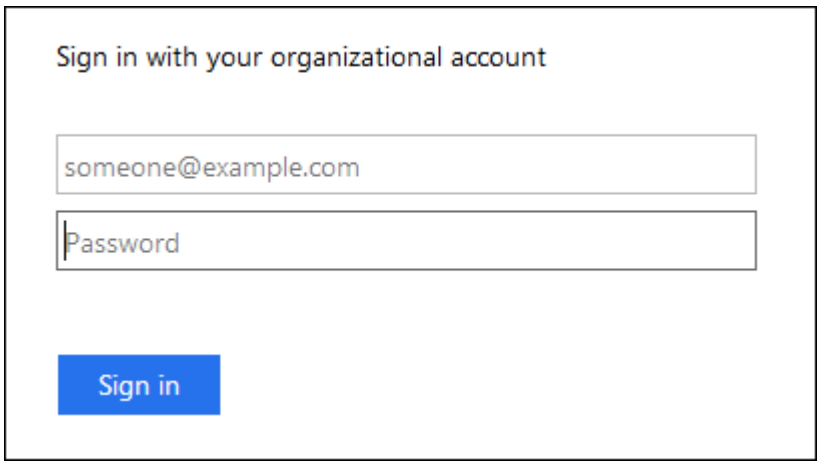
   - Se esta for a primeira vez que você acessou o URL neste navegador, será solicitado um ID de conta:

   - 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. Selecione **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 com permissões de acesso ao StorageGRID, você estará conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário, dependendo da conta selecionada.

   Se a conta de serviço estiver inacessível, você ainda poderá fazer login, contanto que você seja um usuário existente que pertença a um grupo federado com permissões de acesso ao StorageGRID.

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.

Sair quando o SSO estiver 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. Selecione **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 **Observação:** se você usar o Azure para SSO, pode levar alguns minutos para ser desconetado de 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
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.

Requisitos do provedor de identidade

O StorageGRID oferece suporte aos seguintes provedores de identidade SSO (IDP):

- Serviço de Federação do ative Directory (AD FS)
- Azure ative Directory (Azure AD)
- PingFederate

Você deve configurar a federação de identidade para o seu sistema StorageGRID antes de poder configurar um provedor de identidade SSO. O tipo de serviço LDAP que você usa para controles de federação de

identidade que tipo de SSO você pode implementar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ative Directory	• Ative Directory • Azure • PingFederate
Azure	Azure

Requisitos do AD FS

Você pode usar qualquer uma das seguintes versões do AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> 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.

Requisitos adicionais

- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado 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 confiança de parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para StorageGRID, você usa o certificado de servidor como o certificado de assinatura para solicitações StorageGRID.

Se ainda não configurado um certificado personalizado para a interface de gerenciamentoo fez, 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 partes dependentes do StorageGRID, aplicativos empresariais ou conexões SP.

> O uso do certificado de servidor padrão de um nó de administrador em uma conexão de confiança de parte confiável, aplicativo empresarial ou SP não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de iniciar sessão no nó recuperado, tem de atualizar a confiança de parte fidedigna, a aplicação empresarial ou a ligação SP 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 .

Requisitos portuários

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. Controle o acesso através de firewallsConsulte .

Confirme se os 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

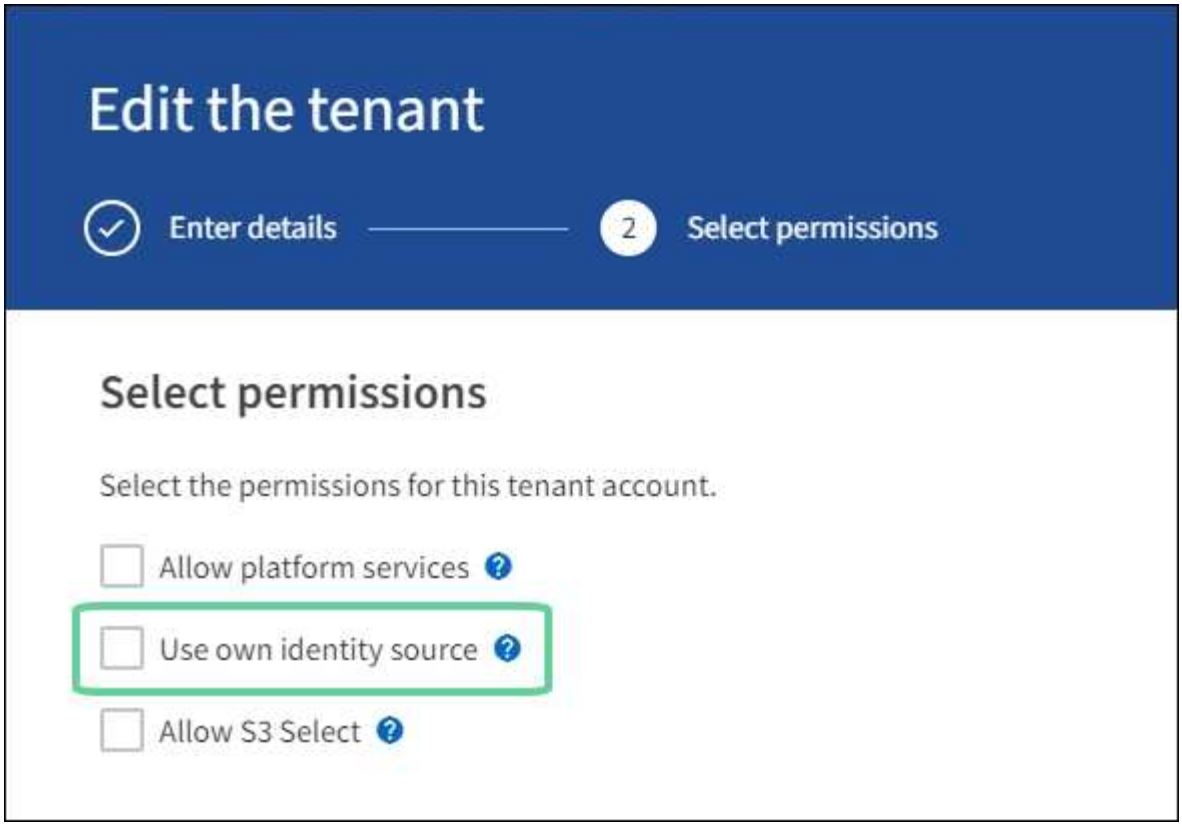
- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de acesso específicas.
- Você já configurou a federação de identidade.

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 **GERENCIAMENTO DE ACESSO** > **federação de identidade**.
   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 selecione **Salvar**.
2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
   a. No Gerenciador de Grade, selecione **CONFIGURATION** > **Access Control** > **Admin Groups**.
   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 selecione **ações** > **Editar**.
   c. Na guia Inserir detalhes, selecione **continuar**.
   d. Se a caixa de seleção **Use own Identity source** estiver selecionada, desmarque a caixa e selecione **Save**.



É apresentada a página do locatário.

a. Selecione a conta de locatário, selecione **entrar** e faça login na conta de locatário como usuário raiz local.
b. No Gerenciador do Locatário, selecione **GERENCIAMENTO 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
- Gerenciar grupos de administradores
- Use uma conta de locatário

Use o modo sandbox

Você pode usar o modo sandbox para configurar e testar o logon único (SSO) antes de habilitá-lo para todos os usuários do StorageGRID. Depois que o SSO estiver ativado, você poderá retornar ao modo sandbox sempre que precisar alterar ou testar novamente a configuração.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem a permissão de acesso root.

- Você configurou a federação de identidade para o seu sistema StorageGRID.
- Para a federação de identidade **tipo de serviço LDAP**, você selecionou o ative Directory ou o Azure, com base no provedor de identidade SSO que você planeja usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ative Directory	• Ative Directory • Azure • PingFederate
Azure	Azure

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 provedor de identidade SSO. Por sua vez, o provedor de identidade SSO envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autenticação foi bem-sucedida. Para solicitações bem-sucedidas:

- A resposta do ative Directory ou PingFederate inclui um identificador universal único (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal de Usuário (UPN).

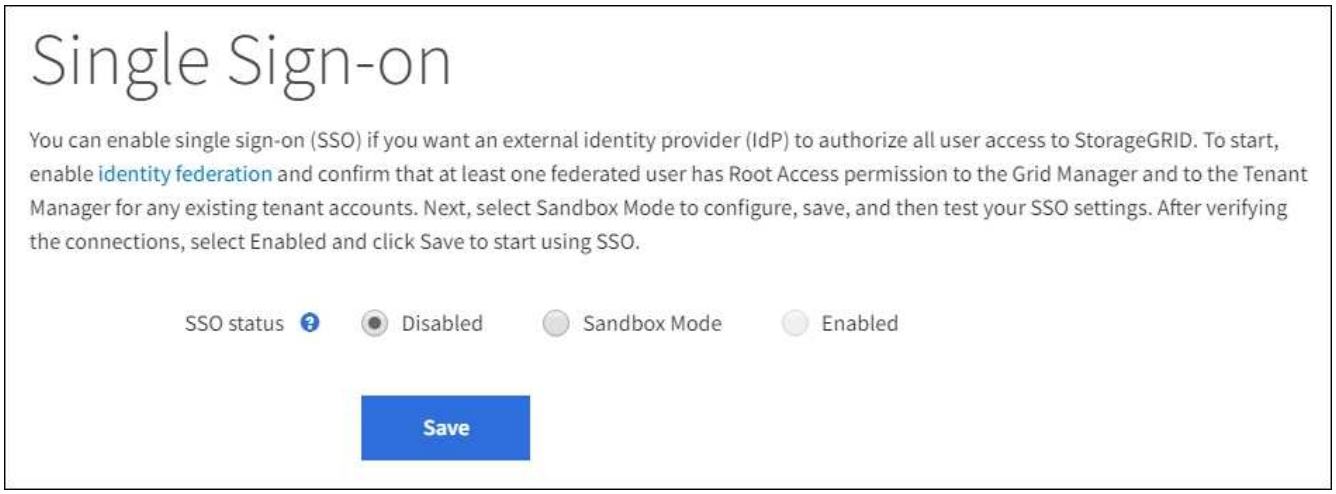
Para permitir que o StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre solicitações de autenticação de usuário, você deve configurar certas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma confiança de parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. 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. Quando você está usando o modo sandbox, os usuários não podem entrar usando SSO.

Acesse o modo sandbox

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.

   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 provedor de identidade como a origem de identidade federada. Requisitos para o uso de logon únicoConsulte .

2. Selecione **Sandbox Mode**.

   A seção Provedor de identidade é exibida.

Insira os detalhes do provedor de identidade

1. Selecione o **SSO type** na lista suspensa.
2. Preencha os campos na seção Provedor de identidade com base no tipo SSO selecionado.

Ative Directory

1. Digite o nome do serviço **Federation** para o provedor de identidade, exatamente como aparece no ative Directory Federation Service (AD FS).

   Para localizar o nome do serviço de federação, vá para Gerenciador do Windows Server. 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.

2. Especifique qual certificado TLS será usado 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 o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

   - **Não use TLS**: Não use um certificado TLS para proteger a conexão.
3. Na seção parte dependente, especifique o **identificador de parte dependente** para StorageGRID. Esse valor controla o nome que você usa para cada confiança de parte confiável no AD FS.
   - 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 mostra o identificador de parte confiável para cada nó Admin em seu sistema, com base no nome do host do nó.

   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.

4. Selecione **Guardar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

Azure

1. Especifique qual certificado TLS será usado 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 o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

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

2. Na seção aplicativo empresarial, especifique o **Nome do aplicativo empresarial** para StorageGRID. Esse valor controla o nome que você usa para cada aplicativo corporativo no Azure AD.
   - 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 mostra um nome de aplicativo corporativo para cada nó Admin em seu sistema, com base no nome do host do nó.

> Você deve criar um aplicativo empresarial para cada nó de administração no sistema StorageGRID. Ter um aplicativo corporativo para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

3. Siga as etapas em Crie aplicativos empresariais no Azure AD para criar um aplicativo corporativo para cada nó de administração listado na tabela.
4. No Azure AD, copie o URL de metadados da federação para cada aplicativo corporativo. Em seguida, cole esse URL no campo **URL de metadados de Federação** correspondente no StorageGRID.
5. Depois de copiar e colar um URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

PingFederate

1. Especifique qual certificado TLS será usado 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 o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

   - **Não use TLS**: Não use um certificado TLS para proteger a conexão.
2. Na seção Fornecedor de Serviços (SP), especifique o **ID de conexão SP** para StorageGRID. Esse valor controla o nome que você usa para cada conexão SP no PingFederate.
   - 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 mostra o ID de conexão do SP para cada nó de administrador no sistema, com base no nome do host do nó.

> Você deve criar uma conexão SP para cada nó de administração no sistema StorageGRID. Ter uma conexão SP para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

3. Especifique o URL de metadados de federação para cada nó Admin no campo **URL de metadados de Federação**.

   Use o seguinte formato:

   ```
   https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
   ```

4. Selecione **Guardar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

Configurar trusts de terceiros confiáveis, aplicativos empresariais ou conexões SP

Quando a configuração é salva, o aviso de confirmação do modo Sandbox é exibido. Este aviso confirma que o modo sandbox está agora ativado e fornece instruções de visão geral.

O StorageGRID pode permanecer no modo sandbox enquanto necessário. No entanto, quando **modo Sandbox** está selecionado na página de logon único, o SSO é desativado para todos os usuários do StorageGRID. Somente usuários locais podem fazer login.

Siga estas etapas para configurar as trusts de parte confiável (ative Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Ative Directory

1. Vá para Serviços de Federação do ative Directory (AD FS).
2. Crie uma ou mais confianças de parte confiáveis para o StorageGRID, usando cada identificador de parte confiável mostrado na tabela na página de logon único do StorageGRID.

   Você deve criar uma confiança para cada nó Admin mostrado na tabela.

   Para obter instruções, vá Criar confiança de parte confiável no AD FSpara .

Azure

1. Na página de logon único para o nó Admin ao qual você está conetado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Vá para o Portal do Azure.
4. Siga as etapas em Crie aplicativos empresariais no Azure AD para carregar o arquivo de metadados SAML para cada nó Admin em seu aplicativo corporativo do Azure correspondente.

PingFederate

1. Na página de logon único para o nó Admin ao qual você está conetado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Vá para PingFederate.
4. Crie uma ou mais conexões de provedor de serviços (SP) para o StorageGRID. Use o ID de conexão do SP para cada nó de administrador (mostrado na tabela na página de logon único do StorageGRID) e os metadados SAML que você baixou para esse nó de administrador.

   Você deve criar uma conexão SP para cada nó de administrador mostrado na tabela.

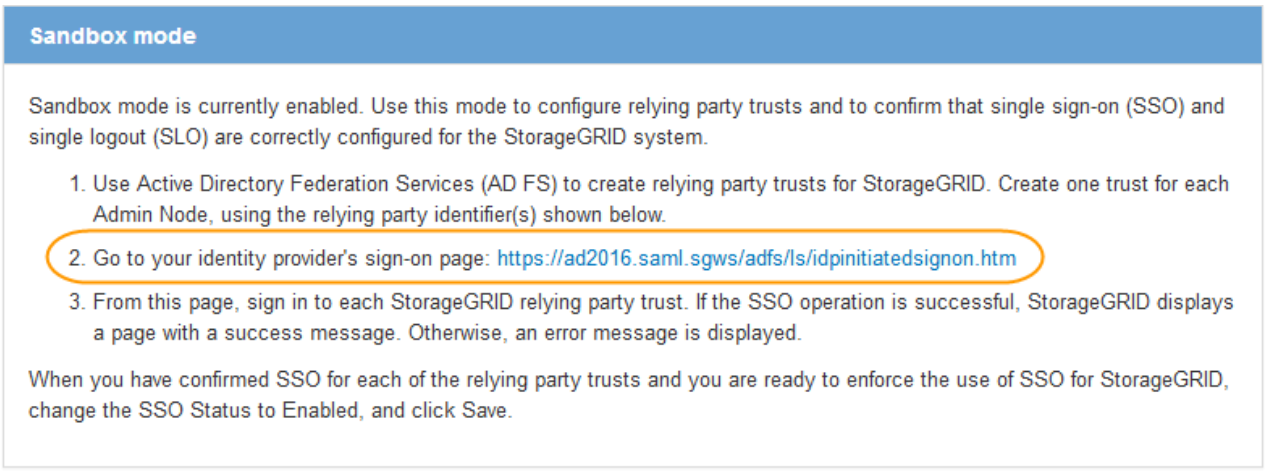
Testar conexões SSO

Antes de aplicar o uso de logon único para todo o sistema StorageGRID, você deve confirmar que o logon único e o logout único estão configurados corretamente para cada nó de administração.

Ative Directory

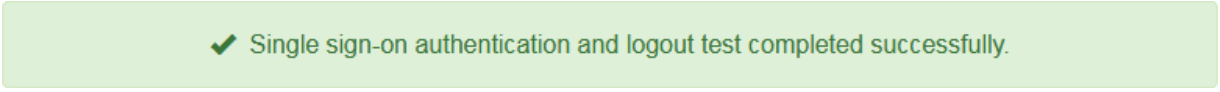
1. Na página de logon único do StorageGRID, localize o link na mensagem do modo Sandbox.

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



2. Selecione o link ou copie e cole o URL em um navegador para acessar a página de logon do provedor de identidade.
3. 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 selecione **entrar**.

4. 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.



   - 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.
5. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

Azure

1. Vá para a página de logon único no portal do Azure.
2. Selecione **Teste este aplicativo**.
3. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

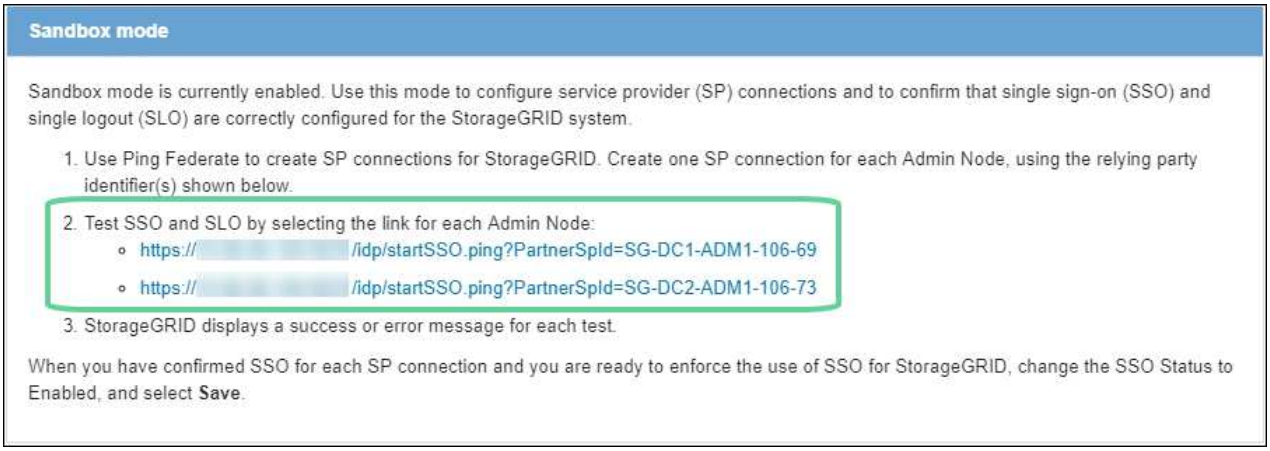
     ✔ Single sign-on authentication and logout test completed successfully.

   - 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.
4. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

PingFederate

1. Na página de logon único do StorageGRID, selecione o primeiro link na mensagem do modo Sandbox.

   Selecione e teste um link de cada vez.

2. Insira as credenciais de um usuário federado.
   - 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.
3. Selecione o próximo link para verificar a conexão SSO para cada nó Admin na grade.

   Se você vir uma mensagem Página expirada, selecione o botão **voltar** no seu navegador e reenvie suas credenciais.

Ative o logon único

Quando você confirmar que pode usar o SSO para fazer login em cada nó de administrador, você pode ativar o SSO para todo o seu sistema StorageGRID.

> Quando o SSO está ativado, todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade e a API de Gerenciamento de Locatário. Os usuários locais não podem mais acessar o StorageGRID.

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
2. Altere o Status SSO para **Enabled**.
3. Selecione **Guardar**.
4. Reveja a mensagem de aviso e selecione **OK**.

   O início de sessão único está agora ativado.

> Se você estiver usando o Portal do Azure e acessar o StorageGRID do mesmo computador que usa para acessar o Azure, verifique se o usuário do Portal do Azure também é um usuário autorizado do StorageGRID (um usuário em um grupo federado que foi importado para o StorageGRID) ou faça logout do Portal do Azure antes de tentar entrar no StorageGRID.

Criar confiança de parte confiável 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.

O que você vai precisar

- Você configurou o logon único para o StorageGRID e selecionou **AD FS** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. Use o modo sandboxConsulte .
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de entidade dependente para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos nós de administração na página de logon único do StorageGRID.

  > 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.
- Se você estiver criando a confiança de parte confiável manualmente, 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.

Sobre esta tarefa

Estas instruções aplicam-se ao Windows Server 2016 AD FS. Se você estiver usando uma versão diferente do AD FS, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Crie 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.

Passos

1. No menu Iniciar do Windows, selecione o ícone do PowerShell com o botão direito 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. Selecione **aplicar** e **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. Selecione **Adicionar regra**.
   d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **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. Selecione **Finish** e **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, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. Use o modo SandboxConsulte para obter instruções.

Crie 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.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e **Gerenciamento do AD FS**.

2. Em ações, selecione **Adicionar confiança de parte dependente**.

3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **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. Selecione **Adicionar regra**:

c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **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. Selecione **Finish** e **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, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. Use o modo SandboxConsulte para obter instruções.

Crie uma confiança de parte confiável manualmente

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

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e **Gerenciamento do AD FS**.
2. Em ações, selecione **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **Iniciar**.
4. Selecione **Digite os dados sobre a parte que depende manualmente** e selecione **Next**.
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, selecione **Adicionar regra**:
   a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **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. Selecione **Finish** e **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. Selecione **Adicionar 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. Selecione **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. Selecione **aplicar** e **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, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. Use o modo sandboxConsulte para obter instruções.

Crie aplicativos empresariais no Azure AD

Você usa o Azure AD para criar um aplicativo corporativo para cada nó de administrador no sistema.

O que você vai precisar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. Use o modo sandboxConsulte .
- Você tem o **Nome do aplicativo Enterprise** para cada nó Admin no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.

> Você deve criar um aplicativo empresarial para cada nó de administração no sistema StorageGRID. Ter um aplicativo corporativo 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 aplicativos empresariais no Azure ative Directory.
- Você tem uma conta do Azure com uma assinatura ativa.
- Você tem uma das seguintes funções na conta do Azure: Administrador Global, Administrador de aplicativos em nuvem, Administrador de aplicativos ou proprietário do responsável do serviço.

Acesse o Azure AD

1. Inicie sessão no "Portal do Azure".
2. Navegue até "Azure ative Directory".
3. "Aplicações empresariais"Selecione .

Crie aplicativos empresariais e salve a configuração SSO do StorageGRID

Para salvar a configuração SSO para o Azure no StorageGRID, você deve usar o Azure para criar um aplicativo corporativo para cada nó de administração. Você copiará os URLs de metadados da federação do Azure e os colará nos campos **URL de metadados da Federação** correspondentes na página de logon único do StorageGRID.

1. Repita as etapas a seguir para cada nó Admin.
   a. No painel aplicativos do Azure Enterprise, selecione **novo aplicativo**.
   b. Selecione **Crie seu próprio aplicativo**.
   c. Para o nome, insira o **Nome do aplicativo da empresa** que você copiou da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.
   d. Deixe o botão de opção **integrar qualquer outro aplicativo que você não encontrar na galeria (não galeria)** selecionado.
   e. Selecione **criar**.
   f. Selecione o link **Get Started** no **2. Configure a caixa Single Sign On** (Início de sessão único) ou selecione o link **Single Sign-On** (Início de sessão único) na margem esquerda.
   g. Selecione a caixa **SAML**.
   h. Copie o URL de metadados de Federação de aplicativos*, que você pode encontrar em **Etapa 3 certificado de assinatura SAML**.
   i. Vá para a página de logon único do StorageGRID e cole o URL no campo **URL de metadados da Federação** que corresponde ao nome do aplicativo **empresa** que você usou.
2. Depois de colar um URL de metadados de federação para cada nó de administrador e fazer todas as outras alterações necessárias na configuração SSO, selecione **Salvar** na página de logon único do StorageGRID.

Faça o download dos metadados SAML para cada nó de administração

Depois que a configuração SSO for salva, você pode baixar um arquivo de metadados SAML para cada nó de administrador no sistema StorageGRID.

Repita estas etapas para cada nó Admin:

1. Inicie sessão no StorageGRID a partir do nó de administração.
2. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
3. Selecione o botão para baixar os metadados SAML para esse nó Admin.
4. Salve o arquivo, que você carregará no Azure AD.

Carregue metadados SAML para cada aplicação empresarial

Depois de baixar um arquivo de metadados SAML para cada nó de administrador do StorageGRID, execute as seguintes etapas no Azure AD:

1. Retorne ao Portal do Azure.
2. Repita estes passos para cada aplicação empresarial:

> Talvez seja necessário atualizar a página aplicativos empresariais para ver os aplicativos adicionados anteriormente na lista.

a. Vá para a página Propriedades do aplicativo corporativo.

b. Defina **atribuição necessária** como **não** (a menos que você queira configurar atribuições separadamente).

c. Aceda à página de início de sessão único.

d. Conclua a configuração SAML.

e. Selecione o botão **Upload metadata file** e selecione o arquivo de metadados SAML que você baixou para o Admin Node correspondente.

f. Depois que o arquivo for carregado, selecione **Save** e, em seguida, selecione **X** para fechar o painel. Você será retornado à página Configurar logon único com SAML.

3. Siga os passos em Use o modo sandbox para testar cada aplicação.

Crie conexões de provedor de serviços (SP) no PingFederate

Você usa o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administrador no seu sistema. Para acelerar o processo, você importará os metadados SAML do StorageGRID.

O que você vai precisar

- Você configurou o logon único para o StorageGRID e selecionou **Ping federate** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. Use o modo sandboxConsulte .
- Você tem o **ID de conexão SP** para cada nó de administrador no sistema. Você pode encontrar esses valores na tabela de detalhes dos nós de administração na página de logon único do StorageGRID.
- Você baixou os **metadados SAML** para cada nó Admin no seu sistema.
- Você tem experiência em criar conexões SP no servidor PingFederate.
- Você tem o "Guia de referência do administrador" para PingFederate Server. A documentação do PingFederate fornece instruções detalhadas passo a passo e explicações.
- Você tem a permissão Admin para PingFederate Server.

Sobre esta tarefa

Estas instruções resumem como configurar o PingFederate Server versão 10,3 como um provedor SSO para o StorageGRID. Se você estiver usando outra versão do PingFederate, talvez seja necessário adaptar essas instruções. Consulte a documentação do PingFederate Server para obter instruções detalhadas sobre o seu lançamento.

Complete pré-requisitos no PingFederate

Antes de criar as conexões SP que você usará para o StorageGRID, você deve concluir as tarefas de pré-requisito no PingFederate. Você usará as informações desses pré-requisitos quando configurar as conexões SP.

Criar armazenamento de dados

Se você ainda não o fez, crie um armazenamento de dados para conetar o PingFederate ao servidor LDAP do AD FS. Use os valores usados configurando a federação de identidadeno StorageGRID.

- * Tipo*: Diretório (LDAP)

- **Tipo LDAP**: Ative Directory
- **Nome do atributo binário**: Insira **objectGUID** na guia atributos binários LDAP exatamente como mostrado.

Criar validador de credenciais de senha

Se você ainda não o fez, crie um validador de credenciais de senha.

- **Type**: LDAP Username Password Credential Validator
- **Armazenamento de dados**: Selecione o armazenamento de dados que você criou.
- **Base de pesquisa**: Insira informações do LDAP (por exemplo,
- **Filtro de pesquisa**: SAMAccountName
- **Escopo**: Subárvore

Criar instância de adaptador IDP

Se você ainda não o fez, crie uma instância de adaptador IDP.

1. Aceda a **Autenticação** > **integração** > **adaptadores IDP**.
2. Selecione **criar nova instância**.
3. Na guia tipo, selecione **HTML form IDP Adapter**.
4. Na guia adaptador IDP, selecione **Adicionar uma nova linha a 'Validadores de credenciais'**.
5. Selecione o validador de credenciais de senha que você criou.
6. Na guia Adapter Attributes (atributos do adaptador), selecione o atributo **username** para **pseudônimo**.
7. Selecione **Guardar**.

Criar ou importar certificado de assinatura[[certificado de assinatura]]

Se ainda não o fez, crie ou importe o certificado de assinatura.

1. Aceda a **Security** > **Signing & Decryption Keys & Certificates**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Quando você cria uma conexão SP no PingFederate, importa os metadados SAML que você baixou do StorageGRID para o nó Admin. O arquivo de metadados contém muitos dos valores específicos que você precisa.

> Você deve criar uma conexão SP para cada nó de administração no sistema StorageGRID, para que os usuários possam fazer login e sair com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP. Em seguida, aceda a Crie conexões SP adicionais para criar quaisquer ligações adicionais de que necessita.

Escolha o tipo de conexão SP

1. Aceda a **aplicações** > **integração** > **ligações SP**.
2. Selecione **criar conexão**.

3. Selecione **não utilize um modelo para esta ligação**.
4. Selecione **Browser SSO Profiles** e **SAML 2,0** como protocolo.

Importar metadados do SP

1. Na guia Importar metadados, selecione **Arquivo**.
2. Escolha o arquivo de metadados SAML que você baixou na página de logon único do StorageGRID para o nó de administração.
3. Revise o Resumo de metadados e as informações na guia informações gerais.

   O ID da entidade do Parceiro e o Nome da conexão são definidos como ID de conexão StorageGRID SP. (Por exemplo, 10.96.105.200-DC1-ADM1-105-200). O URL base é o IP do nó de administração do StorageGRID.

4. Selecione **seguinte**.

Configure o SSO do navegador IDP

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia perfis SAML, selecione as opções **SSO iniciado por SP**, **SLO inicial por SP**, **SSO iniciado por IDP** e **SLO** iniciado por IDP.
3. Selecione **seguinte**.
4. Na guia Assertion Lifetime, não faça alterações.
5. Na guia criação de asserções, selecione **Configurar criação de asserções**.
   a. Na guia Mapeamento de identidade, selecione **Standard**.
   b. Na guia Contrato de Atributo, use o **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.
6. Para estender o contrato, selecione **Excluir** para remover `urn:oid` o , que não é usado.

Instância do adaptador de mapa

1. Na guia Mapeamento de origem de autenticação, selecione **Mapear nova instância de adaptador**.
2. Na guia instância do adaptador, selecione o instância do adaptador que você criou.
3. Na guia método de mapeamento, selecione **recuperar atributos adicionais de um armazenamento de dados**.
4. Na guia origem do atributo e Pesquisa de usuário, selecione **Adicionar origem do atributo**.
5. Na guia armazenamento de dados, forneça uma descrição e selecione o armazenamento de dados que você adicionou.
6. Na guia Pesquisa de diretório LDAP:
   - Digite o **DN base**, que deve corresponder exatamente ao valor inserido no StorageGRID para o servidor LDAP.
   - Para o escopo de pesquisa, selecione **subtree**.
   - Para a classe de objeto raiz, procure o atributo **objectGUID** e adicione-o.
7. Na guia tipos de codificação de atributos binários LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia filtro LDAP, digite **sAMAccountName**.

9. Na guia execução de contrato de atributo, selecione **LDAP (attribute)** na lista suspensa origem e selecione **objectGUID** na lista suspensa valor.
10. Revise e salve a fonte do atributo.
11. Na guia origem do atributo de salvamento de falha, selecione **Abortar a transação SSO**.
12. Reveja o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configure as definições do protocolo

1. Na guia **conexão SP** > **SSO do navegador** > **Configurações do protocolo**, selecione **Configurar configurações do protocolo**.
2. Na guia URL do Serviço ao Consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` URL do ponto final).
3. Na guia URLs de serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL de ponto final.
4. Na guia Allowable SAML Bindings (ligações SAML permitidas), desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são obrigatórios.
5. Na guia Política de assinatura, deixe as caixas de seleção **Require Authn Requests to be signed** e **Always Sign Assertion** selecionadas.
6. Na guia Diretiva de criptografia, selecione **nenhum**.
7. Reveja o resumo e selecione **Concluído** para guardar as definições do protocolo.
8. Revise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

1. Na guia conexão SP, selecione **credenciais**.
2. Na guia credenciais, selecione **Configurar credenciais**.
3. Selecione o certificado de assinatura que você criou ou importou.
4. Selecione **Next** para ir para **Manage Signature Verification Settings**.
   a. Na guia Trust Model (modelo de confiança), selecione **Unancored** (sem ancoragem).
   b. Na guia certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID.
5. Reveja os ecrãs de resumo e selecione **Guardar** para guardar a ligação SP.

Crie conexões SP adicionais

Você pode copiar a primeira conexão SP para criar as conexões SP necessárias para cada nó de administração na grade. Você carrega novos metadados para cada cópia.

> As conexões do SP para diferentes nós de administração usam configurações idênticas, com exceção do ID da entidade do parceiro, URL base, ID da conexão, nome da conexão, verificação de assinatura e URL de resposta do SLO.

1. Selecione **Ação** > **Copiar** para criar uma cópia da conexão SP inicial para cada nó de administração adicional.

2. Introduza a ID da ligação e o nome da ligação para a cópia e selecione **Guardar**.
3. Escolha o arquivo de metadados correspondente ao nó Admin:
   a. Selecione **Ação** > **Atualizar com metadados**.
   b. Selecione **escolha Arquivo** e carregue os metadados.
   c. Selecione **seguinte**.
   d. Selecione **Guardar**.
4. Resolva o erro devido ao atributo não utilizado:
   a. Selecione a nova ligação.
   b. Selecione **Configure Browser SSO > Configure Assertion creation > Attribute Contract**.
   c. Exclua a entrada para **urn:oid**.
   d. Selecione **Guardar**.

Desative o 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 está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de acesso específicas.

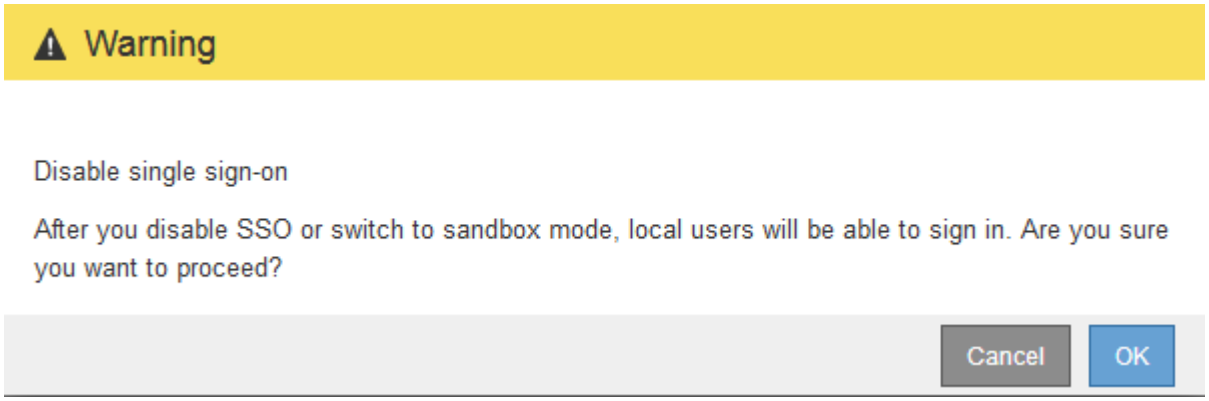
Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.

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

2. Selecione a opção **Disabled** (Desativado).
3. Selecione **Guardar**.

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



4. Selecione **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.

Desative e reative 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 tem permissões de acesso específicas.
- Você tem o `Passwords.txt` arquivo.
- Você sabe 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 **CONFIGURATION** > **access control** > **Single sign-on**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.

c. Selecione **Guardar**.

   Selecionar **Save** na página Single Sign-On (Início de sessão único) reativa automaticamente o SSO para toda a grelha.

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. Selecione **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 sobre direitos autorais

Informações sobre marcas comerciais