Gerenciar grupos e usuários

StorageGRID

NetApp
March 12, 2025

Índice

Gerenciar grupos e usuários

Use a federação de identidade

O uso da federação de identidade torna a configuração de grupos de locatários e usuários mais rápida e permite que os usuários do locatário façam login na conta do locatário usando credenciais familiares.

Configure a federação de identidade para o Gerenciador do Locatário

Você pode configurar a federação de identidade para o Gerenciador do locatário se quiser que grupos de locatários e usuários sejam gerenciados em outro sistema, como o ative Directory, o Azure ative Directory (Azure AD), o OpenLDAP ou o Oracle Directory Server.

Antes de começar

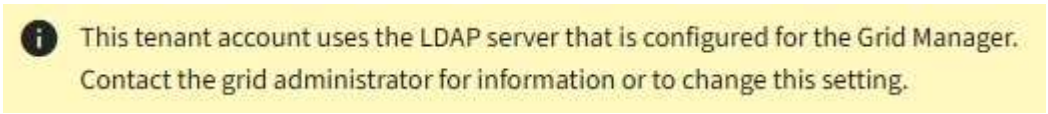
- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

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

Sobre esta tarefa

Se você pode configurar um serviço de federação de identidade para seu locatário depende de como sua conta de locatário foi configurada. Seu locatário pode compartilhar o serviço de federação de identidade configurado para o Gerenciador de Grade. Se você vir essa mensagem ao acessar a página Federação de identidade, não será possível configurar uma origem de identidade federada separada para esse locatário.

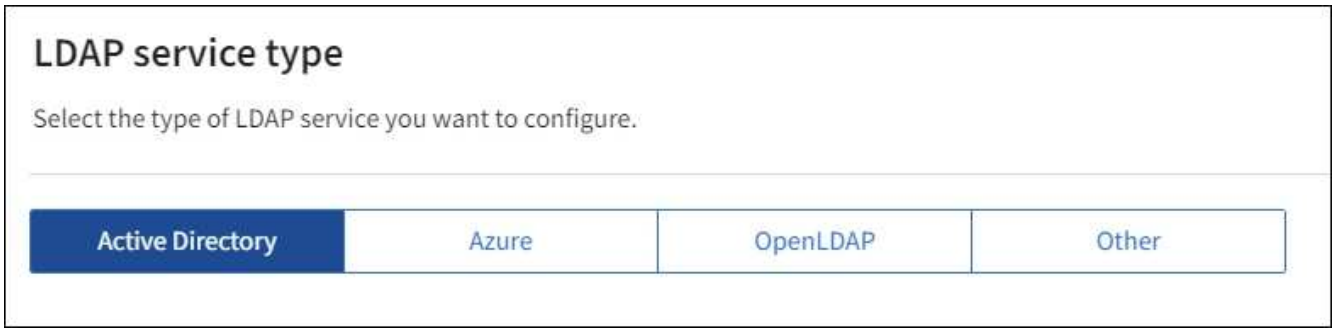


Introduza a configuração

Ao configurar a federação de identificação, você fornece os valores que o StorageGRID precisa para se conetar a um serviço LDAP.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **federação de identidade**.
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.

> Se você alterar a senha no futuro, você deve atualizá-la nesta página.

◦ **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.

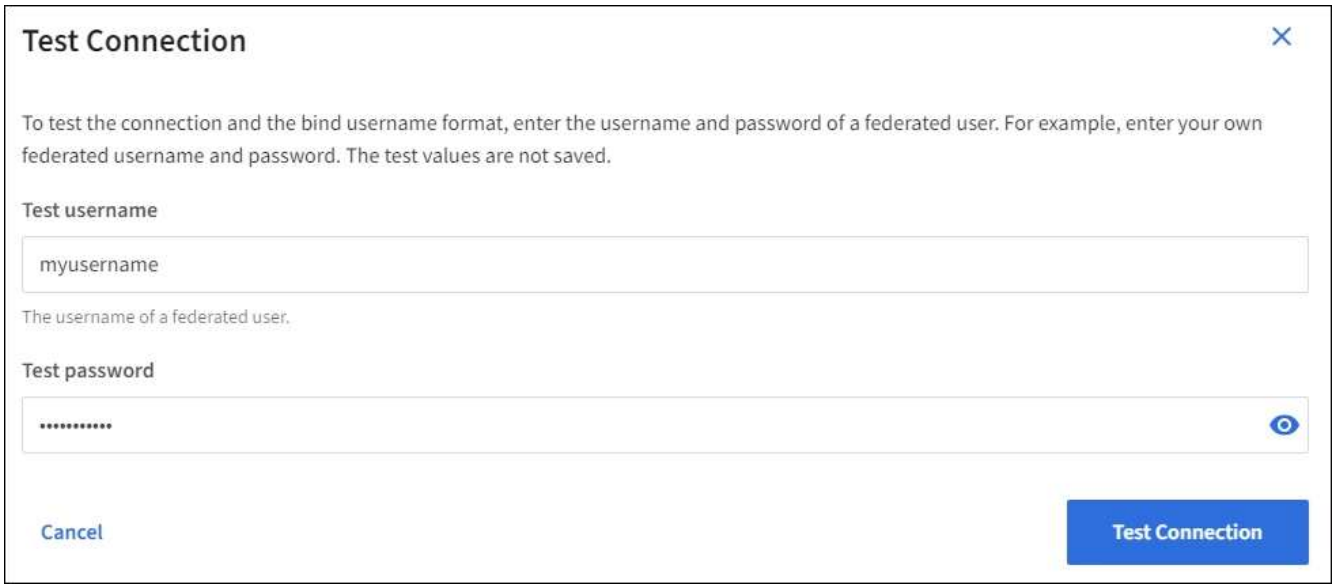
Teste a conexão e salve a configuração

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.

Passos

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - É apresentada uma mensagem "não foi possível estabelecer ligação de teste" se as definições da 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 /.



   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação 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 **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. "Desative o logon único"Consulte .

Passos

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

Diretrizes para configurar o 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 ou 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 locatários

Crie grupos para um locatário do S3

Você pode gerenciar permissões para S3 grupos de usuários importando grupos federados ou criando grupos locais.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se você pretende importar um grupo federado, o "federação de identidade configurada", e o grupo federado já existe na origem de identidade configurada.
- Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para "clonar grupos de locatários e usuários", e você estará conetado à grade de origem do locatário.

Acesse o assistente criar grupo

Como primeira etapa, acesse o assistente criar grupo.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Se sua conta de locatário tiver a permissão **Use Grid Federation Connection**, confirme se um banner azul aparece, indicando que novos grupos criados nessa grade serão clonados para o mesmo locatário na outra grade na conexão. Se este banner não aparecer, você pode estar conetado à grade de destino do locatário.

3. Selecione **criar grupo**.

Escolha um tipo de grupo

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

Passos

1. Selecione a guia **local group** para criar um grupo local ou selecione a guia **Federated group** para importar um grupo da origem de identidade configurada anteriormente.

   Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários pertencentes a grupos locais não poderão fazer login no Gerenciador de locatários, embora possam usar aplicativos clientes para gerenciar os recursos do locatário, com base nas permissões de grupo.

2. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.

     Se sua conta de locatário tiver a permissão **Use Grid Federation Connection**, ocorrerá um erro de clonagem se o mesmo **nome exclusivo** já existir para o locatário na grade de destino.

   - **Federated group**: Insira o nome exclusivo. Para o ative Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
3. Selecione **continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Gerenciador de inquilinos e na API de gerenciamento de inquilinos.

Passos

1. Para **modo de acesso**, selecione uma das seguintes opções:
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do locatário e gerenciar a configuração do locatário.

- **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. 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 uma ou mais permissões para este grupo.

   "Permissões de gerenciamento do locatário"Consulte .

3. Selecione **continuar**.

Defina a política de grupo S3

A política de grupo determina quais permissões de acesso S3 os usuários terão.

Passos

1. Selecione a política que pretende utilizar para este grupo.

Política de grupo	Descrição
Sem acesso S3	Padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
Acesso somente leitura	Os usuários deste grupo têm acesso somente leitura a recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
Acesso total	Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
Mitigação de ransomware	Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que têm o controle de versão de objeto habilitado. Os usuários do Gerenciador de locatários que têm a permissão **Gerenciar todos os buckets** podem substituir essa política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação multifator (MFA), onde disponível.

Política de grupo	Descrição
Personalizado	Os usuários do grupo recebem as permissões especificadas na caixa de texto.

2. Se você selecionou **Personalizado**, digite a política de grupo. Cada política de grupo tem um limite de tamanho de 5.120 bytes. Você deve inserir uma string formatada JSON válida.

   Para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de idioma e exemplos, "Exemplo de políticas de grupo"consulte .

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)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar usuários locais que já existem.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, os usuários selecionados ao criar um grupo local na grade de origem não serão incluídos quando o grupo for clonado para a grade de destino. Por esse motivo, não selecione usuários quando você criar o grupo. Em vez disso, selecione o grupo quando você criar os usuários.

Passos

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.
2. Selecione **criar grupo** e **concluir**.

   O grupo criado aparece na lista de grupos.

   Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver na grade de origem do locatário, o novo grupo será clonado para a grade de destino do locatário. **Success** aparece como **status de clonagem** na seção Visão geral da página de detalhes do grupo.

Crie grupos para um locatário Swift

Você pode gerenciar permissões de acesso para uma conta de locatário Swift importando grupos federados ou criando grupos locais. Pelo menos um grupo deve ter a permissão Swift Administrator, que é necessária para gerenciar os contentores e objetos para uma conta Swift.

> O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se você pretende importar um grupo federado, o "federação de identidade configurada", e o grupo federado já existe na origem de identidade configurada.

Acesse o assistente criar grupo

Passos

Como primeira etapa, acesse o assistente criar grupo.

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Selecione **criar grupo**.

Escolha um tipo de grupo

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

Passos

1. Selecione a guia **local group** para criar um grupo local ou selecione a guia **Federated group** para importar um grupo da origem de identidade configurada anteriormente.

   Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários pertencentes a grupos locais não poderão fazer login no Gerenciador de locatários, embora possam usar aplicativos clientes para gerenciar os recursos do locatário, com base nas permissões de grupo.

2. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.
   - **Federated group**: Insira o nome exclusivo. Para o ative Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
3. Selecione **continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Gerenciador de inquilinos e na API de gerenciamento de inquilinos.

Passos

1. Para **modo de acesso**, selecione uma das seguintes opções:
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do locatário e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. 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. Marque a caixa de seleção **Root Access** se os usuários do grupo precisarem fazer login na API de Gerenciamento de Locatário ou Gerenciamento de Locatário.
3. Selecione **continuar**.

Defina a política de grupo Swift

Os usuários Swift precisam de permissão de administrador para se autenticar na API REST do Swift para criar contentores e ingerir objetos.

1. Marque a caixa de seleção **Swift administrator** se os usuários do grupo precisarem usar a Swift REST API para gerenciar contentores e objetos.
2. 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)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar usuários locais que já existem.

Passos

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

   Se ainda não tiver criado utilizadores locais, pode adicionar este grupo ao utilizador na página utilizadores. "Gerenciar usuários locais"Consulte .

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

   O grupo criado aparece na lista de grupos.

Permissões de gerenciamento do locatário

Antes de criar um grupo de inquilinos, considere quais permissões você deseja atribuir a esse grupo. As permissões de gerenciamento do locatário determinam quais tarefas os usuários podem executar usando o Gerenciador do locatário ou a API de gerenciamento do locatário. Um usuário pode pertencer a um ou mais grupos. As permissões são cumulativas se um usuário pertencer a vários grupos.

Para fazer login no Gerenciador do Locatário ou usar a API de Gerenciamento do Locatário, os usuários devem pertencer a um grupo que tenha pelo menos uma permissão. Todos os usuários que podem entrar podem executar as seguintes tarefas:

- Visualizar o painel de instrumentos
- Alterar sua própria senha (para usuários locais)

Para todas as permissões, a configuração do 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.

Pode atribuir as seguintes permissões a um grupo. Observe que S3 locatários e locatários Swift têm permissões de grupo diferentes.

Permissão	Descrição	Detalhes
Acesso à raiz	Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário.	Os usuários Swift devem ter permissão de acesso root para entrar na conta do locatário.
Administrador	Apenas inquilinos Swift. Fornece acesso total aos contentores e objetos Swift para essa conta de locatário	Os usuários Swift devem ter a permissão Swift Administrator para executar qualquer operação com a SWIFT REST API.
Gerencie suas próprias credenciais S3	Permite que os usuários criem e removam suas próprias chaves de acesso S3.	Os utilizadores que não têm esta permissão não veem a opção de menu **STORAGE (S3)** > **My S3 Access Keys**.
Veja todos os baldes	**S3 locatários**: Permite que os usuários visualizem todos os buckets e configurações de bucket. **Swift tenants**: Permite que os usuários do Swift visualizem todos os contentores e configurações de contentores usando a API de Gerenciamento do locatário.	Os usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**. Essa permissão é substituída pela permissão Gerenciar todos os buckets. Não afeta as políticas de grupo ou bucket S3 usadas por clientes S3 ou console S3. Você só pode atribuir essa permissão aos grupos Swift a partir da API de Gerenciamento de Tenant. Não é possível atribuir essa permissão a grupos Swift usando o Gerenciador de Locações.
Gerenciar todos os buckets	**S3 inquilinos**: Permite que os usuários usem o Gerenciador do locatário e a API de gerenciamento do locatário para criar e excluir buckets do S3 e gerenciar as configurações de todos os buckets do S3 na conta do locatário, independentemente das políticas de bucket ou grupo do S3. **Swift tenants**: Permite que usuários Swift controlem a consistência para contentores Swift usando a API de Gerenciamento de inquilinos.	Os usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**. Esta permissão substitui a permissão Exibir todos os buckets. Não afeta as políticas de grupo ou bucket S3 usadas por clientes S3 ou console S3. Você só pode atribuir essa permissão aos grupos Swift a partir da API de Gerenciamento de Tenant. Não é possível atribuir essa permissão a grupos Swift usando o Gerenciador de Locações.

Permissão	Descrição	Detalhes
Gerenciar endpoints	Permite que os usuários usem o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para criar ou editar endpoints de serviço da plataforma, que são usados como o destino dos serviços da plataforma StorageGRID.	Os usuários que não têm essa permissão não veem a opção de menu **endpoints de serviços da plataforma**.
Use a guia Console do S3	Quando combinada com a permissão Exibir todos os buckets ou Gerenciar todos os buckets, permite que os usuários visualizem e gerenciem objetos na guia Console do S3 na página de detalhes de um bucket.	

Gerenciar grupos

Gerencie seus grupos de locatários conforme necessário para exibir, editar ou duplicar um grupo e muito mais.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

Ver ou editar grupo

Você pode exibir e editar as informações básicas e os detalhes de cada grupo.

Passos

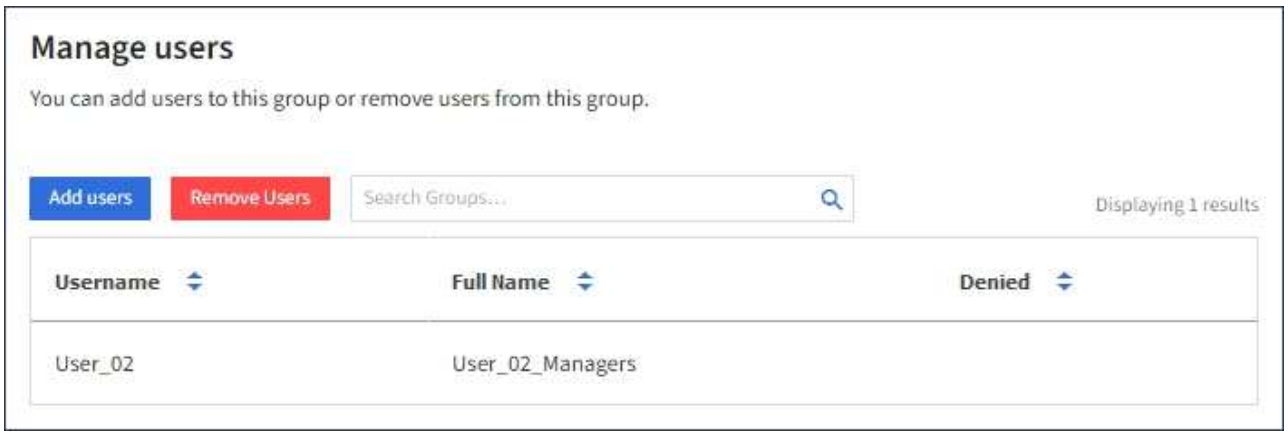
1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Revise as informações fornecidas na página grupos, que lista informações básicas para todos os grupos locais e federados dessa conta de locatário.

   Se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando grupos na grade de origem do locatário:

   - Uma mensagem de banner indica que, se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grade.
   - Conforme necessário, uma mensagem de banner indica se os grupos não foram clonados ao locatário na grade de destino. Você pode tente novamente um clone de grupo que falhou.
3. Se quiser alterar o nome do grupo:
   a. Selecione a caixa de verificação para o grupo.
   b. Selecione **ações** > **Editar nome do grupo**.
   c. Introduza o novo nome.
   d. Selecione **Salvar alterações.**
4. Se você quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome do grupo.

- Marque a caixa de seleção para o grupo e selecione **ações** > **Exibir detalhes do grupo**.

5. Revise a seção Visão geral, que mostra as seguintes informações para cada grupo:
   - Nome do visor
   - Nome único
   - Tipo
   - Modo de acesso
   - Permissões
   - S3 Política
   - Número de usuários neste grupo
   - Campos adicionais se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o grupo na grade de origem do locatário:
     - Status da clonagem, **sucesso** ou **falha**
     - Um banner azul indicando que, se você editar ou excluir esse grupo, suas alterações não serão sincronizadas com a outra grade.
6. Edite as definições do grupo conforme necessário. "Crie grupos para um locatário do S3"Consulte e "Crie grupos para um locatário Swift" para obter detalhes sobre o que introduzir.
   a. Na seção Visão geral , altere o nome de exibição selecionando o nome ou o ícone de edição .
   b. Na guia **permissões de grupo**, atualize as permissões e selecione **Salvar alterações**.
   c. Na guia **Política de grupo**, faça quaisquer alterações e selecione **Salvar alterações**.
      - Se você estiver editando um grupo S3, opcionalmente, selecione uma política de grupo S3 diferente ou insira a string JSON para uma política personalizada, conforme necessário.
      - Se você estiver editando um grupo Swift, opcionalmente selecione ou desmarque a caixa de seleção **Administrador Swift**.
7. Para adicionar um ou mais usuários locais existentes ao grupo:
   a. Selecione a guia usuários.



   b. Selecione **Adicionar usuários**.
   c. Selecione os usuários existentes que você deseja adicionar e selecione **Adicionar usuários**.

      Uma mensagem de sucesso aparece no canto superior direito.

8. Para remover usuários locais do grupo:

a. Selecione a guia usuários.
b. Selecione **Remover usuários**.
c. Selecione os usuários que deseja remover e selecione **Remover usuários**.

   Uma mensagem de sucesso aparece no canto superior direito.

9. Confirme se selecionou **Guardar alterações** para cada secção alterada.

Grupo duplicado

Você pode duplicar um grupo existente para criar novos grupos mais rapidamente.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você duplicar um grupo da grade de origem do locatário, o grupo duplicado será clonado para a grade de destino do locatário.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Marque a caixa de seleção do grupo que deseja duplicar.
3. Selecione **ações** > **grupo duplicado**.
4. "Crie grupos para um locatário do S3"Consulte ou "Crie grupos para um locatário Swift" para obter detalhes sobre o que introduzir.
5. Selecione **criar grupo**.

Repetir o clone do grupo

Para tentar novamente um clone que falhou:

1. Selecione cada grupo que indica *(Falha na clonagem)* abaixo do nome do grupo.
2. Selecione **ações** > **Clone groups**.
3. Veja o status da operação de clone na página de detalhes de cada grupo que você está clonando.

Para obter informações adicionais, "Clonar grupos de locatários e usuários"consulte .

Exclua um ou mais grupos

Pode eliminar um ou mais grupos. Quaisquer usuários que pertençam apenas a um grupo que seja excluído não poderão mais entrar no Gerenciador do locatário ou usar a conta do locatário.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você excluir um grupo, o StorageGRID não excluirá o grupo correspondente na outra grade. Se você precisar manter essas informações em sincronia, exclua o mesmo grupo de ambas as grades.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Selecione a caixa de verificação para cada grupo que pretende eliminar.
3. Selecione **ações** > **Excluir grupo** ou **ações** > **Excluir grupos**.

   É apresentada uma caixa de diálogo de confirmação.

4. Selecione **Excluir grupo** ou **Excluir grupos**.

Gerenciar usuários locais

Você pode criar usuários locais e atribuí-los a grupos locais para determinar quais recursos esses usuários podem acessar. O Gerenciador do Tenant inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, você não pode remover o usuário raiz.

> Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários locais não poderão fazer login no Gerenciador do Locatário ou na API de Gerenciamento do Locatário, embora possam usar aplicativos cliente para acessar os recursos do locatário, com base nas permissões de grupo.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para "clonar grupos de locatários e usuários", e você estará conetado à grade de origem do locatário.

Crie um usuário local

Você pode criar um usuário local e atribuí-lo a um ou mais grupos locais para controlar suas permissões de acesso.

S3 os usuários que não pertencem a nenhum grupo não têm permissões de gerenciamento ou políticas de grupo S3 aplicadas a eles. Esses usuários podem ter acesso ao bucket do S3 concedido por meio de uma política de bucket.

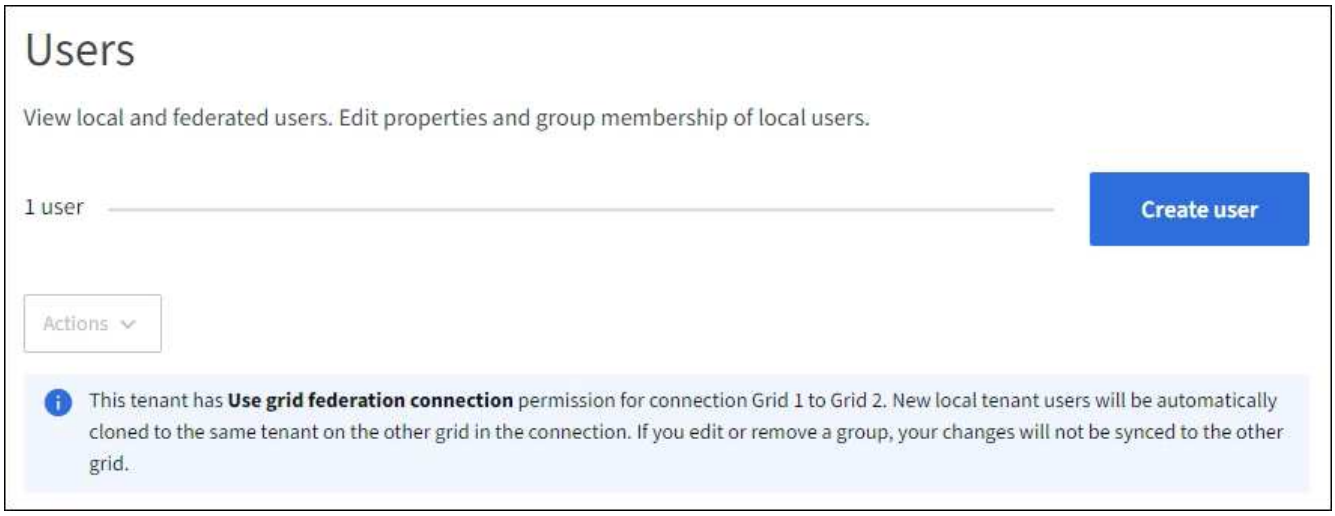
Os usuários Swift que não pertencem a nenhum grupo não têm permissões de gerenciamento ou acesso ao contentor Swift.

Acesse o assistente criar usuário

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.

   Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, um banner azul indica que essa é a grade de origem do locatário. Todos os usuários locais que você criar nesta grade serão clonados para a outra grade na conexão.



2. Selecione **criar usuário**.

Introduza as credenciais

Passos

1. Para a etapa **Insira as credenciais do usuário**, preencha os campos a seguir.

Campo	Descrição
Nome completo	O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
Nome de utilizador	O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados. **Nota**: Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, ocorrerá um erro de clonagem se o mesmo **Username** já existir para o locatário na grade de destino.
Senha e confirmar senha	A senha que o usuário usará inicialmente ao fazer login.
Negar acesso	Selecione **Sim** para impedir que esse usuário faça login na conta de locatário, mesmo que ele ainda possa pertencer a um ou mais grupos. Por exemplo, selecione **Sim** para suspender temporariamente a capacidade de um usuário fazer login.

2. Selecione **continuar**.

Atribuir a grupos

Passos

1. Atribua o usuário a um ou mais grupos locais para determinar quais tarefas podem ser executadas.

   Atribuir um usuário a grupos é opcional. Se preferir, você pode selecionar usuários ao criar ou editar grupos.

Os usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Os usuários terão todas as permissões para todos os grupos aos quais pertencem. "Permissões de gerenciamento do locatário"Consulte .

2. Selecione **criar usuário**.

   Se sua conta de locatário tiver a permissão **Use Grid Federation Connection** e você estiver na grade de origem do locatário, o novo usuário local será clonado para a grade de destino do locatário. **Success** aparece como **status de clonagem** na seção Visão geral da página de detalhes do usuário.

3. Selecione **Finish** para retornar à página usuários.

Ver ou editar utilizador local

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Revise as informações fornecidas na página usuários, que lista informações básicas para todos os usuários locais e federados dessa conta de locatário.

   Se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:

   - Uma mensagem de banner indica que, se você editar ou remover um usuário, suas alterações não serão sincronizadas com a outra grade.
   - Conforme necessário, uma mensagem de banner indica se os usuários não foram clonados para o locatário na grade de destino. Você pode tente novamente um clone de usuário que falhou.

3. Se pretender alterar o nome completo do utilizador:
   a. Selecione a caixa de verificação para o utilizador.
   b. Selecione **ações** > **Editar nome completo**.
   c. Introduza o novo nome.
   d. Selecione **Salvar alterações.**
4. Se você quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome de utilizador.
   - Marque a caixa de seleção para o usuário e selecione **ações** > **Exibir detalhes do usuário**.
5. Revise a seção Visão geral, que mostra as seguintes informações para cada usuário:
   - Nome completo
   - Nome de utilizador
   - Tipo de utilizador
   - Acesso negado
   - Modo de acesso
   - Associação ao grupo
   - Campos adicionais se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:
     - Status da clonagem, **sucesso** ou **falha**
     - Um banner azul indicando que, se você editar este usuário, suas alterações não serão

sincronizadas com a outra grade.

6. Edite as definições do utilizador conforme necessário. Consulte Criar utilizador local para obter detalhes sobre o que introduzir.
   a. Na seção Visão geral , altere o nome completo selecionando o nome ou o ícone de edição .

      Você não pode alterar o nome de usuário.

   b. Na guia **Senha**, altere a senha do usuário e selecione **Salvar alterações**.
   c. Na guia **Access**, selecione **não** para permitir que o usuário faça login ou selecione **Sim** para impedir que o usuário faça login. Em seguida, selecione **Salvar alterações**.
   d. Na guia **teclas de acesso**, selecione **criar chave** e siga as instruções para "Criando as chaves de acesso S3 de outro usuário".
   e. Na guia **grupos**, selecione **Editar grupos** para adicionar o usuário aos grupos ou remover o usuário dos grupos. Em seguida, selecione **Salvar alterações**.
7. Confirme se selecionou **Guardar alterações** para cada secção alterada.

Duplicar utilizador local

Você pode duplicar um usuário local para criar um novo usuário mais rapidamente.

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você duplicar um usuário da grade de origem do locatário, o usuário duplicado será clonado para a grade de destino do locatário.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione a caixa de verificação para o utilizador que pretende duplicar.
3. Selecione **ações** > **usuário duplicado**.
4. Consulte Criar utilizador local para obter detalhes sobre o que introduzir.
5. Selecione **criar usuário**.

Repetir o clone do usuário

Para tentar novamente um clone que falhou:

1. Selecione cada usuário que indica *(Falha na clonagem)* abaixo do nome de usuário.
2. Selecione **ações** > **Clone usuários**.
3. Veja o status da operação de clone na página de detalhes de cada usuário que você está clonando.

Para obter informações adicionais, "Clonar grupos de locatários e usuários"consulte .

Exclua um ou mais usuários locais

Você pode excluir permanentemente um ou mais usuários locais que não precisam mais acessar a conta de locatário do StorageGRID.

Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você excluir um usuário local, o StorageGRID não excluirá o usuário correspondente na outra grade. Se você precisar manter essas informações em sincronia, você deve excluir o mesmo usuário de ambas as grades.

Você deve usar a origem de identidade federada para excluir usuários federados.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione a caixa de verificação para cada utilizador que pretende eliminar.
3. Selecione **ações** > **Excluir usuário** ou **ações** > **Excluir usuários**.

   É apresentada uma caixa de diálogo de confirmação.

4. Selecione **Excluir usuário** ou **Excluir usuários**.

Informações sobre direitos autorais

Informações sobre marcas comerciais