Gerenciamento do acesso do sistema para usuários de locatários

StorageGRID

NetApp
March 10, 2025

Índice

Gerenciamento do acesso do sistema para usuários de locatários

Você concede aos usuários acesso a uma conta de locatário importando grupos de uma origem de identidade federada e atribuindo permissões de gerenciamento. Você também pode criar grupos de locatários locais e usuários, a menos que o logon único (SSO) esteja em vigor para todo o sistema StorageGRID.

- "Usando a federação de identidade"
- "Gerenciando grupos"
- "Gerenciamento de usuários locais"

Usando 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.

- "Configurando uma fonte de identidade federada"
- "Forçando a sincronização com a fonte de identidade"
- "Desativando a federação de identidade"

Configurando uma fonte de identidade federada

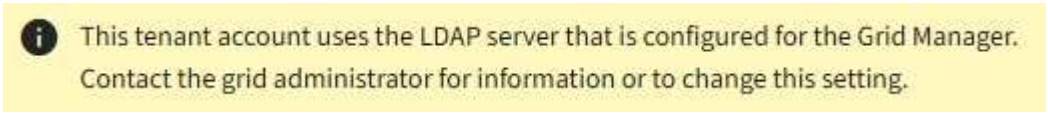
Você pode configurar a federação de identidade se quiser que grupos de locatários e usuários sejam gerenciados em outro sistema, como ative Directory, OpenLDAP ou Oracle Directory Server.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve estar usando o ative Directory, OpenLDAP ou Oracle Directory Server como o provedor de identidade. Se pretender utilizar um serviço LDAP v3 que não esteja listado, tem de contactar o suporte técnico.
- Se você pretende usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade deve estar usando TLS 1,2 ou 1,3.

Sobre esta tarefa

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.



Passos

1. Selecione **GERENCIAMENTO DE ACESSO federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na seção tipo de serviço LDAP, selecione **ative Directory**, **OpenLDAP** ou **Other**.

   Se selecionar **OpenLDAP**, configure o servidor OpenLDAP. Consulte as diretrizes para configurar um servidor OpenLDAP.

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

4. Se você selecionou **Other**, preencha os campos na seção atributos LDAP.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.
   - **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Group unique name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
   - **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
5. Na secção Configurar servidor LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias.
   - **Nome do host**: O nome do host do servidor ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar ao servidor LDAP. A porta padrão para STARTTLS é 389 e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta desde que seu firewall esteja configurado corretamente.
   - **Nome de usuário**: O caminho completo do nome distinto (DN) para o usuário que se conetará ao servidor LDAP. No ative Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

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

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`
   - **Senha**: A senha associada ao nome de usuário.
   - **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você

deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

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

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

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

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

     Esta opção não é suportada se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

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

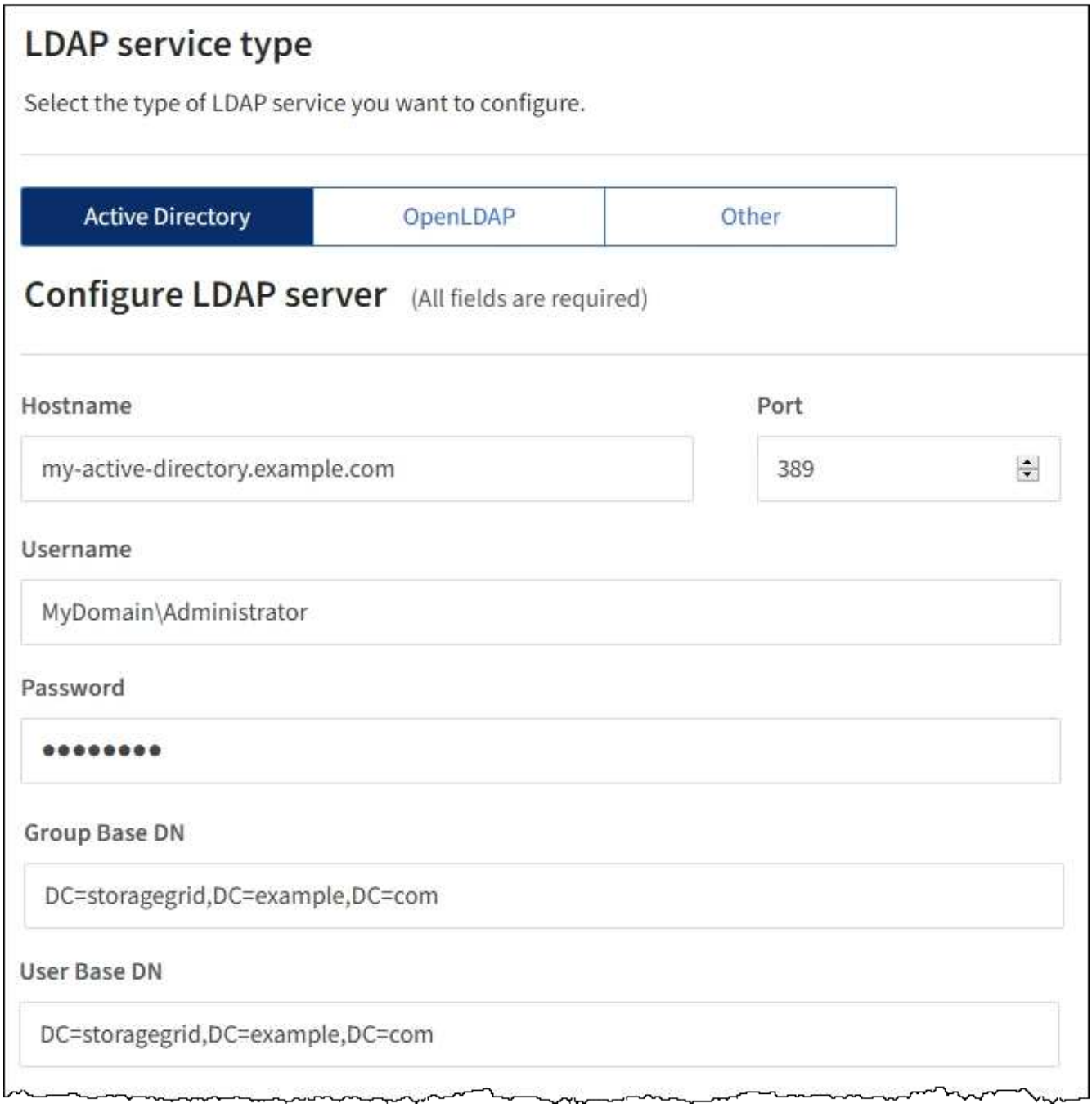
     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

8. Selecione **testar ligação** para validar as definições de ligação para o servidor LDAP.

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

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

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



Informações relacionadas

"Permissões de gerenciamento do locatário"

"Diretrizes para configurar um servidor OpenLDAP"

Diretrizes para configurar um servidor OpenLDAP

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

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as

instruções para manutenção de associação reversa em grupo no Guia do Administrador para OpenLDAP.

Indexação

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

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

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

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

Forçando a sincronização com a fonte de identidade

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- A origem de identidade guardada tem de estar ativada.

Passos

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

   A página de federação de identidade é exibida. O botão **servidor de sincronização** está no canto superior direito da página.

   > ⓘ Se a origem de identidade salva não estiver ativada, o botão **servidor de sincronização** não estará ativo.

2. Selecione **servidor de sincronização**.

   É apresentada uma mensagem de confirmação a indicar que a sincronização foi iniciada com êxito.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Desativando a federação de identidade

Se você tiver configurado um serviço de federação de identidade para esse locatário, poderá desativar temporariamente ou permanentemente a federação de identidade para

grupos de locatários e usuários. Quando a federação de identidade está desativada, não há comunicação entre o sistema StorageGRID e a origem da identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

O que você vai precisar

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

Sobre esta tarefa

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

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso à conta do locatário até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO federação de identidade**.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.
3. Selecione **Guardar**.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Gerenciando grupos

Você atribui permissões a grupos de usuários para controlar quais tarefas os usuários do locatário podem executar. Você pode importar grupos federados de uma origem de identidade, como o ative Directory ou o OpenLDAP, ou criar grupos locais.

> Se o logon único (SSO) estiver habilitado para o seu sistema StorageGRID, os usuários locais não poderão fazer login no Gerenciador do locatário, embora possam acessar os recursos S3 e Swift, com base nas permissões de grupo.

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. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Permissão	Descrição
Acesso à raiz	Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário. **Observação:** os usuários do 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 **Observação:** os usuários do Swift devem ter a permissão Swift Administrator para executar qualquer operação com a Swift REST API.
Gerencie suas próprias credenciais S3	Apenas S3 inquilinos. Permite que os usuários criem e removam suas próprias chaves de acesso S3. Os usuários que não têm essa permissão não veem a opção de menu **ARMAZENAMENTO (S3) My S3 Access Keys**.
Gerenciar todos os baldes	• S3 locatários: 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. Os usuários que não têm essa permissão não veem a opção de menu **Buckets**. • Swift tenants: Permite que usuários Swift controlem o nível de consistência para contentores Swift usando a API de Gerenciamento do locatário. **Observação:** você só pode atribuir a permissão Gerenciar todos os buckets a grupos Swift a partir da API de Gerenciamento de locatário. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de inquilinos.
Gerir pontos finais	Apenas S3 inquilinos. Permite que os usuários usem o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para criar ou editar endpoints, que são usados como o destino para os serviços da plataforma StorageGRID. Os usuários que não têm essa permissão não veem a opção de menu **endpoints de serviços da plataforma**.

Informações relacionadas

"Use S3"

"Use Swift"

Criando grupos para um locatário S3

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.

2. Selecione **criar grupo**.
3. 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.

4. 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.

5. Selecione **continuar**.
6. Selecione um modo de acesso. 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.
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem 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.
7. Selecione as permissões de grupo para este grupo.

   Consulte as informações sobre permissões de gerenciamento de locatários.
8. Selecione **continuar**.
9. Selecione uma política de grupo para determinar quais permissões de acesso S3 os membros deste grupo terão.
   - **No S3 Access**: 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 aos 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.
   - **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto. Consulte as instruções para implementar um aplicativo cliente S3 para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de linguagem e exemplos.
10. 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.

    Neste exemplo, os membros do grupo só podem listar e acessar uma pasta que corresponda ao nome de usuário (prefixo de chave) no intervalo especificado. Observe que as permissões de acesso de outras políticas de grupo e a política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.

11. Selecione o botão que aparece, dependendo se você está criando um grupo federado ou um grupo local:
    - Grupo federado: **Criar grupo**
    - Grupo local: **Continuar**

    Se você estiver criando um grupo local, a etapa 4 (Adicionar usuários) será exibida após selecionar **continuar**. Esta etapa não aparece para grupos federados.

12. Marque a caixa de seleção para cada usuário que deseja adicionar ao grupo e selecione **criar grupo**.

    Opcionalmente, você pode salvar o grupo sem adicionar usuários. Você pode adicionar usuários ao grupo mais tarde ou selecionar o grupo quando adicionar novos usuários.

13. Selecione **Finish**.

    O grupo criado aparece na lista de grupos. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

"Use S3"

Criando 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 que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.

2. Selecione **criar grupo**.
3. 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.

4. 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.
5. Selecione **continuar**.
6. Selecione um modo de acesso. 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.

- **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.
- **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem 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.

7. Defina a permissão Grupo.
   - Marque a caixa de seleção **Root Access** se os usuários precisarem fazer login na API de Gerenciamento de Tenant ou Tenant Manager. (Predefinição)
   - Desmarque a caixa de seleção **Root Access** se os usuários não precisarem de acesso ao Gerenciador do locatário ou à API de Gerenciamento do locatário. Por exemplo, desmarque a caixa de seleção para aplicativos que não precisam acessar o locatário. Em seguida, atribua a permissão **Swift Administrator** para permitir que esses usuários gerenciem contentores e objetos.
8. Selecione **continuar**.
9. Marque a caixa de seleção **Swift administrator** se o usuário precisar usar a Swift REST API.

   Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

10. Selecione o botão que aparece, dependendo se você está criando um grupo federado ou um grupo local:
    - Grupo federado: **Criar grupo**
    - Grupo local: **Continuar**

      Se você estiver criando um grupo local, a etapa 4 (Adicionar usuários) será exibida após selecionar **continuar**. Esta etapa não aparece para grupos federados.

11. Marque a caixa de seleção para cada usuário que deseja adicionar ao grupo e selecione **criar grupo**.

    Opcionalmente, você pode salvar o grupo sem adicionar usuários. Você pode adicionar usuários ao grupo mais tarde ou selecionar o grupo quando criar novos usuários.

12. Selecione **Finish**.

    O grupo criado aparece na lista de grupos. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

"Use Swift"

Visualização e edição de detalhes do grupo

Ao exibir os detalhes de um grupo, você pode alterar o nome de exibição, as permissões, as políticas e os usuários que pertencem ao grupo.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.

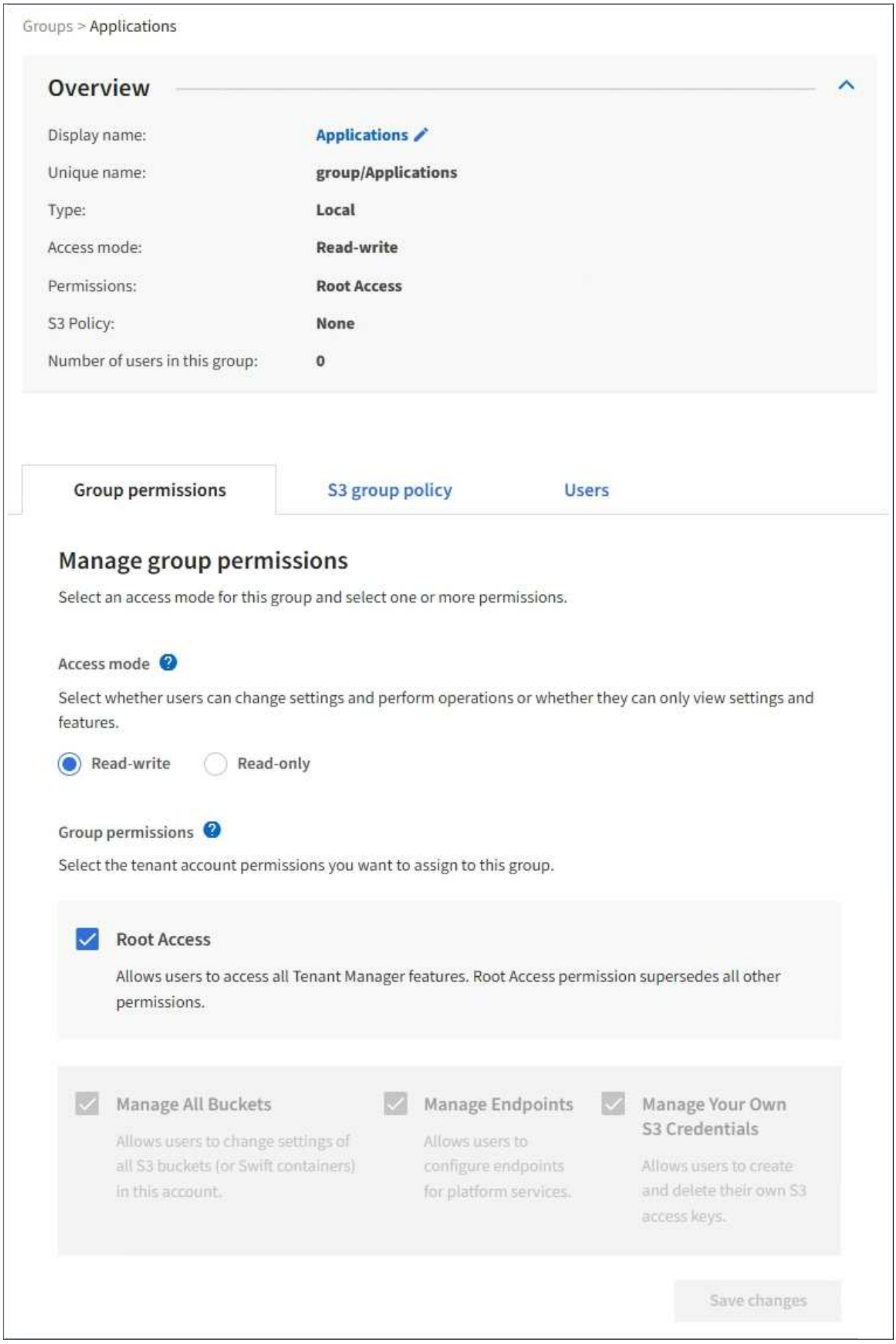
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo cujos detalhes deseja exibir ou editar.

   Alternativamente, você pode selecionar **ações Exibir detalhes do grupo**.

   A página de detalhes do grupo é exibida. O exemplo a seguir mostra a página de detalhes do grupo S3.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Faça alterações nas definições do grupo conforme necessário.

> Para garantir que suas alterações sejam salvas, selecione **Salvar alterações** depois de fazer alterações em cada seção. Quando as alterações são salvas, uma mensagem de confirmação aparece no canto superior direito da página.

   a. Opcionalmente, selecione o nome de exibição ou o ícone de edição para atualizar o nome de exibição.

      Não é possível alterar o nome exclusivo de um grupo. Não é possível editar o nome de exibição de um grupo federado.

   b. Opcionalmente, atualize as permissões.

   c. Para a política de grupo, faça as alterações apropriadas para o seu locatário S3 ou Swift.

      - Se você estiver editando um grupo para um locatário S3, opcionalmente, selecione uma política de grupo S3 diferente. Se você selecionar uma política S3 personalizada, atualize a cadeia de carateres JSON conforme necessário.
      - Se você estiver editando um grupo para um locatário Swift, opcionalmente selecione ou desmarque a caixa de seleção **Administrador Swift**.

        Para obter mais informações sobre a permissão Swift Administrator, consulte as instruções para criar grupos para um locatário Swift.

   d. Opcionalmente, adicione ou remova usuários.

4. Confirme que selecionou **Guardar alterações** para cada secção alterada.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Criando grupos para um locatário S3"

"Criando grupos para um locatário Swift"

Adicionando usuários a um grupo local

Você pode adicionar usuários a um grupo local conforme necessário.

O que você vai precisar

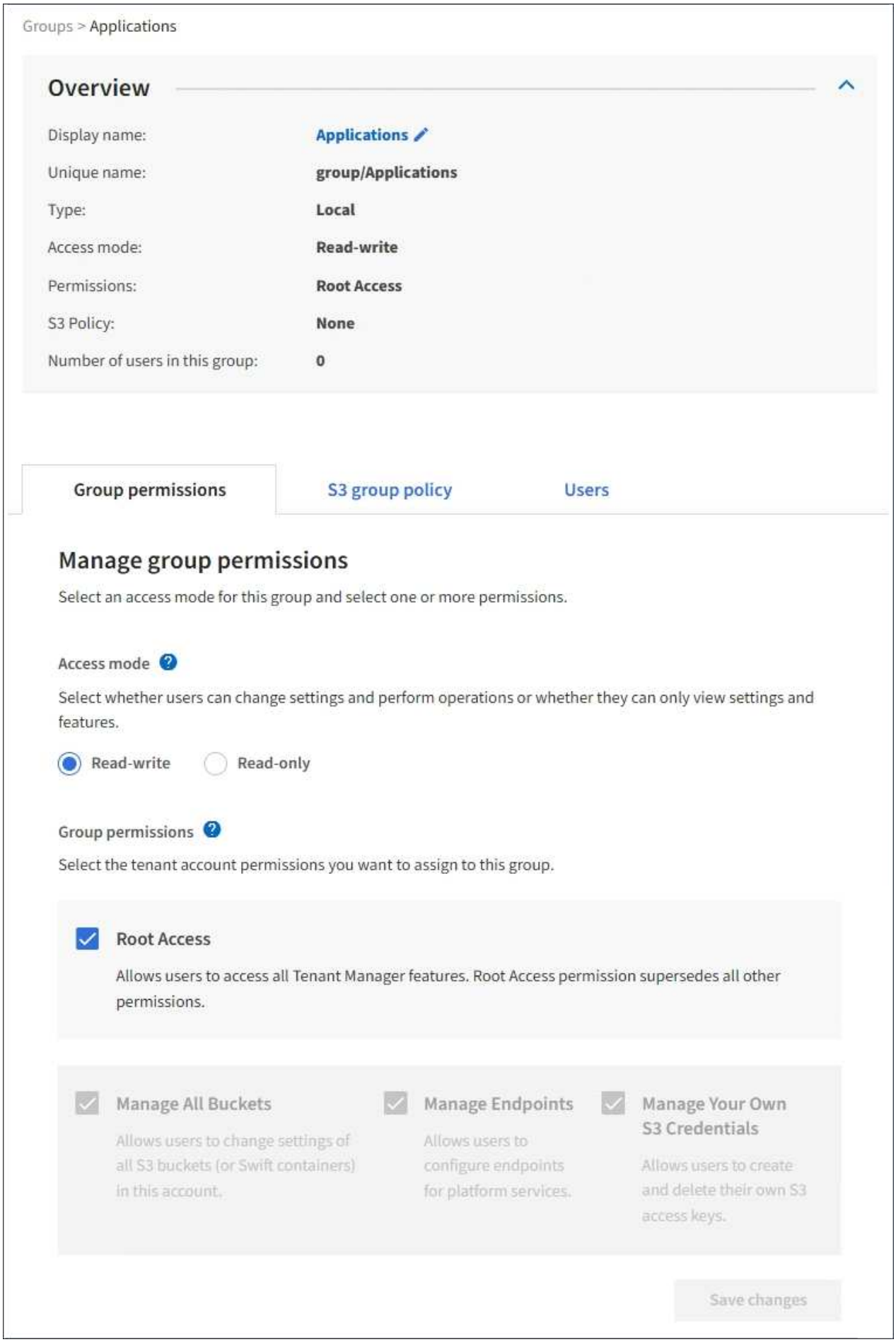
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

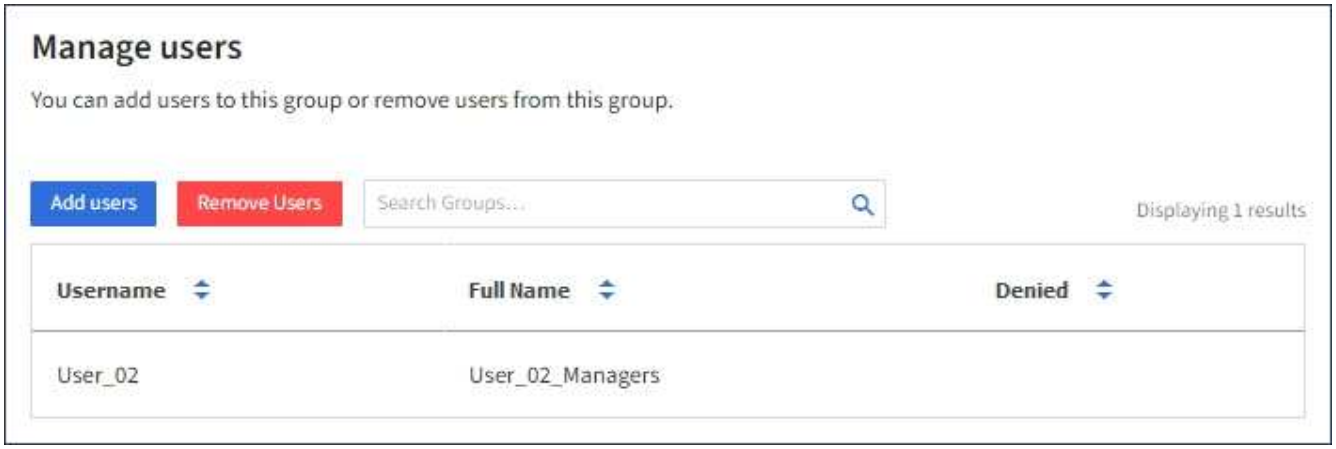
1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo local ao qual deseja adicionar usuários.

   Alternativamente, você pode selecionar **ações Exibir detalhes do grupo**.

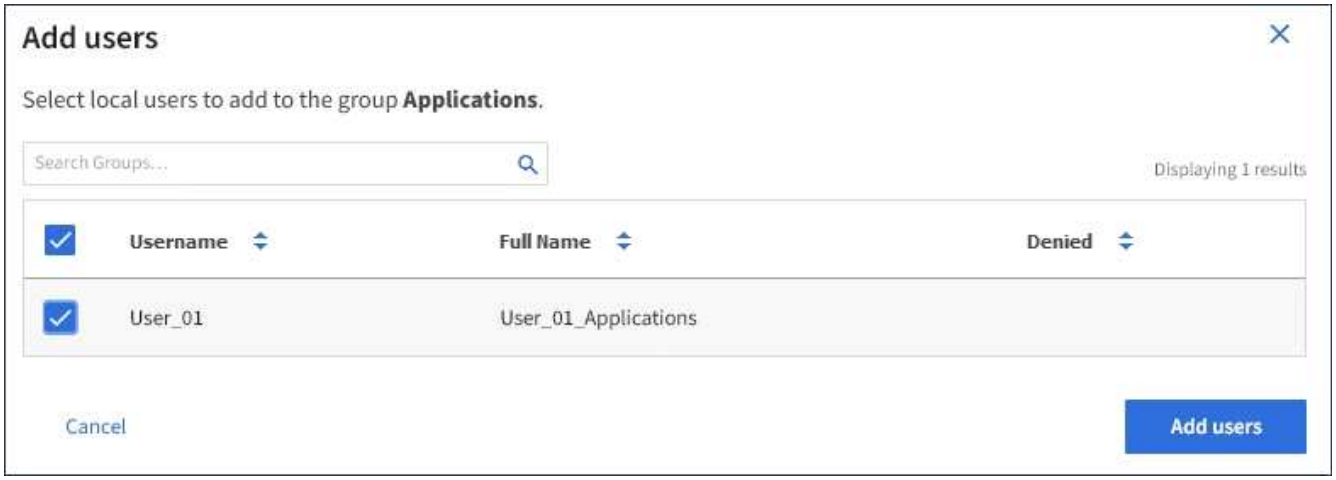
   A página de detalhes do grupo é exibida.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Selecione **Gerenciar usuários** e, em seguida, selecione **Adicionar usuários**.



4. Selecione os usuários que deseja adicionar ao grupo e selecione **Adicionar usuários**.



Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Editar um nome de grupo

Pode editar o nome de apresentação de um grupo. Não é possível editar o nome exclusivo de um grupo.

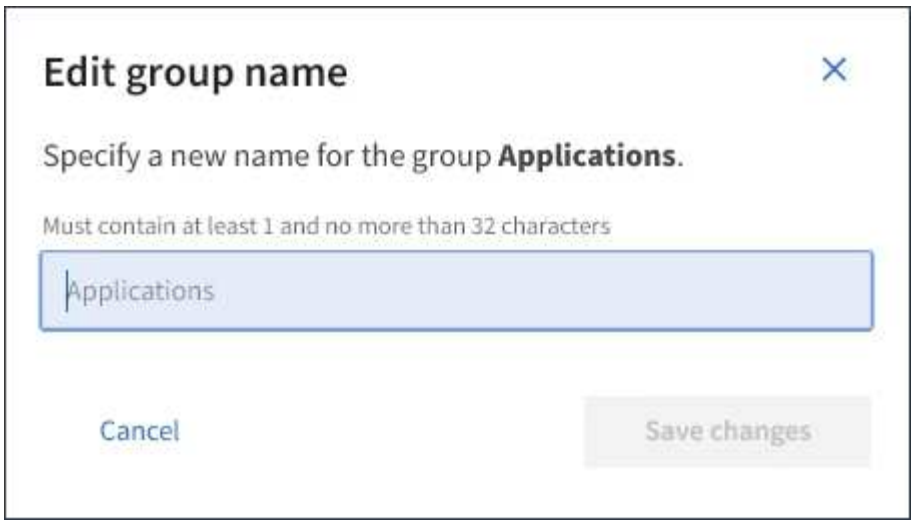
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Marque a caixa de seleção do grupo cujo nome de exibição deseja editar.
3. Selecione **ações Editar nome do grupo**.

   A caixa de diálogo Editar nome do grupo é exibida.



4. Se estiver editando um grupo local, atualize o nome de exibição conforme necessário.

   Não é possível alterar o nome exclusivo de um grupo. Não é possível editar o nome de exibição de um grupo federado.

5. Selecione **Salvar alterações**.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Duplicando um grupo

Você pode criar novos grupos mais rapidamente duplicando um grupo existente.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Marque a caixa de seleção do grupo que deseja duplicar.
3. Selecione **Duplicate group**. Para obter detalhes adicionais sobre a criação de um grupo, consulte as instruções para criar grupos para um locatário S3 ou para um locatário Swift.
4. 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.

5. 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.

6. Selecione **continuar**.
7. Conforme necessário, modifique as permissões para este grupo.
8. Selecione **continuar**.
9. Conforme necessário, se você estiver duplicando um grupo para um locatário S3, opcionalmente, selecione uma política diferente nos botões de opção **Adicionar política S3**. Se você selecionou uma política personalizada, atualize a cadeia de carateres JSON conforme necessário.
10. Selecione **criar grupo**.

Informações relacionadas

"Criando grupos para um locatário S3"

"Criando grupos para um locatário Swift"

"Permissões de gerenciamento do locatário"

Eliminar um grupo

Pode eliminar um grupo do sistema. Quaisquer usuários que pertençam apenas a esse grupo não poderão mais entrar no Gerenciador do Locatário ou usar a conta do locatário.

O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.

2. Marque as caixas de seleção dos grupos que deseja excluir.
3. Selecione **ações Excluir grupo**.

   É apresentada uma mensagem de confirmação.

4. Selecione **Excluir grupo** para confirmar que deseja excluir os grupos indicados na mensagem de confirmação.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Gerenciamento de 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, não é possível remover o usuário root.

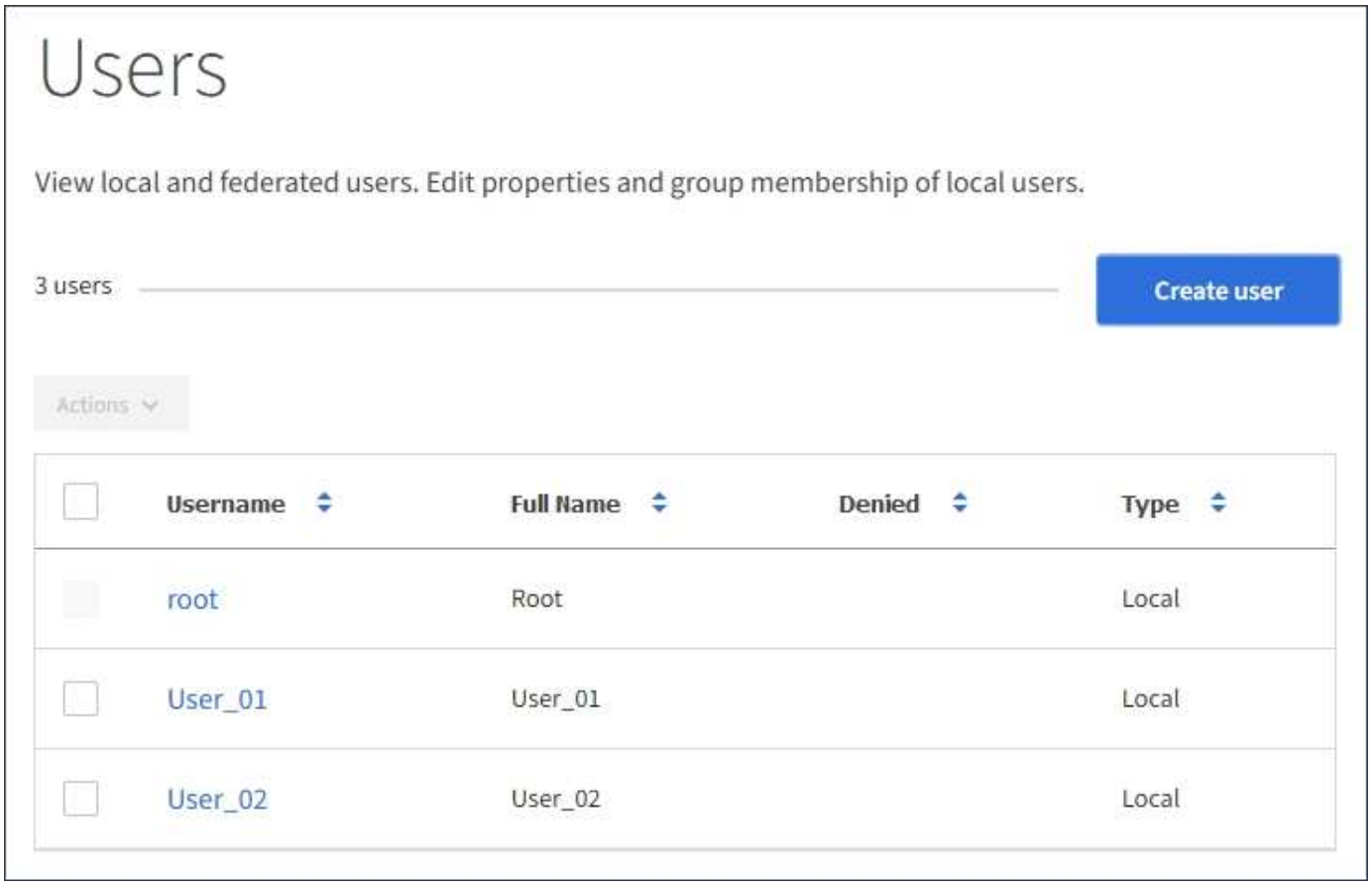
O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários de leitura e gravação que tenha a permissão de acesso root.

> Se o logon único (SSO) estiver habilitado para o seu 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 S3 ou Swift para acessar os recursos do locatário, com base nas permissões de grupo.

Acessando a página usuários

Selecione **GERENCIAMENTO DE ACESSO usuários**.



Criando usuários locais

Você pode criar usuários locais e atribuí-los 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.

Passos

1. Selecione **criar usuário**.
2. Preencha os campos a seguir.
   - **Nome completo**: O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
   - **Nome de usuário**: O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.
   - * Senha*: Uma senha, que é usada quando o usuário entra.
   - **Confirm password**: Digite a mesma senha digitada no campo Senha.

- **Negar acesso**: Se você selecionar **Sim**, esse usuário não poderá entrar na conta de locatário, mesmo que o usuário ainda possa pertencer a um ou mais grupos.

  Como exemplo, você pode usar esse recurso para suspender temporariamente a capacidade de um usuário fazer login.

3. Selecione **continuar**.
4. Atribua o usuário a um ou mais grupos locais.

   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.

5. Selecione **criar usuário**.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Editando detalhes do usuário

Ao editar os detalhes de um usuário, você pode alterar o nome completo e a senha do usuário, adicionar o usuário a diferentes grupos e impedir que o usuário acesse o locatário.

Passos

1. Na lista Users (utilizadores), selecione o nome do utilizador cujos detalhes pretende ver ou editar.

   Alternativamente, você pode selecionar a caixa de seleção para o usuário e, em seguida, selecionar **ações Exibir detalhes do usuário**.

2. Faça alterações nas definições do utilizador, conforme necessário.
   a. Altere o nome completo do usuário conforme necessário selecionando o nome completo ou o ícone de edição na seção Visão geral.

      Você não pode alterar o nome de usuário.

   b. Na guia **Senha**, altere a senha do usuário conforme necessário.
   c. Na guia **Access**, permita que o usuário faça login (selecione **não**) ou impeça que o usuário faça login (selecione **Sim**) conforme necessário.
   d. Na guia **Groups**, adicione o usuário aos grupos ou remova o usuário dos grupos conforme necessário.
   e. Conforme necessário para cada seção, selecione **Salvar alterações**.

      As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Duplicação de usuários locais

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

Passos

1. Na lista usuários, selecione o usuário que deseja duplicar.
2. Selecione **Duplicate user**.
3. Modifique os campos a seguir para o novo usuário.

- **Nome completo**: O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
- **Nome de usuário**: O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.
- * Senha*: Uma senha, que é usada quando o usuário entra.
- **Confirm password**: Digite a mesma senha digitada no campo Senha.
- **Negar acesso**: Se você selecionar **Sim**, esse usuário não poderá entrar na conta de locatário, mesmo que o usuário ainda possa pertencer a um ou mais grupos.

  Como exemplo, você pode usar esse recurso para suspender temporariamente a capacidade de um usuário fazer login.

4. Selecione **continuar**.
5. Selecione um ou mais grupos locais.

   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.

6. Selecione **criar usuário**.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Eliminar utilizadores locais

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

Usando o Gerenciador do Locatário, você pode excluir usuários locais, mas não usuários federados. Você deve usar a origem de identidade federada para excluir usuários federados.

Passos

1. Na lista Users (utilizadores), selecione a caixa de verificação para o utilizador local que pretende eliminar.
2. Selecione **ações Excluir usuário**.
3. Na caixa de diálogo de confirmação, selecione **Excluir usuário** para confirmar que deseja excluir o usuário do sistema.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

"Permissões de gerenciamento do locatário"

Informações sobre direitos autorais

Informações sobre marcas comerciais