



Gerenciar o acesso ao sistema

StorageGRID

NetApp
March 12, 2025

Índice

Gerenciar o acesso ao sistema	1
Use a federação de identidade	1
Configure a federação de identidade para o Gerenciador do Locatário	1
Forçar a sincronização com a fonte de identidade	5
Desativar a federação de identidade	5
Diretrizes para configurar o servidor OpenLDAP	5
Gerenciar grupos	6
Crie grupos para um locatário do S3	6
Crie grupos para um locatário Swift	9
Permissões de gerenciamento do locatário	11
Ver e editar detalhes do grupo	12
Adicione usuários a um grupo local	14
Editar nome do grupo	16
Grupo duplicado	17
Eliminar grupo	18
Gerenciar usuários locais	19
Acesse a página usuários	19
Crie usuários locais	20
Editar detalhes do utilizador	21
Duplicar usuários locais	21
Eliminar utilizadores locais	22

Gerenciar o acesso ao sistema

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 ativo Directory, o Azure ativo Directory (Azure AD), o OpenLDAP ou o Oracle Directory Server.

O que você vai precisar

- Você está conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- Você está usando o ativo 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 OpenLDAP](#)Consulte .
- 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.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Introduza a configuração

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.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

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

- 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 Active 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 Active 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 hífen são ignorados.
 - Group Unique Name:** O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao Active 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 Active 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 hífen são ignorados.
- Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na seção 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 conectar 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 conectará ao servidor LDAP.

No Active 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 caracteres especiais no nome de usuário, como em ou /.

Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

 👁

- 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 conectados 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 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 e remova o usuário de todos os grupos.

Sobreposições de Memberof e refint

As sobreposições membradas 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

Crie grupos para um locatário do 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 conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. [Permissões de gerenciamento do locatário](#)Consulte .
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Para obter informações sobre o S3, [Use S3](#)consulte .

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 ativo 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 caracteres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de caracteres.
 - **Acesso total:** Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de caracteres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de caracteres.
 - **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.

The screenshot shows the AWS IAM console interface for creating a group. On the left, four radio buttons are visible: 'No S3 Access', 'Read Only Access', 'Full Access', and 'Custom'. The 'Custom' option is selected, with a subtext '(Must be a valid JSON formatted string.)'. To the right, a text area contains the following JSON policy string:

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

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.

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 que você vai precisar

- Você deve estar conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- 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**.

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beeec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

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 ativo 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 autenticuem 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](#)

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.

Permissão	Descrição
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	<ul style="list-style-type: none"> • 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. <p>Os usuários que não têm essa permissão não veem a opção de menu Buckets.</p> <ul style="list-style-type: none"> • Swift tenants: Permite que usuários Swift controlem o nível de consistência para contentores Swift usando a API de Gerenciamento do locatário. <p>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.</p>
Gerir pontos finais	<p>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.</p> <p>Os usuários que não têm essa permissão não veem a opção de menu endpoints de serviços da plataforma.</p>

Informações relacionadas

[Use S3](#)

[Use Swift](#)

Ver e editar 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 conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- 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.

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 caracteres 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 seção alterada.

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

Informações relacionadas

[Criar grupos para S3 inquilino](#)

[Crie grupos para o locatário Swift](#)

Adicione usuários a um grupo local

Você pode adicionar usuários a um grupo local conforme necessário.

O que você vai precisar

- Você deve estar conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- 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.

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

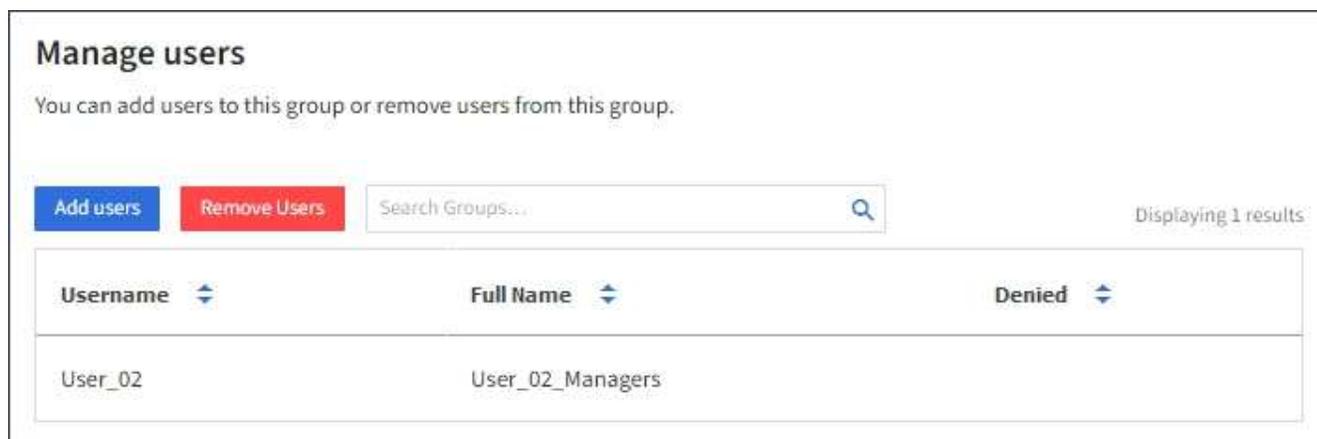
Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

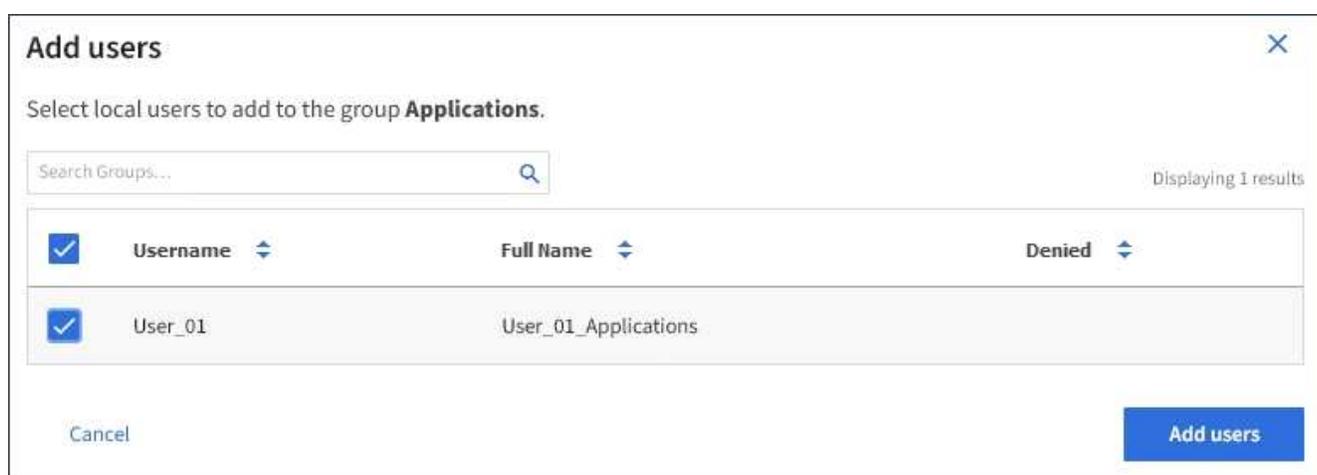
Allows users to create and delete their own S3 access keys.

Save changes

3. Selecione **Users** e, em seguida, selecione **Add Users**.



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 nome do 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 conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. [Permissões de gerenciamento do locatário](#) Consulte .

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.

Edit group name ✕

Specify a new name for the group **Applications**.

Must contain at least 1 and no more than 32 characters

Applications

Cancel Save changes

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.

Grupo duplicado

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

O que você vai precisar

- Você deve estar conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. [Permissões de gerenciamento do locatário](#) Consulte .

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 como criar um grupo, consulte as instruções para criar grupos para [Um inquilino de S3 anos](#) ou para [Um inquilino 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 ativo 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 caracteres JSON conforme necessário.
10. Selecione **criar grupo**.

Eliminar 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 conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. [Permissões de gerenciamento do locatário](#) Consulte .

Passos

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



The screenshot shows the 'Groups' management page. At the top, it says 'Create and manage local and federated groups. Set group permissions to control access to specific pages and features.' Below this, it indicates '2 groups' and has a 'Create group' button. There is an 'Actions' dropdown menu. The main content is a table with the following data:

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

At the bottom right of the table area, there are navigation links: '< Previous 1 Next >'.

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.

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, não é possível remover o usuário root.

O que você vai precisar

- Você deve estar conectado ao Gerenciador do Locatário usando um [navegador da web suportado](#).
- Você deve pertencer a um grupo de usuários de leitura e gravação que tenha a permissão de acesso root. [Permissões de gerenciamento do locatário](#) Consulte .



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.

Acesse a página usuários

Selecione **GERENCIAMENTO DE ACESSO usuários**.

Users

View local and federated users. Edit properties and group membership of local users.

3 users

Create user

Actions

<input type="checkbox"/>	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

Crie 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.

Editar detalhes do utilizador

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 localatário.

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.

Duplicar 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 sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.