Configurando uma fonte de identidade federada

StorageGRID

NetApp
March 10, 2025

Índice

Configurando uma fonte de identidade federada

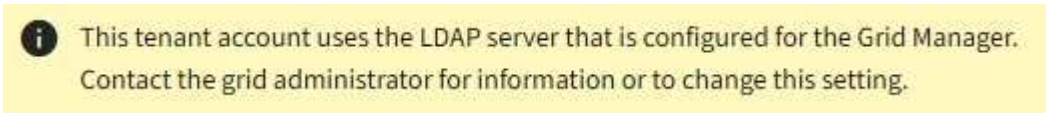
Você pode configurar a federação de identidade se quiser que grupos de locatários e usuários sejam gerenciados em outro sistema, como ative Directory, OpenLDAP ou Oracle Directory Server.

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.

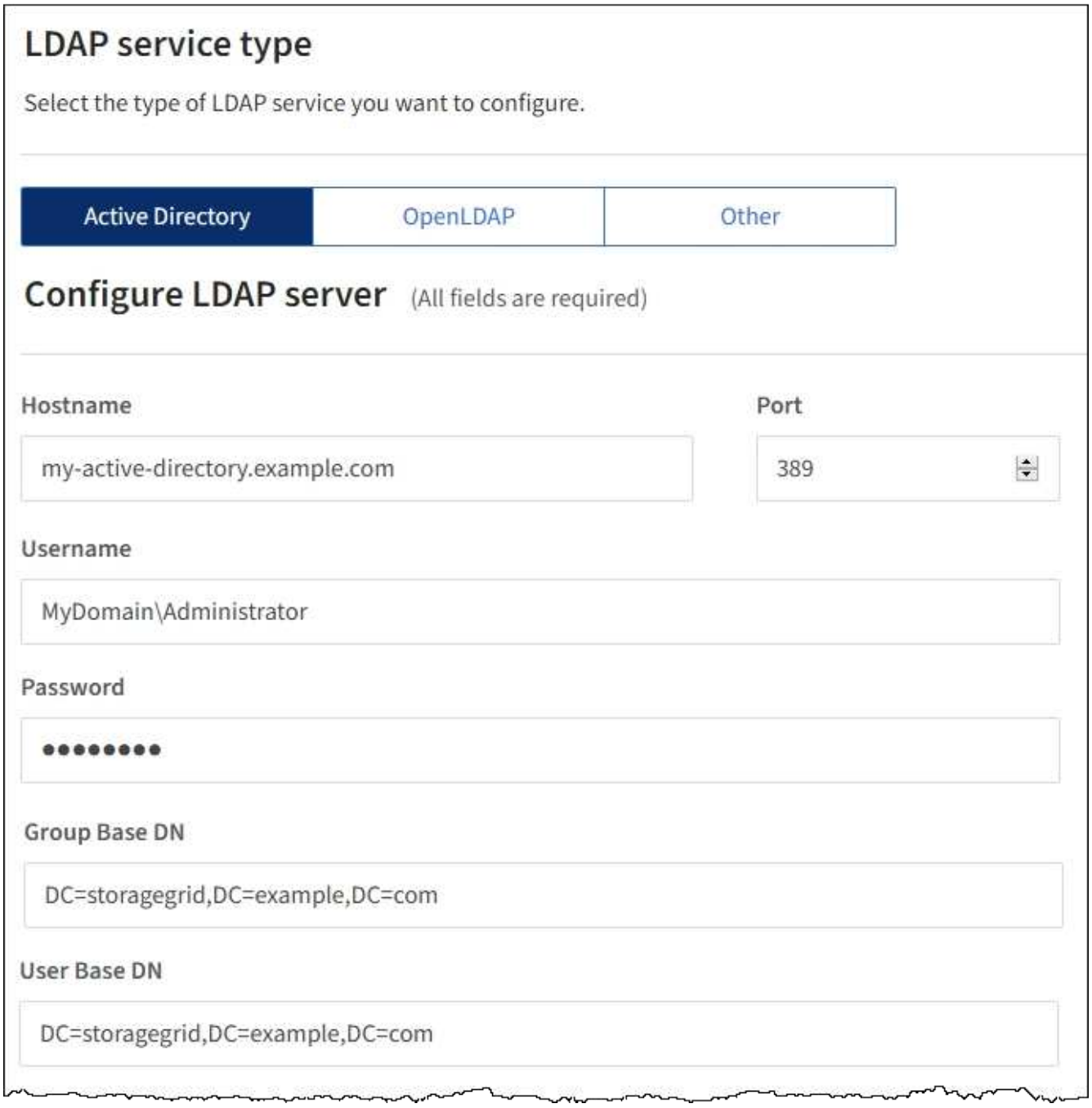
Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

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.

Informações sobre direitos autorais

Informações sobre marcas comerciais