



Configurando uma fonte de identidade federada

StorageGRID

NetApp
March 10, 2025

Índice

Configurando uma fonte de identidade federada	1
Diretrizes para configurar um servidor OpenLDAP	4
Sobreposições de Memberof e refint	4
Indexação	4

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 **Active Directory**, **OpenLDAP** ou **Oracle Directory Server**.

O que você vai precisar

- Você deve estar conectado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve estar usando o **Active 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.



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.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na seção tipo de serviço LDAP, selecione **Active 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 **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 hífens são ignorados.

5. Na seção **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 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`
- **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 `active 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 `active 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 ativo Directory.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory OpenLDAP Other

Configure LDAP server (All fields are required)

Hostname	Port
<input type="text" value="my-active-directory.example.com"/>	<input type="text" value="389"/>
Username	
<input type="text" value="MyDomain\Administrator"/>	
Password	
<input type="password" value="••••••••"/>	
Group Base DN	
<input type="text" value="DC=storagegrid,DC=example,DC=com"/>	
User Base DN	
<input type="text" value="DC=storagegrid,DC=example,DC=com"/>	

Informações relacionadas

["Permissões de gerenciamento do locatário"](#)

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

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.