



Gerenciamento da autenticação

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

This PDF was generated from <https://docs.netapp.com/pt-br/oncommand-unified-manager-95/online-help/task-enabling-remote-authentication.html> on October 23, 2024. Always check docs.netapp.com for the latest.

Índice

Gerenciamento da autenticação	1
Ativar autenticação remota	1
Desativando grupos aninhados da autenticação remota	2
Configurando serviços de autenticação	3
Adicionando servidores de autenticação	4
Testando a configuração dos servidores de autenticação	6
Editando servidores de autenticação	6
Eliminar servidores de autenticação	7
Autenticação com active Directory ou OpenLDAP	7
Habilitando a autenticação SAML	8
Requisitos do provedor de identidade	9
Alterar o provedor de identidade usado para autenticação SAML	11
Desativando a autenticação SAML	11
Descrição das janelas de autenticação e caixas de diálogo	12

Gerenciamento da autenticação

Você pode ativar a autenticação usando LDAP ou ative Directory no servidor do Unified Manager e configurá-la para funcionar com seus servidores para autenticar usuários remotos.

Além disso, você pode ativar a autenticação SAML para que os usuários remotos sejam autenticados por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager.

Ativar autenticação remota

Você pode habilitar a autenticação remota para que o servidor do Unified Manager possa se comunicar com seus servidores de autenticação. Os usuários do servidor de autenticação podem acessar a interface gráfica do Unified Manager para gerenciar objetos e dados de storage.

Antes de começar

Tem de ter a função de Administrador do OnCommand.



O servidor do Unified Manager deve estar conectado diretamente ao servidor de autenticação. Você deve desativar quaisquer clientes LDAP locais, como SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Sobre esta tarefa

Você pode ativar a autenticação remota usando LDAP aberto ou ative Directory. Se a autenticação remota estiver desativada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada por LDAP e LDAPS (Secure LDAP). O Unified Manager usa o 389 como a porta padrão para comunicação não segura e o 636 como a porta padrão para comunicação segura.



O certificado usado para autenticar usuários deve estar em conformidade com o formato X.509.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, selecione **Ativar autenticação remota**.
3. No campo **Authentication Service** (Serviço de autenticação), selecione o tipo de serviço e configure o serviço de autenticação.

Para tipo de autenticação...	Digite as seguintes informações...
Ative Directory	• Nome do administrador do servidor de autenticação em um dos seguintes formatos: ◦ domainname**username ◦ username@domainname ◦ Bind Distinguished Name (Usando a notação LDAP apropriada) • Senha do administrador • Nome diferenciado base (usando a notação LDAP apropriada)
Abra o LDAP	• Vincular nome distinto (na notação LDAP apropriada) • Vincular senha • Nome diferenciado da base

Se a autenticação de um usuário do active Directory demorar muito tempo ou tempo limite, o servidor de autenticação provavelmente levará muito tempo para responder. Desativar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação.

Se você selecionar a opção usar conexão segura para o servidor de autenticação, o Unified Manager se comunicará com o servidor de autenticação usando o protocolo SSL (Secure Sockets Layer).

4. Adicione servidores de autenticação e teste a autenticação.
5. Clique em **Salvar e fechar**.

Desativando grupos aninhados da autenticação remota

Se a autenticação remota estiver ativada, você poderá desativar a autenticação de grupo aninhado para que somente usuários individuais, e não membros de grupo, possam se autenticar remotamente no Unified Manager. Você pode desativar grupos aninhados quando quiser melhorar o tempo de resposta de autenticação do active Directory.

Antes de começar

- Tem de ter a função de Administrador do OnCommand.
- A desativação de grupos aninhados só é aplicável ao usar o active Directory.

Sobre esta tarefa

Desativar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desativado e se um grupo remoto for adicionado ao Unified Manager, os usuários individuais deverão ser membros do grupo remoto para se autenticar no Unified Manager.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, marque a caixa **Desativar pesquisa de grupo aninhado**.
3. Clique em **Salvar**.

Configurando serviços de autenticação

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de fornecer acesso ao Unified Manager. Você pode autenticar usuários usando serviços de autenticação predefinidos (como Active Directory ou OpenLDAP) ou configurando seu próprio mecanismo de autenticação.

Antes de começar

- Tem de ter ativado a autenticação remota.
- Tem de ter a função de Administrador do OnCommand.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página de opções **Setup**, clique em **Management Server > Authentication** (servidor de gestão).
3. Selecione um dos seguintes serviços de autenticação:

Se selecionar...	Então faça isso...
Active Directory	a. Introduza o nome e a palavra-passe do administrador. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base é <code>cn=ou,dc=domain,dc=com</code>.
OpenLDAP	a. Introduza o nome distinto de ligação e a palavra-passe de ligação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base é <code>cn=ou,dc=domain,dc=com</code>.

Se selecionar...	Então faça isso...
Outros	a. Introduza o nome distinto de ligação e a palavra-passe de ligação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for <code>ou@domain.com</code>, o nome distinto base é <code>cn=ou,dc=domain,dc=com</code>. c. Especifique a versão do protocolo LDAP suportada pelo servidor de autenticação. d. Introduza o nome de utilizador, a associação ao grupo, o grupo de utilizadores e os atributos de membro.



Se você quiser modificar o serviço de autenticação, você deve excluir quaisquer servidores de autenticação existentes e adicionar novos servidores de autenticação.

4. Clique em **Salvar e fechar**.

Adicionando servidores de autenticação

Você pode adicionar servidores de autenticação e ativar a autenticação remota no servidor de gerenciamento para que os usuários remotos no servidor de autenticação possam acessar o Unified Manager.

Antes de começar

- As seguintes informações devem estar disponíveis:
 - Nome do host ou endereço IP do servidor de autenticação
 - Número da porta do servidor de autenticação
- Você deve ter habilitado a autenticação remota e configurado o serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários remotos ou grupos no servidor de autenticação.
- Tem de ter a função de Administrador do OnCommand.

Sobre esta tarefa

Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (HA) (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação de parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação está inacessível.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.

2. Na página **Configuração/Autenticação**, clique em **servidor de gerenciamento > Autenticação**.
3. Ative ou desative a opção **Use secure Connection Authentication**:

Se você quiser...	Então faça isso...
Ative-o.	a. Na caixa de verificação Ativar autenticação remota, selecione a opção utilizar ligação segura. b. Na área servidores de autenticação, clique em Adicionar. c. Na caixa de diálogo Adicionar servidor de autenticação, insira o nome de autenticação ou o endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo autorizar host, clique em Exibir certificado. e. Na caixa de diálogo Exibir certificado, verifique as informações do certificado e clique em Fechar. f. Na caixa de diálogo autorizar Host, clique em Yes.  Quando você ativa a opção Use Secure Connection Authentication, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa o 636 como porta padrão para comunicação segura e o número de porta 389 para comunicação não segura.
Desative-o.	a. Na caixa de verificação Ativar autenticação remota, desmarque a opção usar conexão segura. b. Na área servidores de autenticação, clique em Adicionar. c. Na caixa de diálogo Adicionar servidor de autenticação, especifique o nome do host ou o endereço IP (IPv4 ou IPv6) do servidor e os detalhes da porta. d. Clique em Add.

O servidor de autenticação adicionado é exibido na área servidores.

4. Execute uma autenticação de teste para confirmar que é possível autenticar usuários no servidor de autenticação que você adicionou.

Testando a configuração dos servidores de autenticação

Você pode validar a configuração de seus servidores de autenticação para garantir que o servidor de gerenciamento seja capaz de se comunicar com eles. É possível validar a configuração pesquisando um usuário remoto ou grupo remoto de seus servidores de autenticação e autenticando-os usando as configurações configuradas.

Antes de começar

- Você deve ter habilitado a autenticação remota e configurado o serviço de autenticação para que o servidor do Unified Manager possa autenticar o usuário remoto ou o grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa pesquisar o usuário remoto ou grupo remoto desses servidores e autenticá-los.
- Tem de ter a função de Administrador do OnCommand.

Sobre esta tarefa

Se o serviço de autenticação estiver definido como ativo Directory e se você estiver validando a autenticação de usuários remotos que pertencem ao grupo principal do servidor de autenticação, as informações sobre o grupo principal não serão exibidas nos resultados de autenticação.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, clique em **Autenticação de teste**.
3. Na caixa de diálogo **Test User**, especifique o nome de usuário e a senha do usuário remoto ou o nome de usuário do grupo remoto e clique em **Test**.

Se estiver a autenticar um grupo remoto, não deve introduzir a palavra-passe.

Editando servidores de autenticação

Você pode alterar a porta que o servidor do Unified Manager usa para se comunicar com o servidor de autenticação.

Antes de começar

Tem de ter a função de Administrador do OnCommand.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, marque a caixa **Desativar pesquisa de grupo aninhado**.
3. Na área **servidores de autenticação**, selecione o servidor de autenticação que deseja editar e clique em **Editar**.

4. Na caixa de diálogo **Editar servidor de autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

Eliminar servidores de autenticação

Você pode excluir um servidor de autenticação se quiser impedir que o servidor do Unified Manager se comunique com o servidor de autenticação. Por exemplo, se pretender alterar um servidor de autenticação com o qual o servidor de gestão está a comunicar, pode eliminar o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Tem de ter a função de Administrador do OnCommand.

Sobre esta tarefa

Quando você exclui um servidor de autenticação, usuários remotos ou grupos do servidor de autenticação não poderão mais acessar o Unified Manager.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, selecione um ou mais servidores de autenticação que deseja excluir e clique em **Excluir**.
3. Clique em **Yes** para confirmar a solicitação de exclusão.

Se a opção **usar conexão segura** estiver ativada, os certificados associados ao servidor de autenticação serão excluídos juntamente com o servidor de autenticação.

Autenticação com active Directory ou OpenLDAP

Você pode ativar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento para se comunicar com seus servidores de autenticação para que os usuários dentro dos servidores de autenticação possam acessar você pode habilitar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento para se comunicar com seus servidores de autenticação para que os usuários dentro dos servidores de autenticação possam acessar o Unified Manager.

Você pode usar um dos seguintes serviços de autenticação predefinidos ou especificar seu próprio serviço de autenticação:

- Microsoft active Directory



Você não pode usar o Microsoft Lightweight Directory Services.

- OpenLDAP

Você pode selecionar o serviço de autenticação necessário e adicionar os servidores de autenticação apropriados para permitir que os usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais para usuários remotos ou grupos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o LDAP (Lightweight Directory Access Protocol) para autenticar usuários remotos no servidor de autenticação configurado.

Para usuários locais criados no Unified Manager, o servidor de gerenciamento mantém seu próprio banco de dados de nomes de usuário e senhas. O servidor de gerenciamento executa a autenticação e não usa o ativo Directory ou o OpenLDAP para autenticação.

Habilitando a autenticação SAML

Você pode ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

Antes de começar

- Você deve ter configurado a autenticação remota e verificado se ela foi bem-sucedida.
- Você deve ter criado pelo menos um Usuário remoto ou um Grupo remoto com a função Administrador do OnCommand.
- O provedor de identidade (IDP) deve ser suportado pelo Unified Manager e deve ser configurado.
- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao servidor IDP.

Sobre esta tarefa

Depois de ativar a autenticação SAML do Unified Manager, os usuários não poderão acessar a interface gráfica do usuário até que o IDP tenha sido configurado com as informações do host do servidor Unified Manager. Portanto, você deve estar preparado para concluir ambas as partes da conexão antes de iniciar o processo de configuração. O IDP pode ser configurado antes ou depois da configuração do Unified Manager.

Somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager após a autenticação SAML ser ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa configuração não afeta os usuários que acessam o console de manutenção, os comandos do Unified Manager ou ZAPIs.



O Unified Manager é reiniciado automaticamente após concluir a configuração SAML nesta página.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, selecione a guia **Autenticação SAML**.
3. Marque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML*).

São apresentados os campos necessários para configurar a ligação IDP.

4. Insira o URI de IDP e os metadados de IDP necessários para conectar o servidor do Unified Manager ao servidor de IDP.

Se o servidor IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URI IDP para preencher o campo metadados IDP automaticamente.

5. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.

Neste momento, você pode configurar o servidor IDP com essas informações.

6. Clique em **Salvar**.

Uma caixa de mensagem é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

7. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

Resultados

Da próxima vez que os usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do IDP em vez da página de login do Unified Manager.

Depois de terminar

Se ainda não estiver concluído, acesse seu IDP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.



Ao usar o ADFS como provedor de identidade, a GUI do Unified Manager não honra o tempo limite do ADFS e continuará funcionando até que o tempo limite da sessão do Unified Manager seja atingido. Quando o Unified Manager é implantado no Windows, Red Hat ou CentOS, é possível alterar o tempo limite da sessão da GUI usando o seguinte comando da CLI do Unified Manager: `option set absolute.session.timeout=00:15:00` Este comando define o tempo limite da sessão da GUI do Unified Manager para 15 minutos.

Requisitos do provedor de identidade

Ao configurar o Unified Manager para usar um provedor de identidade (IDP) para executar a autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações necessárias para que a conexão com o Unified Manager seja bem-sucedida.

É necessário inserir o URI e os metadados do Unified Manager no servidor IDP. Você pode copiar essas informações da página Autenticação do Unified Manager SAML. O Unified Manager é considerado o provedor de serviços (SP) no padrão SAML (Security Assertion Markup Language).

Padrões de criptografia suportados

- AES (Advanced Encryption Standard): AES-128 e AES-256

- Algoritmo Hash seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- Shibboleth
- Serviços de Federação do Active Directory (ADFS)

Requisitos de configuração ADFS

- Você deve definir três regras de reivindicação na ordem a seguir, necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.

Regra de reclamação	Valor
Nome da conta SAM	ID do nome
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nome não qualificado	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como ""Autenticação de formulários"" ou os usuários podem receber um erro ao fazer logout do Unified Manager ao usar o Internet Explorer. Siga estes passos:
 - a. Abra o Console de Gerenciamento ADFS.
 - b. Clique na pasta Authentication Policies (políticas de autenticação) no modo de exibição de árvore à esquerda.
 - c. Em ações à direita, clique em Editar política de autenticação primária global.
 - d. Defina o método de autenticação da Intranet como ""Autenticação de formulários"" em vez da "Autenticação do Windows" padrão.
- Em alguns casos, o login pelo IDP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Existem duas soluções alternativas para resolver este problema:
 - Siga as instruções identificadas no link para desativar a verificação de revogação no servidor ADFS para a entidade dependente associada a cert AC encadeada:
<http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/>
 - Peça que o servidor da CA resida no servidor ADFS para assinar a solicitação de cert do servidor do Unified Manager.

Outros requisitos de configuração

- O desvio do relógio do Unified Manager é definido para 5 minutos, portanto, a diferença de tempo entre o servidor IDP e o servidor do Unified Manager não pode ser superior a 5 minutos ou a autenticação falhará.
- Quando os usuários tentam acessar o Unified Manager usando o Internet Explorer, eles podem ver a mensagem **o site não pode exibir a página**. Se isso ocorrer, certifique-se de que esses usuários desmarque a opção "Mostrar mensagens de erro HTTP amigáveis" em **Ferramentas > Opções da Internet > Avançado**.

Alterar o provedor de identidade usado para autenticação SAML

Você pode alterar o provedor de identidade (IDP) que o Unified Manager usa para autenticar usuários remotos.

Antes de começar

- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao IDP.

Sobre esta tarefa

O novo IDP pode ser configurado antes ou depois da configuração do Unified Manager.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, selecione a guia **Autenticação SAML**.
3. Insira o novo URI de IDP e os metadados de IDP necessários para conectar o servidor do Unified Manager ao IDP.

Se o IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URL IDP para preencher o campo metadados IDP automaticamente.

4. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
5. Clique em **Save Configuration** (Guardar configuração).

É apresentada uma caixa de mensagem para confirmar que pretende alterar a configuração.

6. Clique em **OK**.

Depois de terminar

Acesse o novo IDP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.

Da próxima vez que os usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na nova página de login do IDP em vez da antiga página de login do IDP.

Desativando a autenticação SAML

Você pode desativar a autenticação SAML quando quiser parar de autenticar usuários remotos por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ativo Directory ou LDAP, executam a autenticação de login.

Sobre esta tarefa

Depois de desativar a autenticação SAML, os utilizadores locais e os utilizadores de manutenção poderão aceder à interface gráfica do utilizador, além dos utilizadores remotos configurados.

Você também pode desativar a autenticação SAML usando o console de manutenção do Unified Manager se não tiver acesso à interface gráfica do usuário.



O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desativada.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, selecione a guia **Autenticação SAML**.
3. Desmarque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML *).
4. Clique em **Salvar**.

Uma caixa de mensagem é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

5. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

Resultados

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IDP.

Depois de terminar

Acesse seu IDP e exclua o URI e os metadados do servidor do Unified Manager.

Descrição das janelas de autenticação e caixas de diálogo

Pode ativar a autenticação LDAP a partir da página Configuração/Autenticação.

Página Configuração/Autenticação

Você pode usar a página Configuração/Autenticação para configurar o Unified Manager para autenticar usuários remotos que tentam fazer login na IU da Web do Unified Manager.

Usando a página Autenticação remota, você pode configurar o Unified Manager para se comunicar com o servidor de autenticação para autenticar usuários remotos.

Usando a página Autenticação SAML, você pode configurar o Unified Manager para se comunicar com um provedor de identidade seguro (IDP) para autenticar usuários remotos.

Página Autenticação remota

Você pode usar a página Autenticação remota para configurar o Unified Manager para se comunicar com o servidor de autenticação para autenticar usuários remotos que tentam fazer login na IU da Web do Unified Manager.

Você deve ter a função Administrador do OnCommand ou Administrador do armazenamento.

Depois de selecionar a caixa de verificação Ativar autenticação remota, pode ativar a autenticação remota utilizando um servidor de autenticação.

- **Serviço de autenticação**

Permite configurar o servidor de gerenciamento para autenticar usuários em provedores de serviços de diretório, como Active Directory, OpenLDAP ou especificar seu próprio mecanismo de autenticação. Você só pode especificar um serviço de autenticação se tiver habilitado a autenticação remota.

- **Active Directory**

- Nome do administrador

Especifica o nome de administrador do servidor de autenticação.

- Palavra-passe

Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for [ou@domain.com](#), o nome distinto base é `cn=ou,dc=domain,dc=com`.

- Desative a Pesquisa de grupos aninhados

Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o Active Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Utilize a ligação segura

Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.

- **OpenLDAP**

- Vincular Nome distinto

Especifica o nome distinto do bind que é usado juntamente com o nome distinto base para encontrar usuários remotos no servidor de autenticação.

- Vincular senha

Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for [ou@domain.com](#), o nome distinto base é `cn=ou,dc=domain,dc=com`.

- Utilize a ligação segura

Especifica que o LDAP seguro é usado para se comunicar com servidores de autenticação LDAPS.

- **Outros**

- Vincular Nome distinto

Especifica o nome distinto do bind que é usado juntamente com o nome distinto base para encontrar usuários remotos no servidor de autenticação que você configurou.

- Vincular senha

Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for [ou@domain.com](#), o nome distinto base é `cn=ou,dc=domain,dc=com`.

- Versão do protocolo

Especifica a versão LDAP (Lightweight Directory Access Protocol) suportada pelo servidor de autenticação. Pode especificar se a versão do protocolo tem de ser detetada automaticamente ou definir a versão para 2 ou 3.

- Atributo Nome Utilizador

Especifica o nome do atributo no servidor de autenticação que contém nomes de login de usuário a serem autenticados pelo servidor de gerenciamento.

- Atributo de associação de grupo

Especifica um valor que atribui a associação do grupo do servidor de gerenciamento a usuários remotos com base em um atributo e valor especificado no servidor de autenticação do usuário.

- UGID

Se os usuários remotos forem incluídos como membros de um objeto `GroupOfUniqueNames` no servidor de autenticação, essa opção permitirá que você atribua a associação do grupo de servidores de gerenciamento aos usuários remotos com base em um atributo especificado nesse objeto `GroupOfUniqueNames`.

- Desative a Pesquisa de grupos aninhados

Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o `Active Directory`, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Membro

Especifica o nome do atributo que o servidor de autenticação usa para armazenar informações sobre os membros individuais de um grupo.

- **Classe Objeto Utilizador**

Especifica a classe de objeto de um usuário no servidor de autenticação remota.

- **Classe Objeto Grupo**

Especifica a classe de objeto de todos os grupos no servidor de autenticação remota.

- **Utilize a ligação segura**

Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.



Se pretender modificar o serviço de autenticação, certifique-se de que elimina quaisquer servidores de autenticação existentes e adiciona novos servidores de autenticação.

Área servidores de autenticação

A área servidores de autenticação exibe os servidores de autenticação com os quais o servidor de gerenciamento se comunica para localizar e autenticar usuários remotos. As credenciais para usuários remotos ou grupos são mantidas pelo servidor de autenticação.

- **Botões de comando**

Permite adicionar, editar ou excluir servidores de autenticação.

- **Adicionar**

Permite adicionar um servidor de autenticação.

Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação do parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação está inacessível.

- **Editar**

Permite editar as definições de um servidor de autenticação selecionado.

- **Eliminar**

Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

Exibe o nome do host ou o endereço IP do servidor de autenticação usado para autenticar o usuário no servidor de gerenciamento.

- **Porto**

Exibe o número da porta do servidor de autenticação.

- * Teste de Autenticação*

Este botão valida a configuração do servidor de autenticação autenticando um usuário ou grupo remoto.

Durante o teste, se você especificar apenas o nome de usuário, o servidor de gerenciamento pesquisará o usuário remoto no servidor de autenticação, mas não autenticará o usuário. Se especificar o nome de utilizador e a palavra-passe, o servidor de gestão procura e autentica o utilizador remoto.

Não é possível testar a autenticação se a autenticação remota estiver desativada.

Página Autenticação SAML

Você pode usar a página Autenticação SAML para configurar o Unified Manager para autenticar usuários remotos usando SAML por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager.

- Você deve ter a função Administrador do OnCommand para criar ou modificar a configuração SAML.
- Tem de ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou grupo remoto.

Depois que a autenticação remota e os usuários remotos tiverem sido configurados, você poderá selecionar a caixa de seleção Habilitar autenticação SAML para habilitar a autenticação usando um provedor de identidade seguro.

- * IDP URI*

O URI para acessar o IDP a partir do servidor do Unified Manager. Exemplos de URIs estão listados abaixo.

Exemplo de URI de ADFS:

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Exemplo de Shibboleth URI:

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **Metadados IDP**

Os metadados IDP em formato XML.

Se o URL de IDP estiver acessível a partir do servidor do Unified Manager, você pode clicar no botão **obter metadados de IDP** para preencher este campo.

- **Sistema anfitrião (FQDN)**

O FQDN do sistema host do Unified Manager, conforme definido durante a instalação. Você pode alterar esse valor, se necessário.

- * Host URI*

O URI para acessar o sistema host do Unified Manager a partir do IDP.

- **Metadados do host**

Os metadados do sistema anfitrião em formato XML.

Informações sobre direitos autorais

Copyright © 2024 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 SOBRESSAIENTES; 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 DOCUMENTOS, 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.