



Use os serviços de diretório

SANtricity software

NetApp
March 17, 2026

Índice

- Use os serviços de diretório 1
 - Adicionar servidor de diretório em SANtricity Unified Manager 1
 - Edite as configurações do servidor de diretório e os mapeamentos de funções em SANtricity Unified Manager 6
 - Remover servidor de diretório 10

Use os serviços de diretório

Adicionar servidor de diretório em SANtricity Unified Manager

Para configurar autenticação para o Access Management, você estabelece a comunicação entre um servidor LDAP e o host que executa o Web Services Proxy para SANtricity Unified Manager. Em seguida, você mapeia os grupos de usuários LDAP para as funções de usuário locais.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Os grupos de usuários devem ser definidos no seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta de vinculação.
- Para servidores LDAPS que utilizam um protocolo seguro, a cadeia de certificados do servidor LDAP deve estar instalada em sua máquina local.

Sobre esta tarefa

Adicionar um servidor de diretório é um processo de duas etapas. Primeiro você insere o nome de domínio e o URL. Se o seu servidor usa um protocolo seguro, você também deve carregar um certificado de CA para autenticação se ele for assinado por uma autoridade de assinatura não padrão. Se você tiver credenciais para uma conta de bind, também pode inserir o nome de usuário e a senha da sua conta. Em seguida, você mapeia os grupos de usuários do servidor LDAP para as funções de usuário locais.


Passos

1. Selecione **Access Management**.
2. Na guia **Directory Services**, selecione **Add Directory Server**.

A caixa de diálogo Adicionar Servidor de Diretório é aberta.

3. Na guia **Configurações do Servidor**, insira as credenciais do servidor LDAP.

Detalhes do campo

Configuração	Descrição
Configurações de configuração	Domínio(s)
Insira o nome de domínio do servidor LDAP. Para vários domínios, insira os nomes de domínio em uma lista separada por vírgulas. O nome de domínio é usado no login (<i>username@domain</i>) para especificar em qual servidor de diretório autenticar.	URL do servidor
Insira a URL para acessar o servidor LDAP no formato <code>ldap[s]://host:port*</code> .	Fazer upload do certificado (opcional)
<div data-bbox="245 1287 302 1341"></div> <p>Este campo aparece somente se um protocolo LDAPS for especificado no campo Server URL acima.</p> <p>Clique em Procurar e selecione um certificado de CA para carregar. Este é o certificado confiável ou cadeia de certificados usado para autenticação do servidor LDAP.</p>	Vincular conta (opcional)

Configuração	Descrição
<p>Insira uma conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisas dentro dos grupos. Insira o nome da conta em um formato do tipo LDAP. Por exemplo, se o usuário de vinculação for chamado "bindacct", então você pode inserir um valor como CN=bindacct,CN=Users,DC=cpoc,DC=local.</p>	<p>Senha de bind (opcional)</p>
<div data-bbox="245 915 302 968" data-label="Image"> </div> <p data-bbox="358 772 472 1108">Este campo aparece quando você insere uma conta de associação.</p> <p data-bbox="212 1157 480 1220">Digite a senha para a conta de bind.</p>	<p>Testar a conexão do servidor antes de adicionar</p>

Configuração	Descrição
<p>Selecione esta caixa de seleção se quiser garantir que o sistema possa se comunicar com a configuração do servidor LDAP que você inseriu. O teste ocorre depois que você clica em Adicionar na parte inferior da caixa de diálogo.</p> <p>Se esta caixa de seleção estiver marcada e o teste falhar, a configuração não será adicionada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e adicionar a configuração.</p>	<p>Configurações de privilégios</p>
<p>DN base de pesquisa</p>	<p>Insira o contexto LDAP para pesquisar usuários, normalmente no formato de <code>CN=Users, DC=cpoc, DC=local</code>.</p>
<p>Atributo de nome de usuário</p>	<p>Insira o atributo que está vinculado ao ID do usuário para autenticação. Por exemplo: <code>sAMAccountName</code>.</p>
<p>Atributo(s) do grupo</p>	<p>Insira uma lista de atributos de grupo do usuário, que é usada para o mapeamento de grupo para função. Por exemplo: <code>memberOf, managedObjects</code>.</p>

4. Clique na guia **Mapeamento de funções**.
5. Atribua grupos LDAP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Nome diferenciado do grupo
Especifique o nome diferenciado (DN) do grupo para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+ -=!/?^\$	
Funções	<p>Clique no campo e selecione uma das funções de usuário local a serem mapeadas para o DN do grupo. Você deve selecionar individualmente cada função que deseja incluir para este grupo. A função Monitor é necessária em combinação com as outras funções para fazer login no SANtricity Unified Manager. As funções mapeadas incluem as seguintes permissões:</p> <ul style="list-style-type: none">• Administrador de armazenamento — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança.• Administrador de segurança — Acesso à configuração de segurança em Access Management e Certificate Management.• Administrador de suporte — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança.• Monitor — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.



A função Monitor é obrigatória para todos os usuários, incluindo o administrador.

6. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
7. Quando terminar com os mapeamentos, clique em **Adicionar**.

O sistema realiza uma validação, garantindo que o array de storage e o servidor LDAP possam se comunicar. Se uma mensagem de erro aparecer, verifique as credenciais inseridas na caixa de diálogo e

insira as informações novamente, se necessário.

Edite as configurações do servidor de diretório e os mapeamentos de funções em SANtricity Unified Manager

Se você já configurou um servidor de diretório no Access Management, pode alterar suas configurações a qualquer momento. As configurações incluem as informações de conexão do servidor e os mapeamentos de grupo para função.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- É necessário definir um servidor de diretório.

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Directory Services**.
3. Se mais de um servidor estiver definido, selecione o servidor que você deseja editar na tabela.
4. Selecione **Visualizar/Editar Settings**.

A caixa de diálogo Configurações do Servidor de Diretório é aberta.

5. Na guia **Server Settings**, altere as configurações desejadas.

Detalhes do campo

Configuração	Descrição
Configurações de configuração	Domínio(s)
O(s) nome(s) de domínio do(s) servidor(es) LDAP. Para múltiplos domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (<i>username@domain</i>) para especificar em qual servidor de diretório autenticar.	URL do servidor
A URL para acessar o servidor LDAP no formato de <code>ldap[s]://host:port</code> .	Vincular conta (opcional)
A conta de usuário somente leitura para consultas de pesquisa contra o servidor LDAP e para pesquisas dentro dos grupos.	Senha de bind (opcional)
A senha da conta de bind. (Este campo aparece quando uma conta de bind é inserida.)	Teste a conexão com o servidor antes de salvar

Configuração	Descrição
Verifica se o sistema pode se comunicar com a configuração do servidor LDAP. O teste ocorre após você clicar em Salvar . Se esta caixa de seleção estiver marcada e o teste falhar, a configuração não será alterada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e reeditar a configuração.	Configurações de privilégios
DN base de pesquisa	O contexto LDAP para pesquisar usuários, normalmente no formato de CN=Users, DC=cpoc, DC=local.
Atributo de nome de usuário	O atributo que está vinculado ao ID do usuário para autenticação. Por exemplo: sAMAccountName.
Atributo(s) do grupo	Uma lista de atributos de grupo do usuário, usada para mapeamento de grupo para função. Por exemplo: memberOf, managedObjects.

6. Na aba **Mapeamento de funções**, altere o mapeamento desejado.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Nome diferenciado do grupo
<p>O nome de domínio para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular:</p> <pre>\.[]{}()<>*+.=!?^\$</pre>	
Funções	<p>As funções a serem mapeadas para o DN do Grupo. Você deve selecionar individualmente cada função que deseja incluir neste grupo. A função Monitor é necessária em combinação com as outras funções para fazer login no SANtricity Unified Manager. As funções incluem o seguinte:</p> <ul style="list-style-type: none">• Administrador de armazenamento — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança.• Administrador de segurança — Acesso à configuração de segurança em Access Management e Certificate Management.• Administrador de suporte — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança.• Monitor — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.



A função Monitor é obrigatória para todos os usuários, incluindo o administrador.

7. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
8. Clique em **Salvar**.

Resultados

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Remover servidor de diretório

Para interromper a conexão entre um servidor de diretório e o Web Services Proxy, você pode remover as informações do servidor na página Access Management. Você pode querer realizar esta tarefa se tiver configurado um novo servidor e, em seguida, quiser remover o antigo.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Directory Services**.
3. Na lista, selecione o servidor de diretório que você deseja excluir.
4. Clique em **Remover**.

A caixa de diálogo Remove Directory Server é aberta.

5. Digite `remove` no campo e clique em **Remover**.

As configurações do servidor de diretório, as configurações de privilégios e os mapeamentos de funções são removidos. Os usuários não podem mais fazer login com credenciais deste servidor.

Informações sobre direitos autorais

Copyright © 2026 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.