



Utilize LDAP

ONTAP 9

NetApp
January 17, 2025

Índice

- Utilize LDAP 1
 - Visão geral do uso do LDAP 1
 - Crie um novo esquema de cliente LDAP 2
 - Crie uma configuração de cliente LDAP 3
 - Associe a configuração do cliente LDAP a SVMs 7
 - Verifique as fontes LDAP na tabela do switch do serviço de nomes 8

Utilize LDAP

Visão geral do uso do LDAP

Se o LDAP for usado no ambiente para serviços de nomes, você precisará trabalhar com o administrador LDAP para determinar os requisitos e as configurações do sistema de storage apropriadas e, em seguida, ativar o SVM como cliente LDAP.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores de nomes, use o `-try-channel-binding` parâmetro com o `ldap client modify` comando.

Para obter mais informações, "[2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows](#)" consulte .

- Antes de configurar o LDAP para ONTAP, você deve verificar se a implantação do site atende às práticas recomendadas para configuração do servidor LDAP e do cliente. Em especial, devem ser satisfeitas as seguintes condições:
 - O nome de domínio do servidor LDAP deve corresponder à entrada no cliente LDAP.
 - Os tipos de hash de senha do usuário LDAP suportados pelo servidor LDAP devem incluir aqueles suportados pelo ONTAP:
 - CRYPT (todos os tipos) e SHA-1 (SHA, SSHA).
 - A partir do ONTAP 9.8, hashes SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 e SSHA-512) também são suportados.
 - Se o servidor LDAP exigir medidas de segurança de sessão, você deve configurá-las no cliente LDAP.

As seguintes opções de segurança de sessão estão disponíveis:

- Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
- INICIE O TLS
- LDAPS (LDAP sobre TLS ou SSL)
- Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
 - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
 - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
 - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
- Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
 - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
 - Se o LDAPS for usado, o servidor LDAP deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
 - Um servidor de certificados já deve estar configurado no domínio.

- Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
 - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
 - Bidirecional
 - One-way, onde o primário confia no domínio de referência
 - Pai-filho
 - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
 - As senhas de domínio devem ser as mesmas para autenticar quando `--bind-as-cifs-server` definido como `true`.

As configurações a seguir não são suportadas com a busca por referência LDAP.



- Para todas as versões do ONTAP:
 - Clientes LDAP em um SVM admin
- Para o ONTAP 9.8 e versões anteriores (eles são suportados em 9.9.1 e posteriores):
 - Assinatura e selagem LDAP (a `-session-security` opção)
 - Conexões TLS criptografadas (a `-use-start-tls` opção)
 - Comunicações através da porta LDAPS 636 (a `-use-ldaps-for-ad-ldap` opção)

- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

Na maioria dos casos, um dos esquemas ONTAP padrão será apropriado. No entanto, se o esquema LDAP em seu ambiente for diferente desses, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar o cliente LDAP. Consulte o administrador LDAP sobre os requisitos para o seu ambiente.

- O uso do LDAP para resolução de nome de host não é suportado.

Para mais informações

- ["Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"](#)
- ["Instale o certificado de CA raiz autoassinado no SVM"](#)

Crie um novo esquema de cliente LDAP

Se o esquema LDAP no ambiente for diferente dos padrões do ONTAP, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar a configuração do cliente LDAP.

Sobre esta tarefa

A maioria dos servidores LDAP pode usar os esquemas padrão fornecidos pelo ONTAP:

- MS-AD-BIS (o esquema preferido para a maioria dos servidores AD do Windows 2012 e posteriores)
- Ad-IDMU (Windows 2008, Windows 2012 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)

- RFC-2307 (SERVIDORES LDAP UNIX)

Se você precisar usar um esquema LDAP não padrão, você deve criá-lo antes de criar a configuração do cliente LDAP. Consulte o administrador LDAP antes de criar um novo esquema.

Os esquemas LDAP padrão fornecidos pelo ONTAP não podem ser modificados. Para criar um novo esquema, você cria uma cópia e modifica a cópia de acordo.

Passos

1. Exiba os modelos de esquema de cliente LDAP existentes para identificar o que deseja copiar:

```
vserver services name-service ldap client schema show
```

2. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

3. Faça uma cópia de um esquema cliente LDAP existente:

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modifique o novo esquema e personalize-o para o seu ambiente:

```
vserver services name-service ldap client schema modify
```

5. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Crie uma configuração de cliente LDAP

Se você quiser que o ONTAP acesse os serviços LDAP ou ative Directory externos em seu ambiente, primeiro é necessário configurar um cliente LDAP no sistema de armazenamento.

O que você vai precisar

Um dos três primeiros servidores na lista de domínios resolvidos do ative Directory deve estar ativo e fornecendo dados. Caso contrário, esta tarefa falha.



Existem vários servidores, dos quais mais de dois servidores estão inativos a qualquer momento.

Passos

1. Consulte o administrador LDAP para determinar os valores de configuração apropriados para o `vserver services name-service ldap client create` comando:

- a. Especifique uma conexão baseada em domínio ou baseada em endereço para servidores LDAP.

As `-ad-domain` opções e `-servers` são mutuamente exclusivas.

- Utilize a `-ad-domain` opção para ativar a detecção de servidor LDAP no domínio do ativo Directory.
 - Você pode usar a `-restrict-discovery-to-site` opção para restringir a descoberta de servidor LDAP ao site padrão CIFS para o domínio especificado. Se você usar essa opção, também precisará especificar o site padrão CIFS com `-default-site`.
- Você pode usar a `-preferred-ad-servers` opção para especificar um ou mais servidores preferenciais do ativo Directory por endereço IP em uma lista delimitada por vírgulas. Depois que o cliente é criado, você pode modificar esta lista usando o `vserver services name-service ldap client modify` comando.
- Use a `-servers` opção para especificar um ou mais servidores LDAP (ativo Directory ou UNIX) por endereço IP em uma lista delimitada por vírgulas.



A `-servers` opção está obsoleta no ONTAP 9.2. A partir de ONTAP 9.2, o `-ldap-servers` campo substitui o `-servers` campo. Este campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

b. Especifique um esquema LDAP padrão ou personalizado.

A maioria dos servidores LDAP pode usar os esquemas somente leitura padrão fornecidos pelo ONTAP. É melhor usar esses esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão (eles são somente leitura) e, em seguida, modificando a cópia.

Esquemas predefinidos:

- MS-AD-BIS

Baseado em RFC-2307bis, este é o esquema LDAP preferido para a maioria das implantações padrão do Windows 2012 e LDAP posteriores.

- AD-IDMU

Baseado no ativo Directory Identity Management para UNIX, esse esquema é apropriado para a maioria dos servidores Windows 2008, Windows 2012 e AD posteriores.

- AD-SFU

Baseado nos Serviços do ativo Directory para UNIX, esse esquema é apropriado para a maioria dos servidores do Windows 2003 e AD anteriores.

- RFC-2307

Baseado em RFC-2307 (*an Approach for using LDAP as Network Information Service*), este esquema é apropriado para a maioria dos servidores UNIX AD.

c. Selecione vincular valores.

- `-min-bind-level {anonymous|simple|sasl}` especifica o nível mínimo de autenticação bind.

O valor padrão é **anonymous**.

- `-bind-dn LDAP_DN` especifica o usuário de vinculação.

Para servidores do ative Directory, você deve especificar o usuário no formulário conta (DOMÍNIO/usuário) ou principal (`user@domain.com`). Caso contrário, você deve especificar o usuário em forma de nome distinto.

- `-bind-password password` especifica a senha de vinculação.

d. Selecione as opções de segurança da sessão, se necessário.

Pode ativar a assinatura e a selagem LDAP ou o LDAP através de TLS, se necessário pelo servidor LDAP.

- `--session-security {none|sign|seal}`

Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

Você também deve definir `-min-bind-level {sasl}`, a menos que você queira que a autenticação de vinculação retorne **anonymous** ou **simple** se a vinculação de assinatura e vedação falhar.

- `-use-start-tls {true|false}` Selecione

Se definido como **true** e o servidor LDAP o suportar, o cliente LDAP utiliza uma ligação TLS encriptada ao servidor. O valor padrão é **false**. Você deve instalar um certificado de CA raiz autoassinado do servidor LDAP para usar essa opção.



Se a VM de armazenamento tiver um servidor SMB adicionado a um domínio e o servidor LDAP for um dos controladores de domínio do domínio inicial do servidor SMB, poderá modificar a `-session-security-for-ad-ldap` opção utilizando o `vserver cifs security modify` comando.

e. Selecione valores de porta, consulta e base.

Os valores padrão são recomendados, mas você deve verificar com o administrador LDAP se eles são apropriados para o seu ambiente.

- `-port port` Especifica a porta do servidor LDAP.

O valor padrão é 389.

Se pretender utilizar Iniciar TLS para proteger a ligação LDAP, tem de utilizar a porta predefinida 389. Iniciar TLS começa como uma conexão de texto simples através da porta padrão LDAP 389, e essa conexão é então atualizada para TLS. Se você alterar a porta, Iniciar TLS falhará.

- `-query-timeout integer` especifica o tempo limite da consulta em segundos.

O intervalo permitido é de 1 a 10 segundos. O valor padrão é 3 segundos.

- `-base-dn LDAP_DN` Especifica o DN base.

Vários valores podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP

estiver ativada). O valor padrão é "" (root).

- `-base-scope {base|onelevel|`subtree`}` especifica o escopo de pesquisa base.

O valor padrão é `subtree`.

- `-referral-enabled {true|false}` Especifica se a busca por referência LDAP está ativada.

A partir do ONTAP 9.5, isso permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP for retornada pelo servidor LDAP primário indicando que os Registros desejados estão presentes nos servidores LDAP referidos. O valor padrão é **false**.

Para pesquisar Registros presentes nos servidores LDAP referidos, o base-DN dos Registros referidos deve ser adicionado ao base-DN como parte da configuração do cliente LDAP.

2. Crie uma configuração de cliente LDAP na VM de armazenamento:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



Você deve fornecer o nome da VM de armazenamento ao criar uma configuração de cliente LDAP.

3. Verifique se a configuração do cliente LDAP foi criada com sucesso:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Exemplos

O comando a seguir cria uma nova configuração de cliente LDAP chamada `ldap1` para que a VM de armazenamento `VS1` funcione com um servidor do Active Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada `ldap1` para que a VM de armazenamento `VS1` funcione com um servidor do Active Directory para LDAP no qual a assinatura e a vedação são necessárias, e a descoberta de servidor LDAP é restrita a um site específico para o domínio especificado:


```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do Active Directory para LDAP onde a busca por referência LDAP é necessária:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1 especificando o DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1, ativando a busca de referência:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

Associe a configuração do cliente LDAP a SVMs

Para ativar o LDAP em um SVM, você deve usar o `vserver services name-service ldap create` comando para associar uma configuração de cliente LDAP ao SVM.

O que você vai precisar

- Um domínio LDAP já deve existir na rede e deve estar acessível ao cluster no qual o SVM está localizado.
- Uma configuração de cliente LDAP deve existir no SVM.

Passos

1. Ative o LDAP no SVM:

```
vserver services name-service ldap create -vserver vserver_name -client-config client_config_name
```



A partir do ONTAP 9.2, o `vserver services name-service ldap create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em contato com o servidor de nomes.

O comando a seguir habilita o LDAP no "VS1"SVM e o configura para usar a configuração de cliente LDAP "ldap1":

```
cluster1::> vserver services name-service ldap create -vserver vs1  
-client-config ldap1 -client-enabled true
```

2. Valide o status dos servidores de nomes usando o comando de verificação ldap do serviço de nomes dos serviços vserver.

O comando a seguir valida servidores LDAP no SVM VS1.

```
cluster1::> vserver services name-service ldap check -vserver vs1  
  
| Vserver: vs1 |  
| Client Configuration Name: c1 |  
| LDAP Status: up |  
| LDAP Status Details: Successfully connected to LDAP server |  
| "10.11.12.13". |
```

O comando name Service check está disponível a partir de ONTAP 9.2.

Verifique as fontes LDAP na tabela do switch do serviço de nomes

Você deve verificar se as fontes LDAP para serviços de nome estão listadas corretamente na tabela de opções de serviço de nomes para o SVM.

Passos

1. Exibir o conteúdo da tabela de opções de serviço de nomes atual:

```
vserver services name-service ns-switch show -vserver svm_name
```

O comando a seguir mostra os resultados do SVM My_SVM:

```

ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM

```

Vserver	Database	Source
-----	-----	-----
My_SVM	hosts	files, dns
My_SVM	group	files,ldap
My_SVM	passwd	files,ldap
My_SVM	netgroup	files
My_SVM	namemap	files

5 entries were displayed.

namemap especifica as fontes para procurar informações de mapeamento de nomes e em que ordem. Em um ambiente somente UNIX, essa entrada não é necessária. O mapeamento de nomes só é necessário em um ambiente misto usando UNIX e Windows.

2. Atualize a ns-switch entrada conforme apropriado:

Se quiser atualizar a entrada ns-switch para...	Digite o comando...
Informações do utilizador	<code>vserver services name-service ns-switch modify -vserver <i>vserver_name</i> -database passwd -sources ldap,files</code>
Informações do grupo	<code>vserver services name-service ns-switch modify -vserver <i>vserver_name</i> -database group -sources ldap,files</code>
Informações do netgroup	<code>vserver services name-service ns-switch modify -vserver <i>vserver_name</i> -database netgroup -sources ldap,files</code>

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.