Configurar serviços de nomes

ONTAP 9

NetApp
January 17, 2025

Índice

Configurar serviços de nomes

Configure a visão geral dos serviços de nome

Dependendo da configuração do seu sistema de storage, o ONTAP precisa ser capaz de procurar informações de host, usuário, grupo ou netgroup para fornecer acesso adequado aos clientes. Você deve configurar serviços de nomes para permitir que o ONTAP acesse serviços de nomes locais ou externos para obter essas informações.

Você deve usar um serviço de nomes como NIS ou LDAP para facilitar pesquisas de nomes durante a autenticação do cliente. É melhor usar o LDAP sempre que possível para maior segurança, especialmente ao implantar o NFSv4 ou posterior. Você também deve configurar usuários e grupos locais caso os servidores de nomes externos não estejam disponíveis.

As informações do serviço de nomes devem ser mantidas sincronizadas em todas as fontes.

Configure a tabela do switch do serviço de nomes

Você deve configurar a tabela de switch de serviço de nomes corretamente para permitir que o ONTAP consulte serviços de nome locais ou externos para recuperar informações de mapeamento de host, usuário, grupo, netgroup ou nome.

O que você vai precisar

Você deve ter decidido quais serviços de nome deseja usar para o mapeamento de host, usuário, grupo, grupo de rede ou nome, conforme aplicável ao seu ambiente.

Se você planeja usar netgroups, todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

Sobre esta tarefa

Não inclua fontes de informação que não estejam a ser utilizadas. Por exemplo, se o NIS não estiver sendo usado em seu ambiente, não especifique a `-sources nis` opção.

Passos

1. Adicione as entradas necessárias à tabela do switch de serviço de nomes:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Verifique se a tabela do switch de serviço de nomes contém as entradas esperadas na ordem desejada:

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Se pretender efetuar quaisquer correções, tem de utilizar os `vserver services name-service ns-switch modify` comandos ou `vserver services name-service ns-switch delete`.

Exemplo

O exemplo a seguir cria uma nova entrada na tabela de opções de serviço de nomes para o SVM VS1 usar o arquivo netgroup local e um servidor NIS externo para procurar informações de netgroup nessa ordem:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Depois de terminar

- Você precisa configurar os serviços de nome especificados para o SVM para fornecer acesso aos dados.
- Se você excluir qualquer serviço de nomes para o SVM, também será necessário removê-lo da tabela de opções de serviços de nomes.

  O acesso do cliente ao sistema de armazenamento pode não funcionar como esperado, se você não conseguir excluir o serviço de nomes da tabela de opções do serviço de nomes.

Configurar usuários e grupos UNIX locais

Configure a visão geral de usuários e grupos UNIX locais

Você pode usar usuários e grupos UNIX locais no SVM para mapeamentos de nomes e autenticação. Você pode criar usuários e grupos UNIX manualmente ou carregar um arquivo contendo usuários ou grupos UNIX a partir de um identificador de recurso uniforme (URI).

Há um limite máximo padrão de 32.768 grupos de usuários UNIX locais e membros de grupo combinados no cluster. O administrador do cluster pode modificar este limite.

Crie um usuário local do UNIX

Você pode usar o `vserver services name-service unix-user create` comando para criar usuários UNIX locais. Um usuário UNIX local é um usuário UNIX criado no SVM como uma opção de serviços de nome UNIX para ser usado no processamento de mapeamentos de nomes.

Passo

1. Criar um usuário local UNIX:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* especifica o nome de usuário. O comprimento do nome de utilizador tem de ter 64 carateres ou menos.

   `-id` *`integer`* Especifica a ID de usuário que você atribui.

   `-primary-gid` *`integer`* Especifica o ID do grupo principal. Isso adiciona o usuário ao grupo principal. Depois de criar o usuário, você pode adicionar manualmente o usuário a qualquer grupo adicional desejado.

Exemplo

O comando a seguir cria um usuário UNIX local chamado johnm (nome completo "John Miller") no SVM

chamado VS1. O usuário tem o ID 123 e o ID do grupo principal 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Carregue usuários UNIX locais a partir de um URI

Como alternativa à criação manual de usuários UNIX locais individuais em SVMs, você pode simplificar a tarefa carregando uma lista de usuários UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI(`vserver services name-service unix-user load-from-uri`)).

Passos

1. Crie um arquivo contendo a lista de usuários UNIX locais que você deseja carregar.

   O arquivo deve conter informações do usuário no formato UNIX `/etc/passwd`:

   `user_name: password: user_ID: group_ID: full_name`

   O comando descarta o valor *`password`* do campo e os valores dos campos após o *`full_name`* campo (*`home_directory`* e *`shell`*).

   O tamanho máximo de ficheiro suportado é de 2,5 MB.

2. Verifique se a lista não contém informações duplicadas.

   Se a lista contiver entradas duplicadas, o carregamento da lista falhará com uma mensagem de erro.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de usuários UNIX locais em SVMs a partir do URI:

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false` `especifica se pretende substituir as entradas. A predefinição é ` `false`.

Exemplo

O comando a seguir carrega uma lista de usuários UNIX locais do URI `ftp://ftp.example.com/passwd` para o SVM chamado VS1. Os usuários existentes no SVM não são sobrescritos pelas informações do URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Crie um grupo UNIX local

Você pode usar o `vserver services name-service unix-group create` comando para criar grupos UNIX locais para o SVM. Grupos UNIX locais são usados com usuários UNIX locais.

Passo

1. Criar um grupo UNIX local:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* especifica o nome do grupo. O comprimento do nome do grupo deve ter 64 carateres ou menos.

   `-id` *`integer`* Especifica o ID do grupo que você atribui.

Exemplo

O comando a seguir cria um grupo local chamado eng no SVM chamado VS1. O grupo tem o ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Adicione um usuário a um grupo UNIX local

Você pode usar o `vserver services name-service unix-group adduser` comando para adicionar um usuário a um grupo UNIX suplementar que seja local para o SVM.

Passo

1. Adicionar um usuário a um grupo UNIX local:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Especifica o nome do grupo UNIX ao qual o usuário será adicionado, além do grupo principal do usuário.

Exemplo

O comando a seguir adiciona um usuário chamado Max a um grupo UNIX local chamado eng no SVM chamado VS1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Carregue grupos UNIX locais a partir de um URI

Como alternativa à criação manual de grupos UNIX locais individuais, você pode carregar uma lista de grupos UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI) usando o `vserver services name-service unix-group load-from-uri` comando.

Passos

1. Crie um arquivo contendo a lista de grupos UNIX locais que você deseja carregar.

   O arquivo deve conter informações de grupo no formato UNIX `/etc/group`:

   `group_name: password: group_ID: comma_separated_list_of_users`

   O comando descarta o valor *`password`* do campo.

   O tamanho máximo de ficheiro suportado é de 1 MB.

   O comprimento máximo de cada linha no arquivo de grupo é de 32.768 carateres.

2. Verifique se a lista não contém informações duplicadas.

   A lista não deve conter entradas duplicadas, ou então carregar a lista falha. Se já houver entradas presentes no SVM, você deve definir o `-overwrite` parâmetro para `true` substituir todas as entradas existentes pelo novo arquivo ou garantir que o novo arquivo não contenha entradas que dupliquem entradas existentes.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de grupos UNIX locais no SVM a partir do URI:

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`especifica se pretende substituir as entradas. A predefinição é `false`. Se você especificar esse parâmetro como `true`, o ONTAP substituirá todo o banco de dados de grupo UNIX local existente do SVM especificado pelas entradas do arquivo que você está carregando.

Exemplo

O comando a seguir carrega uma lista de grupos UNIX locais do URI `ftp://ftp.example.com/group` para o SVM chamado VS1. Os grupos existentes no SVM não são sobrescritos pelas informações do URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Trabalhar com netgroups

Trabalhando com netgroups visão geral

Você pode usar netgroups para autenticação de usuário e para corresponder clientes em regras de política de exportação. Você pode fornecer acesso a netgroups de servidores de nomes externos (LDAP ou NIS) ou pode carregar netgroups de um identificador de recurso uniforme (URI) em SVMs usando o `vserver services name-service netgroup load` comando.

O que você vai precisar

Antes de trabalhar com netgroups, você deve garantir que as seguintes condições sejam atendidas:

- Todos os hosts em netgroups, independentemente da origem (NIS, LDAP ou arquivos locais), devem ter Registros DNS de encaminhamento (A) e reverso (PTR) para fornecer pesquisas de DNS consistentes de encaminhamento e reversão.

  Além disso, se um endereço IP de um cliente tiver vários Registros PTR, todos esses nomes de host devem ser membros do netgroup e ter Registros correspondentes A.

- Os nomes de todos os hosts em netgroups, independentemente de sua origem (NIS, LDAP ou arquivos locais), devem ser corretamente escritos e usar o caso correto. As inconsistências em nomes de host usados em netgroups podem levar a um comportamento inesperado, como verificações de exportação com falha.
- Todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

  Por exemplo, 2011:hu9:0:0:0:0:3:1 tem de ser encurtado para 2011:hu9::3:1.

Sobre esta tarefa

Quando você trabalha com netgroups, você pode executar as seguintes operações:

- Você pode usar o `vserver export-policy netgroup check-membership` comando para ajudar a determinar se um IP de cliente é membro de um determinado netgroup.
- Você pode usar o `vserver services name-service getxxbyyy netgrp` comando para verificar se um cliente faz parte de um netgroup.

  O serviço subjacente para fazer a pesquisa é selecionado com base na ordem configurada do switch do serviço de nomes.

Carregue netgroups em SVMs

Um dos métodos que você pode usar para combinar clientes em regras de política de exportação é usando hosts listados em netgroups. Você pode carregar netgroups de um URI (identificador de recurso uniforme) em SVMs como uma alternativa ao uso de netgroups armazenados em servidores de nomes externos (`vserver services name-service netgroup load`).

O que você vai precisar

Os arquivos netgroup devem atender aos seguintes requisitos antes de serem carregados em um SVM:

- O arquivo deve usar o mesmo formato de arquivo de texto netgroup apropriado que é usado para preencher NIS.

  O ONTAP verifica o formato do arquivo de texto do netgroup antes de carregá-lo. Se o arquivo contiver erros, ele não será carregado e uma mensagem será exibida indicando as correções que você tem que executar no arquivo. Depois de corrigir os erros, você pode recarregar o arquivo netgroup no SVM especificado.

- Todos os carateres alfabéticos nos nomes de host no arquivo netgroup devem estar em minúsculas.
- O tamanho máximo de ficheiro suportado é de 5 MB.
- O nível máximo suportado para netgroups de aninhamento é 1000.
- Somente nomes de host DNS primários podem ser usados ao definir nomes de host no arquivo netgroup.

  Para evitar problemas de acesso à exportação, os nomes de host não devem ser definidos usando Registros DNS CNAME ou round robin.

- As partes de usuário e domínio de triplos no arquivo netgroup devem ser mantidas vazias porque o ONTAP não as suporta.

  Apenas a parte host/IP é suportada.

Sobre esta tarefa

O ONTAP suporta pesquisas netgroup-by-host para o arquivo netgroup local. Depois de carregar o arquivo netgroup, o ONTAP cria automaticamente um mapa netgroup.byhost para ativar as pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas de netgroup locais ao processar regras de política de exportação para avaliar o acesso do cliente.

Passo

1. Carregue netgroups em SVMs a partir de um URI:

   ```
   vserver services name-service netgroup load -vserver vserver_name -source
   {ftp|http|ftps|https}://uri
   ```

   Carregar o arquivo netgroup e construir o mapa netgroup.byhost pode levar vários minutos.

   Se quiser atualizar os netgroups, você pode editar o arquivo e carregar o arquivo netgroup atualizado no SVM.

Exemplo

O comando a seguir carrega definições de netgroup no SVM chamado VS1 a partir do URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verifique o status das definições do netgroup

Depois de carregar netgroups no SVM, você pode usar o `vserver services name-service netgroup status` comando para verificar o status das definições do netgroup. Isso permite determinar se as definições de netgroup são consistentes em todos os nós que fazem backup do SVM.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Verifique o status das definições do netgroup:

   ```
   vserver services name-service netgroup status
   ```

   Pode apresentar informações adicionais numa vista mais detalhada.

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

Depois que o nível de privilégio é definido, o seguinte comando exibe o status do netgroup para todos os SVMs:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Crie uma configuração de domínio NIS

Se um NIS (Network Information Service) for usado em seu ambiente para serviços de nome, você deverá criar uma configuração de domínio NIS para o SVM usando o `vserver services name-service nis-domain create` comando.

Antes de começar

Todos os servidores NIS configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.

Se você pretende usar NIS para pesquisas de diretório, os mapas em seus servidores NIS não podem ter mais de 1.024 carateres para cada entrada. Não especifique o servidor NIS que não está em conformidade com este limite. Caso contrário, o acesso do cliente dependente de entradas NIS pode falhar.

Sobre esta tarefa

Se o seu banco de dados NIS contiver um `netgroup.byhost` mapa, o ONTAP poderá usá-lo para pesquisas mais rápidas. Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente. A partir do ONTAP 9.7, as entradas do NIS `netgroup.byhost` podem ser armazenadas em cache usando os `vserver services name-service nis-domain netgroup-database` comandos.

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

Passos

1. Criar uma configuração de domínio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain
<domain_name> -nis-servers <IP_addresses>
```

Pode especificar até 10 servidores NIS.

> A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

2. Verifique se o domínio foi criado:

```
vserver services name-service nis-domain show
```

Exemplo

O comando a seguir cria uma configuração de domínio NIS para um domínio NIS chamado `nisdomain` no SVM nomeado `vs1` com um servidor NIS em endereço IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

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 deteção de servidor LDAP no domínio do ative 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 ative 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 (ative 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 ative 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 ative 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 ative 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 ative 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 ative 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
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
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	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
Informações do grupo	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Informações do netgroup	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Informações sobre direitos autorais

Informações sobre marcas comerciais