# Configurar serviços de nomes

ONTAP 9

NetApp
January 17, 2025

# Índice

# Configurar serviços de nomes

## Como funciona a configuração do switch do serviço de nomes ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

### Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

| Tipo de banco de dados | Define fontes de serviço de nome para… | Fontes válidas são… |
|---|---|---|
| hosts | Conversão de nomes de host para endereços IP | ficheiros, dns |
| grupo | Procurar informações do grupo de utilizadores | arquivos, nis, ldap |
| passwd | Procurar informações do utilizador | arquivos, nis, ldap |
| grupo de rede | Procurar informações do netgroup | arquivos, nis, ldap |
| namemap | Mapeando nomes de usuários | ficheiros, ldap |

### Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

| Especificar tipo de origem… | Para procurar informações em… | Gerenciado pelas famílias de comando… |
| --- | --- | --- |
| ficheiros | Arquivos de origem local | `vserver services name-service unix-user` `vserver services name-service unix-group`<br><br>`vserver services name-service netgroup`<br><br>`vserver services name-service dns hosts` |
| nis | Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM | `vserver services name-service nis-domain` |
| ldap | Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM | `vserver services name-service ldap` |
| dns | Servidores DNS externos conforme especificado na configuração DNS do SVM | `vserver services name-service dns` |

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

## Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

| Fonte do serviço de nomes externo | Protocolo utilizado para acesso |
| --- | --- |
| NIS | UDP |
| DNS | UDP |
| LDAP | TCP |

**Exemplo**

O exemplo a seguir exibe a configuração do switch do serviço de nomes para o SVM_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para procurar endereços IP para hosts, o ONTAP primeiro consulta os arquivos de origem locais. Se a consulta não retornar nenhum resultado, os servidores DNS serão verificados em seguida.

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM.svm_1. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

**Informações relacionadas**

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

# Utilize LDAP

## Visão geral do LDAP

Um servidor LDAP (Lightweight Directory Access Protocol) permite manter centralmente as informações do usuário. Se você armazenar seu banco de dados de usuários em um servidor LDAP em seu ambiente, poderá configurar seu sistema de storage para procurar informações de usuário em seu banco de dados LDAP existente.

- 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 iguais para autenticar quando `--bind-as-cifs-server` definidas como verdadeiro.

> 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)

- Começando com ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch."
- 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 obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

## Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você deve configurar as configurações de segurança do servidor NFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`. teste

A assinatura LDAP e a vedação no tráfego SMB são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

## Conceitos LDAPS

Você deve entender certos termos e conceitos sobre como o ONTAP protege a comunicação LDAP. O ONTAP pode usar TLS ou LDAPS para configurar sessões autenticadas entre servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX.

### Terminologia

Existem certos termos que você deve entender sobre como o ONTAP usa o LDAPS para proteger a comunicação LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Um protocolo para acessar e gerenciar diretórios de informações. O LDAP é usado como um diretório de informações para armazenar objetos como usuários, grupos e grupos de rede. O LDAP também fornece serviços de diretório que gerenciam esses objetos e atendem solicitações LDAP de clientes LDAP.

- **SSL**

  (Secure Sockets Layer) Um protocolo desenvolvido para enviar informações de forma segura pela Internet. O SSL é suportado pelo ONTAP 9 e posterior, mas foi obsoleto em favor do TLS.

- **TLS**

  (Transport Layer Security) um protocolo de rastreamento de padrões IETF que é baseado nas especificações SSL anteriores. É o sucessor do SSL. O TLS é compatível com o ONTAP 9.5 e posterior.

- **LDAPS (LDAP sobre SSL ou TLS)**

  Um protocolo que usa TLS ou SSL para proteger a comunicação entre clientes LDAP e servidores LDAP.

Os termos *LDAP sobre SSL* e *LDAP sobre TLS* às vezes são usados de forma intercambiável. O LDAPS é suportado pelo ONTAP 9.5 e posterior.

- No ONTAP 9.5-9,8, o LDAPS só pode ser ativado na porta 636. Para fazer isso, use o `-use-ldaps-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.
- A partir do ONTAP 9.9,1, o LDAPS pode ser ativado em qualquer porta, embora a porta 636 permaneça a predefinição. Para fazer isso, defina o `-ldaps-enabled` parâmetro `true` e especifique o parâmetro desejado `-port`. Para obter mais informações, consulte a `vserver services name-service ldap client create` página de manual

É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.

- * Iniciar TLS*

  (Também conhecido como *start_tls*, *STARTTLS* e *STARTTLS*) Um mecanismo para fornecer comunicação segura usando os protocolos TLS.

  O ONTAP usa o STARTTLS para proteger a comunicação LDAP e usa a porta LDAP padrão (389) para se comunicar com o servidor LDAP. O servidor LDAP deve ser configurado para permitir conexões pela porta LDAP 389; caso contrário, as conexões LDAP TLS do SVM ao servidor LDAP falharão.

**Como o ONTAP usa o LDAPS**

O ONTAP oferece suporte à autenticação de servidor TLS, o que permite que o cliente LDAP SVM confirme a identidade do servidor LDAP durante a operação de vinculação. Os clientes LDAP habilitados para TLS podem usar técnicas padrão de criptografia de chave pública para verificar se o certificado e a ID pública de um servidor são válidos e foram emitidos por uma autoridade de certificação (CA) listada na lista de CAs confiáveis do cliente.

O LDAP suporta STARTTLS para criptografar comunicações usando TLS. O STARTTLS começa como uma conexão de texto simples sobre a porta LDAP padrão (389), e essa conexão é então atualizada para TLS.

O ONTAP oferece suporte ao seguinte:

- LDAPS para tráfego relacionado a SMB entre os servidores LDAP integrados ao ative Directory e o SVM
- LDAPS para tráfego LDAP para mapeamento de nomes e outras informações do UNIX

  Servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX podem ser usados para armazenar informações para mapeamento de nomes LDAP e outras informações do UNIX, como usuários, grupos e netgroups.

- Certificados CA raiz autoassinados

  Ao usar um LDAP integrado do ative-Directory, o certificado raiz autoassinado é gerado quando o Serviço de certificados do Windows Server é instalado no domínio. Ao usar um servidor LDAP baseado em UNIX para mapeamento de nomes LDAP, o certificado raiz autoassinado é gerado e salvo usando meios apropriados para esse aplicativo LDAP.

Por predefinição, o LDAPS está desativado.

## Ative o suporte ao LDAP RFC2307bis

Se você quiser usar o LDAP e exigir a capacidade adicional de usar associações a grupos aninhados, você pode configurar o ONTAP para habilitar o suporte ao LDAP RFC2307bis.

**O que você vai precisar**

Você deve ter criado uma cópia de um dos esquemas de cliente LDAP padrão que você deseja usar.

**Sobre esta tarefa**

Em esquemas de cliente LDAP, os objetos de grupo usam o atributo memberUid. Esse atributo pode conter vários valores e lista os nomes dos usuários que pertencem a esse grupo. Em esquemas de cliente LDAP habilitados para RFC2307bis, os objetos de grupo usam o atributo uniqueMember. Este atributo pode conter o nome distinto completo (DN) de outro objeto no diretório LDAP. Isso permite que você use grupos aninhados porque os grupos podem ter outros grupos como membros.

O usuário não deve ser membro de mais de 256 grupos, incluindo grupos aninhados. O ONTAP ignora quaisquer grupos acima do limite de 256 grupos.

Por padrão, o suporte a RFC2307bis está desativado.

> O suporte a RFC2307bis é ativado automaticamente no ONTAP quando um cliente LDAP é criado com o esquema MS-AD-BIS.

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

**Passos**

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Modifique o esquema de cliente LDAP RFC2307 copiado para ativar o suporte RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifique o esquema para corresponder à classe de objeto suportada no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifique o esquema para corresponder ao nome de atributo suportado no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

## Opções de configuração para pesquisas de diretório LDAP

Você pode otimizar as pesquisas de diretório LDAP, incluindo informações de usuário, grupo e netgroup, configurando o cliente LDAP do ONTAP para se conetar a servidores LDAP da maneira mais apropriada para o seu ambiente. Você precisa entender quando os valores padrão de pesquisa base LDAP e escopo são suficientes e quais parâmetros especificar quando os valores personalizados são mais apropriados.

As opções de pesquisa de cliente LDAP para informações de usuário, grupo e netgroup podem ajudar a evitar consultas LDAP com falha e, portanto, falha no acesso de cliente aos sistemas de armazenamento. Eles também ajudam a garantir que as pesquisas sejam o mais eficientes possível para evitar problemas de desempenho do cliente.

### Valores de pesquisa padrão base e escopo

A base LDAP é o DN base padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o DN base. Essa opção é apropriada quando o diretório LDAP é relativamente pequeno e todas as entradas relevantes estão localizadas no mesmo DN.

Se você não especificar um DN base personalizado, o padrão será `root`. Isso significa que cada consulta pesquisa o diretório inteiro. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

O escopo base LDAP é o escopo de pesquisa padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o escopo base. Ele determina se a consulta LDAP pesquisa somente a entrada nomeada, as entradas um nível abaixo do DN ou toda a subárvore abaixo do DN.

Se você não especificar um escopo base personalizado, o padrão será `subtree`. Isso significa que cada consulta pesquisa a subárvore inteira abaixo do DN. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

### Valores de pesquisa de base e escopo personalizados

Opcionalmente, você pode especificar valores de base e escopo separados para pesquisas de usuário, grupo e netgroup. Limitar a base de pesquisa e o escopo das consultas dessa forma pode melhorar significativamente o desempenho, pois limita a pesquisa a uma subseção menor do diretório LDAP.

Se você especificar valores de base e escopo personalizados, eles substituirão a base de pesquisa padrão geral e o escopo para pesquisas de usuário, grupo e netgroup. Os parâmetros para especificar valores de base e escopo personalizados estão disponíveis no nível de privilégio avançado.

| Parâmetro cliente LDAP… | Especifica personalizado… |
| --- | --- |
| `-base-dn` | DN base para todas as pesquisas LDAP os valores múltiplos podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada no ONTAP 9.5 e versões posteriores). |
| `-base-scope` | Escopo base para todas as pesquisas LDAP |

| | |
|---|---|
| `-user-dn` | DNS base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário. |
| `-user-scope` | Escopo base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário. |
| `-group-dn` | DNS base para todas as pesquisas de grupo LDAP |
| `-group-scope` | Escopo base para todas as pesquisas de grupo LDAP |
| `-netgroup-dn` | DNS base para todas as pesquisas de netgroup LDAP |
| `-netgroup-scope` | Escopo base para todas as pesquisas de netgroup LDAP |

**Vários valores DN base personalizados**

Se a estrutura de diretórios LDAP for mais complexa, poderá ser necessário especificar vários DNS base para procurar determinadas informações em várias partes do diretório LDAP. Você pode especificar vários DNS para os parâmetros DN de usuário, grupo e netgroup separando-os com um ponto e vírgula (;) e anexando toda a lista de pesquisa DN com aspas duplas ("). Se um DN contiver um ponto-e-vírgula, você deve adicionar um caractere de escape imediatamente antes do ponto-e-vírgula no DN.

Observe que o escopo se aplica a toda a lista de DNS especificada para o parâmetro correspondente. Por exemplo, se você especificar uma lista de três DNS de usuário e subárvore diferentes para o escopo do usuário, o usuário LDAP pesquisará toda a subárvore para cada um dos três DNS especificados.

A partir do ONTAP 9.5, você também pode especificar LDAP *referral chasing*, o que permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP não for retornada pelo servidor LDAP primário. O cliente usa esses dados de referência para recuperar o objeto de destino do servidor descrito nos dados de referência. Para procurar objetos presentes nos servidores LDAP referidos, o base-DN dos objetos referidos pode ser adicionado ao base-DN como parte da configuração do cliente LDAP. No entanto, os objetos referidos só são procurados quando a busca por referência está ativada (usando a `-referral-enabled true` opção) durante a criação ou modificação do cliente LDAP.

## Melhore o desempenho das pesquisas de diretório LDAP netgroup-by-host

Se o seu ambiente LDAP estiver configurado para permitir pesquisas netgroup-by-host, você poderá configurar o ONTAP para aproveitar isso e realizar pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas do netgroup e reduzir possíveis problemas de acesso ao cliente NFS devido à latência durante as pesquisas do netgroup.

**O que você vai precisar**

Seu diretório LDAP deve conter um `netgroup.byhost` mapa.

Seus servidores DNS devem conter Registros de pesquisa direta (A) e reversa (PTR) para clientes NFS.

Quando você especifica endereços IPv6 em netgroups, você deve sempre encurtar e compactar cada endereço conforme especificado no RFC 5952.

**Sobre esta tarefa**

Os servidores NIS armazenam informações do netgroup em três mapas separados chamados `netgroup` `netgroup.byuser` , e `netgroup.byhost`. O objetivo dos `netgroup.byuser` mapas e `netgroup.byhost` é acelerar as pesquisas de netgroup. O ONTAP pode realizar pesquisas netgroup-by-host em servidores NIS para melhorar os tempos de resposta de montagem.

Por padrão, os diretórios LDAP não têm um `netgroup.byhost` mapa como os servidores NIS. No entanto, é possível, com a ajuda de ferramentas de terceiros, importar um mapa NIS `netgroup.byhost` para diretórios LDAP para permitir pesquisas rápidas netgroup-by-host. Se você tiver configurado seu ambiente LDAP para permitir pesquisas netgroup-by-host, poderá configurar o cliente LDAP do ONTAP com o `netgroup.byhost` nome do mapa, DN e o escopo de pesquisa para pesquisas mais rápidas netgroup-by-host.

Receber os resultados das pesquisas netgroup-by-host com mais rapidez permite que o ONTAP processe regras de exportação com mais rapidez quando os clientes NFS solicitam acesso às exportações. Isso reduz a chance de atraso no acesso devido a problemas de latência de pesquisa do netgroup.

**Passos**

1. Obtenha o nome distinto completo exato do mapa NIS `netgroup.byhost` importado para o diretório LDAP.

   O DN do mapa pode variar dependendo da ferramenta de terceiros usada para importação. Para obter o melhor desempenho, você deve especificar o DN exato do mapa.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Ative as pesquisas netgroup-by-host na configuração de cliente LDAP da máquina virtual de armazenamento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false`Ativar ou desativar a pesquisa netgroup-by-host para diretórios LDAP. A predefinição é `false.

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` Especifica o nome distinto do `netgroup.byhost` mapa no diretório LDAP. Ele substitui o DN base para pesquisas netgroup-by-host. Se você não especificar esse parâmetro, o ONTAP usará o DN base.

   `-netgroup-byhost-scope {base|onelevel subtree`especifica o escopo de pesquisa para pesquisas netgroup-by-host. Se não especificar este parâmetro, a predefinição é `subtree.

   Se a configuração do cliente LDAP ainda não existir, você pode habilitar pesquisas netgroup-by-host especificando esses parâmetros ao criar uma nova configuração de cliente LDAP usando o `vserver services name-service ldap client create` comando.

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

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

**Exemplo**

O comando a seguir modifica a configuração de cliente LDAP existente chamada "ldap_corp" para habilitar pesquisas netgroup-by-host usando o mapa chamado netgroup `netgroup.byhost`.byhost", dc `subtree`

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

**Depois de terminar**

Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente.

**Informações relacionadas**

"IETF RFC 5952: Uma recomendação para representação de texto de endereço IPv6"

## Use LDAP fast bind para autenticação nsswitch

A partir do ONTAP 9.11,1, você pode aproveitar a funcionalidade LDAP *fast bind* (também conhecida como *concurrent bind*) para solicitações de autenticação de cliente mais rápidas e simples. Para utilizar esta funcionalidade, o servidor LDAP tem de suportar a funcionalidade de ligação rápida.

**Sobre esta tarefa**

Sem vinculação rápida, o ONTAP usa o LDAP Simple BIND para autenticar usuários administrativos com o servidor LDAP. Com esse método de autenticação, o ONTAP envia um nome de usuário ou grupo para o servidor LDAP, recebe a senha de hash armazenada e compara o código de hash do servidor com o código de hash gerado localmente a partir da senha do usuário. Se forem idênticos, o ONTAP concede permissão de login.

Com a funcionalidade de vinculação rápida, o ONTAP envia apenas credenciais de usuário (nome de usuário e senha) para o servidor LDAP por meio de uma conexão segura. Em seguida, o servidor LDAP valida essas credenciais e instrui o ONTAP a conceder permissões de login.

Uma vantagem do fast bind é que não há necessidade de o ONTAP suportar cada novo algoritmo de hash suportado por servidores LDAP, porque o hash de senha é executado pelo servidor LDAP.

"Saiba mais sobre como usar o fast bind."

Você pode usar configurações de cliente LDAP existentes para o LDAP fast bind. No entanto, é altamente recomendável que o cliente LDAP seja configurado para TLS ou LDAPS; caso contrário, a senha é enviada por fio em texto simples.

Para ativar o LDAP fast bind em um ambiente ONTAP, você precisa atender a estes requisitos:

- Os usuários de administração do ONTAP devem ser configurados em um servidor LDAP que suporte a vinculação rápida.
- O SVM do ONTAP deve ser configurado para LDAP no banco de dados de switch de serviços de nome (nsswitch).
- As contas de usuário e grupo de administrador do ONTAP devem ser configuradas para autenticação

nsswitch usando vinculação rápida.

**Passos**

1. Confirme com o administrador LDAP que o LDAP FAST BIND é suportado no servidor LDAP.
2. Certifique-se de que as credenciais de utilizador admin do ONTAP estão configuradas no servidor LDAP.
3. Verifique se o administrador ou SVM de dados está configurado corretamente para o LDAP fast bind.

   a. Para confirmar se o servidor LDAP FAST BIND está listado na configuração do cliente LDAP, introduza:

      `vserver services name-service ldap client show`

      "Saiba mais sobre a configuração do cliente LDAP."

   b. Para confirmar `ldap` que é uma das fontes configuradas para o banco de dados nsswitch `passwd`, digite:

      `vserver services name-service ns-switch show`

   "Saiba mais sobre a configuração do nsswitch."

4. Certifique-se de que os usuários de administração estejam autenticando com o nsswitch e que a autenticação LDAP de vinculação rápida esteja habilitada em suas contas.

   ◦ Para usuários existentes, insira `security login modify` e verifique as seguintes configurações de parâmetro:

      `-authentication-method nsswitch`

   `-is-ldap-fastbind true`

   ◦ Para novos utilizadores de administração, consulte "Ative o acesso a contas LDAP ou NIS."

## Apresentar estatísticas LDAP

A partir do ONTAP 9.2, você pode exibir estatísticas LDAP para máquinas virtuais de armazenamento (SVMs) em um sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

**O que você vai precisar**

- Você deve ter configurado um cliente LDAP no SVM.
- Você deve ter objetos LDAP identificados a partir dos quais você pode exibir dados.

**Passo**

1. Veja os dados de desempenho para objetos de contador:

   `statistics show`

**Exemplos**

O exemplo a seguir exibe estatísticas para a amostra chamada **smpl_1** para contadores: avg_processor_busy e CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

## Informações sobre direitos autorais



## Informações sobre marcas comerciais