ネーム サービスを設定する

ONTAP 9

NetApp
February 12, 2026

目次

ネーム サービスを設定する

ONTAP NFSネーム サービスについて学ぶ

ストレージ システムの構成によっては、クライアントに適切なアクセスを提供するために、ONTAPがホスト、ユーザ、グループ、またはネットグループの情報を参照できる必要があります。ONTAPがローカルまたは外部のネーム サービスにアクセスしてこの情報を取得できるように、ネーム サービスを設定する必要があります。

クライアント認証時の名前検索を容易にするために、NISやLDAPなどのネーム サービスを使用する必要があります。特にNFSv4以降を導入する場合は、セキュリティを強化するために、可能な限りLDAPを使用することをお勧めします。また、外部ネーム サーバが利用できない場合に備えて、ローカル ユーザとグループを設定する必要があります。

ネーム サービス情報は、すべてのソースで同期された状態に保つ必要があります。

ONTAP NFSネーム サービス スイッチ テーブルを設定する

ONTAPがローカルまたは外部のネーム サービスを参照して、ホスト、ユーザ、グループ、ネットグループ、または名前のマッピング情報を取得できるようにするには、ネーム サービス スイッチ テーブルを正しく設定する必要があります。

開始する前に

環境に応じて、ホスト、ユーザー、グループ、ネットグループ、または名前のマッピングに使用するネーム サービスを決定する必要があります。

ネットグループを使用する場合は、ネットグループで指定されたすべてのIPv6アドレスをRFC 5952で指定されているとおりに短縮および圧縮する必要があります。

タスク概要

使用されていない情報ソースは含めないでください。たとえば、環境でNISが使用されていない場合は、 `-sources nis`オプションを指定しないでください。

手順

1. ネーム サービス スイッチ テーブルに必要なエントリを追加します。

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

2. ネーム サービス スイッチ テーブルに想定されるエントリが適切な順序で格納されていることを確認します。

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

   修正を行う場合は、 `vserver services name-service ns-switch modify`または `vserver services name-service ns-switch delete`コマンドを使用する必要があります。

例

次の例では、SVM vs1 のネーム サービス スイッチ テーブルに新しいエントリを作成し、ローカル ネットグループ ファイルと外部 NIS サーバを使用して、その順序でネットグループ情報を検索します：

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

終了後の操作

- データ アクセスを提供するには、SVMに指定したネーム サービスを設定する必要があります。
- SVMの名前サービスを削除する場合は、ネーム サービス スイッチ テーブルからも削除する必要があります。

  ネーム サービス スイッチ テーブルからネーム サービスを削除できなかった場合、ストレージ システムへのクライアント アクセスが期待どおりに機能しない可能性があります。

ローカル**UNIX**ユーザおよびグループの設定

ONTAP NFS SVMのローカル**UNIX**ユーザーとグループについて学習します

SVM上のローカルUNIXユーザとグループを、認証と名前マッピングに使用できます。UNIXユーザとグループは手動で作成することも、Uniform Resource Identifier（URI）からUNIXユーザまたはグループを含むファイルをロードすることもできます。

クラスタ内のローカルUNIXユーザー グループとグループ メンバーの合計数は、デフォルトで32,768個に制限されています。クラスタ管理者はこの制限を変更できます。

ONTAP NFS SVMにローカル**UNIX**ユーザーを作成する

`vserver services name-service unix-user create`
コマンドを使用して、ローカルUNIXユーザを作成できます。ローカルUNIXユーザとは、ネームマッピングの処理で使用するUNIXネームサービスオプションとしてSVM上に作成するUNIXユーザです。

手順

1. ローカルUNIXユーザを作成します：

   ```
   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*`ユーザー名を指定します。ユーザー名の長さは64文字以下である必要があります。

   `-id *integer*`割り当てるユーザーIDを指定します。

   `-primary-gid *integer*`プライマリ グループIDを指定します。これにより、ユーザはプライマリ グループに追加されます。ユーザの作成後、必要に応じて任意の追加グループに手動でユーザを追加できます。

例

次のコマンドは、johnmというローカルUNIXユーザ（フルネームは「John Miller」）をvs1というSVM上に作成します。ユーザIDは123で、プライマリ グループIDは100です。

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

ONTAP NFS SVMにローカルUNIXユーザーリストをロードする

SVM で個々のローカル UNIX ユーザーを手動で作成する代わりに、Uniform Resource Identifier（URI(`vserver services name-service unix-user load-from-uri`）からローカル UNIX ユーザーのリストを SVM にロードすることで、タスクを簡素化できます。

手順

1. ロードするローカル UNIX ユーザーのリストを含むファイルを作成します。

   ファイルには、UNIX `/etc/passwd` 形式のユーザー情報が含まれている必要があります：

   `user_name: password: user_ID: group_ID: full_name`

   このコマンドは、 *`password`* フィールドの値と、 *`full_name`* フィールドの後のフィールドの値（ (*`home_directory`* および *`shell`*）を破棄します。

   サポートされるファイルの最大サイズは2.5MBです。

2. リストに重複する情報が含まれていないことを確認します。

   リストに重複したエントリが含まれている場合、リストの読み込みは失敗し、エラーメッセージが表示されます。

3. ファイルをサーバーにコピーします。

   サーバーは、HTTP、HTTPS、FTP、または FTPS 経由でストレージ システムからアクセスできる必要があります。

4. ファイルの URI を確認します。

   URI は、ファイルが配置されている場所を示すためにストレージシステムに提供するアドレスです。

5. ローカル UNIX ユーザーのリストを含むファイルを URI から SVM にロードします：

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

   `-overwrite {true false}` はエントリを上書きするかどうかを指定します。デフォルトは `false`です。

例

次のコマンドは、URI `ftp://ftp.example.com/passwd`からローカルUNIXユーザーのリストをvs1という名前のSVMにロードします。SVM上の既存のユーザーは、URIの情報によって上書きされません。

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

ONTAP NFS SVMにローカルUNIXグループを作成する

`vserver services name-service unix-group create`コマンドを使用して、SVMに対してローカルなUNIXグループを作成できます。ローカルUNIXグループは、ローカルUNIXユーザと共に使用されます。

手順

1. ローカルUNIXグループを作成します：

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

   `-name *group_name*`グループ名を指定します。グループ名の長さは64文字以下である必要があります。

   `-id *integer*` 割り当てるグループIDを指定します。

例

次のコマンドは、vs1という名前のSVM上にengという名前のローカル グループを作成します。このグループのIDは101です。

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

ONTAP NFS SVM上のローカルUNIXグループにユーザーを追加する

`vserver services name-service unix-group adduser`コマンドを使用して、SVMに対してローカルな補足UNIXグループにユーザーを追加できます。

手順

1. ローカル UNIX グループにユーザーを追加します：

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

`-name *group_name*`ユーザーのプライマリ グループに加えて、ユーザーを追加するUNIXグループの名前を指定します。

例

次のコマンドは、vs1 という名前の SVM 上の eng という名前のローカル UNIX グループに max という名前のユーザーを追加します：

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

ONTAP NFS SVM上のURIからローカルUNIXグループをロードする

個々のローカル UNIX グループを手動で作成する代わりに、 `vserver services name-service unix-group load-from-uri`コマンドを使用して、Uniform Resource Identifier（URI）からローカル UNIX グループのリストを SVM にロードできます。

手順

1. ロードするローカル UNIX グループのリストを含むファイルを作成します。

   ファイルには、UNIX `/etc/group` 形式のグループ情報が含まれている必要があります：

   `group_name: password: group_ID: comma_separated_list_of_users`

   コマンドは `*password*`フィールドの値を破棄します。

   サポートされるファイルの最大サイズは 1 MB です。

   グループ ファイル内の各行の最大長は 32,768 文字です。

2. リストに重複する情報が含まれていないことを確認します。

   リストには重複するエントリが含まれていてはなりません。重複するとリストのロードに失敗します。SVMに既にエントリが存在する場合は、 `-overwrite`パラメータを `true`に設定して既存のエントリをすべて新しいファイルで上書きするか、新しいファイルに既存のエントリと重複するエントリが含まれていないことを確認する必要があります。

3. ファイルをサーバーにコピーします。

   サーバーは、HTTP、HTTPS、FTP、または FTPS 経由でストレージ システムからアクセスできる必要があります。

4. ファイルの URI を確認します。

   URI は、ファイルが配置されている場所を示すためにストレージシステムに提供するアドレスです。

5. ローカル UNIX グループのリストを含むファイルを URI から SVM にロードします：

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

   `-overwrite true false`}は、エントリを上書きするかどうかを指定します。デフォルトは `false`です。

このパラメータを `true`に指定すると、ONTAPは指定されたSVMの既存のローカルUNIXグループデータベース全体を、ロードするファイルのエントリに置き換えます。

例

次のコマンドは、URI `ftp://ftp.example.com/group`からローカルUNIXグループのリストをvs1という名前のSVMにロードします。SVM上の既存のグループは、URIの情報によって上書きされません。

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

ネットグループの使用

ONTAP NFS SVMのネットグループについて学ぶ

ネットグループはユーザ認証やエクスポート ルールにおけるクライアントの照合に使用できます。外部ネームサーバ（LDAPまたはNIS）からネットグループへのアクセスを提供したり、 `vserver services name-service netgroup load`コマンドを使用してURI（Uniform Resource Identifier）からSVMにネットグループをロードしたりできます。

開始する前に

ネットグループを操作する前に、次の条件が満たされていることを確認する必要があります：

- ネットグループ内のすべてのホストには、ソース（NIS、LDAP、またはローカル ファイル）にかかわらず、一貫したフォワード（正引き）およびリバース（逆引き）DNSルックアップ結果を提供するために、フォワード（A）およびリバース（PTR）の両方のDNSレコードが必要です。

  また、クライアントのあるIPアドレスに複数のPTRレコードがある場合は、それらすべてのホスト名がネットグループのメンバーであり、対応するAレコードがあることが必要です。

- ネットグループ内のすべてのホストの名前が、そのソース（NIS、LDAP、またはローカル ファイル）に関係なく、正しいスペルで大文字 / 小文字が区別されている必要があります。ネットグループで使用されているホスト名で大文字 / 小文字の表記が統一されていないと、予期しない動作（エクスポート チェックの失敗など）が発生することがあります。
- ネットグループに指定されているすべてのIPv6アドレスは、RFC 5952の規定に従って短縮および圧縮されている必要があります。

  たとえば、2011：hu9：0：0：0：0：3：1 は、2011：hu9：：3：1 に短縮する必要があります。

タスク概要

ネットグループを操作する場合、次の操作を実行できます：

- `vserver export-policy netgroup check-membership`コマンドを使用すると、クライアントIPが特定のネットグループのメンバーであるかどうかを判断できます。
- `vserver services name-service getxxbyyy netgrp`コマンドを使用して、クライアントがネットグループの一部であるかどうかを確認できます。

ルックアップの基盤となるサービスは、設定されているネーム サービス スイッチの順番に基づいて選択されます。

ONTAP NFS SVM上のURIからネットグループをロードする

エクスポートポリシールールでクライアントをマッチングする方法の1つは、ネットグループにリストされているホストを使用することです。外部ネームサーバに保存されているネットグループを使用する代わりに、URI（Uniform Resource Identifier）からSVMにネットグループをロードすることもできます(`vserver services name-service netgroup load`。

開始する前に

ネットグループ ファイルは、SVM にロードされる前に次の要件を満たしている必要があります：

- ファイルでは、NIS の設定に使用されるのと同じ適切なネットグループ テキスト ファイル形式を使用する必要があります。

  ONTAPは、ネットグループのテキストファイルをロードする前にフォーマットをチェックします。ファイルにエラーが含まれている場合、ファイルはロードされず、ファイルに必要な修正内容を示すメッセージが表示されます。エラーを修正したら、指定したSVMにネットグループファイルをリロードできます。

- ネットグループ ファイル内のホスト名のアルファベット文字はすべて小文字にする必要があります。
- サポートされるファイルの最大サイズは 5 MB です。
- ネストされたネットグループでサポートされる最大レベルは 1000 です。
- ネットグループ ファイルでホスト名を定義するときは、プライマリDNSホスト名のみを使用できます。

  エクスポートアクセスの問題を回避するには、DNS CNAME またはラウンドロビンレコードを使用してホスト名を定義しないでください。

- ネットグループ ファイル内のトリプルのユーザーとドメインの部分は ONTAP でサポートされていないため、空のままにしておく必要があります。

  ホスト/IP 部分のみがサポートされます。

タスク概要

ONTAPは、ローカルネットグループファイルに対するホストごとのネットグループ検索をサポートしています。ネットグループファイルをロードすると、ONTAPは自動的にnetgroup.byhostマップを作成し、ホストごとのネットグループ検索を有効にします。これにより、クライアントアクセスを評価するエクスポートポリシールールの処理時に、ローカルネットグループ検索が大幅に高速化されます。

手順

1. URI からネットグループを SVM にロードします：

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

   ネットグループ ファイルのロードとnetgroup.byhostマップの構築には、数分かかることがあります。

ネットグループを更新する場合は、ファイルを編集し、更新されたネットグループファイルを SVM にロードできます。

例

次のコマンドは、HTTP URL `http://intranet/downloads/corp-netgroup`から vs1 という名前の SVM にネットグループ定義をロードします：

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

ONTAP NFS SVMネットグループ定義を確認する

ネットグループをSVMにロードした後、 `vserver services name-service netgroup status`コマンドを使用してネットグループ定義のステータスを確認できます。これにより、SVMをサポートするすべてのノードでネットグループ定義が一貫しているかどうかを確認できます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. ネットグループ定義のステータスを確認します。

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

   より詳細なビューで追加情報を表示できます。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

権限レベルが設定されると、次のコマンドはすべてのSVMのネットグループのステータスを表示します：

```
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
```

ONTAP NFS SVMのNISドメイン構成を作成する

環境内でネーム サービスにNetwork Information Service（NIS）が使用されている場合は、 `vserver services name-service nis-domain create`コマンドを使用してSVMのNISドメイン構成を作成する必要があります。

開始する前に

SVMにNISドメインを設定するためには、設定済みのすべてのNISサーバが使用可能でアクセスできる状態になっている必要があります。

ディレクトリ検索にNISを使用する場合、NISサーバのマップではエントリごとに1,024文字を超えることはできません。この制限を満たしていないNISサーバを指定しないでください。そうしないと、NISエントリに依存するクライアント アクセスが失敗する可能性があります。

タスク概要

NISデータベースに `netgroup.byhost`マップが含まれている場合、ONTAPはそれを使用して検索を高速化できます。 `netgroup.byhost`と `netgroup`のマップは、クライアントアクセスの問題を回避するために、ディレクトリ内で常に同期しておく必要があります。ONTAP 9.7以降では、NIS `netgroup.byhost`エントリを `vserver services name-service nis-domain netgroup-database`コマンドを使用してキャッシュできます。

NISをホスト名解決に使用することはサポートされていません。

手順

1. NISドメイン設定を作成します。

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

最大10台のNISサーバを指定できます。

> ℹ `-nis-servers`フィールドは `-servers`フィールドを置き換えます。 `-nis-servers`フィールドを使用して、NISサーバのホスト名またはIPアドレスを指定できます。

2. ドメインが作成されたことを確認します。

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

例

次のコマンドは、 `vs1`という名前のSVM上で、 `nisdomain`と呼ばれるNISドメインのNISドメイン設定を、IPアドレス `192.0.2.180`のNISサーバを使用して作成します：

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

LDAPの使用

ONTAP NFS SVMでのLDAPネームサービスの使用について学習します

LDAPがネーム サービスに使用されている環境では、LDAP管理者と協力して要件および適切なストレージ システム構成を決定し、SVMをLDAPクライアントとして有効にする必要があります。

ONTAP 9.10.1以降、Active DirectoryとネームサービスのLDAP接続の両方で、LDAPチャネル バインディングがデフォルトでサポートされます。ONTAPは、Start-TLSまたはLDAPSが有効で、セッション セキュリティがsignまたはsealに設定されている場合にのみ、LDAP接続でチャネル バインディングを試行します。ネーム サーバとのLDAPチャネル バインディングを無効化または再有効化するには、 `ldap client modify`コマンドで `-try-channel-binding`パラメータを使用します。

詳細については、"Windows の 2020 年 LDAP チャネル バインディングおよび LDAP 署名要件"を参照してください。

- LDAPをONTAP用に設定する前に、サイト環境がLDAPサーバおよびクライアント設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAPサーバのドメイン名がLDAPクライアント上のエントリと一致する必要があります。
  - LDAPサーバでサポートされるLDAPユーザのパスワード ハッシュ タイプに、ONTAPでサポートされる次のタイプが含まれている必要があります。
    - CRYPT（すべてのタイプ）およびSHA-1（SHA、SSHA）

- ONTAP 9.8以降では、SHA-2ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384、およびSSHA-512）もサポートされます。

◦ LDAPサーバにセッション セキュリティ対策が必要な場合は、LDAPクライアントで設定する必要があります。

以下のセッション セキュリティ オプションを使用できます。

- LDAP署名（データの整合性チェックを提供）およびLDAP署名と封印（データの整合性チェックと暗号化を提供）
- START TLS
- LDAPS（TLSまたはSSL経由のLDAP）

◦ 署名および封印されたLDAPクエリを有効にするには、次のサービスが設定されている必要があります。

- LDAPサーバでGSSAPI（Kerberos）SASLがサポートされている必要があります。
- LDAPサーバに、DNS A/AAAAレコード、およびDNSサーバで設定されたPTRレコードが必要です。
- Kerberosサーバに、DNSサーバ上に存在するSRVレコードが必要です。

◦ START TLSまたはLDAPSを有効にする場合、次の点を考慮する必要があります。

- NetAppでは、LDAPSではなくStart TLSの使用を推奨しています。
- ONTAP 9.5以降でLDAPSを使用する場合は、TLS用またはSSL用にLDAPサーバが有効になっている必要があります。ONTAP 9.0～9.4ではSSLはサポートされません。
- 証明書サーバがドメインで設定済みである必要があります。

◦ LDAPリファーラル追跡を有効にするには（ONTAP 9.5以降）、次の条件を満たしている必要があります。

- 両方のドメインで次のいずれかの信頼関係が設定されている必要があります。
  - 双方向
  - 一方向（プライマリ ドメインがリファーラル ドメインを信頼）
  - 親子
- 参照されているすべてのサーバ名を解決するようにDNSが設定されている必要があります。
- --bind-as-cifs-server が true に設定されている場合、認証にはドメイン パスワードが同じである必要があります。

次の設定はLDAPリファーラル追跡でサポートされていません。

◦ すべてのONTAPバージョン：

- 管理SVM上のLDAPクライアント

◦ ONTAP 9.8以前の場合（9.9.1以降でサポートされます）：

- LDAP署名とシーリング（ `-session-security`オプション）
- 暗号化されたTLS接続（ `-use-start-tls` オプション）
- LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap` オプション）

- SVMでLDAPクライアントを設定する際は、LDAPスキーマを入力する必要があります。

  ほとんどの場合、デフォルトのONTAPスキーマのいずれかで問題ありません。ただし、環境のLDAPスキーマがデフォルトのスキーマと異なる場合は、LDAPクライアントを作成する前にONTAP用の新しいLDAPクライアント スキーマを作成する必要があります。環境の要件については、LDAP管理者にお問い合わせください。

- LDAPをホスト名解決に使用することはサポートされていません。

詳細情報

- "NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"
- "ONTAP SMB SVMに自己署名ルートCA証明書をインストールする"

ONTAP NFS SVM用の新しいLDAPクライアント スキーマを作成する

環境で使用するLDAPスキーマがONTAPのデフォルトと異なる場合は、LDAPクライアント設定を作成する前に、ONTAP用の新しいLDAPクライアント スキーマを作成する必要があります。

タスク概要

ほとんどのLDAPサーバでは、ONTAPが提供する次のデフォルト スキーマを使用できます。

- MS-AD-BIS（Windows Server 2012以降のほとんどのADサーバで優先されるスキーマ）
- AD-IDMU（Windows Server 2008、Windows Server 2012、およびそれ以降のADサーバ）
- AD-SFU（Windows Server 2003以前のADサーバ）
- RFC-2307（UNIX LDAPサーバ）

デフォルト以外のLDAPスキーマを使用する必要がある場合は、LDAPクライアント設定を作成する前にスキーマを作成しておく必要があります。新しいスキーマを作成する前に、LDAP管理者にお問い合わせください。

ONTAPに用意されているデフォルトのLDAPスキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、そのコピーを必要に応じて変更します。

手順

1. 既存のLDAPクライアント スキーマのテンプレートを表示して、コピーするスキーマを特定します。

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

2. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

3. 既存のLDAPクライアント スキーマのコピーを作成します。

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

4. 新しいスキーマを変更し、環境に合わせてカスタマイズします：

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

5. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP NFSアクセス用のLDAPクライアント構成を作成する

環境でONTAPから外部のLDAPやActive Directoryのサービスにアクセスする場合は、まずストレージ システム上でLDAPクライアントを設定する必要があります。

開始する前に

Active Directoryドメイン解決リストの最初の3台のサーバのうち1台が起動していて、データを提供している必要があります。そうでない場合、このタスクは失敗します。

ⓘ 複数のサーバがあり、どの時点でもそのうち3台以上のサーバがダウンしている状態です。

手順

1. LDAP管理者に相談して、 `vserver services name-service ldap client create`コマンドの適切な構成値を決定してください：

   a. LDAPサーバへのドメインベースまたはアドレスベースの接続を指定します。

      `-ad-domain`オプションと `-servers`オプションは相互に排他的です。

      - Active Directoryドメインで LDAPサーバ検出を有効にするには、 `-ad-domain`オプションを使用します。
        - `-restrict-discovery-to-site`オプションを使用すると、LDAPサーバ検出を指定したドメインのCIFSデフォルト サイトに制限できます。このオプションを使用する場合は、 `-default-site`でCIFSデフォルト サイトも指定する必要があります。
      - `-preferred-ad-servers`オプションを使用すると、1つ以上の優先Active DirectoryサーバをIPアドレスでカンマ区切りのリストで指定できます。クライアントの作成後、 `vserver services name-service ldap client modify`コマンドを使用してこのリストを変更できます。
      - `-servers`オプションを使用して、カンマ区切りのリストでIPアドレス別に1つ以上のLDAPサーバー（Active DirectoryまたはUNIX）を指定します。

        ⓘ この `-servers`オプションは非推奨です。 `-ldap-servers`フィールドは `-servers`フィールドに置き換えられます。このフィールドには、LDAPサーバのホスト名またはIPアドレスのいずれかを指定できます。

   b. デフォルトまたはカスタムのLDAPスキーマを指定します。

      ほとんどのLDAPサーバでは、ONTAPによって提供されているデフォルトの読み取り専用スキーマを使用できます。他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。他のスキーマを使用する場合は、デフォルトのスキーマ（読み取り専用）をコピー

し、コピーを変更することによって、独自のスキーマを作成できます。

デフォルトのスキーマ：

- MS-AD-BIS

  RFC-2307bisに基づいて、Windows Server 2012以降のほとんどの標準的なLDAP環境に推奨されるLDAPスキーマです。

- `AD-IDMU`

  Active Directory Identity Management for UNIXに基づいて、このスキーマはWindows Server 2008、Windows Server 2012、およびそれ以降のほとんどのADサーバに適しています。

- `AD-SFU`

  Active Directory Services for UNIXに基づいて、このスキーマはWindows Server 2003以前のほとんどのADサーバに適しています。

- `RFC-2307`

  RFC-2307（*An Approach for Using LDAP as a Network Information Service*）に基づくこのスキーマは、ほとんどのUNIX ADサーバに適しています。

c. バインド値を選択します。

- `-min-bind-level {anonymous|simple|sasl}`最小のバインド認証レベルを指定します。

  デフォルト値は `**anonymous**`です。

- `-bind-dn *LDAP_DN*`バインド ユーザを指定します。

  Active Directoryサーバの場合は、アカウント（DOMAIN\user）またはプリンシパル（user@domain.com）の形式でユーザを指定する必要があります。それ以外の場合は、識別名（CN=user,DC=domain,DC=com）の形式でユーザを指定する必要があります。

- `-bind-password *password*`バインド パスワードを指定します。

d. 必要に応じてセッション セキュリティ オプションを選択します。

LDAP署名と封印（暗号化）、またはLDAP over TLS（LDAPサーバで必要な場合）を有効にできます。

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

  署名(`sign`（データ整合性）、署名とシーリング(`seal`（データ整合性と暗号化）、またはどちらも有効にしない `none`（署名もシーリングも有効にしない）ことができます。デフォルト値は `none`です。

  署名とシーリングのバインドが失敗した場合に `**anonymous**`または `**simple**`にバインド認証をフォールバックさせたくない場合は、 `-min-bind-level {`sasl`も設定する必要があります。

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

`*true*`に設定され、LDAPサーバがサポートしている場合、LDAPクライアントはサーバへの暗号化されたTLS接続を使用します。デフォルト値は`*false*`です。このオプションを使用するには、LDAPサーバの自己署名ルートCA証明書をインストールする必要があります。

ストレージVMのドメインにSMBサーバが追加されており、LDAPサーバがSMBサーバのホームドメインのドメインコントローラの1つである場合は、`vserver cifs security modify`コマンドを使用して`-session-security-for-ad-ldap`オプションを変更できます。

e. ポート、クエリ、およびベースの値を選択します。

デフォルト値を推奨しますが、実際の環境に適しているかどうかをLDAP管理者に確認する必要があります。

- `-port *port*`LDAPサーバ ポートを指定します。

  デフォルト値は`389`です。

Start TLSを使用したLDAP接続の保護を予定している場合は、デフォルトのポート389を使用する必要があります。Start TLSはLDAPのデフォルト ポート389経由でプレーンテキスト接続として開始され、その後TLS接続にアップグレードされます。ポートを変更した場合、Start TLSは失敗します。

- `-query-timeout *integer*`クエリのタイムアウトを秒単位で指定します。

  指定できる範囲は1～10秒です。デフォルト値は`3`秒です。

- `-base-dn *LDAP_DN*`ベースDNを指定します。

  必要に応じて複数の値を入力できます（例：LDAP参照追跡が有効になっている場合）。デフォルト値は""（root）です。

- `-base-scope {base|onelevel|subtree}`は基本検索範囲を指定します。

  デフォルト値は`subtree`です。

- `-referral-enabled {true|false}`は、LDAP参照追跡を有効にするかどうかを指定します。

  ONTAP 9.5以降では、プライマリLDAPサーバから目的のレコードが参照先のLDAPサーバに存在することを示すLDAP参照応答が返された場合、ONTAP LDAPクライアントは検索要求を他のLDAPサーバに参照できるようになります。デフォルト値は`**false**`です。

参照されたLDAPサーバにあるレコードを検索するには、参照されたレコードのベースDNをLDAPクライアント設定の一部としてベースDNに追加する必要があります。

2. Storage VMでLDAPクライアント設定を作成します。

```
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}]
```

LDAPクライアント設定を作成するときは、Storage VM名を指定する必要があります。

3. LDAPクライアント設定が正常に作成されたことを確認します。

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

例

次のコマンドでは、LDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。

```
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
```

次のコマンドでは、署名と封印が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。また、LDAPサーバ検出は指定したドメインの特定サイトに制限されます。

```
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
```

次のコマンドでは、LDAPリファーラル追跡が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1にldap1という名前の新しいLDAPクライアント設定を作成します。

```
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
```

次のコマンドでは、ベースDNを指定することで、Storage VM vs1でldap1という名前のLDAPクライアント設定を変更します。

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

次のコマンドでは、リファーラル追跡を有効にすることで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
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
```

LDAPクライアント設定をONTAP NFS SVMに関連付ける

SVMでLDAPを有効にするには、 `vserver services name-service ldap create`コマンドを使用してLDAPクライアント設定をSVMに関連付ける必要があります。

開始する前に

- LDAPドメインがネットワーク内にすでに存在しており、SVMが配置されているクラスタからアクセスできる必要があります。
- LDAPクライアント設定がSVMに存在している必要があります。

手順

1. SVMでLDAPを有効にします。

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

   > `vserver services name-service ldap create`コマンドは自動構成検証を実行し、ONTAPがネーム サーバに接続できない場合はエラー メッセージを報告します。

   次のコマンドは、「vs1」というSVMでLDAPを有効にし、「ldap1」という名前のLDAPクライアント設定を使用するように設定します。

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

2. vserver services name-service ldap checkコマンドを使用して、ネーム サーバのステータスを検証します。

   次のコマンドは、SVM vs1のLDAPサーバを検証します。

```
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".                                                  |
```

ONTAP NFS SVMのLDAPソースを確認する

ネーム サービスのLDAPソースがSVMのネーム サービス スイッチ テーブルに正しく登録されていることを確認する必要があります。

手順

1. 現在のネーム サービス スイッチ テーブルの内容を表示します：

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

   次のコマンドは、SVM My_SVMの結果を表示します：

```
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`名前マッピング情報を検索するソースとその順序を指定します。UNIXのみの環境では、このエントリは不要です。名前マッピングは、UNIXとWindowsが混在する環境でのみ必要です。

2. `ns-switch`エントリを必要に応じて更新します：

ネーム サービス スイッチ エントリを更新する場合...	コマンドを入力してください...
ユーザ情報	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

ネーム サービス スイッチ エントリを更新する場合...	コマンドを入力してください...
グループ情報	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database group -sources ldap,files`
ネットグループ情報	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`

著作権に関する情報

商標に関する情報