ネームサービスを設定する
ONTAP 9

NetApp
December 20, 2024

目次

ネームサービスを設定する . . . 1
ネームサービスの設定の概要 . . . 1
ネームサービススイッチテーブルを設定する . . . 1
ローカルUNIXユーザおよびグループの設定 . . . 2
ネットグループの使用 . . . 6
NISドメイン設定を作成する . . . 9
LDAPを使用 . . . 10

ネームサービスを設定する

ネームサービスの設定の概要

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権を提供するために ONTAP でホスト、ユーザ、グループ、またはネットグループ情報を検索できるようにする必要があります。この情報を取得するためには、 ONTAP がローカルまたは外部のネームサービスにアクセス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。

NIS や LDAP などのネームサービスは、クライアント認証時の名前検索を容易にするために使用する必要があります。特に NFSv4 以降を導入する際は、セキュリティ強化のために、可能なかぎり LDAP を使用することを推奨します。外部ネームサーバが使用できない場合に備えて、ローカルのユーザとグループも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を維持する必要があります。

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に問い合わせてホスト、ユーザ、グループ、ネットグループ、またはネームマッピングの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。

必要なもの

ホスト、ユーザ、グループ、ネットグループ、またはネームマッピングで現在の環境に該当するように使用するネームサービスを決定しておく必要があります。

ネットグループの使用を計画する場合、ネットグループ内に指定されているすべての IPv6 アドレスは、 RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

タスクの内容

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、ご使用の環境でNISが使用されていない場合は、オプションを指定しない `-sources nis`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
   ```

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

例

次の例は、 SVM vs1 がローカルネットグループファイルを使用し、外部 NIS サーバがネットグループ情報をこの順序で検索するように、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ます。

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

終了後

- データアクセスを提供するには、 SVM 用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 用のネーム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しないと、ストレージシステムへのクライアントアクセスが想定どおりに機能しない場合があります。

ローカル**UNIX**ユーザおよびグループの設定

ローカル**UNIX**ユーザおよびグループの設定の概要

SVM 上で、認証およびネームマッピングにローカル UNIX ユーザおよびグループを使用できます。UNIX ユーザおよびグループは、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 ユーザグループおよびグループメンバーの合計数に対するデフォルトの上限値は 32 、 768 です。クラスタ管理者はこの制限を変更できます。

ローカル**UNIX**ユーザを作成する

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

ステップ

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*`ユーザ名を指定します。ユーザ名は 64 文字以内にする必要があります。

   `-id *integer*`割り当てるユーザ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、ユーザがプライマリグループに追加されます。ユーザを作成したあと、手動でユーザを目的の追加グループに追加できます。

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。ユーザの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"
```

URIからローカルUNIXユーザをロードします。

SVMで個 々 のローカルUNIXユーザを手動で作成する別の方法として、ローカルUNIXユーザのリストをUniform Resource Identifier（URI；ユニフォームリソース識別子）を使用(`vserver services name-service unix-user load-from-uri`してSVMにロードすることもできます。

手順

1. ロードするローカル UNIX ユーザのリストが含まれているファイルを作成します。

   ファイルには、次のUNIX形式でユーザ情報が含まれている必要があり `/etc/passwd`ます。

   user_name: password: user_ID: group_ID: full_name

   このコマンドを実行すると、フィールドの値とフィールド(*home_directory*`の後のフィールドの値が`*full_name*`破棄され `*password*`*shell*` ます）。

   サポートされる最大ファイルサイズは 2.5MB です。

2. リストに重複した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、リストのロードは失敗し、エラーメッセージが表示されます。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX ユーザのリストが含まれているファイルを、 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。デフォルトはです `false`。

例

次のコマンドは、ローカルUNIXユーザのリストを、というURIを使用してvs1というSVM内にロードし`ftp://ftp.example.com/passwd`ます。URI を使用してロードした情報によって SVM 内の既存のユーザが上書きされることはありません。

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

ローカル**UNIX**グループを作成する

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

ステップ

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。グループ名は64文字以下にする必要があります。

   `-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。グループIDは101です。

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

ローカル**UNIX**グループにユーザを追加する

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

ステップ

1. ローカル UNIX グループにユーザを追加します。

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

`-name *group_name*`ユーザのプライマリグループに加えて、ユーザを追加する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 SVM の eng というローカル UNIX グループに、 max という名前のユーザを追加します。

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

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別の方法として、コマンドを使用して、ローカルUNIXグループのリストをUniform Resource Identifier（URI）からSVMにロードすることができます `vserver services name-service unix-group load-from-uri`。

手順

1. ロードするローカル UNIX グループのリストが含まれているファイルを作成します。

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

   `group_name: password: group_ID: comma_separated_list_of_users`

   このコマンドを実行すると、フィールドの値が破棄され `*password*`ます。

   サポートされる最大ファイルサイズは 1MB です。

   グループファイルの 1 行の最大長は、 32 、 768 文字です。

2. リストに重複した情報が含まれていないことを確認します。

   重複するエントリがリストに含まれていてはいけません。含まれていると、リストのロードに失敗します。SVMにすでにエントリがある場合は、パラメータをに `true`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一切含まれないようにする必要があります `-overwrite`。

3. ファイルをサーバにコピーします。

   サーバには、 HTTP 、 HTTPS 、 FTP 、または FTPS 経由でストレージシステムから到達できる必要があります。

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

5. ローカル UNIX グループのリストが含まれているファイルを、 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。デフォルトはです `false`。このパラメータをに指定する `true`と、ONTAPは、指定した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で置き換えます。

例

次のコマンドは、ローカルUNIXグループのリストを、というURIを使用してvs1というSVM内にロードし `ftp://ftp.example.com/group`ます。URI を使用してロードした情報によって SVM 内の既存のグループが上書きされることはありません。

```
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

ネットグループの使用の概要

ネットグループは、ユーザ認証に使用したり、エクスポートポリシールールでクライアントを照合したりするために使用できます。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することも、コマンドを使用してUniform Resource Identifier（URI）からSVMへ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`。

必要なもの

ネットグループを使用する前に、次の条件を満たし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は、ソース（NIS、LDAP、またはローカルファイル）に関係なく、フォワードおよびリバースDNSルックアップの一貫性を提供するために、フォワード（A）およびリバース（PTR）の両方のDNSレコードを持つ必要があります。

  さらに、クライアントのIPアドレスに複数のPTRレコードがある場合、それらのホスト名はすべてネットグループのメンバーであり、対応するAレコードを持っている必要があります。

- ソース（NIS、LDAP、またはローカルファイル）に関係なく、ネットグループ内のすべてのホストの名前のスペルが正しく、大文字と小文字が正しい必要があります。ネットグループで使用されているホスト名に大文字と小文字の不一致があると、予期しない動作（エクスポートチェックの失敗など）が発生する可能性があります。
- 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の指定に従って短縮および圧縮する必要があります。

  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。

タスクの内容

ネットグループについては次の処理を実行できます。

- 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確認できま

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 `vserver services name-service getxxbyyy netgrp`。

  検索を実行するため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序に基づいて選択されます。

ネットグループを**SVM**にロードする

エクスポートポリシールールでクライアントの照合に使用できる方法の 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。ネットグループは、外部ネームサーバに格納されているネットグループを使用する代わりに、Uniform Resource Identifier（URI）を使用(`vserver services name-service netgroup load`してSVMにロードできます。

必要なもの

ネットグループファイルは、 SVM にロードする前に、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、ロードを行う前にネットグループテキストファイル形式をチェックします。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、ファイルで実行する必要のある修正を示すメッセージが表示されます。エラーを修正後に、ネットグループファイルを指定した SVM に再ロードできます。

- ネットグループファイル内のホスト名に含まれる英文字は、すべて小文字にする必要があります。
- サポートされる最大ファイルサイズは 5MB です。
- ネットグループでサポートされる最大ネストレベルは 1000 です。
- ネットグループファイルでホスト名を定義する際に使用できるのは、プライマリ DNS ホスト名のみです。

  エクスポートへのアクセスに関する問題を回避するために、ホスト名の定義には DNS CNAME やラウンドロビンレコードを使用しないでください。

- ネットグループファイル内の 3 つの値のうちユーザおよびドメインの部分は、 ONTAP でサポートされていないので空にしておく必要があります。

  ホスト / IP の部分のみがサポートされます。

タスクの内容

ONTAP は、ローカルネットグループファイルを対象としたホスト単位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したあと、ホスト単位のネットグループ検索を有効にするために netgroup.byhost マップが ONTAP によって自動的に作成されます。これにより、エクスポートポリシールールを処理してクライアントアクセスを評価する際のローカルネットグループ検索にかかる時間が大幅に短縮されます。

ステップ

1. URI から SVM にネットグループをロードします。

```
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。

ネットグループの更新が必要な場合は、ネットグループファイルを編集し、更新されたファイルを SVM にロードすることができます。

例

次のコマンドは、HTTPのURLを使用して、ネットグループ定義をvs1というSVMにロードし`http://intranet/downloads/corp-netgroup`ます。

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

ネットグループの定義のステータスを確認する

SVMにネットグループをロードしたら、コマンドを使用してネットグループの定義のステータスを確認できます `vserver services name-service netgroup status`。これにより、ネットグループの定義が SVM の基盤となるすべてのノードで一貫した状態になっているかどうかを確認することができます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. ネットグループの定義のステータスを確認します。

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

   追加情報をより詳細なビューで表示できます。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

権限レベルを設定したあと、次のコマンドを実行すると、すべての SVM のネットグループのステータスが表示されます。

```
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
```

NISドメイン設定を作成する

環境でNetwork Information Service（NIS；ネットワーク情報サービス）がネームサービスに使用されている場合は、コマンドを使用して、SVMのNISドメイン設定を作成する必要があります `vserver services name-service nis-domain create`。

開始する前に

SVMにNISドメインを設定するには、設定済みのすべてのNISサーバが使用可能で到達可能である必要があります。

ディレクトリ検索での NIS の使用を予定している場合、 NIS サーバ内のマップに 1 、 024 文字を超えるエントリを持たせることはできません。この制限に従っていない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。

タスクの内容

NISデータベースにマップが含まれている場合 `netgroup.byhost`、ONTAPはこのマップを使用して検索を高速化できます。 `netgroup.byhost`ディレクトリ内のマップと `netgroup`マップは、クライアントアクセスに関する問題を回避するために、常に同期されている必要があります。nis.7以降では、コマンドを使用してONTAP 9 `netgroup.byhost`エントリをキャッシュでき `vserver services name-service nis-domain netgroup-database`ます。

ホスト名解決にNISを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。

   > ONTAP 9 .2以降では、 `-nis-servers`フィールドがフィールドに置き換わります `-servers`。この新しいフィールドには、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、という名前のSVM上に、IPアドレスのNISサーバを使用して `192.0.2.180`、という名前の`vs1`NISドメインのNISドメイン設定を作成し `nisdomain`ます。

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

LDAPを使用

LDAPノシヨウホウホウノカイヨウ

現在の環境でLDAPがネームサービスに使用されている場合は、LDAP管理者と協力して要件と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。

10.1以降では、チャネルバインドが**ONTAP 9**接続とネームサービス**LDAP**接続の両方で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署名または封印のいずれか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**チャネルバインドを無効または再度有効にするには、コマンドでパラメータを **`ldap client modify`**使用し **`-try-channel-binding`**ます。

詳細については、を参照してください "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"。

- ONTAP用にLDAPを設定する前に、サイト環境がLDAPサーバとクライアントの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クライアントのエントリと一致している必要があります。
  - LDAPサーバでサポートされるLDAPユーザパスワードのハッシュタイプには、ONTAPでサポートされるハッシュ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サーバで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。

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

- 署名および封印されたLDAPクエリを有効にするには、次のサービスを設定する必要があります。
  - LDAPサーバは、GSSAPI（Kerberos）SASLメカニズムをサポートしている必要があります。
  - LDAPサーバには、DNS A/AAAAレコードと、DNSサーバで設定されたPTRレコードが必要です。
  - Kerberosサーバには、DNSサーバ上にSRVレコードが存在する必要があります。
- START TLSまたはLDAPSを有効にするには、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を使用することを推奨します。
  - LDAPSを使用する場合は、ONTAP 9 .5以降で、TLSまたはSSLに対してLDAPサーバが有効になっている必要があります。ONTAP 9ではSSLはサポートされていません。0-9.4
  - 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以降で）、次の条件を満たす必要があります。
  - 両方のドメインに次のいずれかの信頼関係を設定する必要があります。
    - 双方向
    - 一方向（プライマリがリファーラルドメインを信頼する場合）
    - 親子
  - 参照されるすべてのサーバ名を解決するようにDNSを設定する必要があります。
  - bind-as-cifs-server が true に設定されている場合、認証には両ドメインのパスワードが同じであることが必要です。

  次の設定はLDAPリファーラル追跡では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 以前では（ 9.9.1 以降でサポートされています）：
    - LDAPの署名と封印（ `-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ときは、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が適切です。ただし、環境で使用するLDAPス

キーマがこれらと異なる場合は、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。

- ホスト名解決にLDAPを使用することはサポートされていません。

詳細情報

- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"
- "自己署名ルートCA証明書をSVMにインストールする"

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。

タスクの内容

ほとんどのLDAPサーバでは、ONTAPが提供する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サーバで推奨されるスキーマ）
- AD-IDMU（Windows 2008、Windows Server 2012、およびそれ以降のADサーバ）
- AD-SFU（Windows 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する必要があります。新しいスキーマを作成する前に、LDAP管理者に問い合わせてください。

ONTAPが提供するデフォルトの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、それに応じてコピーを変更します。

手順

1. 既存のLDAPクライアントスキーマ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
```

LDAPクライアント設定を作成する

環境内の外部LDAPサービスまたはActive Directoryサービスに ONTAP からアクセスする場合は、まずストレージシステム上にLDAPクライアントを設定する必要があります。

必要なもの

Active Directoryドメイン解決リストの最初の3つのサーバのいずれかが稼働し、データを提供している必要があります。そうしないと、このタスクは失敗します。

複数のサーバがあり、そのうちどの時点でも3台以上のサーバがダウンしています。

手順

1. LDAP管理者に問い合わせて、このコマンドの適切な設定値を確認し `vserver services name-service ldap client create`ます。

   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`オプションを同時に指定することはできません。

   - オプションを使用し `-ad-domain`て、Active DirectoryドメインでLDAPサーバ検出を有効にします。
     - オプションを使用すると `-restrict-discovery-to-site`、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、でCIFSのデフォルトサイトを指定する必要もあり `-default-site`ます。
   - オプションを使用すると、優先されるActive Directoryサーバをカンマで区切ってIPアドレスで指定できます `-preferred-ad-servers`。クライアントが作成されたら、コマンドを使用してこのリストを変更できます `vserver services name-service ldap client modify`。
   - オプションを使用する `-servers`と、1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）をIPアドレスでカンマで区切って指定できます。

   `-servers`オプションはONTAP 9で廃止されました。2.ONTAP 9.2以降では、 `-ldap-servers`フィールドがフィールドに置き換わります `-servers`。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が提供す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環境で推奨される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 2008、Windows 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 2003以前のほとんどのADサーバに適しています。

- `RFC-2307`

  RFC-2307 （ネットワーク情報サービスとして LDAP を使用するためのアプローチ）に基づいて、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}`最小バインド認証レベルを指定します。

  デフォルト値はです **anonymous**。

- `-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の署名と封印、またはLDAP over TLS（LDAPサーバで必要な場合）を有効にすることができます。

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

  署名(`sign`、データ整合性）、署名と封印(`seal`、データの整合性と暗号化を有効にすることができます。また、 `none`署名と封印のどちらも有効にしないことも可能です。デフォルト値はです `none`。

  {`sasl`バインド認証をにフォールバックする場合、または `**simple**`署名と封印のバインドが失敗した場合以外は、} `**anonymous**`も設定する必要があります `-min-bind-level`。

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

  に設定し、LDAPサーバでサポートされている場合、 **`true`** `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。デフォルト値はです **`false`**。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。

  > Storage VMにSMBサーバがドメインに追加されていて、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、コマンドを使用してオプションを `vserver cifs security modify`変更できます `-session-security-for-ad-ldap`。

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。

    デフォルト値はです `389`。

  Start TLSを使用してLDAP接続を保護する場合は、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。ポートを変更すると、Start TLSが失敗します。

  - `-query-timeout *integer*`クエリー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。デフォルト値は秒です `3`。

  - `-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（LDAPリファーラル追跡が有効な場合など）。デフォルト値は（root）です `""`。

  - `-base-scope{base|onelevel|subtree}` は、ベース検索範囲を指定します。

    デフォルト値はです `subtree`。

  - `-referral-enabled{true|false}` LDAPリファーラル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、必要なレコードが参照先のLDAPサーバに存在することを示すLDAPリファーラル応答がプライマリLDAPサーバから返された場合に、ONTAP LDAPクライアントが他のLDAPサーバへのルックアップ要求を参照できるようになりました。デフォルト値はです **`false`**。

参照されたLDAPサーバに存在す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に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SVMに関連付ける

SVMでLDAPを有効にするには、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 `vserver services name-service ldap create`。

必要なもの

- LDAPドメインがネットワーク内にすでに存在し、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上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`*

   > ONTAP 9 .2以降では `vserver services name-service ldap create`、コマンドによって設定の自動検証が実行され、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が報告されます。

   次のコマンドは、「vs1」SVMでLDAPを有効にし、「ldap1」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".                                                  |
```

ネーム サービスのチェック コマンドはONTAP 9.2以降で使用できます。

ネームサービススイッチテーブルで**LDAP**ソースを確認

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表示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`ネームマッピング情報を検索するソースとその検索順序を指定します。UNIX のみの環境では、このエントリは必要ありません。ネームマッピングは、 UNIX と Windows の両方を使用する混在環境でのみ必要になります。

2. 必要に応じてエントリを更新し `ns-switch`ます。

ns-switch エントリの更新対象	入力するコマンド
ユーザ情報	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database passwd -sources ldap,files`
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