LDAP を使用する

ONTAP 9

NetApp
April 24, 2024

目次

LDAP を使用する

LDAP の使用方法の概要

現在の環境で LDAP がネームサービス用に使用されている場合は、 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 以降では、 LDAP チャネルバインドがデフォルトで Active Directory とネームサービスの両方の LDAP 接続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に設定されている場合にのみ、 LDAP 接続でチャネルバインドを試行します。ネームサーバとのLDAPチャネルバインディングを無効または再度有効にするには、を使用します `-try-channel-binding` パラメータと `ldap client modify` コマンドを実行します

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"。

- LDAP for ONTAP を設定する前に、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している必要があります。
  - LDAP サーバでサポートされている LDAP ユーザパスワードハッシュタイプには、 ONTAP でサポートされてい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。

    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（データの整合性チェックを提供）および LDAP の署名と封印（データの整合性チェックと暗号化を提供）
    - START TLS
    - LDAPS （ 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。
  - TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。
    - ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。
    - LDAPS を使用している場合は、 ONTAP 9.5 以降で LDAP サーバの TLS または SSL 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を設定する必要があります。
      - 双方向
      - 一方向。一次は紹介ドメインを信頼します
      - 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 が設定されていること。
    - 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サポートされません。
>
> - 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（ `-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しています。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。

- 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。

を参照してください。

- "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 にインストールします"

新しい **LDAP** クライアントスキーマを作成します

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。

このタスクについて

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 （ほとんどの Windows Server 2012 以降の AD サーバで推奨されるスキーマ）
- 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 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します

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、の適切な設定値を確認してください `vserver services name-service ldap client create` コマンドを実行します

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` および `-servers` オプションを同時に指定することはできません。

  - を使用します `-ad-domain` Active DirectoryドメインでLDAPサーバ検出を有効にするオプション。

    - を使用できます `-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するオプション。このオプションを使用する場合は、CIFSのデフォルトサイトも指定する必要があります。 `-default-site`。

  - を使用できます `-preferred-ad-servers` カンマで区切ってIPアドレスで1つ以上の優先Active Directoryサーバを指定するオプション。クライアントが作成されたら、を使用してこのリストを変更できます `vserver services name-service ldap client modify` コマンドを実行します

  - を使用します `-servers` カンマで区切ってIPアドレスで1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）を指定するオプション。

> ⓘ 。 `-servers` オプションはONTAP 9.2で廃止されました。ONTAP 9.2以降では、`-ldap-servers` フィールドがに置き換わります `-servers` フィールド。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。その場合は、デフォルトスキーマ（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 を参照してください

  RFC 2307bis に基づいて、ほとんどの標準的な Windows 2012 以降の LDAP 環境で優先される 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 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 サーバで必要な場合は、 LDAP の署名と封印または LDAP over TLS を有効にすることができます。

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

  署名を有効にできます (`sign`、データ整合性）、署名と封印 (`seal`、データ整合性と暗号化）、またはどちらでもない `none`、署名または封印なし）。デフォルト値はです `none`。

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

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

  に設定すると **true** LDAPサーバがサポートしており、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でSMBサーバがドメインに追加されており、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、 `-session-security -for-ad-ldap` オプションを使用します `vserver cifs security modify` コマンドを実行します

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。

  デフォルト値はです `389`。

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。ポートを変更すると、 Start TLS は失敗します。

- `-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。デフォルト値はです 3 秒。

- `-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 リファーラル追跡を有効にした場合など）。デフォルト値はです `""` （ルート）。

- `-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、 LDAP リファーラル追跡を有効にすると、必要なレコードが他の LDAP サーバにあることを示す 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 クライアントがそれらの LDAP サーバに対してルックアップ要求を実行することができます。デフォルト値はです **`false`**。

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。LDAPサーバの検出は指定したドメインの特定の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 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 CN=Users,DC=addomain,DC=example,DC=com
```

次のコマンドは、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 に関連付けます

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

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`*

   > ONTAP 9.2以降では、 `vserver services name-service ldap create` コマンドは設定の自動検証を実行し、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 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. 上の 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** ソースを確認します

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. を更新します `ns-switch` 必要に応じて入力：

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`