LDAPを使用

ONTAP 9

NetApp
December 20, 2024

目次

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