



# LDAPの使用

## ONTAP 9

NetApp  
January 23, 2026

# 目次

|  |   |
|--|---|
| LDAPの使用 .....                                | 1 |
| 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 ..... | 1 |
| 詳細情報 .....                                   | 2 |
| ONTAP NFS SVM用の新しいLDAPクライアント スキーマを作成する ..... | 2 |
| ONTAP NFSアクセス用のLDAPクライアント構成を作成する .....       | 3 |
| LDAPクライアント設定をONTAP NFS SVMに関連付ける .....       | 8 |
| ONTAP NFS SVMのLDAPソースを確認する .....             | 8 |

# 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チャンネル 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接続でチャンネル バインディングを試行します。ネーム サーバとのLDAPチャンネル 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 チャンネル 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（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証明書を実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::> vservice 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::> vservice 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::> vservice 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::> vservice 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::> vservice 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<br>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                           | <pre>vserver services name-service ns-<br/>switch modify -vserver vserver_name<br/>-database passwd -sources ldap,files</pre>   |
| グループ情報                          | <pre>vserver services name-service ns-<br/>switch modify -vserver vserver_name<br/>-database group -sources ldap,files</pre>    |
| ネットグループ情報                       | <pre>vserver services name-service ns-<br/>switch modify -vserver vserver_name<br/>-database netgroup -sources ldap,files</pre> |

## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。