ネーム サービスを設定する

ONTAP 9

NetApp
February 13, 2026

目次

ネーム サービスを設定する

ONTAP NFSネーム サービス スイッチ構成について学ぶ

ONTAPは、UNIXシステムの `/etc/nsswitch.conf` ファイルに相当するテーブルにネーム サービス設定情報を保存します。環境に合わせて適切に設定できるように、テーブルの機能とONTAPでの使用方法を理解しておく必要があります。

ネーム サービス スイッチ テーブルは、ONTAPが特定の種類のネーム サービス情報を取得する際にどのネーム サービス ソースをどの順番で参照するかを決定します。ネーム サービス スイッチ テーブルは、SVMごとに作成および保存されます。

データベース タイプ

テーブルには、次の各データベース タイプについてネーム サービスのリストが格納されます。

データベースの種類	... の名前サービス ソースを定義します。	有効なソースは次のとおりです。
ホスト	ホスト名のIPアドレスへの変換	files、dns
グループ	ユーザ グループ情報の検索	files、nis、ldap
passwd	ユーザ情報の検索	files、nis、ldap
netgroup	ネットグループ情報の検索	files、nis、ldap
namemap	ユーザ名のマッピング	files、ldap

ソース タイプ

ソース タイプによって、該当する情報を取得するために使用するネーム サービス ソースが決まります。

ソース タイプを指定...	...の情報を検索するには	コマンド ファミリによって管理されます...

ファイル	ローカルのソース ファイル	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

ソース タイプを指定...	...の情報を検索するには	コマンド ファミリによって管理されます...
nis	SVMのNISドメイン設定で指定された外部のNISサーバ	`vserver services name-service nis-domain`
ldap	SVMのLDAPクライアント設定で指定された外部のLDAPサーバ	`vserver services name-service ldap`
dns	SVMのDNS設定で指定された外部のDNSサーバ	`vserver services name-service dns`

データ アクセスと SVM 管理認証の両方に NIS または LDAP を使用する予定の場合でも、 `files`を含め、NIS または LDAP 認証が失敗した場合に備えて、フォールバックとしてローカル ユーザーを設定する必要があります。

外部ソースへのアクセスに使用されるプロトコル

ONTAPでは、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部ネーム サービス ソース	アクセスに使用されるプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例では、SVM svm_1のネーム サービス スイッチ情報を表示しています。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

ホストのIPアドレス検索では、最初にローカルのソース ファイルが参照され、結果が返されない場合は、次にDNSサーバが照会されます。

ユーザまたはグループ情報の検索では、ローカルのソース ファイルだけが参照され、結果が返されない場

合、検索は失敗します。

ネットグループ情報の検索では、最初に外部のNISサーバが参照され、結果が返されない場合は、次にローカルのネットグループ ファイルが照会されます。

SVM svm_1のテーブルには、ネーム マッピング用のネーム サービス エントリは含まれていません。そのため、デフォルトの設定に従ってローカルのソース ファイルだけが参照されます。

関連情報

"NetAppテクニカル レポート4668：『Name Services Best Practices Guide』"

LDAPの使用

ONTAP NFS SVMのLDAPについて学ぶ

LDAP（Lightweight Directory Access Protocol）サーバを使用すると、ユーザ情報を一元的に管理できます。ユーザ データベースを環境内のLDAPサーバに格納している場合、既存のLDAPデータベース内のユーザ情報を検索するようにストレージ システムを設定できます。

- 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。
- LDAPSを使用する場合、LDAPサーバでTLSまたはSSL（ONTAP 9.5以降）を有効にする必要があります。SSLはONTAP 9.4～9.0ではサポートされていません。
- 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）

- ONTAP 9.11.1以降では、"ONTAP NFS SVMのnsswitch認証にはLDAP高速バインドを使用します。"を使用できます。
- 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。

詳細については、 "NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"を参照してください。

ONTAP NFS SVMのLDAP署名とシーリングについて学習します

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会に対するLDAPセッション セキュリティを有効にすることができます。Storage Virtual Machine（SVM）のNFSサーバ セキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、秘密鍵技術を用いてLDAPペイロードデータの整合性を確認します。シールは、LDAPペイロードデータを暗号化することで、機密情報をクリアテキストで送信することを回避します。_LDAPセキュリティレベル_オプションは、LDAPトラフィックに署名が必要か、署名とシールが必要か、あるいはどちらも不要かを指定します。デフォルトは `none`です。test

SMB トラフィック上の LDAP 署名とシーリングは、 `vserver cifs security modify`コマンドの `-session-security-for-ad-ldap`オプションを使用して SVM 上で有効になります。

ONTAP NFS SVMのLDAPSについて学ぶ

ONTAPでのLDAP通信の保護方法に関する用語や概念を理解しておく必要があります。ONTAPは、Active Directory統合LDAPサーバ間またはUNIXベースのLDAPサーバ間の認証されたセッションを設定するために、Start TLSまたはLDAP over TLSを使用できます。

用語

ONTAPでのLDAPSを使用したLDAP通信の保護方法に関して理解しておくべき用語があります。

- **LDAP**

  （Lightweight Directory Access Protocol;ライトウェイト ディレクトリ アクセス プロトコル）情報ディレクトリに対するアクセスおよび管理を行うためのプロトコルです。LDAPは、ユーザ、グループ、ネットグループのようなオブジェクトを格納するための情報ディレクトリとして使用されます。またLDAPは、これらのオブジェクトを管理したりLDAPクライアントからの要求を満たしたりするディレクトリ サービスを提供します。

- **SSL**

  （Secure Sockets Layer）インターネット上で情報を安全に送信するために開発されたプロトコルです。SSLは、ONTAP 9以降でサポートされていますが、TLSの導入に伴い廃止されました。

- **TLS**

  （Transport Layer Security） それまでのSSL仕様に基づいたIETF標準の追跡プロトコルです。SSLの後継にあたります。TLSは、ONTAP 9.5以降でサポートされています。

- **LDAPS（SSL または TLS 経由の LDAP）**

  TLSまたはSSLを使用してLDAPクライアントとLDAPサーバ間の通信を保護するプロトコル。「LDAP over SSL」と「LDAP over TLS」という用語は、同じ意味で使用される場合があります。LDAPSはONTAP 9.5以降でサポートされています。

  - ONTAP 9.8～9.5では、LDAPSはポート636でのみ有効にできます。これを行うには、 `vserver cifs security modify`コマンドで `-use-ldaps-for-ad-ldap`パラメータを使用します。
  - ONTAP 9.9.1以降では、ポート636がデフォルトのままですが、LDAPSは任意のポートで有効にできます。有効にするには、 `-ldaps-enabled`パラメータを `true`に設定し、必要な `-port`パラメータを指定します。"ONTAPコマンド リファレンス"の `vserver services name-service ldap client create`の詳細を確認してください。

  NetAppでは、LDAPSではなくStart TLSの使用を推奨しています。

- **TLS**の開始

  （*start_tls*、*STARTTLS*、*StartTLS* とも呼ばれます）TLSプロトコルを使用して安全な通信を提供するメカニズム。

  ONTAPでは、LDAP通信を保護するためにSTARTTLSを使用し、デフォルトのLDAPポート（389）を使用してLDAPサーバと通信します。LDAPサーバは、LDAPポート389経由の接続を許可するように設定する必要があります。そうしないと、SVMからLDAPサーバへのLDAP TLS接続が失敗します。

ONTAPでの**LDAPS**の使用方法

ONTAPはTLSサーバ認証をサポートしています。この認証により、SVMのLDAPクライアントは、バインド操作時にLDAPサーバの識別情報を確認できます。TLSに対応したLDAPクライアントは、公開鍵暗号化の標準的な技法を使用して、サーバの証明書および公開IDが有効であり、かつクライアントの信頼できるCertificate Authority（CA;認証局）のリストにあるCAによって発行されたものであるかどうかをチェックできます。

LDAPでは、TLSを使用した通信の暗号化方法としてSTARTTLSがサポートされています。STARTTLSは標準のLDAP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。

ONTAPでは以下をサポートしています。

- Active Directory統合LDAPサーバとSVMとの間のSMB関連トラフィックに対するLDAPSの使用
- ネーム マッピングやその他のUNIX情報のLDAPトラフィックに対するLDAPSの使用

  Active Directory統合LDAPサーバまたはUNIXベースLDAPサーバのどちらかを使用して、LDAPネーム マッピングの情報やその他のUNIX情報（ユーザ、グループ、ネットグループなど）を格納できます。

- 自己署名ルートCA証明書

  Active-Directory統合LDAPを使用している場合は、Windows Server証明書サービスがドメインにインストールされていると自己署名ルート証明書が生成されます。UNIXベースのLDAPサーバをLDAPネーム マッピングに使用している場合は、該当するLDAPアプリケーションに適切な手段を使用して、自己署名ルート証明書の生成と保存が行われます。

デフォルトでは、LDAPSは無効になっています。

ONTAP NFS SVMのLDAP RFC2307bisサポートを有効にする

LDAPを使用するとともに、ネストされたグループ メンバーシップを使用するための追加機能を必要とする場合は、ONTAPを設定してLDAPのRFC2307bisサポートを有効にすることができます。

開始する前に

デフォルトのLDAPクライアント スキーマのうち、使用するいずれか1つのコピーを作成しておく必要があります。

タスク概要

LDAPクライアント スキーマでは、グループ オブジェクトによってmemberUid属性が使用されます。この属性は、複数の値を格納でき、そのグループに属するユーザの名前を一覧表示できます。RFC2307bis対応

のLDAPクライアント スキーマでは、グループ オブジェクトによってuniqueMember属性が使用されます。この属性には、LDAPディレクトリ内の別のオブジェクトの完全なDistinguished Name（DN;識別名）を含めることができます。これにより、グループに他のグループをメンバーとして追加できるため、ネストされたグループを使用できます。

ユーザは、ネストされたグループを含めて256を超えるグループのメンバーになることはできません。ONTAPは、この256グループの上限を超えるグループをすべて無視します。

デフォルトでは、RFC2307bisサポートは無効になっています。

> MS-AD-BISスキーマを使用してLDAPクライアントを作成すると、RFC2307bisサポートは自動的に有効になります。

詳細については、 "NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"を参照してください。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. コピーしたRFC2307 LDAPクライアント スキーマを変更して、RFC2307bisのサポートを有効にします。

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. LDAPサーバでサポートされているオブジェクト クラスに一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. LDAPサーバでサポートされている属性名に一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

LDAPディレクトリ検索のためのONTAP NFS設定オプション

環境にとって最も適した方法でLDAPサーバに接続するようにLDAPクライアントを構成することで、ユーザ、グループ、およびネットグループ情報を含め、LDAPディレクトリ検索を最適化することができます。デフォルトのLDAPベースおよびスコープ検索値で十分な状況や、カスタム値のほうが適切な場合に指定すべきパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報のLDAPクライアント検索オプションは、LDAPクエリの失敗、ひいてはストレージ システムへのクライアント アクセスの失敗を回避するのに役立ちます。また、クライアントのパフォーマンスに関する問題を回避するために、検索をできるだけ効率的なものにするのにも役立

ちます。

デフォルトのベースおよびスコープ検索値

LDAPベースは、LDAPクライアントがLDAPクエリを実行するために使用するデフォルトのベースDNです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベースDNを使用して行われます。このオプションは、LDAPディレクトリが比較的小さくてすべての関連エントリが同じDN内にある場合に適しています。

カスタムベースDNを指定しない場合、デフォルトは `root`です。つまり、各クエリはディレクトリ全体を検索します。これによりLDAPクエリの成功率は最大化されますが、効率が悪く、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

LDAPベース スコープは、LDAPクライアントがLDAPクエリを実行するために使用するデフォルトのベース スコープです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベース スコープを使用して行われます。LDAPクエリによる検索範囲を、名前付きエントリのみ、DNの1レベル下にあるエントリ、またはDNの下にあるサブツリー全体のどれにするかが決定されます。

カスタムベーススコープを指定しない場合、デフォルトは `subtree`です。つまり、各クエリはDN以下のサブツリー全体を検索します。これによりLDAPクエリの成功率は最大化されますが、効率が悪く、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

カスタム ベースおよびスコープ検索値

必要に応じて、ユーザ、グループ、およびネットグループ検索で、別々のベースおよびスコープ値を指定できます。クエリの検索ベースおよびクエリをこうした形で制限すると、検索対象がLDAPディレクトリのより小さなサブセクションに制限されるため、パフォーマンスを大幅に向上できます。

カスタム ベースおよびスコープ値を指定した場合、ユーザ、グループ、およびネットグループ検索の全般的なデフォルト検索ベースおよびスコープは無視されます。カスタム ベースおよびスコープ値を指定するパラメータは、advanced権限レベルで使用できます。

LDAPクライアントパラメータ…	カスタムを指定します…
`-base-dn`	すべてのLDAP検索のベースDN。必要に応じて複数の値を入力できます（たとえば、ONTAP 9.5以降のリリースでLDAPリファーラル追跡が有効になっている場合など）。
`-base-scope`	すべてのLDAP検索の基本スコープ。
`-user-dn`	すべてのLDAPユーザー検索のベースDN。このパラメータはユーザー名マッピング検索にも適用されます。
`-user-scope`	すべてのLDAPユーザー検索の基本スコープ。このパラメータはユーザー名マッピング検索にも適用されます。
`-group-dn`	すべてのLDAPグループ検索のベースDN。
`-group-scope`	すべてのLDAPグループ検索の基本スコープ。

`-netgroup-dn`	すべてのLDAPネットグループ検索のベースDN。
`-netgroup-scope`	すべてのLDAPネットグループ検索の基本スコープ。

複数のカスタム ベース**DN**値

LDAPディレクトリが複雑な場合は、特定の情報を求めてLDAPディレクトリの複数の部分を検索するために複数のベースDNの指定が必要になる可能性があります。複数のユーザ、グループ、およびネットグループDNパラメータを指定するには、各パラメータをセミコロンで区切り、DN検索リスト全体を二重引用符（"）で囲みます。DNにセミコロンが含まれる場合、DNではセミコロンの直前にエスケープ文字（\）を追加する必要があります。

スコープは、対応するパラメータで指定されているDNのリスト全体に適用されることに注意してください。たとえば、3つの異なるユーザDNのリストとサブツリーをユーザ スコープで指定した場合は、LDAPユーザ検索により、指定された3つのDNのそれぞれでサブツリー全体が検索されます。

ONTAP 9.5以降では、LDAP _referral chasing_も指定できるようになりました。これにより、ONTAPのLDAPクライアントは、プライマリLDAPサーバからLDAPリファーラル応答が返されない場合に、他のLDAPサーバに検索要求を参照できます。クライアントはそのリファーラルデータを使用して、リファーラルデータに記述されているサーバからターゲットオブジェクトを取得します。参照先のLDAPサーバに存在するオブジェクトを検索するには、LDAPクライアント設定の一部として、参照先オブジェクトのbase-dnをbase-dnに追加します。ただし、参照先オブジェクトは、LDAPクライアント作成または変更時に（ `-referral-enabled true`オプションを使用して）リファーラル追跡が有効になっている場合にのみ検索されます。

カスタム**LDAP**検索フィルター

LDAP設定オプションパラメータを使用して、カスタム検索フィルタを作成できます。 `-group-membership-filter`パラメータは、LDAPサーバからグループメンバーシップを検索する際に使用する検索フィルタを指定します。

有効なフィルターの例は次のとおりです：

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

"ONTAPでLDAPを設定する方法"についての詳細をご覧ください。

ONTAP NFS SVMのLDAPディレクトリネットグループ別ホスト検索のパフォーマンスを向上

LDAP環境がホスト単位のネットグループ検索を許可するように設定されている場合は、この機能を利用するようにONTAPを設定し、ホスト単位のネットグループ検索を実行することができます。これにより、ネットグループ検索の処理速度を大幅に引き上げ、ネットグループ検索時のレイテンシによるNFSクライアント アクセスの問題を減らすことができます。

開始する前に

LDAP ディレクトリには `netgroup.byhost` マップが含まれている必要があります。

DNSサーバには、NFSクライアントに対するフォワード（A）およびリバース（PTR）ルックアップ レコードの両方が含まれている必要があります。

ネットグループ内のIPv6アドレスを指定する際には、常にRFC 5952で指定されているとおりに各アドレスを短縮および圧縮する必要があります。

タスク概要

NISサーバは `netgroup`、 `netgroup.byuser`、 `netgroup.byhost`という3つの個別のマップにネットグループ情報を保存します。 `netgroup.byuser`マップと `netgroup.byhost`マップの目的は、ネットグループ検索を高速化することです。ONTAPは、NISサーバ上でホストごとのネットグループ検索を実行し、マウント応答時間を短縮できます。

デフォルトでは、LDAPディレクトリにはNISサーバのような `netgroup.byhost`マップはありません。ただし、サードパーティ製ツールを使用すれば、NIS `netgroup.byhost`マップをLDAPディレクトリにインポートして、ホストごとのネットグループ検索を高速化できます。LDAP環境でホストごとのネットグループ検索を許可するように設定している場合は、ONTAPのLDAPクライアントに `netgroup.byhost`マップ名、DN、検索範囲を指定して設定することで、ホストごとのネットグループ検索を高速化できます。

ホスト単位のネットグループ検索の結果をより迅速に受け取ることで、ONTAPは、エクスポートへのアクセスをNFSクライアントから要求されたときに、より速くエクスポート ルールを処理できます。これにより、ネットグループ検索によるレイテンシの問題によってアクセスが遅延する可能性が低下します。

手順

1. LDAP ディレクトリにインポートした NIS `netgroup.byhost` マップの正確な完全識別名を取得します。

   マップのDNは、インポートに使用したサードパーティ ツールによって異なる場合があります。最高のパフォーマンスを得るために、正確なマップDNを指定してください。

2. 権限レベルをadvancedに設定します： `set -privilege advanced`
3. Storage Virtual Machine（SVM）のLDAPクライアント設定でホスト別ネットグループ検索を有効にします： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false}` は、LDAPディレクトリのホスト別ネットグループ検索を有効または無効にします。デフォルトは `false`です。

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name`LDAPディレクトリ内の `netgroup.byhost`マップの識別名を指定します。これは、ネットグループとホスト間の検索におけるベースDNを上書きします。このパラメータを指定しない場合、ONTAPは代わりにベースDNを使用します。

   `-netgroup-byhost-scope {base|onelevel subtree}` は、ネットグループによるホスト検索の検索範囲を指定します。このパラメータを指定しない場合、デフォルトは `subtree`です。

   LDAPクライアント構成がまだ存在しない場合は、 `vserver services name-service ldap client create`コマンドを使用して新しいLDAPクライアント構成を作成するときにこれらのパラメータを指定することにより、ホスト別のネットグループ検索を有効にすることができます。

`-ldap-servers`フィールドは `-servers`フィールドを置き換えます。 `-ldap-servers`フィールドを使用して、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。

4. admin権限レベルに戻ります： `set -privilege admin`

例

次のコマンドは、既存のLDAPクライアント構成「ldap_corp」を変更し、 netgroup.byhost「nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com」という名前のマップとデフォルトの検索範囲 `subtree`を使用して、ホストごとのネットグループ検索を有効にします：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

終了後の操作

クライアント アクセスの問題を回避するには、ディレクトリ内の `netgroup.byhost`と `netgroup`マップを常に同期しておく必要があります。

関連情報

"IETF RFC 5952：IPv6アドレステキスト表現に関する推奨事項"

ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する

ONTAP 9.11.1以降では、LDAP_ファスト バインド_機能（_コンカレント バインド_とも呼ばれます）を利用して、クライアント認証要求をより高速かつシンプルにすることができます。この機能を使用するには、LDAPサーバがファスト バインド機能をサポートしている必要があります。

タスク概要

高速バインドを使用しない場合、ONTAPはLDAP簡易バインドを使用してLDAPサーバで管理者ユーザを認証します。この認証方式では、ONTAPがLDAPサーバにユーザ名またはグループ名を送信し、サーバに格納されているハッシュ パスワードを受け取って、サーバ ハッシュ コードをユーザ パスワードから生成されたローカル ハッシュ パスコードと比較します。この2つが一致した場合、ONTAPはログイン権限を付与します。

高速バインド機能を使用する場合、ONTAPはセキュアな接続を介してLDAPサーバにユーザ クレデンシャル（ユーザ名とパスワード）を送信するだけです。LDAPサーバは受け取ったクレデンシャルを検証し、ログイン権限を付与するようにONTAPに指示します。

高速バインドの利点の1つは、パスワードのハッシュ化はLDAPサーバで実行されるため、LDAPサーバでサポートされるすべての新しいハッシュ アルゴリズムをONTAPでサポートする必要がないことです。

"高速バインドの使用について説明します。"

開始する前に

LDAP高速バインドには、既存のLDAPクライアント設定を使用できます。ただし、パスワードがプレーンテキストでネットワークに送信されないように、LDAPクライアントにTLSまたはLDAPSを設定しておくことを強く推奨します。

ONTAP環境でLDAP高速バインドを有効にするには、次の要件を満たす必要があります。

- 高速バインドをサポートするLDAPサーバにONTAP管理者ユーザが設定されている必要があります。
- ONTAP SVMのネーム サービス スイッチ（nsswitch）データベースにLDAPが設定されている必要があります。
- ONTAP管理者ユーザおよびグループのアカウントに高速バインドを使用したnsswitch認証が設定されている必要があります。
- 高速バインドが成功するには、管理者の UID 番号と GID 番号が入力され、照会可能である必要があります。

手順

1. LDAP管理者に問い合わせて、LDAPサーバでLDAP高速バインドがサポートされていることを確認します。
2. LDAPサーバにONTAP管理者ユーザのクレデンシャルが設定されていることを確認します。
3. 管理SVMまたはデータSVMにLDAP高速バインドが正しく設定されていることを確認します。

   a. LDAP高速バインド サーバがLDAPクライアント設定にリストされていることを確認するには、次のように入力します。

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

      "LDAPクライアント設定については、こちらを参照してください。"

   b. `ldap`がnsswitch `passwd`データベースに設定されたソースの1つであることを確認するには、次のように入力します：

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

   "nsswitchの設定については、こちらを参照してください。"

4. 管理者ユーザがnsswitchで認証されていること、および管理者のアカウントでLDAP高速バインド認証が有効になっていることを確認します。

   ◦ 既存のユーザーの場合は、 `security login modify`を入力して次のパラメータ設定を確認します：

      ```
      -authentication-method nsswitch

      -is-ldap-fastbind true
      ```

      `security login modify`
      の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

   ◦ 新しい管理者ユーザーの場合は、"LDAPまたはNIS ONTAPアカウントアクセスを有効にする"を参照してください。

ONTAP NFS SVMのLDAP統計を表示する

ストレージ システム上のStorage Virtual Machine（SVM）のLDAP統計を表示して、パフォーマンスを監視し、問題を診断できます。

開始する前に

- SVM に LDAP クライアントを設定しておく必要があります。
- データを表示できるLDAPオブジェクトを特定しておく必要があります。

手順

1. カウンタ オブジェクトのパフォーマンス データを表示します。

```
statistics show
```

例

次の例では、*smpl_1*というサンプルのカウンタ：avg_processor_busyとcpu_busyの統計を表示します。

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

関連情報

- "statistics show"
- "statistics start"
- "statistics stop"

著作権に関する情報

商標に関する情報