ネームサービスを設定

ONTAP 9

NetApp
April 24, 2024

目次

ネームサービスを設定

ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf` UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP 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。ONTAP では、 SVM ごとに個別のネームサービススイッチテーブルが保持されます。

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。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、 DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、 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	情報の検索先	使用するコマンド

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	情報の検索先	使用するコマンド
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管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります `files` また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

外部ソースへのアクセスに使用するプロトコル

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。

外部のネームサービスソース	アクセスに使用するプロトコル
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 アドレスの検索では、 ONTAP は最初にローカルのソースファイルを参照します。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、 ONTAP はローカルのソースファイルだけを参照します。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、 ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカル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、 ONTAP はデフォルトでローカルのソースファイルだけを参照します。

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

LDAP を使用する

LDAPの概要

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 LDAP サーバに保存する場合、既存の LDAP データベース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 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。
    - の認証では、ドメインパスワードが同じである必要があります `--bind-as-cifs-server` trueに設定します。

> 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）

- ONTAP 9.11.1以降では、を使用できます "nsswitch認証のためのLDAP高速バインド。"
- 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。

追加情報の場合は、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 』"。

LDAP の署名と封印の概念

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、シークレットキーのテクノロジを使用して、 LDAP ペイロードデータの整合性を確認します。封印は、 LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP ト

ラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトはです `none`。テスト

SMBトラフィックに対するLDAPの署名と封印は、を使用してSVMで有効にします `-session-security-for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

LDAPSの概念

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 LDAP サーバ間の認証されたセッションの設定に Start TLS または LDAPS を使用できます。

用語集

ONTAP での LDAP 通信の保護に LDAPS を使用する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 ）情報ディレクトリにアクセスして管理するためのプロトコルです。LDAP は、ユーザ、グループ、ネットグループなどの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。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も提供します。

- **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 ）従来の 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ます。

- * LDAPS （ LDAP over SSL または TLS ） *

  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*」は同じ意味で使用されることがあります。LDAPSはONTAP 9.5以降でサポートされます。

  - ONTAP 9.5-9.8 では、 LDAPS はポート 636 でのみ有効にできます。そのためには、を使用します `-use-ldaps-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します
  - ONTAP 9.9.1以降では、任意のポートでLDAPSを有効にできますが、デフォルトはポート636です。これを行うには、を設定します `-ldaps-enabled` パラメータの値 `true` そして目的のものを指定してください `-port` パラメータ詳細については、を参照してください `vserver services name-service ldap client create` のマニュアルページ

  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。

- * TLS を開始 *

（ *START_TLS*,*STARTTLS* 、 *_StartTLS* とも呼ばれます）。 TLS プロトコルを使用してセキュアな通信を提供するメカニズムです。

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 ID 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 では次の機能がサポートされます

- Active Directory 統合 LDAP サーバと SVM の間の SMB 関連トラフィックに使用する LDAPS
- LDAPS ：ネームマッピングやその他の UNIX 情報で使用する LDAP トラフィックに使用します

  Active Directory 統合 LDAP サーバまたは UNIX ベース LDAP サーバのいずれかを使用して、 LDAP ネームマッピングおよびユーザ、グループ、ネットグループなどのその他の UNIX 情報の格納に使用できます。

- 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。

LDAP の **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。

必要なもの

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。

このタスクについて

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。この属性には複数の値を含めることができ、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。

このユーザは、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 サポートが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、 ONTAP では RFC2307bis サポートが自動的に有効になります。

追加情報の場合は、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 』"。

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設定オプション

環境にとって最も適切な方法で LDAP サーバに接続するように ONTAP LDAP クライアントを設定することで、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の問題を回避するために、検索をできるだけ効率的に行うことができます。

デフォルトのベースおよびスコープ検索値です

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、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、デフォルトはです `root`。つまり、各クエリでディレクトリ全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったり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検索スコープです。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、デフォルトはです `subtree`。つまり、各クエリで DN の下にあるサブツリー全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったり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と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させることができます。

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一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	カスタム指定要素
`-base-dn`	すべての LDAP 検索のベース DN 複数の値を必要に応じて入力できます（ ONTAP 9.5 以降のリリースで LDAP リファーラル追跡を有効にした場合など）。
`-base-scope`	すべての LDAP 検索のベーススコープ
`-user-dn`	すべての LDAP ユーザ検索のベース DN このパラメータは、環境ユーザ名マッピング検索も行います。
`-user-scope`	すべての LDAP ユーザ検索のベーススコープ：このパラメータは、環境ユーザ名マッピング検索も行います。
`-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 グループ検索のベーススコープ

`-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ベーススコープ

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ことがあります。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ている場合は、 DN の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。

scope 環境は、対応するパラメータに指定されている のリスト全体を表します。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。

また、 ONTAP 9.5 以降では、 LDAP_referral_c追いかけ _ を指定することもできます。これにより、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かった場合に、 ONTAP LDAP クライアントがその他の LDAP サーバへのルックアップ要求を参照することができます。クライアントは、このリファーラルデータに記載されたサーバからターゲットオブジェクトを取得します。参照された LDAP サーバにあるオブジェクトを検索するには、参照されたオブジェクトのベース DN を LDAP クライアント設定の一部としてベース DN に追加します。ただし、参照されたオブジェクトは、（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 `-referral-enabled true` オプション）LDAPクライアントの作成時または変更時

LDAP ディレクトリのホスト単位ネットグループ検索のパフォーマンスを向上させます

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。

必要なもの

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

DNS サーバには、 NFS クライアントのフォワード（ 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ときは、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。

このタスクについて

NISサーバは、と呼ばれる3つの個別のマップにネットグループ情報を格納します `netgroup`、`netgroup.byuser`および `netgroup.byhost`。の目的 `netgroup.byuser` および `netgroup.byhost` マップはネットグループ検索を高速化するためのものです。ONTAP は、マウントの応答時間を短縮するために NIS サーバ上でホスト単位のネットグループ検索を実行できます。

デフォルトでは、LDAPディレクトリにはそのようなはありません `netgroup.byhost` NISサーバと同様のマ

ッピングただし、サードパーティのツールを使用すると、NISをインポートできます `netgroup.byhost` LDAPディレクトリにマッピングして、ホスト単位の高速ネットグループ検索を有効にします。ホスト単位のネットグループ検索を許可するようにLDAP環境を設定している場合は、を使用してONTAP LDAPクライアントを設定できます `netgroup.byhost` ホスト単位のネットグループ検索を高速化するために、名前、DN、および検索範囲をマッピングします。

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 クライアントがエクスポートへのアクセスを要求した場合、より高速に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遅延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. NISの完全な識別名を取得します `netgroup.byhost` LDAPディレクトリにインポートしたマップ。

   マップ 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ります。最高のパフォーマンスを得るには、正確なマップ DN を指定する必要があります。

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単位の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}` LDAPディレクトリのホスト単位のネットグループ検索を有効または無効にします。デフォルトはです `false`。

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` の識別名を指定します `netgroup.byhost` LDAPディレクトリにマッピングします。これにより、ホスト単位のネットグループ検索のベース DN が無効になります。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、ホスト単位のネットグループ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、デフォルトのが使用されます `subtree`。

   LDAPクライアント設定がまだ存在しない場合は、を使用して新しいLDAPクライアント設定を作成するときにこれらのパラメータを指定することで、ホスト単位のネットグループ検索を有効にできます `vserver services name-service ldap client create` コマンドを実行します

   > ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、 LDAP サーバのホスト名または IP アドレスを指定できます。

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

例

次のコマンドは、「ldap_corp」という名前の既存のLDAPクライアント設定を変更して、を使用したホスト単位のネットグループ検索を有効にします `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`：

```
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
```

完了後

。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。

関連情報

"IETF RFC 5952 ：『 A Recommendation for IPv6 Address Text Representation 』"

nsswitch認証にLDAP高速バインドを使用できます

ONTAP 9.11.1以降では、ldap_fast bind_fルキノ ウ（_コンカレントbind_とも呼ばれます）を利用して、クライアント認証要求を迅速かつ簡単に行うことができます。この機能を使用するには、LDAPサーバが高速バインド機能をサポートしている必要があります。

このタスクについて

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サーバで管理ユーザを認証します。この認証方式では、ONTAP がユーザまたはグループの名前をLDAPサーバに送信し、保存されているハッシュパスワードを受信して、サーバのハッシュコードをユーザパスワードからローカルに生成されたハッシュパスコードと比較します。同一の場合、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と、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）のみを送信します。LDAPサーバはこれらのクレデンシャルを検証し、ONTAP にログイン権限を付与するように指示します。

高速バインドの利点の1つは、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。パスワードハッシュはLDAPサーバによって実行されるためです。

"高速バインドの使用方法について説明します。"

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、LDAPクライアントがTLSまたはLDAPS用に設定されていることを強く推奨します。設定されていない場合は、パスワードがプレーンテキストでネットワーク経由で送信されます。

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。

- ONTAP 管理者ユーザは、高速バインドをサポートするLDAPサーバで設定する必要があります。
- ネームサービススイッチ（nsswitch）データベースにLDAP用にONTAP SVMが設定されている必要があります。
- 高速バインドを使用してnsswitch認証を行うには、ONTAP 管理者ユーザアカウントとグループアカウントを設定する必要があります。

手順

1. 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LDAP管理者に確認してください。

2. ONTAP 管理者ユーザクレデンシャルがLDAPサーバで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説明します。"

   b. 確認してください `ldap` は、nsswitchに設定されているソースの1つです `passwd` データベースに次のように入力します

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

   "nsswitch設定の詳細は、こちらをご覧ください。"

4. 管理ユーザがnsswitchで認証されていること、およびアカウントで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。

   - 既存のユーザの場合は、と入力します `security login modify` 次のパラメータ設定を確認します。

     ```
     -authentication-method nsswitch
     ```

   `-is-ldap-fastbind true`

   - 新しい管理者ユーザについては、を参照してください "LDAPまたはNISアカウントアクセスを有効にします。"

LDAP統計を表示します。

ONTAP 9.2 以降では、パフォーマンスを監視して問題を診断するために、ストレージシステム上の Storage Virtual Machine （ SVM ）の LDAP 統計を表示することができます。

必要なもの

- SVM で 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。

ステップ

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

次の例は、オブジェクトのパフォーマンスデータを表示します `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```