テクニカル レポート

ONTAPでLDAPを設定する方法

マルチプロトコルNAS ID管理

NetApp
Justin Parisi
2021年5月| TR-4835

概要

このテクニカルレポートでは、NetApp® ONTAP® ベースのシステムでマルチプロトコルNAS用にLightweight Directory Access Protocol（LDAP）ID管理を設定する方法について説明します。本ドキュメントは、TR-4073：『Secure UnifiedAuthentication』を補完するものであり、代わりとなるものと考えられます。ネームサービスのベストプラクティスについては、TR-4668：『NameServices Best Practices Guide』を参照してください。

目次

表一覧

図一覧

概要

このテクニカルレポートでは、NetApp ONTAPソフトウェアを実行するNetAppストレージシステムでのUNIX ID管理およびマルチプロトコルNASアクセスのネームマッピングのための方法としてのLightweight Directory Access Protocol（LDAP）の設定について説明します。一元化されたネームサービスとしてLDAPを使用することで、マルチプロトコルNAS環境で拡張性、一貫性、および容易な管理が実現します。マルチプロトコルNASアクセスにより、エンタープライズストレージシステムとスケールアウトストレージシステムは、Linuxベースと Windowsベースの両方のオペレーティングシステムを実行するクライアントに、それぞれNFSプロトコルとCIFS / SMBプロトコル経由でアクセスを提供できます。

本ドキュメントの主な内容

- ONTAP 9.7以降
- CentOS / Red Hat Enterprise Linux（RHEL）7以降
- FreeIPA 4.8以降
- Windows Server 2012以降でのMicrosoft Active Directory LDAP

その他のクライアントおよびLDAPサーバの設定については、製品のベンダーにお問い合わせください。以前のバージョンのONTAPのほとんどはこのTRにも適用されますが、このドキュメントに記載されている一部の機能やコマンドが欠落している可能性があります。

LDAPとは

LDAPは、Internet Engineering Task Force（IETF）と呼ばれる国際委員会によって開発された標準のディレクトリアクセスプロトコルです。LDAPは、異種プラットフォーム間でネットワークオブジェクトを検索するために使用できる、汎用のネットワークベースのディレクトリサービスを提供することを目的としています。LDAPv3は現在実装されている標準バージョンです。

LDAPモデルは、LDAPディレクトリストアとの通信方法、ディレクトリ内のオブジェクトの検索方法、ストア内のオブジェクトの説明方法、およびディレクトリへのアクセスに使用されるセキュリティを定義します。LDAPでは、ストアに記述されているオブジェクトをカスタマイズおよび拡張できます。したがって、LDAPストアを使用して、さまざまな種類の多様な情報を格納できます。初期のLDAP導入の多くは、電子メールやWebアプリケーションなどのアプリケーションのディレクトリストアとしてLDAPを使用し、従業員情報を格納することに重点を置いていました。ここ数年、LDAPは、ネットワークベースの認証および許可に使用される情報のディレクトリストアとして受け入れられてきました。多くの企業では、ネットワークディレクトリストアとしてNetwork Information Service（NIS）をLDAPに置き換えています。

UNIX ID管理用のLDAPは、Active DirectoryまたはRFC 2307準拠の任意のLDAPプロバイダを通じて提供できます。ONTAPソフトウェアは多数のLDAPサーバをサポートしており、IETFが策定した標準に準拠したLDAPサーバのサポートを要求できます。

クラスタ管理ログインのID管理にLDAPを使用することもできますが、このドキュメントではその使用範囲については説明していません。LDAPをクラスタログインで使用する場合は、製品ドキュメントを参照してください。

UNIX LDAPサーバとしてのMicrosoft Active Directory

Microsoftは、Windows 2000/2003 Active DirectoryからLDAPv3をディレクトリストアとして実装しました。Microsoft LDAPの実装は標準ベースであるため、Microsoft Active Directory LDAPを使用してUNIXユーザおよびグループ情報を格納できます。この機能を使用すると、WindowsとUNIXの両方に基づいて、ネットワークのディレクトリサービスとディレクトリストアを統合できます。Windows 2008 R2より前のバージョンでは、ネイティブのActive Directory LDAPには、UNIXの認証と許可に必要な情報を保持するために必要な属性の定義が含まれていませんでした。したがって、これらのバージョンでこの情報を保持するために必要なオブジェクトを使用してMicrosoft Active Directoryスキーマを拡張する必要があります。Windows 2008 R2以降では、Active DirectoryでUNIXスキーマ拡張がデフォルトで提供されており、それらを実装するためにスキーマを変更する必要はありません。

LDAPには何が格納されますか。

LDAPには、マルチプロトコルNASアクセスで使用される次の情報を格納できます。

- ユウサメイ
- グループ名
- ユーザID（UID）とグループID（GID）の数値
- ホーム ディレクトリ
- ログインシェル
- ネットグループ、DNS名、IPアドレス
- グループ メンバーシップ

ONTAPはどのようにLDAPと連動しますか。

ONTAPでは、次の2つの方法のいずれかでLDAPを使用できます。

- ユーザ名、数値ID、グループ、グループメンバーシップ、ネットグループ、NASプロトコルの処理用のネームマッピングなど
- クラスタ管理用のPrivileged Access Management（PAM；特権アクセス管理）およびクラスタ管理用のONTAP System Managerログインの操作

このドキュメントでは、主にNASプロトコルの操作で使用するLDAPについて説明します。ただし、「LDAPクラスタ管理のための認証」セクションでは、LDAPサーバを使用して、クラスタログイン/認証のユーザとグループをホストし、他のアクセスを許可する方法について説明しています。

マルチプロトコルNASとは

マルチプロトコルNASは、その名のとおり、複数のNASプロトコルを使用した統合NASアクセスです。NetAppストレージシステムでマルチプロトコルNASを使用すると、使用するプロトコルの種類に関係なく、すべてのオペレーティングシステムのユーザが同じデータセットにシームレスにアクセスできるようになります。マルチプロトコル環境に関連するプロトコルは、CIFS / SMBとNFSです。

マルチプロトコルNASは混合モードとも呼ばれますか。

よくある誤解として、マルチプロトコルNASは混合モードとも呼ばれます。この考え方では、NASを実行するNetAppストレージシステムを実装する際に混乱が生じます。これは、mixedセキュリティ形式の概念も存在するためです。mixedセキュリティ形式については、このドキュメントの「セキュリティ形式」のセクションで後述します。

CIFS / SMBとは

CIFS（Common Internet File System）/ Server Message Block（SMB）は、主にMicrosoft Windowsを実行するオペレーティングシステム上のイーサネットベースのネットワーク間でファイルを共有する方法です。CIFSは、Windows 2000で導入されたネイティブファイル共有プロトコルです。最新のオペレーティングシステムでは、クライアントとサーバ間の通信の基盤プロトコルとしてSMBを使用します。

CIFS/SMBは、Sambaなどのサードパーティの実装を通じて、Apple、Linux、Oracle SolarisなどのWindows以外のオペレーティングシステムでも使用されています。NetAppストレージシステム上のWindows以外のオペレーティングシステムでのCIFS / SMBのサポートは状況によって異なり、Interoperability Matrix Tool（IMT）を参照してください。ONTAPのCIFS / SMBの詳細については、TR-4191：『Best Practices Guide for ONTAP 8.2.x Windows File Services』を参照してください。

注： CIFSとSMBにはさまざまな意味がありますが、本ドキュメントではこれらの用語を同じ意味で使用しています。

NFSとは

NFS（Network File System）は、主にLinux、Oracle Solaris、UNIX、HP-UXなどを実行するオペレーティングシステム上で、イーサネットベースのネットワーク間でファイルを共有する方法です。NFSは、Request for Comments（RFC）と呼ばれるドキュメントを通じてIETFによって定義された一連の標準に従います。これらの標準には、エンタープライズレベルのNFSアクセスを提供するすべての主要なNFSクライアント/サーバベンダーが準拠しています。NFSは基盤となる一連のメッセージに依存し、基盤となるメッセージは使用しているNFSのバージョンによって異なります。ONTAPでのNFSの詳細については、TR-4067：『NFS Best Practices and Implementation Guide』を参照してください。

ONTAPでの認証

NetApp ONTAPはUNIXベースのオペレーティングシステム上に構築されているため、通常、ネイティブのNFS環境ではアクセスに関する問題がほとんど発生しません。特にボリュームやqtreeでUNIXセキュリティ形式を使用している場合は、基盤となる方法が同じであるため、アクセスが容易になります。詳細については、本レポートの「セキュリティ形式」を参照してください。

ただし、ボリュームおよびqtreeのセキュリティ形式がNTFSの場合にアクセスするには、NFSクライアントが有効なWindowsユーザへのユーザマッピングを実行する必要があります。NTFS Access Control List（ACL；アクセス制御リスト）はNFSクライアントでは認識されないため、この手順は必須です。したがって、ストレージシステムは、ユーザが認証可能かどうか、およびNTFS ACLを介したアクセス権があるかどうかをクライアントが判断するためのアービトレータとして機能する必要があります。

CIFS / SMB環境では、ボリュームのセキュリティ形式がNTFSであっても、これらのプロトコルを使用するクライアントがシステムにアクセスする前に、一般的なWindows > UNIXユーザ認証に合格する必要があるため、さまざまな問題が発生します。また、ユーザマッピングを使用してプロトコル混在環境でファイル所有者が正確に表示されるようにすることで、ストレージ管理者の負担がさらに大きくなる可能性があります。

同機種NAS環境と異機種NAS環境

一部のサイトでは、純粋なWindows環境または純粋なUNIX環境を使用して、すべてのデータが次のいずれか1つだけを使用してアクセスされます。

- CIFS / SMBおよびNTFSファイルセキュリティ
- NFSおよびUNIXファイルセキュリティ（モードビットまたはNFSv4.x ACL）

ただし、多くのサイトでは、WindowsクライアントとUNIXクライアントの両方からデータセットにアクセスできる必要があります。このような環境では、ONTAPでマルチプロトコルNASが標準でサポートされます。ユーザがネットワークで認証され、適切な共有権限またはエクスポート権限と必要なファイルレベルの権限の両方が割り当てられると、UNIXホストからNFSを使用してデータにアクセスするか、WindowsホストからCIFS / SMBを使用してデータにアクセスできるようになります。マルチプロトコルNASアクセスを使用する場合、オプションであっても、mixedセキュリティ形式（「mixedモード」と呼ばれることもあります）のボリュームおよびqtreeを使用する必要はありません。

マルチプロトコルNASを使用する理由

ONTAPでマルチプロトコルNASを使用すると、明確なメリットがいくつかあります。クライアントが異なるNASプロトコルを使用してデータセットにシームレスに同時にアクセスできるようになれば、次のようなメリットが得られます。

- ストレージ管理タスク全体を削減
- NASが複数のクライアントからアクセスする場合、データのコピーを1つだけ格納する必要がある
- プロトコルに依存しないNAS。ストレージ管理者は、ACLの形式とエンドユーザに提供されるアクセス制御を制御できます。
- NAS環境でのアイデンティティ管理の一元化

ONTAPは25年以上にわたり、エンタープライズクラスのマルチプロトコルNASアクセスを提供してきました。スケールアウトONTAPクラスタとNetApp ONTAP FlexGroupボリュームの登場により、ストレージ管理者はマルチプロトコルNAS環境の柔軟性をさらに高めることができます。

マルチプロトコルNASのユースケース

マルチプロトコルNASの最も一般的な使用方法は次のとおりです。

- ホーム ディレクトリ
- ソースコードリポジトリ
- 研究とエンジニアリングのシェア
- 画像リポジトリ
- オーディオとビデオの編集とレンダリング

マルチプロトコルアクセスにおける一般的な課題

多くの組織は、柔軟性のためにマルチプロトコルNASアクセスを使用したいと考えています。一方、マルチプロトコルNASの難しさは、プロトコル間での共有の概念に固有の一連の課題を生み出すという認識があります。この認識は現実に基づいていますが、基盤となるインフラがマルチプロトコルNASアクセス向けに準備されていない場合に限ります。たとえば、アイデンティティ管理のニーズに合わせてLDAPサーバをセットアップすると、マルチプロトコルNAS環境を大幅に簡素化できます。

次のような課題がありますが、これらに限定されません。

- 複数のプロトコル、オペレーティングシステム、ストレージシステムに関する知識の要件
- ネームサービスサーバ（DNS、LDAP、NISなど）の実用的な知識
- 次のような外部要因
  - 複数の部門やITグループ（WindowsグループやUNIXグループなど）の処理
  - 企業買収
  - ドメイン統合
  - 再編成
  - 多数の可動部品

UNIX ID管理にLDAPなどの有効なネームサービスを使用することで、ONTAPによるマルチプロトコルNASの処理を大幅に簡易化できます。LDAPとActive Directoryを併用すると、NFS / UNIX IDとSMB / Windows IDの両方に対して一元化されたネームサービスが提供されるため、運用がさらに簡易化されます。

LDAPのコンポーネントと考慮事項

NetApp ONTAPは、Storage Virtual Machine（SVM）と呼ばれる一連の概念によってストレージを管理します。これらのコンポーネントは、マルチテナントストレージ運用のための個別のストレージサイロとして機能します。そのため、LDAPの設定と処理はSVMレベルで実行されます。つまり、各SVMで必要に応じて独自のLDAPクライアント設定とスキーマを使用できます。ONTAPとそのSVMは、他のNASクライアントと同様に、LDAPサーバに対するLDAPクライアントとして機能します。ユーザ、グループ、およびネームマッピングルールの整合性を維持するために、複数のソースでユーザ、グループ、およびネームマッピングルールを設定しなくても、ONTAPクライアントとNASクライアントで同じLDAPサーバソースを共有できます。

LDAPの基本

次のセクションでは、LDAPの基本事項とその仕組みについて説明します。

- デフォルトでは、LDAPは通常のトラフィック用にTCPポート389で動作し、Secure Sockets Layer（SSL）を使用するセキュアLDAP用にポート636で動作します。セキュリティ上の目的でLDAPポートを変更できます。ポート636を使用する場合、ONTAP 9.8以前はバインドにLDAPSを使用していました。LDAPサーバがLDAPサーバ用に設定されていない場合、またはONTAP内のLDAPクライアントがLDAPS用に設定されていない場合、バインドは失敗します。ONTAP 9.9.1までは、636以外の代替ポートは使用できません。別のLDAPSポートを使用するには、`-ldaps-enabled true` LDAPクライアント設定でを指定する必要があります。また、代替ポートを使用するようにLDAPサーバも設定する必要があります。
- Active Directory LDAPは、グローバルカタログポート3268でLDAPトラフィックを処理することもできます。ONTAP 9.9.1以降では `-port`、オプションでポートを指定し、を使用することで、セキュアなグローバルカタログポート（3269）を使用できます。`-ldaps-enabled true`
- LDAP情報は、LDAPサーバのフラットファイルに格納され、LDAPスキーマによって整理されます。LDAPクライアントは、LDAPサーバ上のスキーマに基づいて要求と検索を調整するように設定する必要があります。
- LDAPクライアントは、LDAPバインド（基本的にはLDAPサーバへのログイン）を使用してクエリを開始します。クライアント上のLDAPバインド設定は、LDAPサーバによって定義されたセキュリティメカニズムを使用するように設定されています。LDAPサーバでは、少なくとも安全性が最も低い匿名バインドが許可されます。ほとんどのLDAPサーバは、バインドに関してある程度のセキュリティメカニズムに依存しています。時々、それらは単純なユーザー名とパスワードの交換である。それ以外の場合、バインドは暗号化通信用にSSLまたはKerberos/Generic Security Service API（GSSAPI）によって保護されます。ONTAPは、LDAPバインドでこれらすべてのメソッドをサポートしています。さらに、ONTAPでは、CIFS/SMBマシンアカウントを使用してLDAPをWindows Active Directoryにバインドできます。
- LDAPに保存されているユーザおよびグループ情報は、RFC 2307で定義されている標準のLDAP検索要求を使用してクライアントから照会されます。さらに、RFC 2307bisのような新しいメカニズムでは、より合理化されたユーザおよびグループの検索が可能になります。また、LDAPクライアントとサーバの設定を使用して、これらの検索と応答が暗号化によって保護されるように設定することもできます。
- LDAPサーバには、NFSエクスポートルール設定で使用するネットグループ情報だけでなく、ユーザとグループの情報も格納できます。
- 初期要求が初期サーバで見つからない場合、LDAPサーバはチェイスリファーラルを使用して他のLDAPサーバに要求を参照できます。バージョン9.5以降のONTAPでは、チェイスリファーラルがサポートされます。詳細については、「LDAPリファーラル（チェイスリファーラル）」を参照してください。
- ONTAP 9.8以前のLDAPチェイスリファーラルでは、LDAPSやその他の暗号化された検索方法は使用できません。ONTAP 9.9.1以降では、LDAPS / TLS経由のセキュアなLDAPリファーラルがサポートされます。詳細については、バグ1144216を参照してください。
- ONTAPでは、設定された秒数が経過するとタイムアウトするようにLDAPクエリを設定できます。デフォルトでは、クエリは3秒後にタイムアウトします。
- クエリを高速化し、大規模なLDAPスキーマのクロールを回避するには、指定された場所と識別名（DNS）に基づいてLDAPクエリをフィルタリングします。
- ONTAPのLDAPクライアント設定では、IPアドレスまたはホスト名を使用してLDAPサーバを定義することも、単にDNSサービス（SRV）レコードを使用して関連付けられたLDAPサーバを検索することもできます。

ONTAPによるLDAPを使用した認証要求の処理方法

ユーザがONTAP NAS共有に対して認証を試みると、ONTAPはユーザのIDを調べて、そのユーザが要求している内容にアクセスできるかどうかを確立しようとします。名前検索は、ONTAPのネームマッピングにも重要です。

初期認証が実行されます。これは、UID、GID、およびグループメンバーシップの数値を収集するためのユーザの検証です。この認証は、アクセスを要求しているユーザが実際にシステムに存在するかどうかを判断するためにも使用されます。ONTAPでこの情報が収集される場所は`ns-switch`、SVMのネームサービススイッチ（）の設定方法によって異なります。ユーザおよびグループ情報の有効なネームサービスソースは、ローカルファイル（`passwd` および `group`）、NIS、およびLDAPです。ONTAPは、指定されたネームサービスソースをリストされた順に照会します。

ns-switch コマンドセットを使用してネームサービススイッチを設定します。

```
cluster::> ns-switch ?
  (vserver services name-service ns-switch)
  create                      Create a new Name Service Switch table entry
  delete                      Remove a Name Service Switch table entry
  modify                      Change a Name Service Switch table entry
  show                        Display Name Service Switch configuration

cluster::> ns-switch show -vserver DEMO
  (vserver services name-service ns-switch show)
                              Source
Vserver         Database      Order
--------------- ------------ ------------
DEMO            hosts         dns,
                              files
DEMO            group         ldap,
                              files
DEMO            passwd        ldap,
                              files
DEMO            netgroup      files,
                              ldap
DEMO            namemap       ldap,
                              files
```

LDAPを指定した場合、ユーザ検索が必要になったときに、ONTAPは、LDAPサーバにアクセスできるSVMの論理インターフェイス（LIF）を使用します。これらのLIFには、データLIFまたはSVM管理LIFを使用できます。SVM内のLIFがLDAPサーバに到達できないと、ネームサービス要求が失敗します。

LDAPが名前検索に使用されるとONTAPが判断すると、次のプロセスが実行されます。

1. ONTAPは最初に接続キャッシュをチェックし、LDAPサーバへの接続がすでに確立されているかどうかを確認します。キャッシュされている接続がない場合、ONTAPはLDAPクライアント設定を使用して、設定で指定されているサーバへの接続を試行します。ホスト名を指定すると、DNSルックアップが実行されます。Active Directoryドメインが使用されている場合は、DNS SRVレコード検索が実行されます。
2. 定義されたLDAPサービスポートを介したTCP接続が成功すると、ONTAPはクライアント設定で定義されたクレデンシャルを使用してLDAPサーバへの「バインド」（ログイン）を試行します。
3. バインドに成功すると、ONTAPはLDAPクライアントで定義されているクライアントスキーマを使用してLDAPサーバへのLDAP検索クエリを実行します。クエリーでは、次の情報がサーバに渡されます。
   - ベース/ユーザDN（検索範囲を絞り込むため）
   - 検索範囲タイプ（subtree、、baseonelevel）
   - オブジェクトクラス（そのクラス内のオブジェクトのみを検索する場合）
   - UID /ユーザ名
   - 要求された属性（uid、uidNumber、gidNumber、unixUser、Passwordname、unixHomeDirectory、loginShell）
4. 最初の要求でユーザが見つからず、チェイスリファーラルが有効になっている場合、ONTAPは他のLDAPサーバを試行します。ユーザが見つからず、クライアント設定に複数のDNSが定義されている場合、ONTAPは他のDNSを試行します。いずれのシナリオでもユーザが見つからない場合は、エラーが返され、ONTAPは次に使用可能な ns-switch ソースを試行します。ユーザが見つからない場合、要求は失敗し、アクセスは拒否されます。
5. 要求が成功すると、ONTAPは将来の使用のためにユーザ属性をキャッシュに格納します。

処理の流れは、障害が発生した場合に覚えておくことが重要です。これは、LDAP要求が機能していない理由と方法を絞り込むのに役立ちます。LDAP検索の失敗の詳細については、「一般的な問題とトラブルシューティングの手順」を参照してください。

セキュリティ形式

ONTAPでは、権限は、ボリューム、qtree、ファイル、またはフォルダのセキュリティ形式の設定方法によって管理されます。ONTAPストレージ管理者は、ボリュームおよびqtreeについてのみ、クラスタからセキュリティ形式を管理できます。ファイルおよびフォルダのセキュリティ形式は、ファイルまたはフォルダの書き込み先に基づいて設定されます。たとえば、NTFSセキュリティ形式のボリュームにファイルが書き込まれたりコピーされたりすると、そのファイルにもNTFSセキュリティ形式が割り当てられます。ボリュームまたはqtreeのセキュリティ形式を反転しても、既存のファイルまたはフォルダのセキュリティ形式やACLは変更されません。ONTAPでは、ボリュームごとに独立したセキュリティ形式を設定できます。また、qtreeごとに独自のセキュリティ形式を設定することもできます。このアプローチにより、ユーザデータを柔軟に管理できます。特にホームディレクトリのシナリオでは、一部のユーザがWindowsクライアントから権限を管理し、他のユーザがLinuxクライアントから権限を管理します。

セキュリティ形式は、一貫したアクセス権セットを維持するために使用されます。特に、クラスタ内の同じデータセットに対してNFSプロトコルとSMBプロトコルの両方を使用する場合に使用されます。セキュリティ形式は、権限形式の言い回しにすぎません。データのACLをどのように管理しますか。

ONTAPには、マルチプロトコルNASで使用する次の3つのセキュリティ形式があります。

- **NTFS：**このスタイルでは、標準のWindowsアクセス許可モデルとロジックが使用されます。Windowsアクセス権に適用されるルールと同じルールが、NTFSセキュリティ形式のボリュームおよびqtreeに適用されます。NTFSセキュリティ形式を使用してボリュームおよびqtreeの権限と所有者を変更できるのは、Windowsクライアントだけです。権限を変更しようとするNFSクライアントは失敗します。NFSサーバとNFSのエクスポートポリシーの設定方法によっては、エラーが表示される場合と表示されない場合があります。

  ONTAPクラスタCLIからストレージレベルのアクセス保護または `vserver security file-directory` コマンドセットを使用して、ファイルレベルやフォルダレベルまでNTFS権限を管理することもできます。

- **UNIX。**このセキュリティ形式では、UNIX形式の権限構造を使用します。`chmod 755`所有者/グループ/その他との読み取り/書き込み/実行のモードビット（など）や、ユーザとグループのACLをよりきめ細かく管理するためのNFSv4.x ACLが含まれています。ONTAPではサポートされていないPOSIX ACLは含まれません。UNIXセキュリティ形式のボリュームおよびqtreeでは、NFSクライアントのみを使用してアクセス権を管理します。Windowsクライアントでは、CIFSサーバの設定に応じてモードビット権限を表示できますが、NFSv.x ACLを表示できるのはSMB 1.0でのみです。このSMB 1.0は廃止されています。SMB 2.0以降のバージョンでは、NFSv4.x ACL情報を適切に解析できません。WindowsクライアントはUNIXの権限や所有者を変更できません。

  UNIXモードビット権限はクラスタCLIから設定できますが、最上位のボリュームとqtreeにのみ設定できます。ファイル権限はクライアントから設定されます。ONTAP CLIからファイル所有者を設定できるのは、NetApp FlexClone® ボリュームテクノロジを使用している場合のみです。NFSv4.x ACLは、NFSv4.xを使用するクライアントからのみ設定できます。また、ONTAPのNFSサーバでNFSv4.x ACLのサポートを有効にしている場合にのみ設定できます。このACL管理の制限には、セキュリティACLと監査形式ACLが含まれます。

- **mixed（混在）**このセキュリティ形式は、有効なレベルでは常にNTFSまたはUNIXのいずれかになります。ただし、他のセキュリティ形式とは異なり、mixedでは、ファイルまたはフォルダの権限が最後に変更されたACLの形式に基づいて有効な形式が変更されます。この形式は、NFSクライアントから書き込みを行い、あとでWindowsクライアントから権限を変更する必要があるアプリケーションなど、クライアントが任意のプロトコルの権限をいつでも変更できる必要がある場合に便利です。マルチプロトコルNAS環境では、特にネームマッピングやネームサービスが適切に設定されていないと、mixedセキュリティ形式の性質や変更機能が複雑になる可能性があります。そのため、特定のユースケースが必要な場合を除き、NetAppではmixedセキュリティ形式は推奨されません。

ONTAP CLIからセキュリティ形式と権限を表示する方法については、を参照してくださいvserver security file-directory show。

ONTAPテノネエムマツヒンク

ネームマッピングは、（Linux/UNIXベースのオペレーティングシステム上の）ONTAPが、NFSプロトコルとCIFS / SMBプロトコル間のマルチプロトコルNASアクセスを処理する方法です。ボリュームのセキュリティ

形式は常にUNIXまたはNTFSのいずれかであるため、ネームマッピングを使用すると、データオブジェクトに設定した適切なACLが適用されていることを確認できます。

デフォルトでは、ONTAPは、WindowsとUNIXで同じ名前のユーザをマッピングします。ネームマッピングルールを使用して管理者の介入は必要ありません。たとえば、という名前のUNIXユーザは `techontap`、`techontap` 特別なネームマッピングを必要とせずに、という名前のWindowsユーザに暗黙的にマッピングされます。

Windowsでユーザの名前がUNIXでの名前と異なる場合（またはその逆）、ONTAPはユーザを適切にマッピングするためにより多くの情報を必要とします。この情報は、次の3つの場所のいずれかから取得できます。

- ネームサービスマッピング（LDAPなど）
- SVMレベルで設定されるネームマッピングルール
- デフォルトのUNIXまたはWindowsユーザ（NFSまたはCIFSサーバレベルで設定）

ユーザに有効なネームマッピングが存在しない場合、認証要求は失敗し、ONTAPでホストされているNASデータにアクセスしようとすると、クライアントにアクセスまたは権限が拒否されます。

有効なネームマッピングが存在するが、UNIXユーザまたはWindowsユーザを誤ったWindowsユーザまたはUNIXユーザにマッピングすると、次のような結果になる可能性があります。結果としては、ファイルやフォルダへのアクセスが正しくない場合や、ファイルやフォルダに設定されている所有者が正しくない場合（CIFSファイルがnobodyとして表示される場合や、NFSエクスポートで65534として表示される場合など）などがあります。

ネームマッピングルール

ONTAPでは、個々に指定したユーザに対してだけでなく、ホスト名とクライアントに対してもネームマッピングルールを設定できます。ただし、グループとユーザのマッピングにはネームマッピングルールを使用できません。

ネームマッピングルールは、オプションで指定した3つの方向に使用できます。 `-direction`

- **WIN-UNIX** は、Windowsユーザ名をUNIXユーザ名にマッピングするために使用されます。を使用すると、ユーザ名にWindows Active Directoryドメインを指定できます `DOMAIN\\user format`。これらのネームマッピングルールは、ONTAPセキュリティ形式のオブジェクトに対する権限とアクセス権を決定する際に使用する適切なUNIXユーザを決定するのに役立ちます。
- **unix-win** は、UNIX名をウィンドウ名にマッピングするために使用されます。UNIX名はWindowsにマッピングする必要があるため、ユーザ名で指定します。ONTAPは、受信したUNIX数値UIDをネームサービスサーバまたはローカルファイルを使用して名前に変換できる必要があります。UIDにマッピングできないUNIXユーザ名がない場合、マッピング要求は数値UIDを使用してのWindowsユーザを検索し `DOMAIN/{numericID}`ます。これらのネームマッピングルールは、ONTAPセキュリティ形式のオブジェクトに対する権限とアクセス権を決定する際に使用する適切なWindowsユーザを決定するのに役立ちます。
- **krb-unix** は、NFS Kerberos Service Principal Name（SPN；サービスプリンシパル名）マッピングに使用されます。デフォルトでは、NFS Kerberos SPNは `nfs nfs/host@DOMAIN.COMNAME@DOMAIN.COM`、Kerberos要求でのサービス名（の部分など）またはユーザ/マシンアカウントの部分を使用してマッピングを試みます。ストレージ管理者が、ONTAPで1対1のマッピングを行わずに、それらのSPNのネームマッピングを制御したい場合があります。これらのシナリオについては、TR-4616で詳しく説明しています。

正規表現

ONTAPでは、標準の正規表現（regex）値をネームマッピングルールで使用できます。UNIX名とWindows名が1：1ではなく、単純な正規表現値で十分に近い場合に、ネームマッピングルールのグローバル置換機能とワイルドカード機能を提供できます。

たとえば、すべてのWindows名が `first.last` nameの形式に従っていて、UNIX環境でが使用されている場合 `first_last`、正規表現を使用してユーザ名のすべてのドットをアンダースコアにマッピングできます。この正規表現は次のようになります。

```
cluster::*> vserver name-mapping show -vserver DEMO -direction win-unix
```

```
Vserver:   DEMO
Direction: win-unix
Position Hostname          IP Address/Mask
---------- ---------------------- ----------------------
1        -                      -                      Pattern: (.+)\\(.+)\.(.+)
                                                   Replacement: \2_\3
```

上記のルールを指定しないと、user.nameのようなユーザ名がデフォルトのユーザにマッピングされます。

```
cluster::*> diag secd name-mapping show -node ontap9-tme-8040-01 -vserver DEMO -direction win-
unix -name NTAP\user.name

'NTAP\user.name' maps to 'pcuser'
```

このルールでは、が DOMAIN\user.name UNIXユーザにマッピングされ user_nameます。

```
cluster::*> diag secd name-mapping show -node ontap9-tme-8040-01 -vserver DEMO -direction win-
unix -name NTAP\user.name

'NTAP\user.name' maps to 'user_name'
```

ルートへの管理者のマッピング（およびその逆）

ONTAPには、すべての管理ユーザをルートにマッピングするオプションと、ルートをWindows管理者にマッピングするオプションが用意されています。その目的は、ネームマッピングルールに関係なく、複数のNASプロトコルですべての管理ユーザを同じように扱うことです。

たとえば、という名前のWindowsユーザの prof1 有効なUNIXユーザ名がである場合、prof1デフォルトのネームマッピングはです NTAP\prof1 == prof1。

Windowsユーザ prof1 がドメインまたはローカル管理者グループのメンバーである場合は -is-admin-users-mapped-to-root-enabled、CIFS / SMBオプションを有効にすると、そのユーザがルートにマッピングされます。

次の例は show-creds NTAP\prof1、Windowsユーザに対するコマンドの出力を示しています。ネームマッピングとWindowsグループメンバーシップ（ **太字**）をメモします。

```
cluster::*> cifs option show -vserver DEMO -fields is-admin-users-mapped-to-root-enabled
vserver is-admin-users-mapped-to-root-enabled
---------- ---------------------------------------------
DEMO    true

cluster::*> vserver services access-check authentication show-creds -vserver DEMO -win-name
NTAP\prof1

 UNIX UID: prof1 <> Windows User: NTAP\prof1 (Windows Domain User)

 GID: ProfGroup
 Supplementary GIDs:
  ProfGroup
  group1
  group2
  group3
  sharedgroup

 Primary Group SID: NTAP\DomainUsers (Windows Domain group)

 Windows Membership:
  NTAP\group2 (Windows Domain group)
  NTAP\DomainUsers (Windows Domain group)
  NTAP\sharedgroup (Windows Domain group)
  NTAP\group1 (Windows Domain group)
  NTAP\group3 (Windows Domain group)
  NTAP\ProfGroup (Windows Domain group)
  Service asserted identity (Windows Well known group)
  BUILTIN\Backup Operators (Windows Alias)
  BUILTIN\Users (Windows Alias)
```

```
 User is also a member of Everyone, Authenticated Users, and Network Users

 Privileges (0x2086):
  SeBackupPrivilege
  SeRestorePrivilege
  SeChangeNotifyPrivilege
```

これで、このユーザがSVMのローカルAdministratorsグループに追加されると、ルートにマッピングされます。

```
cluster::*> local-group add-members -vserver DEMO -group-name BUILTIN\administrators -member-
names NTAP\prof1
  (vserver cifs users-and-groups local-group add-members)

cluster::*> local-group show-members -vserver DEMO -group-name administrators
  (vserver cifs users-and-groups local-group show-members)

          Vserver: DEMO
       Group Name: BUILTIN\Administrators
      Member Name: DEMO\Administrator
                   NTAP\Domain Admins
                   NTAP\prof1

cluster::*> vserver services access-check authentication show-creds -vserver DEMO -win-name
NTAP\prof1

 UNIX UID: root <> Windows User: NTAP\prof1 (Windows Domain User)

 GID: daemon
 Supplementary GIDs:
  daemon

 Primary Group SID: NTAP\DomainUsers (Windows Domain group)

 Windows Membership:
  NTAP\group2 (Windows Domain group)
  NTAP\DomainUsers (Windows Domain group)
  NTAP\sharedgroup (Windows Domain group)
  NTAP\group1 (Windows Domain group)
  NTAP\group3 (Windows Domain group)
  NTAP\ProfGroup (Windows Domain group)
  Service asserted identity (Windows Well known group)
  BUILTIN\Backup Operators (Windows Alias)
  BUILTIN\Administrators (Windows  Alias)
  BUILTIN\Users (Windows Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users

 Privileges (0x22b7):
  SeBackupPrivilege
  SeRestorePrivilege
  SeTakeOwnershipPrivilege
  SeSecurityPrivilege
  SeChangeNotifyPrivilege
```

ユーザがルートにマッピングされ、NAS共有にファイルを書き込む場合、所有権にはそのネームマッピングが反映されます。次の例では、が `prof1` という名前のSMBからファイルを書き込み `mappedroot.txt`、所有者はになります `root`。

```
# su prof1
sh-4.2$ cd /profgroup
sh-4.2$ ls -la
total 8
drwxrwxrwx  2 root                root      4096 Feb 21 14:59 .
drwxrwxrwx 11 root                root      4096 Feb 3 09:34 ..
-rwxrwxrwx  1 root                ProfGroup    0 Feb 21 14:59 mappedroot.txt
-rw-r--r--  1 prof1               ProfGroup    0 Aug 30 10:30 newfile1
-rw-r--r--  1 prof1               ProfGroup    0 Aug 30 10:30 newfile2
```

ネームマッピングへのLDAPの使用

サーバ上のLDAPスキーマが正しく設定されていて、ONTAP SVMのLDAPクライアントスキーマにネームマッピングに使用される割り当て済みのLDAP属性が反映されていれば、LDAPをネームマッピングリソースにすることができます。たとえば、1：1に一致しない対応するWindowsユーザ名にUNIXユーザをマッピングするには `uid`、`sAMAccountName` LDAPクライアント設定で（UNIXユーザ名の場合）と（Windowsユーザ名の場合）を組み合わせて使用できます。使用される属性は、LDAPの設定前の手順で検出された内容によって異なります。詳細については、「設定」を参照してください。

LDAPスキイマ

LDAPスキーマは、LDAPサーバが情報を整理および収集する方法です。LDAPサーバスキーマは一般に同じ標準に準拠していますが、LDAPサーバプロバイダによってスキーマの表示方法が異なる場合があります。ONTAPには、管理者が使用できる読み取り専用スキーマが組み込まれています。これらのスキーマを使用してLDAPを設定することも、読み取り/書き込み可能なスキーマにコピーすることもできます。これらのオプションを使用すると、デフォルトスキーマと同じ属性を持たないLDAPサーバのスキーマ属性を変更できます。LDAPスキーマは、LDAPクライアントを設定する前に存在している必要があります。

クラスタによるLDAPクエリでは、スキーマを使用して特定の属性を使用してユーザに関する情報（UIDなど）を検索できるため、名前検索を高速化するために使用されます。クラスタがエントリを検索できるようにするには、スキーマ属性がLDAPサーバ内に存在している必要があります。そうしないと、LDAPクエリからデータが返されず、認証要求が失敗することがあります。

たとえば、UID番号（など `root=0`）をクラスタから照会する必要があり、AD-IDMUスキーマスタイルを使用するようにクラスタが設定されている場合は、スキーマ属性 `RFC 2307 uidNumber Attribute` が使用されます。AD-IDMUのデフォルトスキーマでは、`uidNumber` そのクエリに属性が使用されます。

LDAPサーバがその情報に別のスキーマ属性を使用している場合、クエリはその情報を見つけることができません。

使いやすく構成しやすいように、ONTAPにはいくつかのデフォルトの読み取り専用スキーマテンプレートが用意されています。これらのスキーマテンプレートは、通常、特定のLDAPサーバに対応します。表2 に、ONTAPが提供するLDAPスキーマテンプレートと、それぞれに対応するLDAPサーバを示します。つまり、特定のタイプのLDAPサーバを使用する場合、そのサーバでリストされているスキーマは通常、そのサーバで機能する必要があります。

RFC 2307bis

RFC 2307は、Request for Commentsメモ「An Approach for Using LDAP as a Network Information Service」（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）と題されています。RFC 2307bisはRFC 2307の拡張であり、のサポートが追加されて `posixGroup`います。これにより、`uniqueMember` `memberUid` LDAPスキーマの属性を使用するのではなく、属性を使用して補助グループの動的検索が可能になります。この属性には、ユーザの名前だけを使用するのではなく、LDAPデータベース内の別のオブジェクトの完全な識別名（DN）が含まれます。したがって、グループは他のグループをメンバーとして持つことができ、グループをネストすることができます。RFC 2307bisのサポートにより、オブジェクトクラスのサポートも追加されて `groupOfUniqueNames`います。

このRFC拡張は、Microsoft Active Directoryが通常の管理ツールを使用してユーザーとグループを管理する方法に適しています。たとえば、RFC 2307bisのサポートがない場合、ユーザの補足グループをLDAPクエリに確実に入力するには、`memberUid` 必要なグループのフィールドに、そのグループに属するユーザを入力する必要があります。この手順は、古いバージョンのActive Directory（Windows Server 2012以降で廃止）で使用できる従来のUNIX属性タブ、または新しいバージョンのWindowsでは属性エディタタブまたはWindows PowerShellを使用して実行します。このタスクは、ユーザをグループのメンバーとして追加するという、通常のWindowsグループ管理方法に対する追加の手順です。

RFC 2307bisでは、Windowsユーザをグループに追加すると（そのグループに有効な数値GIDがある場合）、LDAPルックアップは通常のWindows属性から必要な補足グループ情報を取得し、数値GIDを自動的に検索します。

そのため、NetAppでONTAPクライアントを設定するときは、RFC 2307bisを有効にすることを強く推奨します。スキーマの作成時に有効にします。デフォルトでは `MS-AD-BIS`、ONTAPが提供するスキーマで使用できます。

グループメンバーシップおよび補足グループ

LDAPを使用して、ユーザのグループメンバーシップを制御したり、ユーザの追加グループを返すことができます。この動作は、スキーマ属性によって制御されます。

プライマリGID

ONTAPが適切に検索できるようにするには、LDAPユーザに常にプライマリGIDが定義されている必要があります。ユーザのプライマリGIDは、schema属性によって定義され `-gid-number-attribute`ます。通常、この属性はです `gidNumber`。`gid` またはのような場合もあり `primaryGid`ます。適切な属性については、LDAP管理者に確認してください。

ユーザにプライマリUNIX GIDがない場合は、ユーザが有効なUNIX UIDと数値を持っていても、ONTAPは要求に失敗します。

```
cluster::*> getxxbyyy getpwbyname -node node1 -vserver DEMO -username test -show-source true
-use-cache false -show-granular-err true
  (vserver services name-service getxxbyyy getpwbyname)
NIS:
Error code:    NS_ERROR_NONE
Error message: No error
LDAP:
Error code:    NS_ERROR_NOT_FOUND
Error message: Entry not found
DNS:
Error code:    NS_ERROR_NONE
Error message: No error
FILES:
Error code:    NS_ERROR_NOT_FOUND
Error message: Entry not found
Deterministic Result: Authoritative Error


Error: command failed: Failed to resolve test. Reason: Entry not found for "username: test".
```

セカンダリGID、補助GID、補助GID

セカンダリグループ、補助グループ、補助グループは、ユーザがプライマリGIDの外部に属しているグループです。LDAPでは、次の2つの方法で定義されます。

- `memberUid`
- RFC 2307bis

LDAPでは、使用中のLDAPスキーマ設定に基づいてグループメンバーシップを照会できます。たとえば、RFC 2307bisが有効になっている場合、スキーマで定義されているRFC 2307bis属性に基づいてLDAP検索が行われます（このドキュメントの「RFC 2307bis」セクションを参照）。ユーザの追加グループが想定どおりに表示されない場合は、問題クライアントスキーマが正しく設定されていない可能性があります。詳細については、セクション「一般的な問題とトラブルシューティングの手順」を参照してください。

許可される補助GIDと補助GIDの数の増加

Remote Call（RPC；リモート手順コール）には、1つのNFS要求で処理できる補助GIDの最大数に特定の制限があります。の最大数 `AUTH_SYS/AUTH_UNIX` は16、`AUTH_GSS`（Kerberos）の最大数は32です。このプロトコル制限は、ONTAPだけでなく、多くのNFSサーバにも影響します。ONTAPでのNFSの制限を回避するには、次のNFSサーバオプションを使用します。

```
auth-sys-extended-groups
```

```
extended-groups-limit
```

また、LDAPクライアントスキーマを使用すると、RFC 2307bis（デフォルトは256、1、024）で使用できるグループを増やすことができます。

```
-maximum-groups-rfc2307bis
```

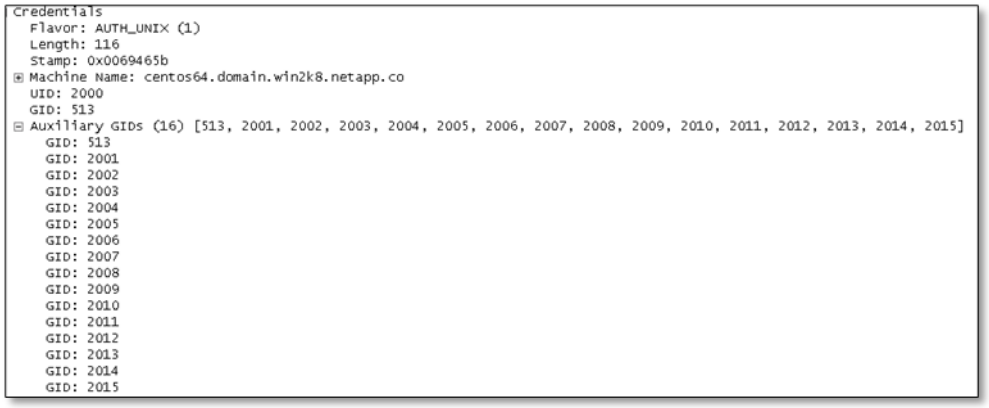
仕組み

グループ制限を拡張するオプションは `manage-gids`、他のNFSサーバのオプションと同じように機能します。基本的に、このオプションは、ユーザが属する補助GIDのリスト全体をダンプするのではなく、ファイルまたはフォルダでGIDの検索を実行し、代わりにその値を返します(図1)。

mountdのマニュアルページから、次の手順を実行します。

```
/.'\
```

図1）16個のGIDを持つRPCパケット



制限値16を超えるGIDは、プロトコルによってドロップされます。ONTAPの拡張GIDオプションを使用すると、新しいNFS要求を受信すると、ONTAPはユーザのグループメンバーシップに関する情報を要求します。拡張GIDは外部ネームサービスで使用できます。また、ユーザとグループが適切に設定されている場合は、クラスタでローカルに使用できます。ローカルファイルを使用する場合は `unix-group adduser(s)`、コマンドを使用して、ローカルUNIXユーザが複数のグループのメンバーであることを確認します。

```
COMMANDS
     adduser - Add a user to a local UNIX group

     addusers - Add a list of users to a local UNIX group
```

拡張GIDのパフォーマンスへの影響

グループを拡張しても、パフォーマンスへの影響は最小限に抑えられます。一般的には、1桁台の割合が低く抑えられます。メタデータNFSワークロードが大きいほど、特にシステムのキャッシュへの影響が大きくなる可能性があります。パフォーマンスは、ネームサービスサーバの速度とワークロードによっても影響を受けることがあります。ネームサービスサーバが過負荷になると応答が遅くなり、GIDのプリフェッチに遅延が発生します。

Active Directory LDAPデノカクチョウGIDニカンスルコウリョジコウ

Microsoft Active Directory LDAPサーバでは、`MaxPageSize` 属性はデフォルトの1、000に設定されます。この設定は、LDAPクエリで1、000を超えるグループが切り捨てられることを意味します。拡張グループに対して1、024の値が完全にサポートされる `MaxPageSize` ようにするには、1、024の値を反映するように属性を変更する必要があります。この値を変更する方法については、Microsoft TechNetの「Ntdsutil.exeを使用してActive DirectoryでLDAPポリシーを表示および設定する方法」を参照してください。

この値の変更について懸念がある場合は、Microsoftサポートに連絡して、TechNetライブラリの記事MaxPageSize Is Set Too Highを参照してください。

LDAP検索の識別名とスコープ

次のセクションでは、LDAPスキーマのアーキテクチャと、識別名（DNS）とスコープを使用した検索による検索の実行方法について説明します。

シキベツメイ

DNは、カンマで区切った一連の相対DNS（RDN）です。LDAPでは、基本的にフォルダ構造であり、ユーザ、グループ、マシンアカウント、ネットグループなどのオブジェクトのローカル性を指定します。

たとえば、Active Directoryでは、ドメイン自体をDNとして表すことができます。のドメインは `domain.netapp.com` のDNになり `dc=domain,dc=netapp,dc=com`ます。表1 に、DNSで使用される一般的なRDNタイプを示します。

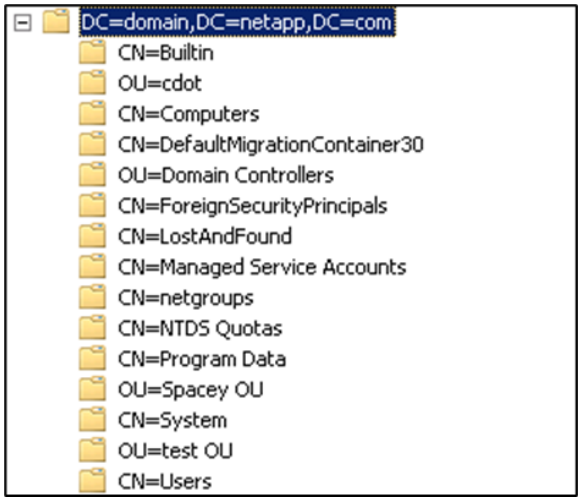
表1）LDAPの一般的なRDN値

文字列	属性タイプ
DC	`domainComponent`
CN	`commonName`
OU	`organizationalUnitName`
止	`organizationName`

ONTAP LDAPクライアント設定では、ベース、ユーザ、グループ、およびネットグループLDAP検索のDNを指定できます。

図2では、ADSI Editを使用してLDAP DNSのフォルダ構造を表示しています。

図2）LDAP DNフォルダ構造



DNを指定する理由

図2では、多数のフォルダにユーザ、グループ、ネットグループを含めることができます。のベースDN `dc=domain,dc=netapp,dc=com` がのドメインを表している場合は `domain.netapp.com`、LDAPクライアントがベースDNを使用するように指定されている可能性があります。ただし、すべてのクエリは、`dc=domain,dc=netapp,dc=com`検索範囲に応じて、以下にリストされている各DNをクロールする必要があります。そのため、ネームサービスや認証検索のレイテンシが増大し、原因認証の失敗、アクセスの問題、またはクライアント接続の問題が発生する可能性があります。この問題を回避するには、ネームサービスクエリをできるだけ早く返すことが重要です。ユーザ、グループ、およびネットグループ検索でDNSを指定すると、

LDAPサーバへの要求をフィルタリングすることで、必要な速度を達成できます。

たとえば、のDNにユーザが存在する場合、`cn=Users,dc=domain,dc=netapp,dc=com`のベースDNではなく、そのDNでユーザオブジェクトを検索するようにユーザDNクライアント設定フィールドを指定できます `dc=domain,dc=netapp,dc=com`。この設定により、ベースの下に存在する他のDNSを検索する必要がなくなります。このアプローチは、数百、場合によっては数千のDNSが存在する大規模な環境で特に重要です。

複数のDNS

オブジェクト検索に複数のDNSを指定できます。そのため、ユーザ、グループ、ネットグループはLDAPの複数の場所に存在していても、DNで検索をフィルタリングできます。複数のDNSを指定する場合は、エントリを二重引用符で囲みます。そうしないと、コマンドは失敗します。

```
cluster::*> ldap client modify -client-config DOMAIN -vserver SVM -user-dn
cn=users,dc=domain,dc=netapp,dc=com;OU=cdot,dc=domain,dc=netapp,dc=com
  (vserver services ldap client modify)

Error: "OU=cdot,dc=domain,dc=netapp,dc=com" is not a recognized command
```

注: DNSの間にセミコロン区切り文字が使用されていることを確認してください。カンマを使用して値を区切ると、クラスタはエントリを単一のDNとして認識します。

同じユーザ名を持つユーザが複数のDNSに存在し、数値UIDが異なる場合は、それらの数値UIDがLDAP環境の他の場所に存在しないかぎり、NFS検索は適切に機能します。

NFS数値IDの処理

NTFS ACLが関係していないかぎり、NFSv3では数値IDのみを使用してアクセスします。たとえば、ユーザがユーザ1234としてNFSv3マウントにアクセスし、基盤となる権限がUNIX形式である場合、すべてのONTAPが1234 UIDを使用してアクセスを許可または拒否します。

ただし、NFSv4.xではUIDから名前への解決方法が2つあります。デフォルトでは、NFSv4.xで `v4-numeric-ids` オプションを使用する場合と同様に、NFSv4.xでは数値IDが使用されます。

```
[-v4-numeric-ids {enabled|disabled}] - NFSv4 Support for Numeric Owner IDs
This optional parameter specifies whether to enable the support for numeric string identifiers in
NFSv4 owner attributes. The default setting is enabled at the time of creation.
```

また、NFSv4.xでID文字列を使用することもできます。この場合、数値IDはユーザ名に解決される必要があり、そのユーザ名はクライアントとサーバの同じドメインに存在する必要があります。たとえば、UID 1234は、などのユーザ名にマッピングする必要があります `user@DOMAIN.COM`。そうしないと、そのユーザは `nobody` クライアントのNFSv4.x構成ファイルで指定されたユーザに引き下げられます。ID文字列の解決を強制するには、`v4-numeric-ids` を無効にする必要があります。

同一のユーザ名と異なるUIDの例

たとえば、という名前のユーザが `v4user` クライアントマシン上およびLDAP内に2つの異なる数値UIDを持つローカルに存在する場合、ファイルの作成とアクセスの動作は `ns-switch`、構成（使用するUIDを制御）とNFSサーバの設定によって異なります。

が `ns-switch` クライアントで最初にLDAPを使用する場合、ユーザはユーザ情報用に保存されているLDAPになります。この例では、クライアントは `ns-switch` 次のようにユーザ解決用に設定されています。

```
passwd:     sss files
```

この設定は、users()passwdがLDAPを使用してからローカルファイルを使用することを意味します。これは、ユーザ名が同じでUIDが異なる複数のLDAPサーバの動作に似ています。

例のクライアントでは、v4user LDAPクライアントが無効でローカルファイルが使用されている場合は次のようになります。

```
# id v4user
uid=1005(v4user) gid=1005(v4user) groups=1005(v4user)
```

LDAPクライアントが実行されている場合、ユーザは次のように表示されます。

```
# id v4user
uid=877(v4user) gid=10000(Domain Users) groups=10000(Domain Users)
```

LDAPクライアントが実行されていないときにファイルが書き込まれると、UIDは1005になります。

```
-rwx------   1       1005       1005   23 Feb 3 16:38 v4user_file
```

LDAPクライアントの実行中にファイルが書き込まれると、ユーザ名がすべてのファイルで同一であっても、UIDは877になります。

```
-rwx------   1        877      10000   22 Feb 3 16:39 v4user_file3

# ls -la | grep v4user
-rwx------   1 v4user               v4user                   23 Feb 3 16:38 v4user_file
-rwx------   1 v4user               v4user                   26 Feb 3 16:19 v4user_file2
-rwx------   1 v4user               Domain Users             22 Feb 3 16:39 v4user_file3
-rwx------   1 v4user               Domain Users              0 Feb 3 10:34 v4user_file4

# ls -lan | grep v4user
-rwx --------1       1005       1005   23 Feb 3 16:38 v4user_file
-rwx --------1       1005       1005   26 Feb 3 16:19 v4user_file2
-rwx --------1        877      10000   22 Feb 3 16:39 v4user_file3
-rwx --------1        877      10000    0 Feb 3 10:34 v4user_file4
```

v4-numeric-ids NFSサーバでこのオプションを無効にすると、LDAPで解決できるユーザだけが正しく表示されます。クライアントが両方のユーザについて認識しているにもかかわらず、ONTAPがNFSv4.xアクセスの変換方法を認識しているのは、このユーザだけです。

```
cluster::*> nfs server show -vserver DEMO -fields v4-numeric-ids
vserver v4-numeric-ids
---------- ------------------
DEMO    disabled

sh-4.2$ ls -la | grep v4user
-rwx------   1 nobody               nobody         23 Feb  3 16:38 v4user_file
-rwx------   1 nobody               nobody         26 Feb  3 16:19 v4user_file2
-rwx------   1 v4user               Domain Users   22 Feb  3 16:39 v4user_file3
-rwx------   1 v4user               Domain Users    0 Feb  3 10:34 v4user_file4

sh-4.2$ ls -lan | grep v4user
-rwx------   1   99    99   23 Feb 3 16:38 v4user_file
-rwx------   1   99    99   26 Feb 3 16:19 v4user_file2
-rwx------   1  877 10000   22 Feb 3 16:39 v4user_file3
-rwx------   1  877 10000    0 Feb 3 10:34 v4user_file4
```

同じ名前でUIDが異なる複数のユーザ名を持つ問題は、アクセスに影響します。アクセスは、ユーザ名ではなく、UIDの権限によって異なります。基盤となるUIDが異なるためにクライアントに同じユーザ名が表示されることがありますが、アクセスが拒否される可能性があります。

次の例ではv4user、UID 1005()の所有権がに設定されてい v4user_fileます。他のユーザやグループはそのファイルにアクセスできません。

```
-rwx------   1       1005       1005   23 Feb 3 16:38 v4user_file
```

ただし、NFSマウントにアクセスするユーザは、実際にはUID 877です。

```
sh-4.2$ id
uid=877(v4user) gid=10000(Domain Users) groups=10000(Domain Users)
```

その結果、v4user（877）は v4user（1005）と同じではないため、1005が所有するファイルへのアクセスは拒否されます。

```
sh-4.2$ cat v4user_file
cat: v4user_file: Permission denied
```

このユーザはUID 877であるため、v4user_file3 所有者も877であるため、へのアクセスは成功します。

```
-rwx --------1        877      10000   22 Feb 3 16:39 v4user_file3

sh-4.2$ cat v4user_file3
This is the LDAP user
```

アクセスに関する混乱を防ぐために、v4-numeric-ids ファイルが所有者として表示されるようにするには、を無効にし nobodyます。ただし、最終的には、複数のDNSを使用して予測可能なアクセス権限を実現する場合は、すべてのUIDとユーザ名が一意であることを確認してください。

ケンサクスコオト

DNSに加えて、LDAPクエリの検索範囲も指定できます。スコープはLDAPクエリの開始点であり、検索を実行するベースDNからの深度を示します。 ONTAPのLDAPクエリで有効な検索範囲は base、subtree、および onelevelです。

ベース

base 検索範囲は、指定したベースDNに対してのみLDAP検索を実行することを示します。

たとえば、ユーザDNがに設定され cn=users,dc=domain,dc=netapp,dc=com、ベース検索範囲が指定されている場合、LDAP検索はに対してのみ実行され cn=users,dc=domain,dc=netapp,dc=comます。DN内のオブジェクトは含まれません。baseは非常にリテラルな検索範囲であるため、NetAppでは推奨していません。

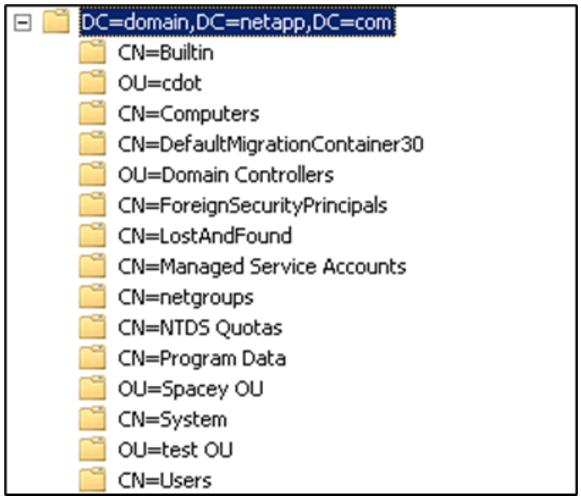
サブツリー

subtree 検索範囲は、指定されたDNより下のすべてのレベルを検索します。

たとえば、ユーザDNがに設定され cn=users,dc=domain,dc=netapp,dc=com、サブツリー検索範囲が指定されている場合、以下のすべてのオブジェクトに対してLDAP検索が実行されます。cn=users,dc=domain,dc=netapp,dc=com（他のコンテナを含む）。NetAppでは、ほとんどの場合、検索範囲としてサブツリーを推奨します。ただし、指定したDNが効果的にフィルタリングするのに十分なレベルになっている必要があります。

図3では 、のDNの dc=domain,dc=netapp,dc=com 下に複数のコンテナがあります。の検索範囲が subtree 使用されている場合、LDAPクエリは以下の各DNを検索します。「dc=domain,dc=netapp,dc=com」DNは subtree、などの検索でより詳細なレベルで指定することもできます cn=users,dc=domain,dc=netapp,dc=com。

図3）LDAP DNコンテナ



ワンレベル

onelevel 検索範囲では、DN自体も含めて、指定されたDNの1つ下のレベルでのみ検索されますが、その1つ下のレベルのエントリは検索されません。

たとえば、ユーザDNがに設定され cn=users,dc=domain,dc=netapp,dc=com、1つのレベルの検索範囲が指定されている場合、LDAP検索は1つ下のレベルのDNSでのみ実行されます。
「cn=users,dc=domain,dc=netapp,dc=com」

```
cluster::*> ldap client modify -client-config DOMAIN -vserver SVM -user-dn
"cn=users,dc=domain,dc=netapp,dc=com" -user-scope onelevel
  (vserver services ldap client modify)
```

ONTAP 8.3以降のバージョンでは、次のコマンドを使用してadvanced権限でユーザIDを照会できます。

```
cluster::*> getxxbyyy getpwbyname -vserver DEMO -username prof1 -node node1
  (vserver services name-service getxxbyyy getpwbyname)
pw_name: prof1
pw_passwd:
pw_uid: 1100
pw_gid: 1101
pw_gecos:
pw_dir:
pw_shell:
```

ONTAP 9.6以降では、次のコマンドも使用できます。

```
cluster::*> access-check authentication translate -vserver DEMO -unix-user-name prof1
```

DNがより高いレベルに設定されている場合、検索は失敗します。

```
cluster::*> ldap client modify -client-config DOMAIN -vserver SVM -user-dn
"dc=domain,dc=netapp,dc=com" -user-scope onelevel
  (vserver services ldap client modify)

cluster::*> access-check authentication translate -vserver DEMO -unix-user-name prof1

Vserver: SVM (internal ID: 3)

Error: Acquire UNIX credentials procedure failed
  [ 0 ms] Name 'prof1' not found in UNIX authorization source
            LOCAL
  [     0] Connecting to LDAP (NIS & Name Mapping) server
```

```
            10.x.x.x
  [     5] Using a new connection to 10.x.x.x
  [     7] Name 'prof1' not found in UNIX authorization source
            LDAP
  [     7] Could not get a user ID for name 'prof1' using any
            NS-SWITCH authorization source
**[     7] FAILURE: Unable to retrieve UID for UNIX user prof1

Error: command failed: Failed to resolve user name to a UNIX ID. Reason: "SecD Error: object not
found".
```

非常に細かいレベルでフィルタリングする場合は `onelevel`、検索範囲が最適です。ただし、正しいDNSが指定されていない場合、`onelevel` 検索スコープを使用するとルックアップが失敗する可能性があります。

Centrifyの統合と考慮事項

Windows 2016以降を実行するWindows Active Directory LDAPサーバでは、[プロパティ]ダイアログボックスの[UNIX属性]タブが廃止されました。推奨される方法は、Windows PowerShellまたはActive Directory Users and Computers GUIからの高度な属性管理です。

多くのユーザーがいる大規模な環境の管理は煩雑になる可能性があるため、Centrifyなどのサードパーティ製品では、アイデンティティ管理に対する単一コンソールのアプローチを提供することで、Windowsクライアントと Linuxクライアント間のユーザー認証を簡素化しようとしています。

ONTAPは、RFC 2307標準に準拠している限り、任意のLDAPプロバイダーと完全に互換性があります。

CentrifyなどのサードパーティLDAPプロバイダでONTAPを使用するには、LDAP管理者に問い合わせて、LDAPサーバがスキーマ内でユーザ、グループ、ネットグループ、およびグループメンバーシップをどのように表示するかに関する情報を取得する必要があります。たとえば、一部のLDAPプロバイダは `uid` ユーザ名にを使用し、他のプロバイダは `uid` ユーザの数値IDを示すためにを使用します。場合によっては、LDAPプロバイダ間でオブジェクトクラスが大きく異なることがあります。ONTAPをLDAPクライアントとして設定する前に、ユーザの次のスキーマ属性を確認しておく必要があります。

- ユーザーオブジェクトクラス
- ユウサメイ
- 数値UID
- プライマリGID
- ホーム ディレクトリ
- UNIXパスワード
- ジェコス

グループおよびグループメンバーシップについて、次の情報を入手する必要があります。

- グループオブジェクトクラス
- 数値GID
- グループ名
- `memberUid` がグループメンバーシップに対して設定されているかどうか
- LDAPサーバがグループメンバーシップにRFC 2307bisを使用しているかどうか（Active Directoryで実行可能）

Windows Active Directoryの場合、PowerShellを使用してLDAPユーザおよびグループにこれらの属性を照会できます。

UNIX LDAPサーバの場合は、などのユーティリティを使用できます `ldapsearch`。

必要な情報を収集したら、このドキュメントの「カスタムLDAPスキーマの作成」セクションの手順に従って、Centrify LDAPルックアップを構成するカスタムスキーマを作成します。

LDAPリファーラル（チェイスリファーラル）

LDAPリファーラルを使用すると、ONTAPでUNIXユーザとグループが複数のLDAPサーバに存在する環境をサポートできます。LDAPリファーラルが無効（デフォルト）の場合、ONTAPはLDAPサーバでユーザを検索します。そのユーザがLDAPサーバに存在しない場合は、クエリが実行され、検索が失敗します。

LDAPリファーラルが有効（`-referral-enabled true`）で複数のLDAPサーバがリストされている場合、最初のLDAPサーバでユーザが見つからないと、リスト内の他のLDAPサーバに対してリファーラルが発行され、ユーザが存在するかどうかが確認されます。LDAPクエリは、これらの追加の検索の実行に時間がかかります。また、必要な追加時間は、ネットワークの遅延、LDAPスキーマのサイズ、指定されたLDAPサーバの数によって異なります。LDAPリファーラルを有効にして検索がタイムアウトする場合は、`-query- timeout` オプションを使用してLDAPクエリタイムアウトをデフォルトの3秒から最大10秒に増やすことができます。

ONTAP 9.8以前でLDAP over StartTLS/LDAPSが使用されている場合、LDAPリファーラルはサポートされません。ONTAP 9.9.1では、セキュアチェイスリファーラルのサポートが追加されました。

構成

このセクションでは、NetApp ONTAPのLDAPクライアント設定についてのみ説明します。NFSクライアントのLDAP設定については、クライアントのドキュメントを参照してください。LDAPサーバの設定については、使用しているLDAPサーバのマニュアルを参照してください。

ONTAP System Managerの設定サポートはほとんどがデフォルトのスキーマに限定されており、一部の設定値が欠落しています。また、主にMicrosoft Active Directory LDAPの設定に焦点を当てているため、このTRではCLIの設定についてのみ説明します。

LDAPの設定は、一般に次の手順で行います。

1. 構成情報（サーバのIPアドレスと名前、LDAPスキーマ情報、バインド情報など）を収集します。
2. LDAPスキーマを選択または作成します。
3. LDAPクライアント設定を作成します。
4. LDAP設定を作成します。
5. `ns-switch` LDAPを使用するように変更します。
6. LDAPをテストします。

LDAP環境情報：事前設定

ONTAPをLDAPクライアントとして設定する前に、すべての設定を容易にするためにいくつかの情報を収集する必要があります。

開始する前に

本番環境のSVMにLDAPを導入する前に、新しいテスト用SVMを作成してLDAP設定を正確に取得し、本番環境のSVMに導入することを推奨します。本番環境にLDAPクライアント設定を導入しようとすると、LDAPが正常に動作していないとユーザ認証が失敗するリスクがあります。

新しいテスト用SVMに必要なのは、本番環境と同じLDAPサーバにアクセスできるデータLIFだけです。

成功基準は、管理者が生成したLDAP呼び出しに基づきます。この呼び出しについては、「LDAP機能のテスト」を参照してください。

LDAPセキュリティの決定事項

LDAP接続では、バインドとLDAP検索に暗号化を使用できます。ONTAPには、LDAP接続を保護するためのオプションがいくつか用意されています。

- CIFS/SMBサーバとしてバインド（CIFS/SMBマシンアカウントを使用してNT LAN Manager [NTLM]またはKerberosを介してバインド）
- SMBの署名と封印（LDAPにWindows Active Directoryを使用する場合）
- STARTTLSまたはLDAP over SSL（一度に有効にできるのは1つだけ）

使用されているセキュリティ方法を確認するには、LDAP管理者と連携することが重要です。LDAPのセキュリティが適用されることがあるため、ONTAPのLDAPクライアント設定では、単にLDAPを動作させるために、提供されたセキュリティ方式を使用する必要があります。

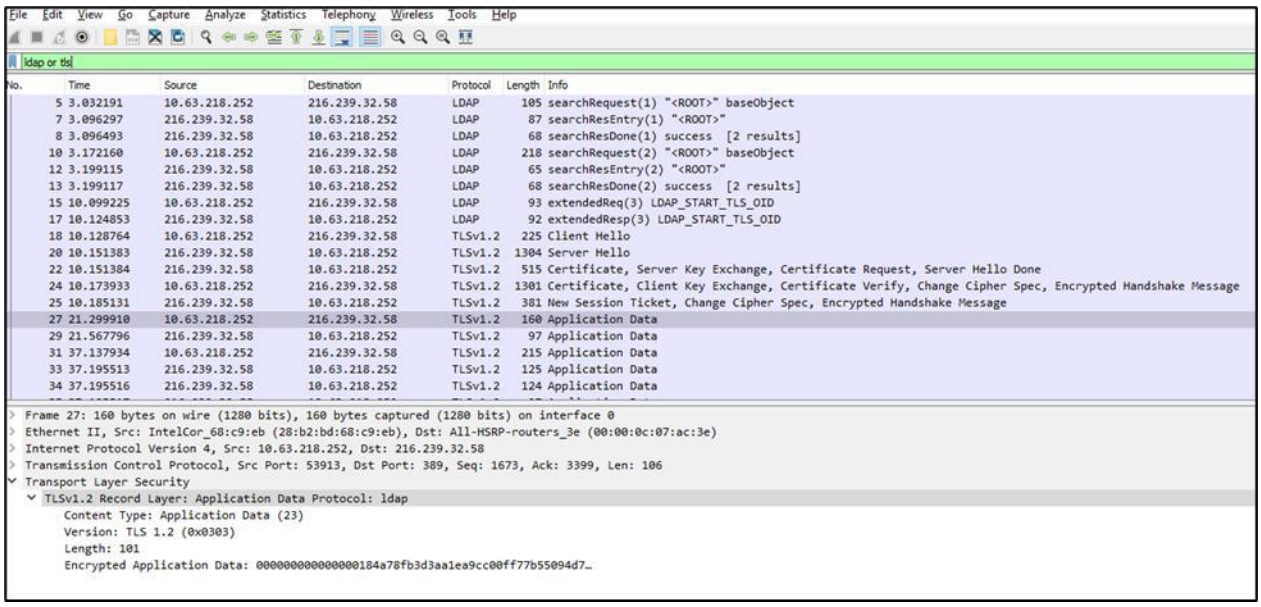
ONTAP for LDAPでのLDAP over SSLまたはStartTLSの設定については、「セキュアなLDAPの設定」を参照してください。

Transport Layer SecurityとLDAP over SSLの比較を開始する

ONTAPは、ポート636を使用するLDAP over SSL（LDAPS）と、Start Transport Layer Security（StartTLS）（ポート389）を使用するLDAPの両方を提供します。LDAPSはこの時点でレガシーと見なされており、RFC 1777は1995年に公開されている。LDAP over StartTLSは 2000年にRFC 2830で導入され、2006年にRFC 4511でLDAPv3標準に統合された。StartTLSが標準化されると、LDAPベンダーはLDAPSを廃止と呼び始めました。

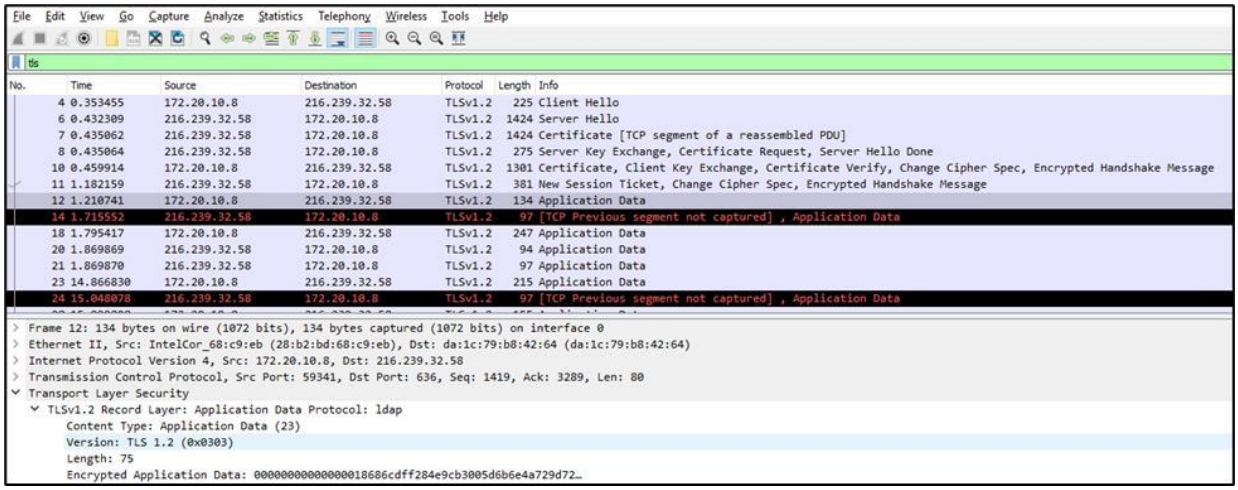
元々 ONTAPではLDAP暗号化でStartTLSのみがサポートされていましたが、ONTAP 9.5以降のバージョンではLDAPSの利用が一般的になりました。通常、StartTLSではプレーンテキストの有名なLDAPポート389が使用されていても、StartTLS（Windows Active Directoryを使用する場合はLDAPの署名と封印）をLDAP暗号化として使用します。StartTLSでは、最初のLDAP接続が確立されると、StartTLS OIDが交換され、証明書が比較され、すべてのトラフィックがTLSを使用して暗号化されます。図4に示すパケットキャプチャは、LDAPバインド、StartTLSハンドシェイク、およびそれに続くTLSで暗号化されたLDAPトラフィックを示しています。

図4）StartTLS LDAPトラフィックのパケットトレース



LDAPSは証明書交換も使用し、TLSを使用して暗号化します。トレースには、ポート636経由のトラフィックのみが表示されます。図5 に、LDAPSカンバセーションからのパケットキャプチャのトラフィックを示します。

図5）LDAPSトラフィックのパケットトレース



LDAPSとStartTLSには、主に次の2つの違いがあります。

- STARTTLSはLDAP標準に含まれていますが、LDAPSは含まれていません。そのため、LDAPライブラリのサポートが異なる場合や、機能がすべてのケースで機能する場合としない場合があります。
- 暗号化に失敗した場合、StartTLSでは設定を通常のLDAPにフォールバックできます。LDAPSではサポートされません。そのため、StartTLSは柔軟性と耐障害性を備えていますが、設定を誤るとセキュリティリスクも発生します。

ほとんどの場合、StartTLSまたはLDAPSの選択は優先事項ですが、完全な標準準拠のために、NetAppではStartTLSを推奨しています。

注： ONTAP LDAPクライアントでは、LDAPS（`-use- start-tls true`でポート636を設定）またはStartTLS（およびポート389を設定）のみを設定できます。両方を同時に有効にすることはできません。

StartTLSを使用する場合のセキュリティに関する考慮事項

STARTTLSを使用すると、管理者は必要に応じて通常のLDAPトラフィックにフォールバックできますが、セキュリティ上の理由から、ほとんどのLDAP管理者はこのトラフィックを許可したくありません。NetAppでは、StartTLSを保護してLDAP通信を保護するために、次のことを推奨しています。

- StartTLSが有効になっていて、証明書が設定されていることを確認します。
- 内部環境では自己署名証明書を使用できますが、外部LDAPでは認証局を使用します。証明書の詳細については、Microsoft TechNetの「自己署名SSLと認証局の違い」を参照してください。
- StartTLSを使用しないLDAPクエリとバインドを禁止します。LDAPサーバベンダーが提供するLDAPサーバの設定手順に従います。
- ONTAPのLDAPクライアントで最小バインドレベル（`-min- bind-level`）をSASLに設定して、LDAPクライアントがプレーンテキストクレデンシャルを送信できないように制限します。

Microsoft LDAPチャネルバインドの要件

Windows Active Directoryドメインコントローラに関する脆弱性のため、ONTAPとのLDAP通信に影響を与える可能性のあるWindowsサーバのデフォルト設定が変更されています。詳細については、Microsoft Security Advisory ADV190023を参照してください。

基本的に、Microsoft Windowsは、管理者がLDAP署名とチャネルバインディングを有効にすることを推奨し始めます。LDAPクライアントがチャネルバインディングトークンとLDAP署名をサポートしている場合は、チャネルバインディングと署名が必要になり、新しいMicrosoftパッチによってレジストリオプションが設定されます。

ONTAPへの影響

ONTAPへの影響は、他のLDAPクライアントと同じです。クライアントがサポートするものには、それらのものが必要になります。セキュリティ設定がサポートされていない場合は、変更は必要ありません。ただし、ONTAPの場合、次の2つのことを意味します。

- ONTAPは現在チャネルバインディングをサポートしていないため、変更は必要ありません。
- ONTAPはLDAP署名をサポートしています。そのため、パッチをWindowsに適用するときにLDAP署名が有効になっていないと、SMBとLDAP UNIX ID管理の両方でONTAP LDAP通信が失敗します。

修正手順

Windowsパッチの適用後にLDAP署名要件をに明示的に設定した場合は、`off`修正は必要ありません。パッチによって明示的な変更が上書きされることはありません。ただし、このオプションを一度も設定していない場合は、パッチによってオプションがに変更され `on`ます。CIFS / SMBを使用しているONTAP場合は、ONTAP 9.8よりも前のバージョンでこれらの変更を管理できるように、CIFS / SMBサーバオプション `-session-security-for-ad-ldap` をに設定する必要があります `sign`。UNIXのユーザおよびグループ検索にLDAPとActive Directoryを使用する場合は、StartTLS（`-use-start-tls`）、LDAPS（ポート636と証明書）、またはLDAPの署名と封印（`-session-security sign`）も使用する必要があります。

注： ONTAP 9.8では、バグ1289739がユーザ操作なしでこの問題に対処しています。

詳細については、NetAppナレッジベースの記事「Microsoftセキュリティアドバイザリ ADV190023 for Remote Authentication Using LDAP」の影響を参照してください。

DNS

LDAPサーバでは、特にActive Directoryを使用している場合にDNSが使用されることがよくあります。

LDAP用にSVMを設定する前に、LDAPサーバとサービスのレコードを含むDNS設定を作成する必要があります。DNS呼び出しでは、SVM内の少なくとも1つのデータLIFまたはSVM管理LIFがDNSサーバにアクセスできる必要があります。

この設定はSVMレベルで実行されます。

```
cluster::> dns create ?
   [-vserver] <vserver name>          Vserver
   [-domains] <text>, ...             Domains
   [-name-servers] <IP Address>, ... Name Servers
  [[-timeout] {1..5}]                 Timeout (secs) (default: 2)
  [ -attempts {1..4} ]                Maximum Attempts (default: 1)
  [ -skip-config-validation [true] ] Skip Configuration Validation
```

DNSが機能しているかどうかをテストする方法については、「トラブルシューティングツール」を参照してください。

LDAPサーバ情報

収集する必要があるLDAPサーバ情報は次のとおりです。

- LDAPサーバのタイプ（Windows Active Directory、Red Hatなど）
- LDAPサーバのIPアドレス、ホスト名、またはActive Directoryドメイン
- DNおよび範囲情報の検索
- LDAPのDNS SRVレコード情報
- LDAPサーバがロードバランサ/ネットワークアドレス変換（NAT）アドレスの背後にあるかどうか
- LDAPサーバ ポート
- バインドのLDAPサーバセキュリティレベル（anonymous、simple、またはsasl）
- LDAP over SSLが使用されているかどうか

- チェイスリファーラルが使用されているかどうか（リファーラルの詳細については、RFC 4511を参照）

LDAPスキーマ設定

ONTAPでSVMをLDAPクライアントとして設定する前に、スキーマを選択して設定する必要があります。前述したように、ONTAPにはいくつかのデフォルトスキーマテンプレートが用意されています。表2は 、使用するスキーマテンプレートのガイダンスとして使用できます。通常はデフォルト値を使用できます。バリエーションがある場合は、これらのスキーマテンプレートをカスタムLDAPスキーマにコピーし、必要な特定の属性を変更することで、それらのスキーマテンプレートを開始点として使用できます。

注: これらのスキーマテンプレートはほとんどの場合適用されますが、CentrifyやQuestなどのサードパーティのLDAP管理ツールでは異なる場合があります。

表2）ONTAP LDAPスキーマテンプレートと対応するLDAPサーバ

LDAPスキーマ	LDAPサーバのサポート
AD-SFU	Windows 2003以前
AD-IDMU	Windows 2003 R2以降
MS-AD-BIS	Windows 2003 R2以降 （詳細については、「RFC 2307bis」を参照してください）。
RFC 2307	ほとんどのUNIX/Linuxベースの LDAPサーバ （Red HatやAppleなど）

スキーマを選択する前に、使用されているLDAPスキーマ属性がONTAPが提供するスキーマと一致するかどうかを確認します。確認のために、LDAP環境を管理しているチームへの連絡が必要になる場合があります。`ldapsearch` コマンド（ユーザとグループの出力をダンプして属性を表示）またはPowerShell（Microsoft Active Directoryを使用している場合）を使用して、スキーマを照会することもできます。詳細については、LDAP管理者にお問い合わせください。

`ldapsearch` ユーザ情報をダンプする例を次に示します。

一般的なLDAP検索の例

ユーザまたはグループの情報をダンプするPowerShellコマンドの例：

```
C:\> Get-ADUser -Identity [username] -Properties *
C:\> Get-ADGroup -Identity [groupname] -Properties *
```

属性とオブジェクトクラス

LDAPスキーマ出力では、属性とオブジェクトクラスの2種類の値を指定できます。

オブジェクトクラスは、LDAPクエリが特定のオブジェクトを検索する方法です。たとえば、ユーザーオブジェクトを検索する場合、定義されたオブジェクトクラスは、そのクラス内のすべてのオブジェクトを検索するようにクエリに指示します。

属性は、各オブジェクトを一意にする実際のオブジェクトの値です。

たとえば、複数のユーザが同じオブジェクトクラスに属していても、各ユーザに一意の名前と数値のUIDが割り当てられているとします。

LDAPクエリの出力から、使用する適切なLDAPスキーマを選択できます。オブジェクトクラスは、使用しているLDAPサーバによって異なります。表3を参照してください。

表3）LDAPスキーマオブジェクトクラス

Value	LDAPスキーマオブジェクトクラス（LDAPスキーマタイプ）
`User/posixAccount` オブジェクトクラス	`User`（Active Directory）* `posixAccount`（RFC 2307）*

Value	LDAPスキーマオブジェクトクラス（LDAPスキーマタイプ）
Group/posixGroup オブジェクトクラス	Group（Active Directory）* posixGroup（RFC 2307）*
NIS netgroupオブジェクトクラス	nisNetgroup（すべてのデフォルトスキーマ）*
groupOfUniqueNames オブジェクトクラス	groupOfUniqueNames（RFC 2307）* Group（Active Directory）*
windowsToUnix ネームマッピングオブジェクトクラス	posixAccount（RFC 2307）* ユーザ（Active Directory）*
NISオブジェクトクラス	nisObject（すべてのデフォルトスキーマ）*

*優先値またはデフォルト値。

最も重要な属性値を表4に示します。

表4）LDAPスキーマ属性

Value	LDAPスキーマ属性（LDAPスキーマタイプ）
ユーザ名	UID（すべてのデフォルトスキーマ）* Name（Active Directory） GivenName（Active Directory） sAMAccountName（Active Directory）
グループ名	CN（すべてのデフォルトスキーマ）* Name（Active Directory） sAMAccountName（Active Directory）
数値UID	uidNumber（すべてのデフォルトスキーマ）*
数値GID	uidNumber（すべてのデフォルトスキーマ）*
ホーム ディレクトリ	homeDirectory（RFC 2307）* unixHomeDirectory（Active Directory）*
グループ メンバーシップ	memberUid（RFC 2307）* memberUid（Active Directory 2008以前） Member（Active Directory 2008 R2以降）* UniqueMember（RFC 2307bis）*
WindowsからUNIXへのネームマッピング（非対称ネームマッピング用）	sAMAccountName（Active Directory）* windowsAccount（RFC 2307）*
NISマップ名	nisMapName（すべてのデフォルトスキーマ）*
NISマップエントリ	nisMapEntry（すべてのデフォルトスキーマ）*
NISネットグループトリプル	nisNetgroupTriple（すべてのデフォルトスキーマ）*
NISネットグループメンバー	memberNisNetgroup（すべてのデフォルトスキーマ）*

*優先値またはデフォルト値。

LDAPカンキヨウセツテイ

これで必要な情報を収集できました。次に、LDAP設定の作成を開始します。一部の手順は他の手順に依存するため、特定の順序に従う必要があります。通常は、次の順序に従ってください。

1. LDAPクライアントスキーマを選択、作成、または設定します。

2. SVM用のLDAPクライアント設定を作成します。
3. SVMで使用するLDAPを有効にします。
4. `ns-switch` LDAPを使用するように変更します。
5. LDAP検索をテストする。

LDAPスキイマ

まず、LDAPスキーマが必要です。これは、作成時にLDAPクライアント設定にスキーマが必要になるためです。スキーマを選択する前に適切な情報が収集されていることを確認するには、このレポートの「LDAPスキーマ構成」セクションを参照してください。

LDAPスキーマを選択してください

適切なLDAPスキーマを特定したら、ONTAPのLDAPスキーマテンプレートをLDAPサーバ環境のものと比較して比較できます。

注： LDAPスキーマテンプレートの例については、本レポートの付録の「LDAPスキーマテンプレート」を参照してください。

使用可能なスキーマテンプレートに必要なものがある場合は、LDAPクライアント設定手順に進みます。よりカスタマイズされたLDAPスキーマが必要な場合は、必要なスキーマに最も近いLDAPスキーマテンプレートを選択し、次のセクション「カスタムLDAPスキーマの作成」に進みます。

カスタムLDAPスキーマの作成

デフォルトテンプレートは読み取り専用であるため、使用可能なデフォルトテンプレートに存在しないLDAPスキーマを使用する必要がある場合は、新しい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には、テンプレートから新しいLDAPクライアントスキーマにスキーマをコピーします。

変更およびカスタマイズのためにLDAPスキーマテンプレートを新しいLDAPスキーマにコピーするには、次のコマンドを使用します。

```
cluster::*> ldap client schema copy ?
  [ -vserver <vserver name> ]              *Vserver
   [-schema] <text (size 1..32)>           *Schema Template
   [-new-schema-name] <text (size 1..32)> *New Schema Template Name
```

を使用する新しいスキーマを作成したら、ldap client schema modifyコマンドを使用して変更を加えることができます。

```
cluster::*> ldap client schema modify ?
  [ -vserver <vserver name> ]                         Vserver (default: cluster)
   [-schema] <text (size 1..32)>                      Schema Template
  [[-comment] <text>]                                 Comment
  [ -posix-account-object-class <text> ]              RFC 2307 posixAccount Object Class
  [ -posix-group-object-class <text> ]                RFC 2307 posixGroup Object Class
  [ -nis-netgroup-object-class <text> ]               RFC 2307 nisNetgroup Object Class
  [ -uid-attribute <text> ]                           RFC 2307 uid Attribute
  [ -uid-number-attribute <text> ]                    RFC 2307 uidNumber Attribute
  [ -gid-number-attribute <text> ]                    RFC 2307 gidNumber Attribute
  [ -cn-group-attribute <text> ]                      RFC 2307 cn (for Groups) Attribute
  [ -cn-netgroup-attribute <text> ]                   RFC 2307 cn (for Netgroups) Attribute
  [ -user-password-attribute <text> ]                 RFC 2307 userPassword Attribute
  [ -gecos-attribute <text> ]                         RFC 2307 gecos Attribute
  [ -home-directory-attribute <text> ]                RFC 2307 homeDirectory Attribute
  [ -login-shell-attribute <text> ]                   RFC 2307 loginShell Attribute
  [ -member-uid-attribute <text> ]                    RFC 2307 memberUid Attribute
  [ -member-nis-netgroup-attribute <text> ]           RFC 2307 memberNisNetgroup Attribute
  [ -nis-netgroup-triple-attribute <text> ]           RFC 2307 nisNetgroupTriple Attribute
  [ -enable-rfc2307bis {true|false} ]                 Enable Support for Draft RFC 2307bis
  [ -group-of-unique-names-object-class <text> ]      RFC 2307bis groupOfUniqueNames Object Class
  [ -unique-member-attribute <text> ]                 RFC 2307bis uniqueMember Attribute
  [ -windows-to-unix-object-class <text> ]     Data ONTAP Name Mapping windowsToUnix Object Class
```

```
  [ -windows-account-attribute <text> ]        Data ONTAP Name Mapping windowsAccount Attribute
  [ -windows-to-unix-attribute <text> ]        Data ONTAP Name Mapping windowsToUnix Attribute
  [ -windows-to-unix-no-domain-prefix {true|false} ]
                                               No Domain Prefix for windowsToUnix Name Mapping
  [ -maximum-groups-rfc2307bis {1..1024} ]     *Maximum groups supported when RFC 2307bis enabled
  [ -nis-object-class <text> ]                        RFC 2307 nisObject Object Class
  [ -nis-mapname-attribute <text> ]                   RFC 2307 nisMapName Attribute
  [ -nis-mapentry-attribute <text> ]                  RFC 2307 nisMapEntry Attribute
```

注: ほとんどの場合、カスタムスキーマは必要ありません。で始まるデフォルトのスキーマを使用できます。

LDAPクライアント設定

で使用できる有効なLDAPスキーマが作成されたので、LDAPクライアント設定を作成できます。この設定では、LDAPサーバの接続と照会に必要なパラメータを定義します。ONTAP SVMのクライアント設定を構築するには、本レポートの「LDAPサーバ情報」セクションで収集したデータを使用します。

表5 に、diag権限で変更するためのLDAPクライアント設定オプションを示します。

表5）LDAPクライアント設定オプション（diag権限）

設定オプション	意味
-vserver	LDAP設定を所有するSVMを指定してください。
-client-config	このオプションは、クライアント設定の名前です。
-ldap-servers	このオプションは、LDAPサーバまたはホスト名のリストです。Microsoft Active Directory LDAPを使用する場合はad-domain、代わりに-を使用します。
-servers (deprecated)	-ldap-servers 代わりにを使用します。
-ad-domain	このオプションは、LDAPサーバの検索と名前解決に使用するActive Directoryドメインを定義します。このオプションを指定すると、ONTAPはActive Directory LDAPサーバのDNS SRVレコード検索を使用します。Linux/UNIX LDAPサーバを使用する場合は、を使用し -ldap-servers ます。 Active Directoryで使用するLDAPサーバを指定する場合は -preferred-ad-servers、に加えてを使用します -ad-domain。
-bind-as-cifs-server	このオプションは、SVMにCIFS / SMBサーバがある場合にのみ使用します。CIFSサーバとしてバインドすると、LDAP検索では、CIFS / SMBマシンアカウントのクレデンシャルを使用してActive Directoryにログインし、LDAPクエリを実行します。
-schema	このオプションは、使用するLDAPスキーマを定義します。
-port	このオプションを使用すると、LDAPポートを変更できます。LDAPのデフォルトは389です。LDAPSの場合、ポートは636です。Active Directory LDAPでグローバルカタログ検索を行う場合は、ポート3268を使用します。
-query-timeout	このオプションは、クエリがタイムアウトするまでの時間を定義します。デフォルトは3秒です
-min-bind-level	このオプションは、LDAPバインドに許可される最小バインドセキュリティを定義します。
-bind-dn	このオプションは、LDAPバインド/ログインに使用するユーザを定義します。形式は次のとおりです。 • Username • Username@domain.com（Active Directory） • DOMAIN\username（Active Directory） • DN=username,DN=domain,DN=com

設定オプション	意味
-base-dn	このオプションは、LDAPクエリのベース検索DNを定義します。を使用する場合は-ad-domain、自動的にActive DirectoryドメインDNに設定されます。たとえば、が domain.com ベースになり DN DC=domain,DC=comます。
-base-scope	このオプションは、ベース検索範囲を定義します。デフォルトはです subtree。
-user-dn	このオプションは User、オブジェクトクラスの検索DNを定義します。クエリを高速化するためにフィルタリングが必要な場合は、このオプションを使用します。このオプションを空白のままにすると、ONTAPはベース検索DNを使用します。
-user-scope	このオプションは User、オブジェクトクラスの検索範囲を定義します。デフォルトはです subtree。
-group-dn	このオプションは Group、オブジェクトクラスの検索DNを定義します。クエリを高速化するためにフィルタリングが必要な場合は、このオプションを使用します。このオプションを空白のままにすると、ONTAPはベース検索DNを使用します。
-group-scope	このオプションは Group、オブジェクトクラスの検索範囲を定義します。デフォルトはです subtree。
-netgroup-dn	このオプションは Netgroup、オブジェクトクラスの検索DNを定義します。クエリを高速化するためにフィルタリングが必要な場合は、このオプションを使用します。このオプションを空白のままにすると、ONTAPはベース検索DNを使用します。
-netgroup-scope	このオプションは Netgroup、オブジェクトクラスの検索範囲を定義します。デフォルトはです subtree。
-use-start-tls	このオプションは start-tls、がLDAPのセキュリティ保護に使用されるかどうかを定義します。STARTTLSはポート389を使用し、LDAP over SSL（LDAPS）では**ありません**。LDAPSの場合は、LDAPポートを636に変更します。
-is-netgroup-byhost-enabled	このオプションは、ネットグループをネットグループ名で照会する falseか（に設定）、ホスト名で照会するか（に設定）trueを定義します。詳細については、本ドキュメントの「ネットグループをホストするためのLDAPの使用」を参照してください。
-netgroup-byhost-dn	このオプションは Netgroup-by-host、オブジェクトクラスの検索DNを定義します。クエリを高速化するためにフィルタリングが必要な場合は、このオプションを使用します。このオプションを空白のままにすると、ONTAPはベース検索DNを使用します。
-netgroup-byhost-scope	このオプションは Netgroup-by-host、オブジェクトクラスの検索範囲を定義します。デフォルトはです subtree。
-session-security	このオプションは、セッションセキュリティのレベルを定義します。 Signseal、sign、および sealnone は有効なオプションです。
-skip-config-validation	設定の検証では、設定が適用される前にLDAPサーバへの接続とテストが試行されます。このオプションを使用すると、これらの手順をスキップできます。デフォルトはに設定されてい trueます。
-referral-enabled	このオプションは、ONTAPがLDAPサーバでチェイスリファーラル機能を使用するかどうかを定義します。これにより、要求されたオブジェクトが指定された最初のLDAPサーバに存在しない場合に、LDAPクエリが他のLDAPサーバに接続できるようになります。
-group-membership-filter	このパラメータは、LDAPサーバからグループメンバーシップを検索するときに使用するカスタムLDAP検索フィルタを指定します。有効なフィルタの例としては (cn=*99)、(cn=1*)、(|(cn=*22)(cn=*33)) などがあります。

例については、本ドキュメントの後半の付録セクション「LDAPクライアント設定の例」を参照してください。

LDAPクライアント設定- SVMスコープ

LDAPでLDAPクライアント設定を作成する場合は、次の2つの選択肢のいずれかを選択できます。

- `-vserver` **オプションを明示的に設定し**ます。このオプションを選択すると、指定したSVMのみがクライアント設定を使用できるようになり、さまざまな顧客ベースが共有する環境でセキュアマルチテナンシー機能を提供できます。
- **この** `-vserver` **オプションは空白のままにし**ます。このオプションを選択すると、クライアント設定が作成され、クラスタ内のすべてのSVMで使用できるようになります。このオプションは、環境内の複数のSVM間でLDAPクライアント設定を共有する必要がある場合に役立ちます。

LDAPを有効にする

LDAPクライアント設定が完了したので、`ldap create` SVMでコマンドを実行してLDAPを有効にする必要があります。

```
cluster::> ldap create ?
   [-vserver] <vserver name>          Vserver
   [-client-config] <text>            LDAP Client Configuration
  [[-skip-config-validation] [true|false]] Skip Configuration Validation
```

この設定では、SVMにLDAPの使用を許可するだけで、SVMの `ns-switch` 設定が変更されるまで認証要求には関与しません。

LDAP設定の検証をスキップ

設定でチェックを実行できるようにするにはNetApp、を `-skip-config- validation` に設定することを推奨します `false`。これがデフォルト値であるため、オプションを指定しない場合は設定チェックが実行されます。これは、`ldap check` コマンドを実行したときに表示されるのと同じチェックを使用します。

LDAPサーバの設定が原因でLDAPの設定が失敗することがあります。たとえば、設定の検証では、インデックスなしのbaseObjectグローバルクエリが実行されます。一部のLDAPサーバー(openDJなど)では、この手順を無効にする必要があります。そのため、ONTAPを使用してクエリをブロックするサーバーに接続すると、チェックは失敗します。これらのサーバではLDAPを引き続き使用できますが、`-skip-config-validation` をに設定して問題を回避する必要があり `true`ます。詳細については、バグ1328101を参照してください。

SVMネームサービススイッチ（ns-switch）を変更する

ONTAPでは、SVM `ns-switch` の設定でLDAPを指定するまで名前検索にLDAPの使用が開始されず、`ns-switch` コマンドで指定されたデータベースに対してのみLDAPが使用されます。LDAPを有効なネームサービスとして指定できる対象は次のとおりです。

- `Passwd`
- `Group`
- `Namemap`
- `Netgroup`

ここでは、使用可能なネームサービスデータベースについて説明します。特定のサービスにLDAPを使用する予定がない場合は、LDAPを有効にしないでください。たとえば、LDAPがネームマッピングルールの有効なネームサービスソースとして指定されていて、ネームマッピングを実行するように設定されていない場合、ネームマッピングが遅延する可能性があります。詳細については、「ネームマッピングへのLDAPの使用」セクションを参照してください。

```
cluster::> ns-switch modify ?
  (vserver services name-service ns-switch modify)
    -vserver <vserver name>                          Vserver
   [-database] {hosts|group|passwd|netgroup|namemap} Name Service Switch Database
   [-sources] {files|dns|ldap|nis}, ...               Name Service Source Order
```

LDAP機能のテスト

設定が完了し、ネームサービス要求とID要求にLDAPを使用するようにONTAP SVMが設定されたので、機能をテストする必要があります。このテストを行うには、diag権限を無効にしてください。diag権限を開始するには、次のコマンドを使用します。

```
cluster::> set diag
```

この設定により、すべての診断コマンドとトラブルシューティングコマンドが使用可能になります。

LDAP接続

これらのコマンドは、LDAPサーバにアクセスできるかどうか、およびLDAPサーバに接続できるかどうかのトラブルシューティングに役立ちます。ただし、ONTAP 9.5以降では、接続または設定問題がある場合、ONTAPで設定の変更が適用される前にチェックが自動的に実行されるため、LDAPとDNSの設定コマンドは失敗します。たとえば、LDAPクライアントで変更を行うと、ONTAPはネットワーク接続、LDAPバインドをチェックし、クライアント設定で設定されているDNSを検索します。これらのチェックのいずれかが失敗すると、設定を変更するコマンドは失敗します。`skip-config-validation` trueオプションを指定すると、このチェックを省略できます。

DNSルックアップ

DNS呼び出しを使用してLDAPサーバをホスト名またはIPアドレスで検索するには、次のコマンドを使用します。

```
getxxbyyy gethostbyname -node [node1] -vserver [SVM] -hostname [ldap.ntap.local]
getxxbyyy gethostbyaddr -node [node1] -vserver [SVM] -ipaddress [10.10.10.10]
```

次の情報を前方検索に使用することもできます。

```
diag secd dns forward-lookup -node [node1] -vserver [SVM] -hostname [hostname]
```

SRVレコードを検索するには、次のコマンドを使用します。

```
diag secd dns srv-lookup -node [node1] -vserver [SVM] -lookup-string [_ldap._tcp.ntap.local]
```

ネットワークping

LDAPサーバへのpingを実行すると、SVM LIFがLDAPに到達できるかどうかを確認できます。ただし、一部のネットワークではInternet Control Message Protocol（ICMP）トラフィックがブロックされるため、pingが正しく機能しない可能性があることに注意してください。pingを実行するときは、LDAPトラフィックに参加しているLIFをpingで使用するように、SVM名とデータLIF名を定義してください。

```
cluster::*> ping ?
   { -node <nodename>                    Node
   |  -lif <lif-name> }                  Logical Interface
    -vserver <vserver>                   Vserver
  [ -use-source-port {true|false} ]      *(DEPRECATED)-Use Source Port of Logical Interface
   [-destination] <Remote InetAddress>   Destination
  [ -show-detail|-s [true] ]             Show Detail Output
  [ -record-route|-R [true] ]            Record Route
  [ -verbose|-v [true] ]                 Show All ICMP Packets
  [ -packet-size <integer> ]             Packet Size
  [ -count <integer> ]                   Count
  [ -wait <integer> ]                    Packet Send Wait Time (secs)
  [ -flood [true] ]                      *Flood Ping
  [ -disallow-fragmentation|-D [true] ]  Disallow Packet Fragmentation (default: false)
  [ -wait-response <integer> ]           Packet Response Wait Time (ms) (default: 10000)
```

LDAP接続テスト

LDAP（およびその他のネームサービスサーバ）接続をテストするには、を使用し `diag secd connections test`ます。

```
cluster::*> diag secd connections test -node [node1]-vserver [SVM]
```

接続を表示するには、次のコマンドを使用します。

```
cluster::*> diag secd connections show ?
   [-node] <nodename>          *Node
   [-vserver] <vserver>        *Vserver
  [[-type] <text>]             *Cache type (lsa,netlogon,ldap-ad,ldap-nis-namemap)
  [ -key <text> ]              *Connection key
```

接続キャッシュをクリアするには、次のコマンドを使用します。

```
cluster::*> diag secd connections clear ?
   [-node] <nodename>          *Node
   [-vserver] <vserver>        *Vserver
  [[-type] <text>]             *Cache type (lsa,netlogon,ldap-ad,ldap-nis-namemap)
  [ -key <text> ]              *Connection key
```

または、`ldap check` コマンドを使用することもできます。

```
cluster::*> ldap check -vserver DEMO

                  Vserver: DEMO
Client Configuration Name: DEMO
              LDAP Status: up
      LDAP Status Details: Successfully connected to LDAP server "10.x.x.x".
   LDAP DN Status Details: All the configured DNs are available.
```

LDAP名の検索とグループメンバーシップ

ONTAP 9.3以降ではネームサービスの動作が変更されたため、LDAP名検索はSVMレベルで実行されます。そのため、getxxbyyyコマンドを使用してLDAPテストを実行する必要があります。getXXbyYYを参照してください。

ユーザのグループメンバーシップの例を次に示します。

```
cluster::*> getxxbyyy getgrlist -node node1 -vserver DEMO -username prof1 -show-granular-err true
-use-cache false -show-source true
  (vserver services name-service getxxbyyy getgrlist)
Source used for lookup: LDAP
pw_name: prof1
Groups: 1101 1201 1202 1203 1220
NIS:
Error code:    NS_ERROR_NONE
Error message: No error
LDAP:
Error code:    NS_FOUND
Error message: Entry found
DNS:
Error code:    NS_ERROR_NONE
Error message: No error
FILES:
Error code:    NS_ERROR_NOT_FOUND
Error message: Entry not found
Deterministic Result: Success
```

を使用して、名前の検索と翻訳を実行することもできます `secd`。

```
cluster::*> diag secd authentication show-ontap-admin-unix-creds ?
  [ -node <nodename> ]         *Node (default: ontap9-tme-8040-01)
   [-vserver] <vserver>        *Vserver
   { [-unix-user-name] <text> *Unix User Name
   | [-uid] <integer> }        *Unix User ID

cluster::*> diag secd authentication translate ?
  [ -node <nodename> ]          *Node Name (default: ontap9-tme-8040-01)
   [-vserver] <vserver>         *Vserver Name
   { [-uid] <integer>           *UNIX User ID
   | [-gid] <integer>           *UNIX Group ID
   | [-sid] <text>              *Windows SID
```

```
   | [-unix-user-name] <text>   *UNIX User Name
   | [-unix-group-name] <text> *UNIX Group Name
   | [-win-name] <text> }       *Windows Name
```

ONTAP 9.6以降では `vserver services access-check`、「ONTAP CLIコマンドによるLDAPのトラブルシューティング」セクションに記載されているadvanced権限のコマンドを使用できます。

```
cluster::*> vserver services access-check ?
  authentication>             *Check Authentication Information
  dns>                        *Check DNS Lookups
  name-mapping>               *Check Name Mapping Operations
  server-discovery>           *Check Server Discovery Information

cluster::*> vserver services access-check authentication show-ontap-admin-unix-creds -vserver
DEMO -unix-user-name prof1
       User Id: 1100
      Group Id: 1101
Home Directory: /home/prof1
   Login Shell: /bin/sh
```

マルチプロトコルNAS環境でのネームマッピング

同じデータセットに対してNFSとCIFS / SMBを使用する場合、それらのファイルやフォルダにアクセスするには、UNIXユーザとWindowsユーザの間でネームマッピングを行う必要があります（逆に）。ネームマッピングの方法は、環境で使用されているボリュームおよびqtreeのセキュリティ形式によって異なります。たとえば、ボリュームでNTFSセキュリティが使用されていて、ユーザがNFS経由でボリュームにアクセスする場合、NFSはNTFS ACLを認識しないため、ユーザをWindowsユーザにマッピングして適切な権限レベルを確認する必要があります。

特定のWindowsユーザにマッピングされているUNIXユーザを確認するには、次のコマンドを実行します。

```
cluster::*> diag secd name-mapping show -node [node] -vserver [SVM] -direction win-unix -name
[username or DOMAIN\username]
```

ONTAP 9.6以降では、`access-check.`

```
cluster::*> access-check name-mapping show -vserver [SVM] -direction win-unix -name [username]
```

UNIXからWindowsへのネームマッピングの場合は、次のコマンドを実行します。

```
cluster::*> diag secd name-mapping show -node [node] -vserver [SVM] -direction unix-win -name
[username]

cluster::*> access-check name-mapping show -vserver [SVM] -direction unix-win -name [username]
```

Kerberos Service Principal Name（SPN；サービスプリンシパル名）からUNIXユーザ（Kerberos NFSの場合）には、次のコマンドを実行します。

```
cluster::*> diag secd name-mapping show -node [node] -vserver [SVM] -direction krb-unix -name
[SPN]

cluster::*> access-check name-mapping show -vserver [SVM] -direction krb-unix -name [SPN]
```

ネームマッピング値は、次のいずれかの場所から情報を収集します。

- ONTAPでのデフォルトの1：1のネームマッピング（`user user`両方の名前がネームサービスで見つかった場合は常ににマッピングされます）
- ネームマッピングルール（ローカルまたはLDAP内）
- デフォルトのWindowsユーザまたはUNIXユーザ（`-default-unix-user -default-win-user`それぞれCIFSサーバオプションとNFSサーバオプションで設定）

ただし、ネームマッピングは関係式の一部にすぎません。マルチプロトコル環境を使用する場合は、これらの要求に適切なグループメンバーシップがすべて設定されていることを確認する必要があります。ユーザに関するすべての情報を照会するには、次のコマンドを実行します。

```
cluster::*> diag secd authentication show-creds ?
  [ -node <nodename> ]                 *Node (default: ontap9-tme-8040-01)
   [-vserver] <vserver>                *Vserver
   { [-uid] <integer>                  *UID
   | [-sid] <text>                     *SID
   | [-unix-user-name] <text>          *Unix User Name
   | [-win-name] <text> }              *Windows Name
  [[-list-name] {true|false}]          *Display Translated Names (default: true)
  [ -list-id {true|false} ]            *Display IDs (default: false)
  [ -clientIp <IP Address> ]           *Client IP Address
  [ -skip-domain-group {true|false} ]  *Skip Domain Groups (default: false)
```

ONTAP 9.6以降では、次のコマンドを実行します。

```
cluster::*> access-check authentication show-creds ?
  (vserver services access-check authentication show-creds)
  [ -node <nodename> ]                 *Node (default: ontap9-tme-8040-01)
   [-vserver] <vserver>                *Vserver
   { [-uid] <integer>                  *UID
   | [-sid] <text>                     *SID
   | [-unix-user-name] <text>          *Unix User Name
   | [-win-name] <text> }              *Windows Name
  [[-list-name] {true|false}]          *Display Translated Names (default: true)
  [ -list-id {true|false} ]            *Display IDs (default: false)
  [ -clientIp <IP Address> ]           *Client IP Address
  [ -skip-domain-group {true|false} ] *Skip Domain Groups (default: false)
```

上記のコマンドは、マルチプロトコル環境でネームマッピング、UNIXグループメンバーシップ、Windowsグループメンバーシップ、数値IDなど、すべてのユーザ情報を取得します。このコマンドは、NFSとCIFS / SMBの両方が設定され、使用中の場合にのみ機能します。このコマンドの出力例については、付録A：コマンド例およびその他の情報を参照してください。

UNIX ID管理にActive Directoryを使用するLDAP

UNIX ID管理にMicrosoft Active Directoryを使用すると、次のような利点があります。

- Kerberos（Key Distribution Center [KDC]）とのネイティブ統合
- ネイティブLDAPレプリケーションと冗長性
- グローバルカタログ検索によるフォレストレベルのレプリケーション
- LDAP処理による信頼できるドメインのサポート

以降のセクションでは、これらの概念の一部について詳しく説明します。

ドメインコントローラの冗長性とレプリケーション

デフォルトでは、Active Directoryは15分ごとにデータベースをドメインコントローラにレプリケートします。ドメイン内のすべてのオブジェクトは、ユーザーオブジェクトとコンピュータオブジェクト、およびそれらの属性を含む複数の場所にコピーされます。したがって、1つのドメインに複数のドメインコントローラを配置することで、LDAPおよびKerberosの単一点障害を排除できます。

LDAPサーバに障害が発生すると、プライマリLDAPサーバが接続テストに失敗すると、ONTAPは追加のLDAPサーバに移行します。次のサーバは、LDAPクライアントの設定方法によって異なります。

- サーバリストが指定されている場合は、リスト内の次のサーバが使用されます。
- 負荷分散されたホスト名を使用する場合は、ロードバランサの次のサーバが使用されます。
- Active Directoryドメインを使用する場合は、DNSサービスレコード（SRV）ルックアップで提供される次のサーバが使用されます。

UNIXのID管理サーバとしてのドメインコントローラの使用

Microsoft Active Directoryは、LDAP UNIX ID管理サーバとしてネイティブに機能しません。新しいWindowsバージョン（Windows 2012以降）では、UNIX属性はスキーマに存在しますが、入力されません。そのため、Windows 2008以前のバージョンのようにスキーマを拡張する必要がなくなりました。

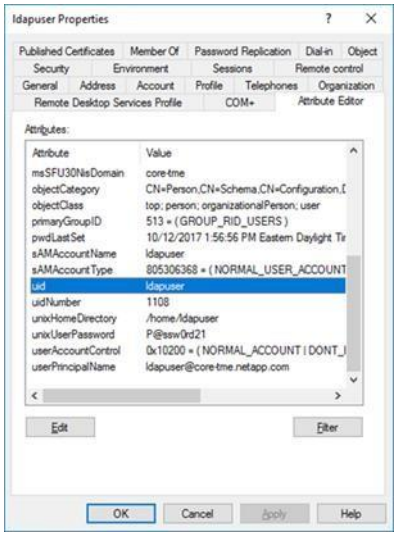
UNIXユーザ、グループ、およびネットグループを利用するには、UNIX情報をUNIX属性に入力する必要があります。Windows Server 2012以前のバージョンでは、図6に示すように[UNIX Attributes]タブが用意されていました。このタブでは、GUIを使用してこれらのエントリを入力できます。

UNIX属性

図6）Windows Server 2012の[UNIX Attributes]タブ

Windows 2016以降のバージョンでは、[UNIX Attributes]タブのサポートが廃止されました。Windows 2016以降でUNIX属性を管理するには、PowerShellまたは[属性エディタ]タブを使用します（「**エラー！有効なブックマークの自己参照ではありません。**および「Active DirectoryでのUNIX属性の変更」を参照）。[属性エディタ]タブは、Windows Server 2012でも使用できます。

図7）Windows 2016の[Attribute Editor]タブ



ONTAPがLDAPクエリに使用するUNIX属性 ONTAPは、ユーザを検索

するときに、標準のLDAP検索機能を使用します。

注: 詳細については、この ldapsearchページを参照してください。

クエリは、NAS共有に入ってくるユーザーまたはグループに基づいて作成されます。ONTAPはこの情報を収集し、`ldapsearch` クエリを作成します。

たとえば、のNFSユーザIDが `1234` NFSv4.xまたはNTFS ACLを使用してエクスポートにアクセスしようとする場合、ONTAPはそのユーザIDをACLで解決できるUNIX名に変換する必要があります。`ns-switch` データベースでLDAPが指定されている場合は、LDAPが使用されます。

ONTAPは、SVMのLDAPクライアントで設定されているLDAPスキーマ（「LDAPスキーマ」を参照）で割り当てられている属性を使用して検索します。MS-AD-BISスキーマで `uid-number-attribute` は、が値を使用し `uidNumber`、`posix-account-object-class` 値はです。`User`

```
cluster::*> ldap client schema show -schema MS-AD-BIS -fields posix-account-object-class,uid-
number-attribute
vserver        schema     posix-account-object-class uid-number-attribute
-------------- ---------- ---------------------------------- --------------------------
DEMO           MS-AD-BIS  User                               uidNumber
```

したがって、数値IDの場合、`1234` LDAP検索構文は次のようになります。

```
(&(objectClass=User)(uidNumber=1234))
```

このクエリは、`GetXXbyYY` 本ドキュメントの「トラブルシューティングツール」セクションに記載されているコマンドを使用して、ONTAPからシミュレートできます。

表6）、表7、および表8 に、MS-AD-BISスキーマに基づく、ユーザーおよびグループのWindows Active Directory UNIX ID管理で使用される標準属性または最も一般的な属性を示します。MS-AD-BISスキーマは、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。カスタムスキーマの詳細については、「LDAPスキーマ」を参照してください。

ONTAPがLDAPクエリに使用するUNIXユーザ属性

表6）標準のUNIXユーザ属性（MS-AD-BISスキーマ）

LDAPクライアントスキーマ属性（ONTAP LDAPクライアント）	LDAP属性値（LDAPサーバ）
-posix-account-object-class	User
-uid-attribute	uid
-uid-number-attribute	uidNumber
-gid-number-attribute	gidNumber
-gecos-attribute name	unixHomeDirectory
-home-directory-attribute	name
-user-password-attribute	unixUserPassword
-login-shell-attribute	LoginShell
-windows-to-unix-attribute	sAMAccountName

グループ属性

表7）標準のUNIXグループ属性（MS-AD-BISスキーマ）

LDAPクライアントスキーマ属性（ONTAP LDAPクライアント）	LDAP属性値（LDAPサーバ）
-posix-group-object-class	Group
-cn-group-attribute	cn
-gid-number-attribute	gidNumber
-member-uid-attribute	memberUid
-group-of-unique-names-object-class	Group
-unique-member-attribute	Member

注： memberUid Member 属性/セカンダリグループとの比較については、「Secondary、Supplemental、and auxiliary GID」を参照してください。

NetApp属性

表8）標準UNIXネットグループ属性（MS-AD-BISスキーマ）

LDAPクライアントスキーマ属性（ONTAP LDAPクライアント）	LDAP属性値（LDAPサーバ）
-nis-netgroup-object-class	nisNetgroup
-cn-netgroup-attribute	Name
-member-nis-netgroup-attribute	memberNisNetgroup
-nis-netgroup-triple-attribute	nisNetgroupTriple
-nis-object-class	nisObject*
-nis-mapname-attribute	nisMapName*

LDAPクライアントスキーマ属性（ONTAP LDAPクライアント）	LDAP属性値（LDAPサーバ）
-nis-mapentry-attribute	nisMapEntry*

注： *が付いたエントリはに使用され netgroup.byhostます。

Active DirectoryでのUNIX属性の変更

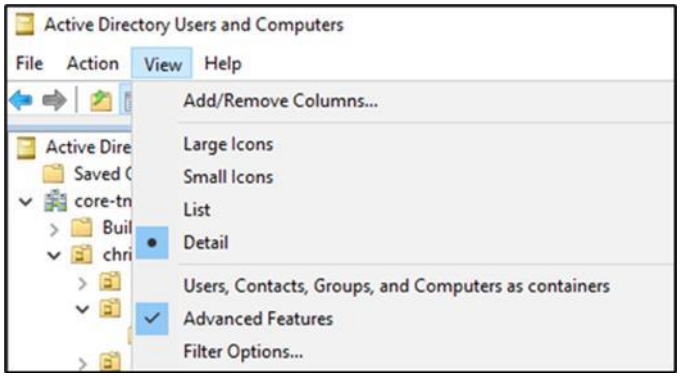
Windowsユーザ名またはグループを作成するときに、Active Directory内のそのオブジェクトにUNIX属性を関連付けることもできます。最新のWindowsオペレーティングシステムでは、UNIXオブジェクトを作成および変更するには、GUIとPowerShellの2つのオプションがあります。

GUIを使用したUNIXオブジェクトの作成と変更

管理者がActive Directoryを管理する最も一般的な方法は、Active Directoryユーザーとコンピュータ(ADUC) Microsoft管理コンソール(MMC)を使用することです。

MMCを使用すると、ユーザとグループを作成したあとに変更して、LDAPクライアントで使用するUNIX属性を設定できます。ADUCを使用してユーザーまたはグループを作成する場合、UNIX属性を入力する方法はありません。そのため、後でオブジェクトをダブルクリックし、Windows Server 2012以降のバージョンでは[属性エディタ]タブを使用する必要があります。[属性エディター（Attributes Editor）]タブはデフォルトでは表示されません。MMCで[拡張機能（Advanced Features）]ビューを有効にする必要があります。図8を参照してください。

図8）[Enable Advanced Features]を選択して[Attributes Editor]タブを表示



拡張機能を有効にしてユーザープロパティを開いたら'属性エディタでUNIX属性を変更できます編集する必要がある属性の詳細については、表6 および 表7 のユーザー属性とグループ属性のリストを参照してください。

Active Directory LDAPでのネットグループの作成と編集の詳細については、「ONTAP interaction with Active Directory LDAP for netgroups」を参照してください。

PowerShellを使用したUNIXオブジェクトの作成と変更

PowerShellには、ユーザとグループのネイティブコマンドレット（New-ADUser、New-ADGroup）も用意されています。これらのコマンドレットを使用すると、CLIまたはオートメーションを使用してユーザとグループを作成および管理できます。PowerShellでは、- OtherAttributes オブジェクトの作成時にオプションを使用してUNIX属性を設定できます。

たとえば、user1 uidNumber がで 5555、gidNumber がのというユーザを作成する場合は 1101、次のPowerShellコマンドを使用します。

```
PS C:\> New-ADUser -SamAccountName user1 -UserPrincipalName user1@NTAP.LOCAL -Name user1 -
OtherAttributes @{'uid'="user1";'uidNumber'="5555";'gidNumber'="1101"} -Enabled 1 -
PasswordNeverExpires 1 -AccountPassword (Read-Host -AsSecureString "password" -Force)
Password -Force: **********
```

ONTAPから、このユーザを照会できるようになりました。

```
cluster::*> getxxbyyy getpwbyname -node ontap9-tme-8040-02 -vserver DEMO -username user1 -show-
source true -use-cache false
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name: user1
pw_passwd:
pw_uid: 5555
pw_gid: 1101
pw_gecos:
pw_dir:
pw_shell:
```

既存のユーザとグループは、Set-ADUser およびを使用して Set-ADGroupそれぞれ変更できます。これらのコマンドでは、-Add -Replace オプションまたはオプションを使用して、UNIXエントリを追加または置換できます。次の例では、に2つ目のUIDまたはユーザ名を追加できます user1。

```
PS C:\> Set-ADUser -Identity user1 -Add @{'uid'="user1alt"}
```

これで、UNIXユーザは user1 またはを使用し user1alt てUIDを照会できるようになり 5555ます。

```
cluster::*> getxxbyyy getpwbyname -node node2 -vserver DEMO -username user1 -show-source true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name:  user1alt
pw_passwd:
pw_uid: 5555
pw_gid: 1101
pw_gecos:
pw_dir:
pw_shell:

cluster::*> getxxbyyy getpwbyname -node node2 -vserver DEMO -username user1alt -show-source true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name:  user1alt
pw_passwd:
pw_uid: 5555
pw_gid: 1101
pw_gecos:
pw_dir:
pw_shell:
```

セカンダリグループと補助グループ

多くの場合、UNIXユーザはプライマリグループの外部にある複数のグループのメンバーです。LDAPではこれらのグループを照会できますが、Active Directory LDAPではグループメンバーシップを検索する方法として、を使用する方法 memberUid とを使用する方法の2つがあります。Member

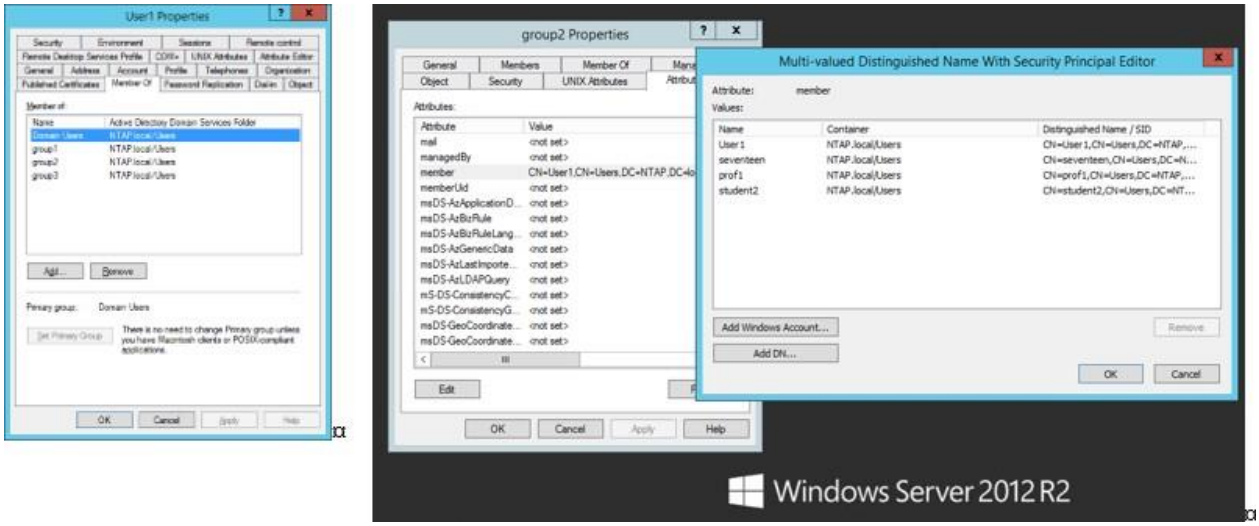
注： グループを作成するときは、GID番号を負の値（-1など）にすることはできません。負の値を使用すると、その数値に対するONTAPクエリは「値が大きすぎてデータ型に格納できません」というエラーで失敗します。

RFC 2307：標準方式（memberUid）

Active Directory LDAPでユーザのセカンダリグループを表示する方法の1つは、memberUid Active Directoryのグループオブジェクトに存在する属性を利用することです。ユーザが memberUid リストに追加されると、LDAPはLDAPクエリ中にそれらのグループを返すことができます。欠点は、Active Directoryでは、ユーザーがWindowsグループに追加されたときに、その属性が自動的に入力されないことです。
Manual intervention is required.

たとえば、Windows管理者が user1、group1、group2、という名前のWindowsグループにを追加した場合、group3Member Active Directoryには属性のみが入力されます。図9では、group2 memberUid にエントリがあるにもかかわらず、フィールドにエントリがないことに注意してください Member。

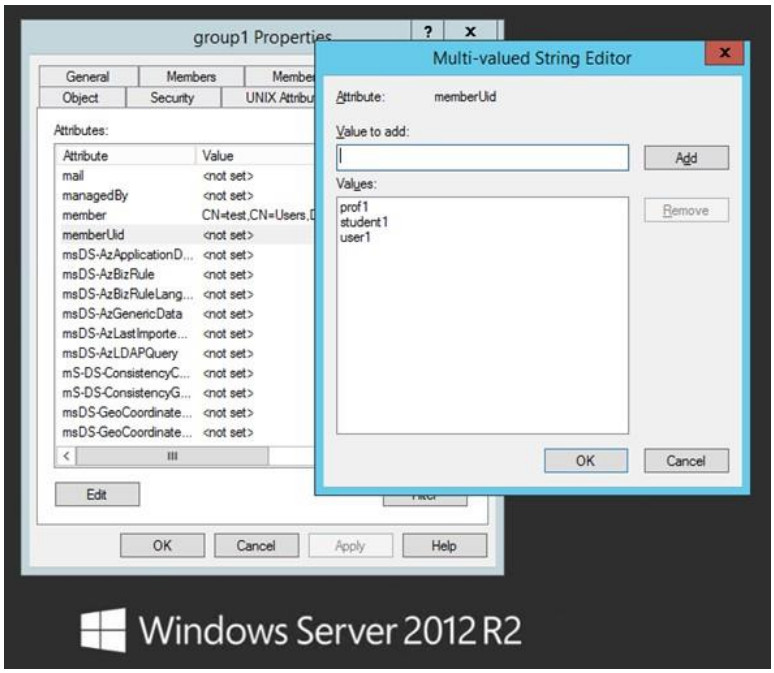
図9）Windowsグループへのユーザの追加



memberUid 各グループのが追加用に変更されていないかぎり、user1そのユーザのUNIXグループメンバーシップのチェックでは、それらのグループが適切に表示されません。この memberUid 属性は複数値の文字列であり、複数のユーザーをリストに追加できることを意味します。

図10の次の例では、ユーザがに追加されてい group1ます。

図10）memberUid属性の例



ONTAPでは user1、どのUNIXグループメンバーシップがあるかを確認します。Group1 (gidNumber 1201)には memberUid データが入力されており、リストに表示されて group2いますが、(gidNumber 1202)には memberUid データが入力されておらず、リストには表示されていません。RFC 2307bis機能はディセーブルです。

```
cluster::*> ldap client schema modify -schema DEMO -enable-rfc2307bis false
```

```
cluster::*> getxxbyyy getgrlist -node ontap9-tme-8040-01 -vserver DEMO -username user1 -use-cache
false
  (vserver services name-service getxxbyyy getgrlist)
pw_name: user1
Groups: 1101 1201
```

RFC 2307bis（メンバー）

RFC 2307bisは、ユーザーとのグループメンバーシップを照会するもう1つの方法であり、Windows Active Directory環境に最適です。前のセクションでは、ユーザーをWindowsグループに追加すると、Active Directoryによって `Member` 属性が入力されますが（図9を参照）、`memberUid` 属性は入力されません（図10）。そのため、UNIXユーザのセカンダリグループメンバーシップが適切に読み込まれません。

RFC 2307bisが有効な場合、ONTAPは、`-unique-member-attribute` LDAPクライアントスキーマで設定されているを照会します。デフォルトでは `Member`、MS-AD-BISスキーマはその属性にを使用します。

前のセクションで説明した設定と同じSVMで、RFC 2307bisサポートを有効にして、ユーザメンバーシップまたはグループメンバーシップにその他の変更を加えることはありません。次に、同じgroup listコマンドを実行して、適切なグループメンバーシップを確認します。

```
cluster::*> ldap client schema modify -schema DEMO -enable-rfc2307bis true

cluster::*> getxxbyyy getgrlist -node ontap9-tme-8040-01 -vserver DEMO -username user1 -use-cache
false
  (vserver services name-service getxxbyyy getgrlist)
pw_name: user1
Groups: 1101 1201 1202 1203
```

詳細については、「RFC 2307bis」を参照してください。

UNIX ID管理でのフォレスト内の信頼できるドメインの使用

Active Directoryを使用すると、フォレスト内の2つのドメイン間に信頼を設定し、それらの親ドメインの下に子ドメインを持つことができます。これらの環境のデフォルトの動作では、最初のLDAPサーバにユーザまたはグループがない場合に、LDAPリファーラルを使用して追加のLDAPサーバを照会します。ONTAP 9.5以降のバージョンではリファーラルがサポートされます。リファーラルの詳細については、「LDAPリファーラル（チェイスリファーラル）」を参照してください。

ドメイン信頼のトラブルシューティングコマンドについては、「トラブルシューティングツール」の項を参照してください。

Active Directoryグローバルカタログ検索

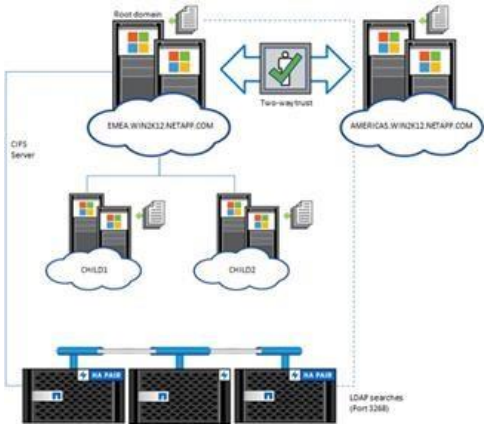
UNIX ID管理にWindows Active Directoryを使用している場合は、グローバルカタログを利用して、UNIX属性の入力、ドメインフォレスト間でのレプリケーション、およびポート3268を介したONTAPでのクエリを行うことができます。この設定では、同じフォレスト内に複数の信頼できるドメインを作成できます。すべての信頼できるドメインには、一意のUNIXユーザおよびグループが割り当てられ、フォレストの最上位レベルに複製されます。このアプローチにより、ONTAPはフォレストレベルで検索できるようになり、LDAPリファーラルが不要になります。

新しい属性をグローバルカタログにレプリケートする

デフォルトでは、UNIX属性はグローバルカタログに複製されません。そのため、Active Directoryに複製を指示するまで、グローバルカタログで検索することはできません。図11 に、グローバルカタログ検索でのLDAP検索に使用できる信頼できるドメインの設定例を示します。

デフォルトでは、UNIX属性はグローバルカタログに複製されません。そのため、Active Directoryに複製を指示するまで、グローバルカタログで検索することはできません。図11 に、グローバルカタログ検索でのLDAP検索に使用できる信頼できるドメインの設定例を示します。

図11）グローバルカタログ検索を使用する信頼できるドメイン



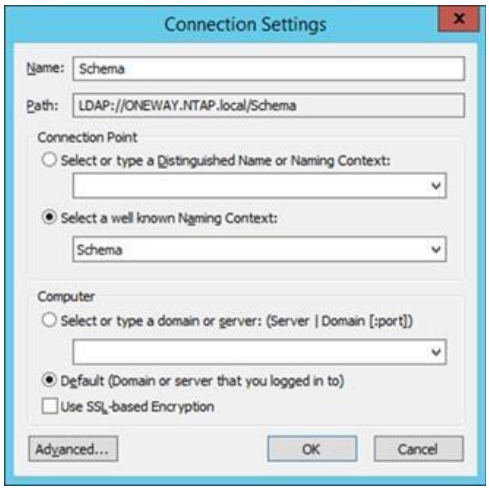
グローバルカタログにレプリケートする属性の設定方法

Active Directoryは、バックエンドスキーマを使用してオブジェクトの動作を制御します。このスキーマは変更できますが、変更には特別な手順が必要です。

スキーマを変更する場合はMicrosoftに連絡することをお勧めしますが、スキーマ属性を変更するには、次の手順を実行します。この例はWindows Server 2012 R2 Active Directoryドメインコントローラで実行されたものです。これらの手順がお使いのWindowsのバージョンで機能することを確認してください。

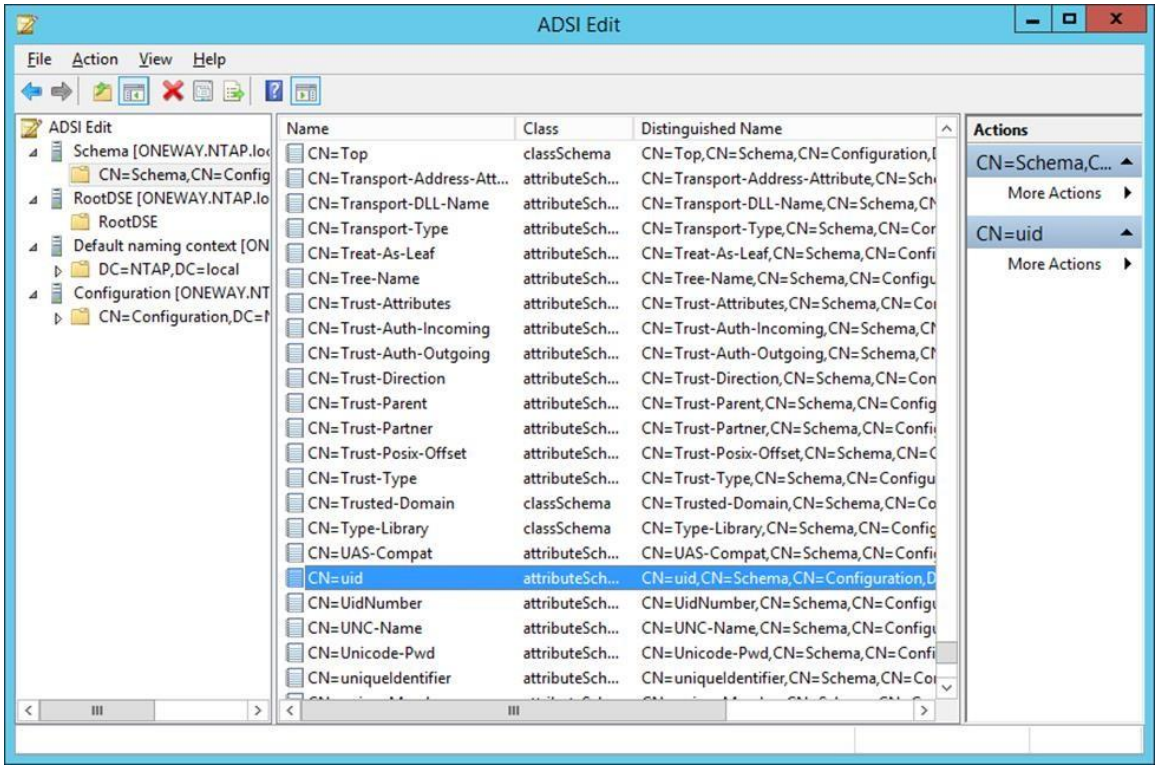
スキーマ属性を変更するには、ADSI Editを使用し、Schema Naming Contextに接続します(図12)。

図12）スキーマネーミングコンテキストへの接続



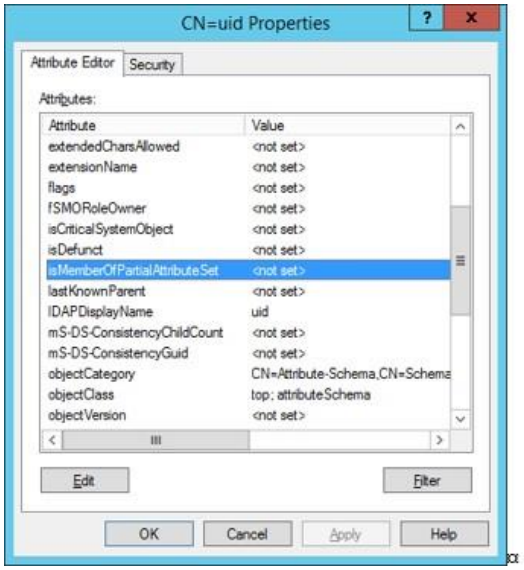
Schema Naming Contextに接続したら、CN=Schema、CN=Configuration、DC=NTAP、DC=localフォルダから属性に移動できます。属性はCN=AttributeNameとして表示されます（CN=uidなど）。図13を参照してください。

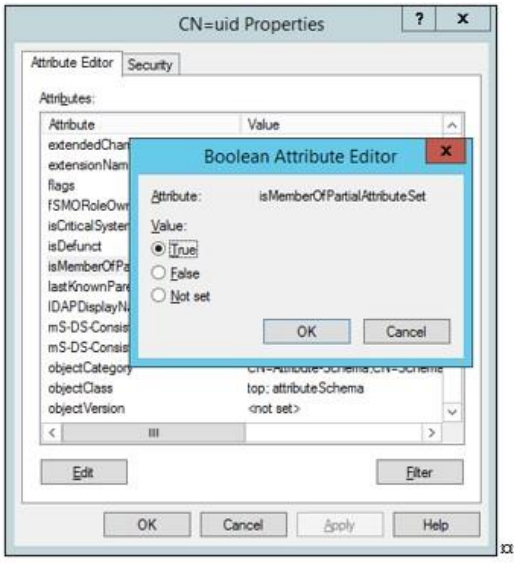
図13）スキーマネーミングコンテキストの形式



グローバルカタログにレプリケートする属性が見つかったら、その属性をダブルクリックするか、右クリックして[プロパティ（Properties）]を選択します。次に、`isMemberOfPartialAttributeSet` 値に移動します。その値をダブルクリックして、オプションをTrueに切り替え、[OK]をクリックしてから[適用]をクリックします。図14を参照してください。

図14）isMemberOfPartialAttributeSet属性





PowerShellと次のコマンドを使用して属性を変更することもできます。

```
PS C:\> Set-ADObject 'CN=uidNumber,CN=Schema,CN=Configuration,DC=NTAP,DC=local' -Replace
@{isMemberOfPartialAttributeSet="TRUE"}
```

ONTAP for Windows 2008 R2以降でグローバルカタログLDAP検索を使用できるようにするには、次のUNIX属性を変更してグローバルカタログサーバ間でレプリケートする必要があります。

```
gecos
gidNumber
memberUid
nisMapName (if using netgroups)
nisMapEntry (if using netgroups)
nisNetgroupTriple (if using netgroups)
uid
uidNumber
unixHomeDirectory
unixUserPassword
```

値がに設定されているUNIX LDAP属性を確認するには `TRUE`、次のPowerShellコマンドを使用します。

```
PS C:\> Get-ADObject -SearchBase "cn=Schema,cn=Configuration,dc=ntap,dc=local" -LDAPFilter
"(isMemberOfPartialAttributeSet=TRUE)" -Properties lDAPDisplayName | Select lDAPDisplayName |
findstr -i "member uid gid unix"
fRSMemberReference
netbootGUID
netbootDUID
objectGUID
msFVE-VolumeGuid
msFVE-RecoveryGuid
uid
member
unixUserPassword
uidNumber
gidNumber
unixHomeDirectory
memberUid
```

次のことに注意してください。

- 検索にグローバルカタログサーバを使用すると、それらのサーバに大きな負荷とトラフィックが追加される可能性があります。LDAP検索にグローバルカタログを使用する場合は、負荷を処理するのに十分なサーバがあることを確認してください。
- Active Directoryスキーマの変更は非常に危険です。注意して修正し、すべての変更を詳細に文書化します。可能であれば、Microsoftのサポートにお問い合わせください。

属性をグローバルカタログにレプリケートするように変更したら、15分間のレプリケーションウィンドウを待つか、Active Directoryサイトとサービスを使用して強制的にレプリケーションを実行できます。

ONTAP LDAPクライアントでグローバルカタログ検索を有効にするには、LDAPポート (`- port`)を3268に変更するだけです。

例：

```
cluster::*> ldap client modify -vserver DEMO -client-config DEMO -port 3268
cluster::*> ldap client show -vserver DEMO -fields port
vserver client-config port
---------- ----------------- -----
DEMO     DEMO           3268
```

この例では、Active Directoryグローバルカタログが`UNIX`属性をレプリケートするように変更される前に、検索が失敗しました。

```
cluster::*> getxxbyyy getpwbyname -node node1 -vserver DEMO -username prof1
  (vserver services name-service getxxbyyy getpwbyname)

Error: command failed: Failed to resolve prof1. Reason: Entry not found for "username: prof1".
```

変更後、検索は成功しました。

```
cluster::*> getxxbyyy getpwbyname -node node1 -vserver DEMO -username prof1
  (vserver services name-service getxxbyyy getpwbyname)
pw_name: prof1
pw_passwd:
pw_uid: 1100
pw_gid: 1101
pw_gecos: Professor
pw_dir: /home/prof1
pw_shell: /bin/sh
```

LDAPを使用したネームマッピングルールの提供

UNIXユーザ、グループ、ネットグループに加えて、ONTAP SVMで静的なネームマッピングエントリを作成する代わりに、LDAPを使用してネームマッピングを照会することもできます。マルチプロトコルNAS環境では、UNIXユーザとWindowsユーザが権限の読み取り、書き込み、ナビゲートを行う際の一貫性を維持するために、ネームマッピングが必要です。

ネームマッピングルールには主に2つの概念があります。

- 対称ネームマッピングは、同じユーザ名を使用するUNIXユーザとWindowsユーザ間のネームマッピングです。たとえば、Windowsユーザは `DOMAIN\justin` UNIXユーザにマッピングされます。 `justin`
- 非対称ネームマッピングは、異なるユーザ名を使用するUNIXユーザとWindowsユーザの間のネームマッピングです。たとえば、Windowsユーザ `DOMAIN\justin` がUNIXユーザにマッピングされ `nfsdudeabides`ます。

ONTAPは、ネームマッピングルールを必要とせずに対称ネームマッピングを標準でサポートし、ネームマップ `ns-switch` データベースで非対称ネームマッピングをサポートします。

ONTAPでのネームマッピングの処理順序

ユーザがNASマウントまたは共有に対して認証を試みると、ONTAPは特定の順序でネームマッピングメカニズムを使用して有効なユーザまたはネームマップエントリを検索します。この順序は、最終的には、でネームマップ値に指定された最初のネームサービスデータベース値によって `vserver services name-service ns-switch`決まります。次の例では、ONTAPは最初にローカルファイルを試行し、次にLDAPを試行します。`Local files` ネームマップ値の場合、のSVMのネームマッピングテーブル内のエントリを意味します `vserver name-mapping`。

```
cluster::> vserver services name-service ns-switch show -vserver DEMO -database namemap

                    Vserver: DEMO
Name Service Switch Database: namemap
   Name Service Source Order: files, ldap
```

ネームマッピングにLDAPを使用する場合、ONTAPは使用するように設定されているすべてのLDAPサーバを使用します。通常は対称ネームマッピングですが、非対称値を使用することもできます。

注： ネームマップデータベースに外部サービスを指定するのは、実際に非対称ネームマッピングに使用されている場合のみです。ネームマッピングルールが設定されていないサーバを指定すると、要求のレイテンシが増大し、認証や失敗に時間がかかります。

ユーザのネームサービスエントリにネームマッピングが見つからない場合、ONTAPはNFSサーバまたはCIFS / SMBサーバに設定されているデフォルト値にフォールバックしようとします。この値の使用方法は、アクセスを試みているプロトコル、ボリュームのセキュリティ形式、および要求されたネームマッピング方向によって異なります。表9 にその違いを示します。

表9）マルチプロトコルNASアクセスのネームマッピングとデフォルトユーザに関する考慮事項

プロトコル	セキュリティ形式	ネームマッピングの方向	デフォルトユーザ
NFS	UNIX	N/A（UID検索のみ）	N/A

プロトコル	セキュリティ形式	ネームマッピングの方向	デフォルトユーザ
NFS	NTFS	UNIX > Windows	デフォルトのWindowsユーザ（NFSオプション `default-win- user`）
CIFS / SMB	UNIX	Windows > UNIX	デフォルトのUNIXユーザ（CIFSオプションのデフォルト `unix- user; pcuse`は-r）
CIFS / SMB	NTFS	Windows > UNIX（初期認証） NTFS ACLは初期エントリ後に使用されます。	デフォルトのUNIXユーザ（`default-unix- user; pcuser` デフォルトはCIFSオプション）

LDAPテノWindowsカラUNIXユウサヘノヒタイシヨウメイマツヒンク

ONTAPのLDAPからの双方向の非対称ネームマッピングを使用している環境の場合は、WindowsとUNIXのネームマッピング用にSVMごとにネームマッピングルールを作成します。ただし、SVMあたりのルール数は1、024個に制限されています。クラスタで許可されている数よりも多くのルールが必要な場合は、LDAPサーバ属性を変更して、Windowsユーザ名と同じ値のUNIXユーザ名を含める必要があります。この場合でも、クライアントは希望のUID/GIDを取得します。

表10 のLDAPクライアントスキーマオプションを使用して、ネームマッピングを処理するようにLDAPを設定できます。

表10）LDAPクライアントスキーマのオプション

新しいLDAPスキーマ属性	キノウ
`-windows-to-unix-object-class`	WindowsからUNIXへのネームマッピングオブジェクトクラスを定義するLDAP属性を提供します。オブジェクトクラスは、複数のLDAPオブジェクトをグループ化して検索を高速化するために使用されます。AD-IDMUのデフォルト値はです `User`。RFC 2037スキーマの場合、値はに設定されます `posixAccount`。
`-windows-to-unix-attribute`	WindowsユーザをUNIXユーザにマッピングするために使用する値のLDAP属性を指定します。ONTAPのAD-IDMUスキーマのデフォルト値はです `sAMAccountName`。RFC 2307スキーマの場合、この値のデフォルトはです `windowsAccount`。
`-windows-to-unix-no-domain- prefix`	このオプションは、の属性値に `- windows-to-unix-attribute` ドメインプレフィックスを追加するかどうかを制御します。（デフォルトはです `false`）。`sAMAccountName` は（ではなく `DOMAIN\username`）単一のユーザ名で表され、`msDS- PrincipalName` はLDAP検索で使用できる値ではないため、ドメインプレフィックスは、機能的な非対称ネームマッピングを有効にするために必要になる場合があります。この値の必要性は、使用されているLDAPスキーマと属性、および複数の一意のWindowsドメインに複数のドメイン名マッピングが存在するかどうかによって異なります。

これらのオプションを使用すると、WindowsからUNIXへの双方向の非対称ネームマッピングと、LDAPサーバからUNIXからWindowsへの双方向のネームマッピングが可能になります。これらのオプションの属性値は、環境によって異なります。

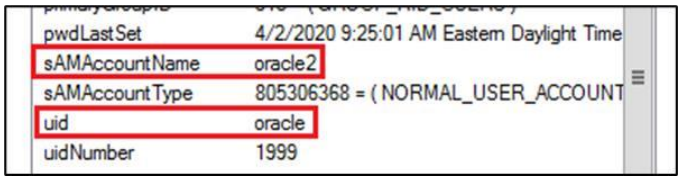
ほとんどのActive Directory LDAPサーバでは、非対称ネームマッピングの値は次のとおりです。

```
-windows-to-unix-object-class User
-windows-account-attribute sAMAccountName
```

上記の値を使用すると、Active Directory LDAPは最初からネームマッピングと連携して機能します。デフォルトスキーマのバリエーションはすべて考慮する必要があります。

ユーザのLDAPでユーザ名のマッピングを設定するには、`uid` 属性のフィールドに別の名前のユーザを入力します。`uid` とのユーザ名に図15の違いがあることに注意してください `sAMAccountName`。

図15）LDAPを使用した非対称ネームマッピング



次の例は、oracle2という名前のWindowsユーザへの、oracle2という名前のUNIXユーザのマッピング（およびその逆）を示しています。

UNIX > WindowsおよびWindows > UNIXネームマッピングの使用例

```
cluster::*> access-check name-mapping show -vserver DEMO -direction win-unix -name oracle

'oracle2' maps to 'oracle'

cluster::*> access-check name-mapping show -vserver DEMO -direction unix-win -name oracle2

'oracle2' maps to 'NTAP\oracle2'
```

UNIXユーザからWindowsユーザへの非対称ネームマッピング

ONTAPで定義されているLDAPスキーマには、名をWindows名にマッピングするときに使用するLDAPスキーマ属性を定義する「ONTAPネームマッピングwindowsAccount属性」（`-windows-account-attribute`）という属性が含まれています。この属性のデフォルト値はsAMAccountNameです。これは、新しいユーザーが作成されるときにWindowsアカウントで使用される標準フィールドです。

この値は、必要に応じてカスタムLDAPクライアントスキーマを作成することで変更できます。詳細については、「カスタムLDAPスキーマの作成」を参照してください。

複数ドメインにわたるUNIXからWindowsへのネームマッピング

シナリオによっては、UNIXからWindowsへのネームマッピングで、異なるドメインに属する複数のユーザを考慮しなければならない場合があります。

例：

- `DEMO` SVMのにCIFS / SMBサーバがあり `NTAP.LOCAL`、UNIXユーザにもLDAPを使用しています。
- `DEMO`のLDAPクライアントが `NTAP.LOCAL` UNIXユーザ検索をポイントしています。
- `DEMO` 新しい企業B社を買収し、という新しいSVMを作成します。`COMPANYB`
- 企業BのActive Directoryドメイン `CORE-TME.NETAPP.COM` にもUNIXユーザが含まれています。
- `NTAP.LOCAL CORE-TME.NETAPP.COM` 双方向の信頼関係が構築されています
- この信頼は、両方のドメインが相手のドメイン内のWindowsユーザに照会できることを意味します。

ここでの目的は、どのドメインに属しているかに関係なく、UNIXユーザからWindowsユーザへのネームマッピングをONTAPで実行できるようにすることです。ドメインは信頼されているため、両方のSVMが問題のない他のドメインのWindowsユーザを検出できます。

```
cluster::*> access-check authentication translate -vserver DEMO -win-name CORE-TME\ldapuser
S-1-5-21-1426196048-1826357187-2923433760-3643

cluster::*> access-check authentication translate -vserver COMPANYB -win-name NTAP\student2
S-1-5-21-3552729481-4032800560-2279794651-1109
```

ただし、まず最初に、両方のSVMがUNIXユーザの場所に関係なくLDAPでUNIXユーザを検出できる必要があります。LDAPクライアントの初期設定では、各SVMは独自のUNIXユーザを検索できますが、信頼できるドメインのUNIXユーザは検索できません。

```
cluster::*> access-check authentication translate -vserver COMPANYB -unix-user-name ldapuser
1108
cluster::*> access-check authentication translate -vserver COMPANYB -unix-user-name prof1
  (vserver services access-check authentication translate)

Vserver: COMPANYB (internal ID: 3)

Error: Acquire UNIX credentials procedure failed
  [  6 ms] Hostname found in Name Service Cache
  [     7] Hostname found in Name Service Cache
  [    16] Successfully connected to ip 10.193.67.93, port 389 using
           TCP
**[    24] FAILURE: User 'prof1' not found in UNIX authorization
**         source LDAP.
  [    24] Entry for user-name: prof1 not found in the current
           source: LDAP. Ignoring and trying next available source
  [    25] Entry for user-name: prof1 not found in the current
           source: FILES. Entry for user-name: prof1 not found in
           any of the available sources
  [    25] Unable to retrieve UID for UNIX user prof1

Error: command failed: Failed to resolve user name to a UNIX ID. Reason: "SecD Error: object not
found".
```

複数のドメインを双方向に正しくマッピングするには、いくつかの手順を実行する必要があります。

1. 複数の一意のLDAPサーバを検索するようにLDAPクライアントを設定します。
2. 複数のドメイン間でUNIXからWindowsへのマッピングを設定します。

手順1：複数の一意のLDAPサーバを検索するようにLDAPクライアントを設定する

両方のSVMがLDAPでユーザを検索できるようにするには、Active Directoryに次の2つのオプションがあります。

- 「Active Directoryグローバルカタログ検索」セクションに従って、UNIX属性をグローバルカタログにレプリケートするようにActive Directoryを構成します。
- LDAPリファーラルを活用します（「LDAPリファーラル（追跡リファーラル）」の項を参照）。

各オプションにはいくつかの要件があります。

グローバルカタログLDAPによるUNIX IDの検索

グローバルカタログを使用して複数のドメインで作業するLDAP検索には、次のものが必要です。

- 同じフォレスト内の複数のドメイン：
  - 異なるフォレスト内の複数のドメインはグローバルカタログにアクセスできません。
- ドメイン信頼は適切に機能します。
- グローバルカタログのフォレストレベルに複製されたUNIX属性。
- フォレストのActive Directoryドメイン用に設定されているONTAP SVM LDAPクライアント。
- 適切に機能するDNS。

- ドメイン間で同期された時間。
- LDAPクライアントがポート3268に設定されている（ポート3269はONTAPではサポートされていません）。
- 両方のドメインのオブジェクトを表示できるバインドユーザ。

UNIX IDのLDAPリファーラル

ドメインが異なるフォレストにある場合、またはグローバルカタログを使用できない場合は、LDAPリファーラルを使用できます。Windows Active DirectoryベースではないLDAPサーバにもLDAPリファーラルを使用できます。LDAPリファーラルが正しく機能するには、次の条件を満たしている必要があります。

- LDAPリファーラルがSVM LDAPクライアントで有効になっている（`-referrals-enabled`）。
- LDAPポート389が使用されます（ポート636はLDAPリファーラルでは使用できません）。
- LDAPサーバはリファーラル（チェイスリファーラルとも呼ばれる）をサポートできます。
- LDAPサーバリスト（`-servers`）は、複数のLDAPサーバ（IPアドレスまたはホスト）または負荷分散されたIPアドレスを持つ完全修飾ドメイン名（FQDN）であるか、Active Directoryドメイン（-ad-domain）が設定され、DNSにLDAPサーバの複数のSRVレコードが設定されているかのいずれかです。
- 複数のDNSがベースDN（`-base-dn`）で設定され、オプションでユーザ、グループ、およびネットグループDN（`-user-dn`、`-group-dn`、`-netgroup-dn`）でも設定されます。
- バインドレベル（`-min-bind-level`）およびバインドDN（`-bind-dn`）は、リストされているすべてのLDAPサーバにバインドできます。

次の例では `NTAP.LOCAL`、LDAPリファーラルを使用してドメインと `CORE-TME.NETAPP.LOCAL` ドメインの両方のLDAPサーバ（同じフォレスト内にない信頼できるドメイン）を照会するようにLDAPクライアントが設定されています。

LDAPリファーラルを使用する複数ドメインのLDAPクライアント設定の例

この例では、LDAPリファーラル追跡が機能するために必要なフィールドが黄色で強調表示されています。

```
cluster::> ldap client show -client-config LDAP

                                  Vserver: COMPANYB
                Client Configuration Name: LDAP
                         LDAP Server List: -
            (DEPRECATED)-LDAP Server List: -
                  Active Directory Domain: ntap.local
       Preferred Active Directory Servers: -
Bind Using the Vserver's CIFS Credentials: true
                           Schema Template: DEMO2
                         LDAP Server Port: 389
                      Query Timeout (sec): 3
        Minimum Bind Authentication Level: sasl
                            Bind DN (User): -
                                   Base DN: DC=CORE-TME,DC=NETAPP,DC=COM;DC=NTAP,DC=LOCAL
                       Base Search Scope: subtree
              Vserver Owns Configuration: true
     Use start-tls Over LDAP Connections: false
                  Client Session Security: none
                    LDAP Referral Chasing: true
```

上記の例では、Active Directoryドメインはです `NTAP.LOCAL`。`DNS SRV LDAP CORE-TME` ドメインのDNSサーバにレコードが追加され、`CORE-TME` ゾーンがセカンダリゾーンとしてDNSサーバに追加されました。ONTAPはSVMから両方を照会できます。

```
cluster::*> access-check dns srv-lookup -vserver COMPANYB -lookup-string _ldap._tcp.core-
tme.netapp.com
Got 4 Ip Addresses
10.193.67.200
2001:db8::1
10.193.67.181
10.193.67.93

cluster::*> access-check dns srv-lookup -vserver COMPANYB -lookup-string _ldap._tcp.ntap.local
```

```
Got 4 Ip Addresses
10.193.67.236
10.193.67.200
2001:db8::1
10.193.67.181
```

上記の設定を使用すると、両方のドメインのUNIXユーザを照会できるようになります。

```
cluster::*> access-check authentication translate -vserver COMPANYB -unix-user-name ldapuser
  (vserver services access-check authentication translate)
1108

ontap9-tme-8040::*> access-check authentication translate -vserver COMPANYB -unix-user-name prof1
  (vserver services access-check authentication translate)
1100
```

UNIXユーザIDとグループIDの競合

同一のユーザ名または数値IDが複数のドメインに存在する場合があります。この状況では、正しいUID、ユーザ名、またはGIDがわからないため、ONTAPで問題が発生する可能性があります。代わりに、最初に見つかったものを返します。LDAP検索に複数のドメインを使用する場合は、ユーザとグループの検索の不一致を避けるために、ドメイン間でユーザまたはグループが重複しないようにしてください。

手順2：複数のドメインにわたるUNIXからWindowsへのマッピングを構成する

あるユーザが1つのLDAPクライアント設定（UNIX LDAPやCentrifyなど）でUNIXユーザとしてのみ存在し、別のドメイン内の有効なWindowsユーザにマッピングできる必要がある場合があります。

次の例では CORE-TME、という名前のにユーザを作成し user、UNIXユーザ名をに設定しています username。非対称のネームマッピングルールはないため、username は CORE-TME\username デフォルトでという名前のWindowsユーザを検索します。このコマンドを実行すると、UNIX UIDは検出されますが、有効なWindowsユーザに NTAP\username NTAP.LOCAL マッピングできません。という名前の有効なWindowsユーザがSVMで正しく認識され、WindowsがUNIXに適切にマッピングされている場合でも、マッピングは失敗します。

```
cluster::*> access-check authentication show-creds -vserver COMPANYB -unix-user-name username
-list-name true -list-id true
  (vserver services access-check authentication show-creds)

Vserver: COMPANYB (internal ID: 3)

Error: Get user credentials procedure failed
   [ 0 ms] Determined UNIX id 1998 is UNIX user 'username'
  [     0] Trying to map 'username' to Windows user 'username' using
           implicit mapping
  [     1] Using a cached connection to
           stme-infra02.core-tme.netapp.com
  [     2] Could not find Windows name 'username'
  [     2] Unable to map 'username'. No default Windows user defined.
**[     2] FAILURE: Name mapping for UNIX user 'username' failed. No
**         mapping found

Error: command failed: Failed to get user credentials. Reason: "SecD Error: Name mapping does not
exist".


cluster::*> access-check authentication show-creds -vserver COMPANYB -win-name NTAP\username -
list-name true -list-id true
  (vserver services access-check authentication show-creds)

 UNIX UID: 1998 (username) <> Windows User: S-1-5-21-3552729481-4032800560-2279794651-1242
(NTAP\username (Windows Domain User))

 GID: 513 (Domain Users)
 Supplementary GIDs:
  513 (Domain Users)
```

```
 Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows
Domain group)

 Windows Membership:
  S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows Domain group)
  S-1-18-2   Service asserted identity (Windows Well known group)
  S-1-5-21-0-0-0-497   NT AUTHORITY\Claims Valid (Windows Well known group)
 User is also a member of Everyone, Authenticated Users, and Network Users
```

UNIXユーザが Windowsユーザと同じ信頼できるドメインに属している場合は、UNIXからWindowsへのネームマッピングが機能します。設定は必要ありません。たとえば、LDAP設定がをポイントして CORE-TME おり、という名前のユーザが prof1 NTAP.LOCAL 対応するWindowsユーザと一緒に住んでいる場合、想定どおりに動作します。

```
cluster::*> access-check authentication show-creds -vserver COMPANYB -unix-user-name prof1 -list-
name true -list-id true
  (vserver services access-check authentication show-creds)

 UNIX UID: 1100 (prof1) <> Windows User: S-1-5-21-3552729481-4032800560-2279794651-1110
(NTAP\prof1 (Windows Domain User))

 GID: 1101 (ProfGroup)
 Supplementary GIDs:
  1101 (ProfGroup)
  10000 (Domain Users)
  1201 (group1)
  1202 (group2)
  1203 (group3)
  1220 (sharedgroup)

 Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-1111   NTAP\ProfGroup (Windows
Domain group)

 Windows Membership:
  S-1-5-21-3552729481-4032800560-2279794651-1106   NTAP\group2 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows Domain group)
 User is also a member of Everyone, Authenticated Users, and Network Users
```

このシナリオで、ドメイン間でUNIXからWindowsへのマッピングを正しく機能させるには、次の2つの手順を実行する必要があります。

- すべてのUNIXユーザをドメインおよびユーザのワイルドカードにマッピングするUNIXからWindowsへのネームマッピングルールを作成します。
- name-mapping-search ONTAPが他の信頼できるドメインでUNIXからWindowsへのネームマッピングを検索するように、SVMにエントリを追加します。

この例では、次の処理を実行します。

```
cluster::*> vserver name-mapping create -vserver COMPANYB -direction unix-win -pattern * -
replacement *\\* -position 1

cluster::*> name-mapping-search add -vserver COMPANYB -trusted-domains NTAP.LOCAL
```

この手順を実行すると、以前は作業していなかった username UNIXユーザがWindowsユーザにマッピングされNTAP\usernameます。

```
cluster::*> access-check authentication show-creds -vserver COMPANYB -unix-user-name username -
list-name true -list-id true
  (vserver services access-check authentication show-creds)

 UNIX UID: 1998 (username) <> Windows User: S-1-5-21-3552729481-4032800560-2279794651-1242
(NTAP\username (Windows Domain User))

 GID: 513 (Domain Users)
 Supplementary GIDs:
  513 (Domain Users)
```

```
 Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows
Domain group)

 Windows Membership:
  S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows Domain group)
  S-1-18-2   Service asserted identity (Windows Well known group)
  S-1-5-21-0-0-0-497   NT AUTHORITY\Claims Valid (Windows Well known group)
User is also a member of Everyone, Authenticated Users, and Network Users
```

Active Directoryライトウェイトディレクトリサービス

ドメインコントローラ全体を設定する代わりに、スタンドアロンのWindowsサーバを使用してUNIXユーザおよびグループにLDAPサービスを提供できます。たとえば、ユーザとグループを処理する場所が必要で、Kerberos認証が不要な場合や、アプリケーションにLDAP機能だけが必要な場合は、Lightweight Directory Services（LDS）を使用できます。このディレクトリサービスは、Active Directory LDS機能を介して使用できます。

LDSでユーザ、グループ、およびネットグループを管理するには、ADSI Editを使用する必要があります。Active Directoryユーザーやコンピュータなどのユーティリティは、ドメインユーザーの管理を目的としており、スタンドアロンLDSインスタンスでは動作しません。

Active Directory LDSをUNIX IDで使用するように設定するには、「Active Directory LDS Identity Mapping for Services for NFS」を参照してください。

ONTAPでActive Directory LDSを使用するには、他のLDAPサーバと同じ設定手順を実行します。次の例は、ONTAP SVMから、Windows 2019で実行されているスタンドアロンのActive Directory LDSサーバへのクエリを示しています。

```
cluster::*> getxxbyyy getpwbyname -node node1 -vserver NFS -username lds -show-source true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name: lds
pw_passwd:
pw_uid: 1001
pw_gid: 1101
pw_gecos:
pw_dir:
pw_shell:
```

セキュアなLDAPの設定

ONTAPは、TLS 1.2やAES-256 Kerberosなどの業界標準のセキュリティメカニズムを使用したエンドツーエンドの暗号化により、ネットワークを介したLDAP通信を保護するためのいくつかの方法を提供します。次の項では、これらの方法の概要を設定する方法について説明します。詳細な手順については、LDAPサーバベンダーのマニュアルを参照してください。

STARTTLSとLDAPS

このレポートの「Start Transport Layer Security vs. LDAP over SSL」セクションでは、StartTLSとLDAPSの違いについて説明します。両方のアプリケーションの設定は非常によく似ています。どちらのアプリケーションでも、LDAPサーバとONTAP SVMに証明書が存在する必要があります。セットアップのこの部分は一般的に最も複雑です。

ONTAP LDAPクライアントの設定は比較的簡単です。LDAPSの場合は、ポートを636に設定すると、ONTAPはバインドとクエリにLDAPSを使用することを認識します。StartTLSを使用するには、ポートを389に設定し、`-use- start-tls` オプションを有効にします。残りの処理はONTAPが実行します（証明書がSVMにインストールされている場合）。

LDAPSまたはStartTLSを設定するには、一般的に次の3つの手順を実行します。

1. LDAPサーバに証明書サービスを設定します。

2. `security certificate` コマンドを使用して、目的のSVMに証明書をインストールします。
3. StartTLSまたはLDAPSを使用するようにLDAPクライアントを設定します。

以降のセクションでは、これらの手順について詳しく説明します。

FreeIPAでの証明書の管理

次のリンクを使用して、LDAPで使用する証明書をFreeIPAで作成します。

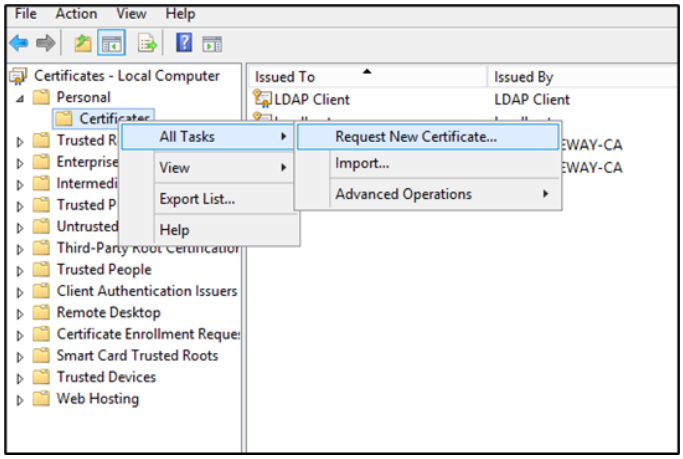
- FreeIPA: LDAPを使用したHOWTO/クライアント証明書認証
- Red Hat：ユーザ、ホスト、サービスの証明書の管理

Windows Active Directory LDAPでの証明書の管理

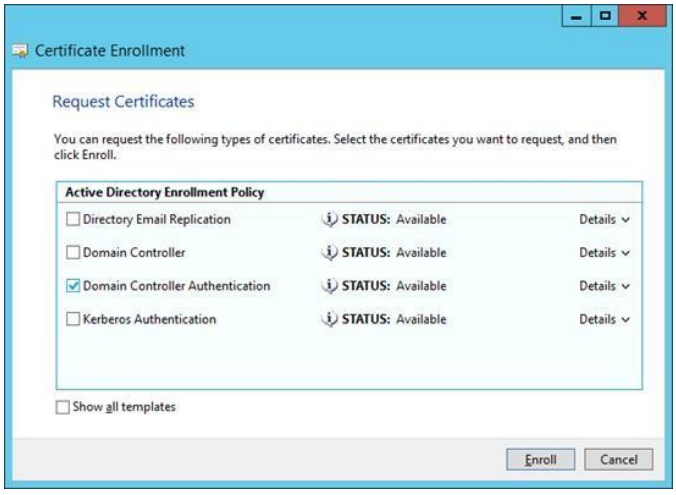
Windows Active Directoryで証明書を管理するには、証明書機能を環境にインストールして設定しておく必要があります。この機能を使用すると、SSLまたはStartTLSを使用するセキュアなLDAPのONTAPで使用するために必要な証明書を生成できます。Microsoftの手順を使用するか、Microsoftにお問い合わせください。

証明書機能をインストールした後、証明書を管理するには、次の手順を実行します。

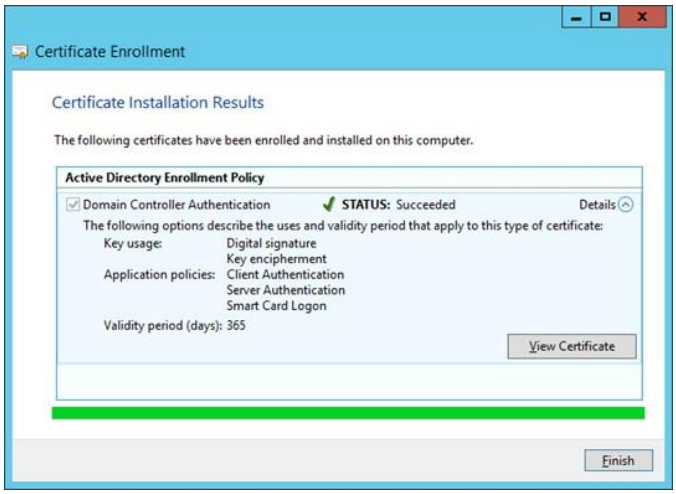
1. [コンピュータ証明書の管理]ウィンドウに移動します。[個人]>[証明書]を右クリックし、[すべてのタスク]>[新しい証明書の要求]を選択します。



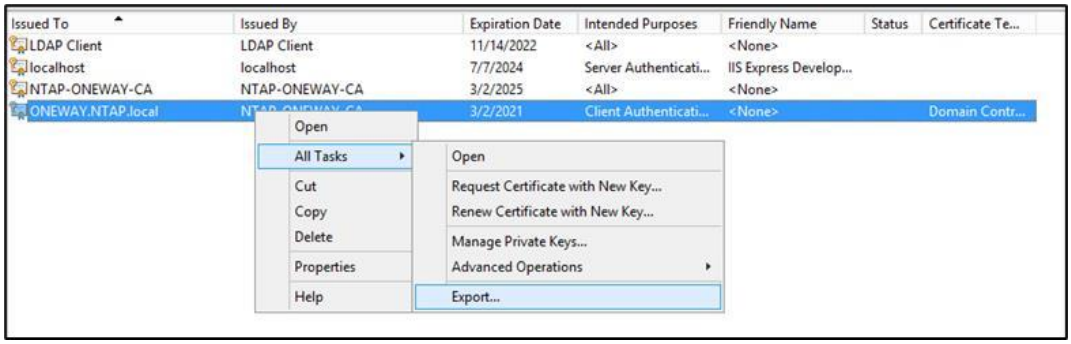
2. Certificate Enrollment（証明書登録）ウィザードに従って、登録ポリシーとしてDomain Controller Authentication（ドメインコントローラ認証）を選択します。



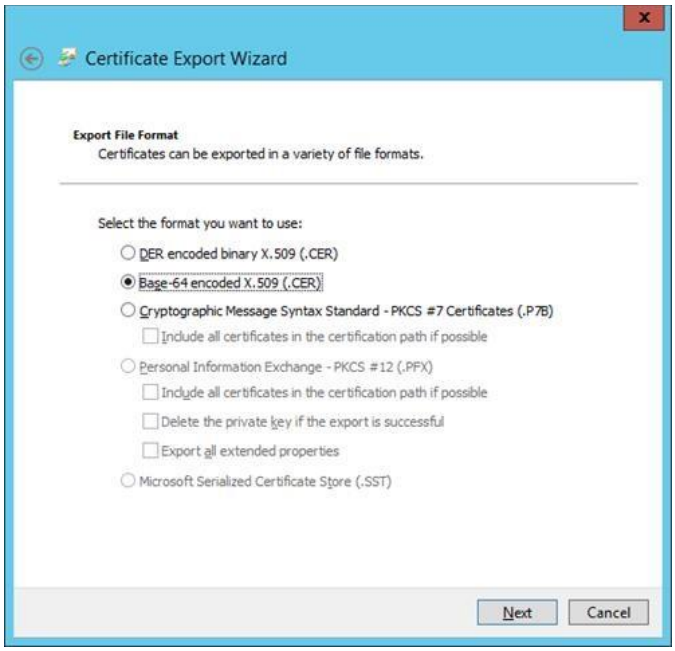
3. [登録]をクリックすると、証明書をエクスポートする準備が整います。



4. [Personal]>[Certificates]フォルダの新しい証明書に移動します。Active Directoryドメインと同じ名前にする必要があります。右クリックして、[すべてのタスク]>[エクスポート]を選択します。



5. 証明書のエクスポートウィザードを使用して、新しい `.cer` ファイルを作成します。このファイルを使用して、LDAP over SSLまたはStartTLS用のONTAP SVMに証明書をインストールします。Base-64 `.cer` では、すぐに使用できるファイルが提供されます。DERでエンコードされたバイナリは `certutil`、Windowsのを使用して変換する必要があります。



6. ウィザードが完了したら、`.cer` ファイルを開くことができます。次で始まる長いテキスト文字列が表示されます。

```
-----BEGIN CERTIFICATE-----
```

7. これで、ONTAP SVMに証明書をインストールする準備ができました。

ONTAPへの証明書のインストール

ONTAPのSVMは `security certificate`、コマンドを使用してLDAPサーバからセキュリティ証明書をインポートする方法を提供します。

```
cluster::*> security certificate ?
  ca-issued>                  Show Digital Certificates Issued by Self-Signed CA
  config>                     The config directory
  create                      Create and Install a Self-Signed Digital Certificate
  delete                      Delete an Installed Digital Certificate
  file>                       *Show Digital Certificate files
  generate-csr                Generate a Digital Certificate Signing Request
  install                     Install a Digital Certificate
  print                       Display the contents of a certificate
  remove-precluster-cert      *This command removes the auto-generated precluster certificate
from all nodes
  rename                      Rename a certificate
  show                        Display Installed Digital Certificates
  show-generated              Display ONTAP generated certificates
  show-truststore             Display default truststore certificates
  show-user-installed         Display user installed certificates
  sign                        Sign a Digital Certificate using Self-Signed Root CA
  truststore>                 truststore
```

管理SVMにはデフォルトでいくつかの既知のCA証明書（VerisignやAmazonなど）が含まれており、必要に応じてコピーして他のSVMで使用できます。`security certificate install` コマンドは、Active Directory LDAPであるかどうかに関係なく、任意の証明書タイプを指定して使用できます。

前のセクションでは、Active Directory LDAPで使用する自己署名証明書を生成する方法について説明しました。この証明書を使用するには、次のコマンドを実行して `server-ca` 証明書をインストールします。

```
cluster::*> security certificate install -type server-ca -vserver DEMO -cert-name MS-LDAP
```

そのコマンドが実行されると、.cer ファイルの内容をコピーして貼り付けるように求められます。この手順が完了したら、Enterキーを押して証明書をインストールします。

```
You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: NTAP-ONEWAY-CA
Serial: 5500000004B5165DB556062E5E000000000004
```

証明書を表示するには、次のコマンドを使用します。

```
cluster::*> security certificate show -vserver DEMO -common-name MS-LDAP
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- ---------------------------------------------- ----------------
DEMO       5500000004B5165DB556062E5E000000000004
                           ONEWAY-DOMAIN-AUTH                     server-ca
    Certificate Authority: NTAP-ONEWAY-CA
          Expiration Date: Tue Mar 02 17:21:13 2021
```

テストできるようになりました。

LDAPSまたはStartTLSの設定とテスト

server-ca LDAPサーバから証明書をインストールしたら、LDAPのバインドとクエリで使用するStartTLSまたはLDAPSを有効にすることができます。証明書の設定またはインストールに誤りがあると、ONTAPは、指定されたセキュリティ設定を使用して基本的なバインドを実行できない場合、構成の変更やLDAPクライアントの作成を阻止します。たとえば、適切な証明書が設定されていない場合、次のエラーが発生します。

```
cluster::*> ldap client modify -client-config DEMO -vserver DEMO -use-start-tls true

Error: Validate the Ldap configuration procedure failed
  [ 6 ms] Hostname found in Name Service Cache
  [     7] Successfully connected to ip 10.193.67.236, port 389
           using TCP
  [    13] Unable to start TLS: Server is unavailable
  [    13] Additional info: 00000000: LdapErr: DSID-0C09102C,
           comment: Error initializing SSL/TLS, data 0, v2580
  [    13] Unable to connect to LDAP (NIS & Name Mapping) service on
           oneway.ntap.local
  [    13] No servers available for LDAP_NIS_AND_NAME_MAPPING,
           vserver: 10, domain: .
**[    13] FAILURE: Unable to make a connection (LDAP (NIS & Name
**         Mapping):), result: 6940
Error: command failed: The LDAP client configuration "DEMO" for Vservers "DEMO" is an invalid
configuration.

cluster::*> ldap client modify -client-config DEMO -vserver DEMO -port 636

Error: Validate the Ldap configuration procedure failed
  [ 4 ms] Hostname found in Name Service Cache
  [    10] Successfully connected to ip 10.193.67.236, port 636
           using TCP
  [    67] Unable to start LDAPS: Can't contact LDAP server
  [    67] Unable to connect to LDAP (NIS & Name Mapping) service on
           oneway.ntap.local (Error: Can't contact LDAP server)
  [    67] No servers available for LDAP_NIS_AND_NAME_MAPPING,
           vserver: 10, domain: .
**[    67] FAILURE: Unable to make a connection (LDAP (NIS & Name
**         Mapping):), result: 6940
Error: command failed: The LDAP client configuration "DEMO" for Vservers "DEMO" is an invalid
configuration.
```

このアプローチは、誤ったLDAP設定によるシステム停止からの保護手段です。-skip-config-validation オプションを使用すると、このチェックを省略できます。

LDAP over SSLまたはStartTLSが機能していることを示す兆候は、`create modify` コマンドまたはコマンドがエラーなく機能するという事実にすぎません。

```
cluster::*> ldap client modify -client-config DEMO -vserver DEMO -use-start-tls true

Warning: You may also want to modify "-use-start-tls-for-ad-ldap" option to "true" using "vserver
cifs security modify" command for the following Vserver(s): DEMO.
```

「ONTAP CLI commands for LDAP troubleshooting」セクションのコマンドを使用して、追加のチェックを実行できます。

図16 と 図17 は、StartTLSとLDAPSを使用する同一のLDAPクエリからのパケットキャプチャの例です。通信はほぼ同じですが、StartTLSにはTLSハンドシェイクがあり、ポート389を介して転送されます。

図16）LDAP StartTLSのパケットキャプチャ

No.	Time	Source	Destination	Protocol	Length	Info
113	11.666463	10.193.67.237	10.193.67.236	DNS	81	Standard query 0xf22e SRV _ldap._tcp.ntap.local
114	11.666685	10.193.67.236	10.193.67.237	DNS	134	Standard query response 0xf22e SRV _ldap._tcp.ntap.local SRV 0 100 389 oneway.ntap.local A 10.193.67.236
118	11.668039	10.193.67.237	10.193.67.236	LDAP	97	extendedReq(1) LDAP_START_TLS_OID
119	11.668187	10.193.67.236	10.193.67.237	LDAP	112	extendedResp(1) LDAP_START_TLS_OID
120	11.672492	10.193.67.237	10.193.67.236	TLSv1.2	281	Client Hello
121	11.675113	10.193.67.236	10.193.67.237	TLSv1.2	1929	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
123	11.677428	10.193.67.237	10.193.67.236	TLSv1.2	260	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
124	11.679146	10.193.67.236	10.193.67.237	TLSv1.2	173	Change Cipher Spec, Encrypted Handshake Message
125	11.683812	10.193.67.237	10.193.67.236	TLSv1.2	1495	Application Data
126	11.684520	10.193.67.236	10.193.67.237	TLSv1.2	359	Application Data
127	11.687963	10.193.67.237	10.193.67.236	TLSv1.2	311	Application Data
128	11.688896	10.193.67.236	10.193.67.237	TLSv1.2	407	Application Data

図17）LDAPSのパケットキャプチャ

No.	Time	Source	Destination	Protocol	Length	Info
152	3.473521	10.193.67.237	10.193.67.236	DNS	81	Standard query 0x1a3d SRV _ldap._tcp.ntap.local
153	3.473672	10.193.67.236	10.193.67.237	DNS	134	Standard query response 0x1a3d SRV _ldap._tcp.ntap.local SRV 0 100 389 oneway.ntap.local A 10.193.67.236
157	3.482542	10.193.67.237	10.193.67.236	TLSv1.2	281	Client Hello
158	3.485094	10.193.67.236	10.193.67.237	TLSv1.2	1929	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
160	3.487064	10.193.67.237	10.193.67.236	TLSv1.2	260	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
161	3.489659	10.193.67.236	10.193.67.237	TLSv1.2	173	Change Cipher Spec, Encrypted Handshake Message
162	3.490151	10.193.67.237	10.193.67.236	TLSv1.2	1495	Application Data
163	3.491023	10.193.67.236	10.193.67.237	TLSv1.2	359	Application Data
164	3.494340	10.193.67.237	10.193.67.236	TLSv1.2	311	Application Data
165	3.495495	10.193.67.236	10.193.67.237	TLSv1.2	407	Application Data

LDAPの署名と封印（LDAPセッションセキュリティ）

Windows Active Directory LDAPを使用すると、セキュリティ証明書を設定する必要なく、LDAP通信をネイティブで保護できます。このメソッドを制御するLDAPクライアントオプションはです `-session-security`。LDAPの署名と封印を使用する場合は 、「CIFS / SMBサーバのセキュリティに関する考慮事項」の説明に従って、CIFS / SMBセキュリティ設定の構成も検討してください。

セッションセキュリティを設定するには、次の3つのオプションがあります。

- **なし。**セッションセキュリティは適用されません。
- **サインだ**セッションセキュリティは、署名（整合性検証）LDAPセッションに対してのみ適用されます。このセットアップでは、LDAPクエリをネットワーク経由でパケットキャプチャに表示できます。
- **封印だ**セッションセキュリティは、LDAPセッションの署名と封印の両方に適用されます。この設定では、LDAPクエリは暗号化され、パケットキャプチャには表示されません。

当然のことながら、署名と封印は最も安全ですが、処理に最もオーバーヘッドがかかり、クエリに多少の遅延が発生する可能性があります。結果は、ネットワークの負荷、サーバの負荷、およびクエリのサイズによって異なります。NetAppでは、テストを実施することを推奨しています。

図18 と 図19 は、LDAPの署名と封印のパケットキャプチャと、パケットキャプチャで表示できるものと表示できないものの違いを示しています。

図18）署名を有効にしたLDAPのパケットキャプチャ

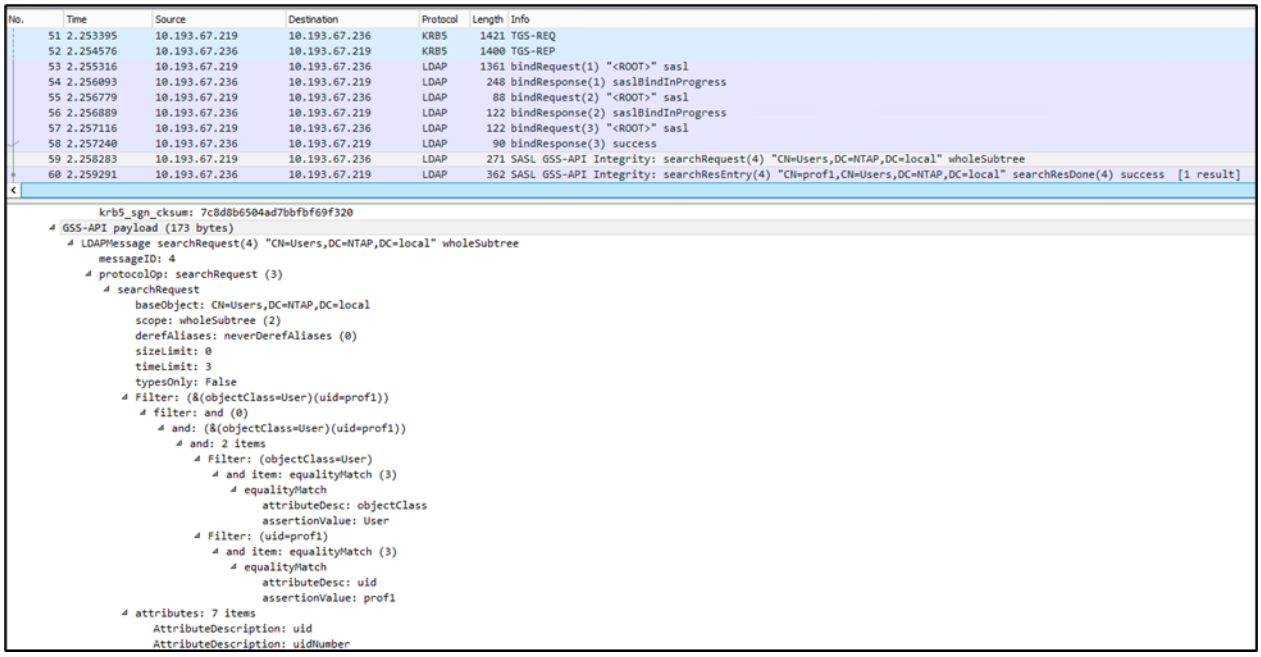
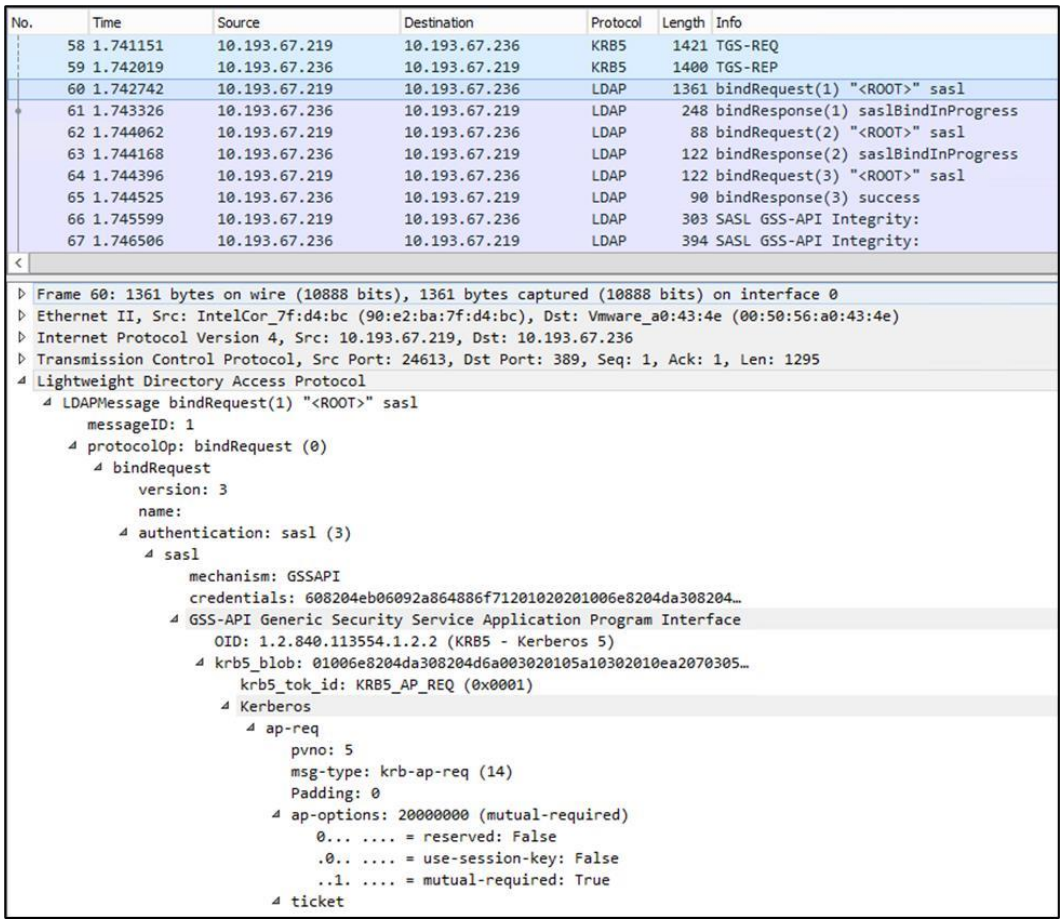


図19）署名と封印を有効にしたLDAPのパケットキャプチャ

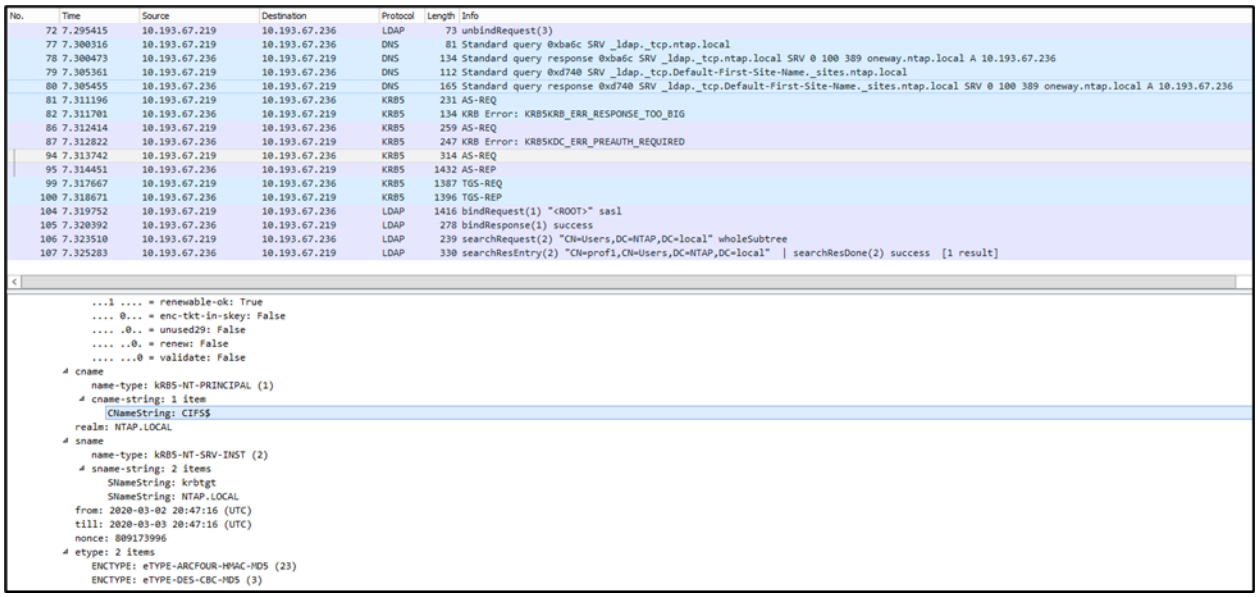


CIFS/SMBサアハトシテノハイント

UNIXユーザおよびグループの検索にWindows Active Directory LDAPを使用し、同じSVMにCIFS / SMBサーバも設定されている場合は、ユーザ名/パスワードまたは匿名バインドを使用する代わりに、CIFS / SMBサーバマシンアカウントを使用してLDAPにバインドできます。CIFS / SMBサーバとしてのバインドは簡単です。 `-bind-as-cifs-server true` LDAPクライアントでオプションをに設定し、設定されているCIFS / SMBサーバに適切なDNSエントリがあることを確認します。ONTAPは、CIFS/SMBサーバの作成時にCIFS/SMBサーバのKerberos SPNを自動的に設定します。

CIFS / SMBマシンアカウントとしてのバインドでは、Active Directoryドメインと同じセキュリティメカニズムを使用します。マシンアカウント認証は `GSS- SPNEGO`、まずKerberosを使用してネゴシエートしようとします。有効なSPNがKDCに存在する場合は、KDCで使用可能な最も強力なサポートされている暗号化タイプでKerberosバインドが使用されます。Windows 2008以降では、暗号化はAES-256です。図20 は、CIFS / SMBサーバを使用したLDAPバインドのパケットキャプチャを示しています。

図20）CIFS / SMBサーバとしてのLDAPバインディングのパケットキャプチャ



Kerberos SPNを使用できない場合、マシンアカウント認証はNTLMにフォールバックされます。ドメインでNTLMがブロックされている場合、ONTAP LDAPクライアントはユーザ名とパスワードが設定されているかどうかを確認します。そうしないと、バインドは失敗します。

CIFS / SMBサーバとしてバインドする場合の考慮事項

CIFS / SMBサーバとしてバインドする場合は、次の点を考慮してください。

- CIFS / SMBのライセンスが設定されていること、およびCIFS / SMBサーバが設定されていることを確認してください。
- 使用しているCIFSサーバ名に対応するDNSエントリが存在することを確認します。
- ONTAPのSVMにDNSが設定されていることを確認します。
- LDAPクライアントで、Active Directoryドメインに `-ad-domain` オプションが設定されていることを確認します。
- LDAPクライアントの最小バインドレベル（`-min-bind-level`）をSASLに設定します。
- ドメインでNTLMが無効になっている場合は、Kerberosバインドが失敗した場合に備えて、フォールトトレランス用にバインドユーザとパスワードを設定することを検討してください。

CIFS / SMBサーバのセキュリティに関する考慮事項

LDAPサービスにActive Directoryを使用する場合は、LDAPトラフィックの保護を強化するためにCIFS / SMB固有のオプションもいくつか設定できます。

advanced権限で使用できるオプションは次のとおりです。

```
cluster::*> cifs security modify -vserver DEMO ?
  [ -kerberos-clock-skew <integer> ]
Maximum Allowed Kerberos Clock Skew
  [ -kerberos-ticket-age <integer> ]
Kerberos Ticket Lifetime
  [ -kerberos-renew-age <integer> ]
Maximum Kerberos Ticket Renewal Days
  [ -kerberos-kdc-timeout {1..23} ]
Timeout for Kerberos KDC Connections (Secs)
  [ -is-signing-required {true|false} ]
Require Signing for Incoming CIFS Traffic
  [ -is-password-complexity-required {true|false} ]
Require Password Complexity for Local User Accounts
  [ -use-start-tls-for-ad-ldap {true|false} ]
Use start_tls for AD LDAP Connections
  [ -is-aes-encryption-enabled {true|false} ]
Is AES-128 and AES-256 Encryption for Kerberos Enabled
  [ -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb} ]
LM Compatibility Level
  [ -is-smb-encryption-required {true|false} ]
Require SMB Encryption for Incoming CIFS Traffic
  [ -session-security-for-ad-ldap {none|sign|seal} ]
Client Session Security
  [ -smb1-enabled-for-dc-connections {false|true|system-default} ]
SMB1 Enabled for DC Connections
  [ -smb2-enabled-for-dc-connections {false|true|system-default} ]
SMB2 Enabled for DC Connections
  [ -referral-enabled-for-ad-ldap {true|false} ]
LDAP Referral Chasing Enabled For AD LDAP Connections
  [ -use-ldaps-for-ad-ldap {true|false} ]
```

CIFS / SMBセキュリティオプションは、CIFS / SMB通信のLDAP検索に適用されます。Active DirectoryとのUNIX LDAP通信には、LDAPクライアント設定を使用します。最大限のセキュリティを確保するには、CIFS / SMBとLDAPクライアントの両方のセキュリティ設定を使用します。

ネットグループヲホストスルタメノLDAPノシヨウ

LDAPではネットグループ機能を利用できますが、NISでは利用できません。ネットグループを使用すると、ストレージ管理者はグループを使用して一連のホストへのアクセスを制御できます。ホストごとに複数の異なるルールを作成する必要はありません。LDAPでは、ONTAPを使用して、ホスト名、IPアドレス、およびネットグループエントリを格納および照会できます。NISサーバとしてのLDAPの使用については、RFC 2307で説明されています。現在、ONTAPのネットグループでは、ホスト名とIPアドレスのみがサポートされています。

LDAPのNISオブジェクトおよび属性について

LDAPのNISオブジェクトタイプは、`objectClass` 属性によって決まります。`objectClass` オブジェクトに設定される属性によって、ONTAPおよびその他のLDAPクライアントがネットグループ関連オブジェクトをLDAPに照会する方法が決まります。ネットグループの場合、`nisNetgroup` オブジェクトクラスは、Active DirectoryやFreeIPAを含むほとんどのスキーマでデフォルトで使用されます。表11 に概要を示します。

表11）ネットグループのオブジェクトクラスタイプ

objectclass	使用目的	使用される共通属性
`nisMap`	NISマップ	`nisMapName`
`nisNetgroup`	ネットグループ	`nisMapName` `nisNetgroupTriple`

objectclass	使用目的	使用される共通属性
nisObject	ネットグループ netgroup.byhost エントリ	nisMapEntry nisMapName

NISオブジェクトに関する用語

表12 に、NISオブジェクトの特定の側面に関する用語を示します。

表12）NISオブジェクトの用語

期間	定義
NISマップ	NISマップは /etc、LinuxおよびUNIXクライアントのディレクトリにある一般的なファイルを一元管理し、置き換えるように設計されています。 ONTAPで現在サポートされているNISマップタイプは次のとおりです。 Passwd.byname および passwd.byuid Group.byname group.bygid Netgroup netgroup.byhost （ONTAP 8.3以降） ONTAPは現在、NISでのホスト名解決をサポートしていません。NISマップの詳細については、「Oracle NISマップ」を参照してください。
Netgroup	ネットグループは、権限およびエクスポートアクセスのチェックに使用される（ホスト、ユーザ、ドメイン）トリプルのセットです。ONTAPは現在、ネットグループエントリ内のホストのみをサポートしています。ネットグループでは、区切り文字としてカンマ（,）のみを使用する必要があります。 ネットグループの詳細については、Linuxのマニュアルページ と FreeBSDのマニュアルページを参照してください。
三重	ネットグループトリプルは、ネットグループファイル内の一連のエントリを意味し、（ホスト、ユーザ、ドメイン）で構成されます。ONTAPの有効なトリプルは(host,,)で構成されます。空白のフィールドを指定する場合は、使用するオペレーティングシステムに対応したネットグループファイルの標準ガイダンスに従ってください。ダッシュなどの特殊文字を使用すると、原因検索が失敗してアクセスが拒否される場合があります。ネットグループのトリプルで使用されるホスト名は、ONTAPでのDNS解決が必要です。ネットグループ変換のベストプラクティスについては、TR-4067および TR-4668のネームサービスのベストプラクティスを参照してください。
netgroup.byhost	netgroup.byhost エントリは、ネットグループ全体を照会するのではなく、ホスト単位でネームサービスにグループメンバーシップを照会することで、ネットグループ検索を高速化するために使用されます。エントリが多いネットグループの場合、このプロセスによって検索時間が大幅に短縮され、パフォーマンスが向上します。 netgroup.byhost サポートの詳細については、netgroup.byhostのサポートを参照してください。

ネットグループヨウノONTAPトActive Directory LDAPノソウゴウンヨウセイ

ONTAPが提供するスキーマでは、次の属性によってネットグループとそのメンバーの検索が制御されます。

```
-nis-netgroup-object-class
-nis-netgroup-triple-attribute
-member-nis-netgroup-attribute
-cn-netgroup-attribute
```

ONTAP 8.3以降では、次の属性がサポート対象として提供され netgroup.byhostます。詳細については、netgroup.byhostのサポートセクションを参照してください。

```
-nis-object-class
-nis-mapname-attribute
```

```
-nis-mapentry-attribute
```

LDAPクライアントスキーマを変更して、ネットグループのデフォルト属性を変更できます。ほとんどの場合、提供されている読み取り専用テンプレートは機能しますが、場合によっては、スキーマテンプレートを新しいテンプレートにコピーして変更する必要があります。スキーマの詳細については、このドキュメントの「LDAPスキーマ」の項を参照してください。

Active Directoryスキーマには、Windows Server 2012以降でデフォルトで追加された次のスキーマ属性があります（ONTAPで使用されるデフォルト属性は太字で示されています）。

```
memberNisNetgroup
msSFU30Name
msSFU30NetgroupHostAtDomain
msSFU30NetgroupUserAtDomain
msSFU30NisDomain
NisMap
nisMapEntry
nisMapName
nisNetgroup
nisNetgroupTriple
nisObject
```

Active Directory LDAPを使用したネットグループの作成

Active Directoryネットグループは `nis2ad`、ユーティリティ、`nismap`PowerShell、または ADSI Editなどの GUIツールを使用して制御できます。

nismapを使用したNISオブジェクトの作成

を使用すると `nis2ad`、既存のマップをNISからActive Directoryに移行したり、ローカルファイルからNISマップを作成したりできます。このユーティリティは、Windows 2008以降のIdentity Management for UNIX機能に含まれています。ただし、`netgroup` AD-IDMUで作成されるデフォルトのNISマップの外に新しいNISマップを作成しない限り、通常は必要ありません。

`nismap` コマンドを使用すると、`nis2ad` の機能に加えて、NISマップをきめ細かく管理できます。

`-e` このフラグは、netgroup/nismapエントリをリストします。この形式は、NISネットグループファイルで使用される形式と、Linuxのマニュアルページで説明されている形式と同じです。

注：この `ipHostNumber` 属性は、ほとんどのLDAPサーバおよびクライアントのNISホストIP情報の検索に使用されます。ONTAPはこの属性をサポートしていません。

`nismap` **コマンド例を次に示します。**

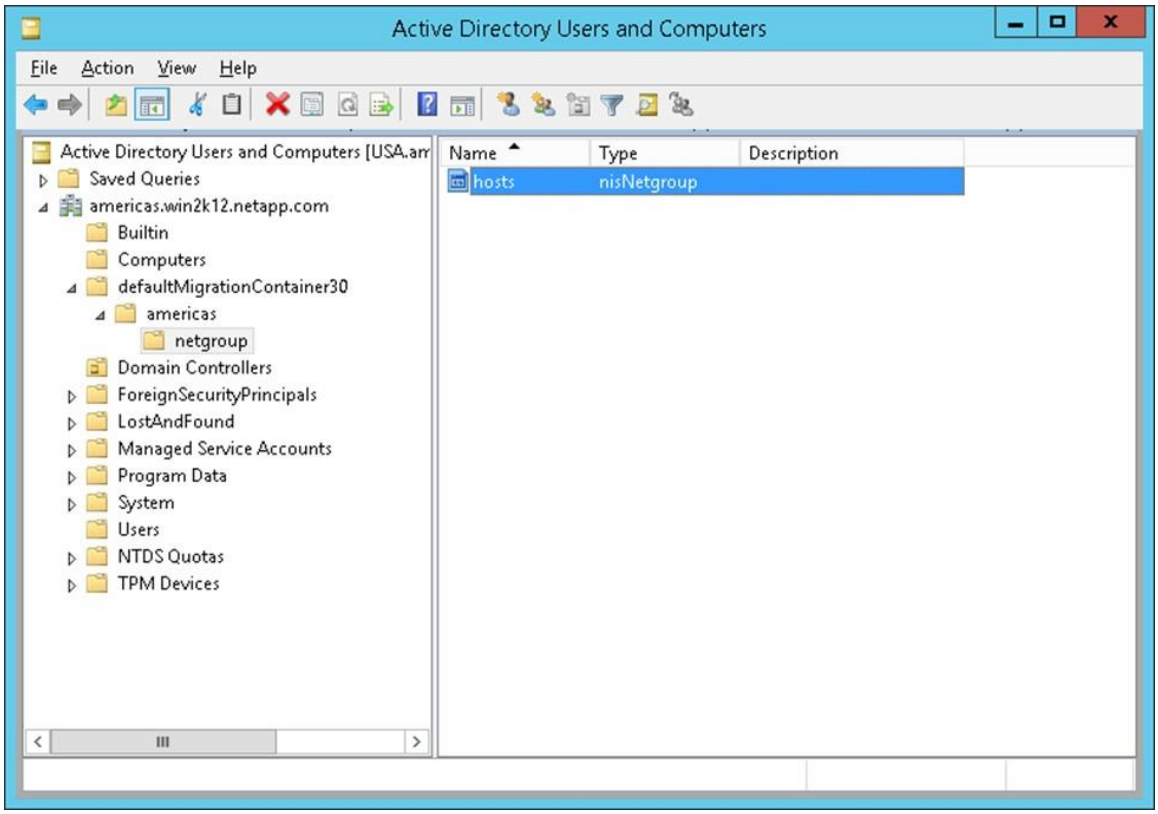
```
C:\>nismap add -a americas -s USA -c C:\nisadd.txt -e "hosts
(host1,,) (host2,,)" netgroup
Activity = Adding map = 'netgroup'...
SUCCESS
Adding the object in Active Directory Domain Services.
Object = 'hosts'
Object class = 'NisNetgroup'
container =
'CN=netgroup,CN=americas,CN=DefaultMigrationContainer30,DC=americas,DC=win2k12,DC=netapp,DC=com'.

SUCCESS
adding NIS entries to AD
```

上記の例では、次のようになりました（図21を参照）。

- という名前のオブジェクト `hosts` が作成されました。
- のオブジェクトクラス `NisNetgroup` がオブジェクトに適用されました。
- デフォルトのコンテナは `'CN=netgroup,CN=americas,CN=DefaultMigrationContainer30,DC=americas,DC=win2k12,DC=netapp,DC=com'.`

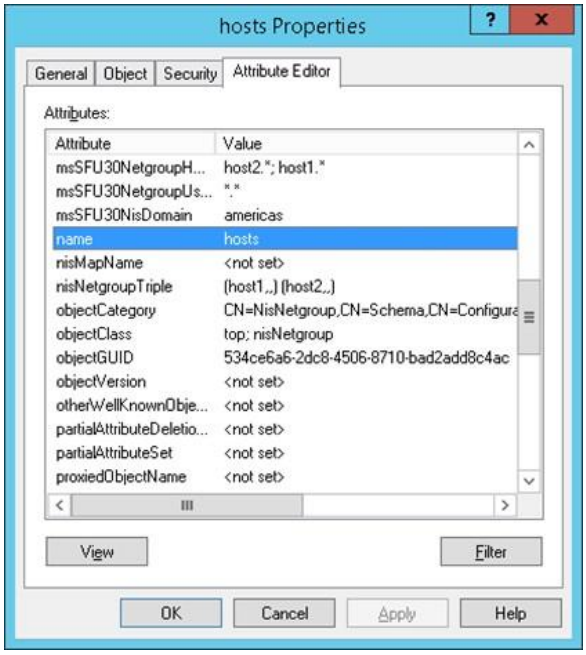
ネットグループDNは、`-netgroup-dn` フィールドを使用してONTAPでLDAPクライアントを設定するときに使用され、ネットグループLDAPクエリのDNフィルタリングが提供されます。

図21）nismapを使用してActive Directory LDAPに作成されたホストネットグループの例



オブジェクトの属性を表示するには'属性をダブルクリックして属性エディタ(Attribute Editor)を選択します
図22を参照してください

図22）Active Directory LDAPでのネットグループのプロパティ



PowerShellを使用した新しいネットグループの作成または管理

PowerShellには、より使い慣れたツールを使用してネットグループの作成や管理を行うためのコマンドレットも用意されています。

これらのコマンドレットは次のとおりです。

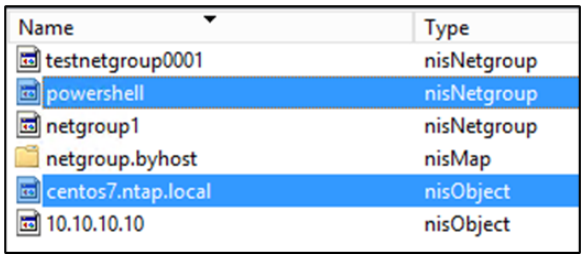
```
New-NfsNetgroup
Get-NfsNetgroup
Set-NfsNetgroup
Remove-NfsNetgroup
```

たとえば、powershellホストが centos7.ntap.local メンバーであるという新しいネットグループを作成します。

```
C:\> New-NfsNetgroup -NetGroupName powershell -AddMember centos7.ntap.local -LdapNamingContext
"OU=netgroups,DC=NTAP,DC=local" -LdapServer ntap.local
```

上記のコマンドを実行すると、というネットグループ powershell というホストエントリの2つのエントリが指定した場所に作成されます。centos7.ntap.local 図23を参照してください。

図23）Active DirectoryでNew-NfsNetgroupによって作成されたエントリ



デフォルトでは、これらのエントリはONTAPの従来のネットグループ機能を使用します。この機能は、ネットグループを照会し、ネットグループ内のすべてのホストをフェッチして、ネットグループキャッシュにデータを取り込みます。

`netgroup.byhost` 機能を使用するようにホストエントリを変更するには、`Rename-ADObject` PowerShellコマンドレットを使用してオブジェクトの名前を変更します。この手順は、`.*` DNSクエリの終了がONTAPで認識されるように、ホスト名を変更して名前の末尾に付加する必要があります。

例：

```
PS C:\> Rename-ADObject -Identity "CN=centos7.ntap.local,OU=netgroups,DC=NTAP,DC=local" -NewName
centos7.ntap.local.*
```

そのあと、`netgroup.byhost` Active Directoryで作成されたネットグループの機能を使用できます。`netgroup.byhost` 機能の詳細についてはnetgroup.byhost、本ドキュメントのセクション「サポート」を参照してください。

ADSI Editを使用した新しいNISオブジェクトの作成

NISオブジェクトを作成するもう1つの方法は、Active DirectoryのADSI編集ツールを使用することです。ADSI Editを使用するには、ADSI Editがインストールされていることを確認します。

メモ： **ADSI Editは、**Active Directoryスキーマを正しく使用しないと重大な損傷を受ける可能性があるため、細心の注意を払って使用する必要があります。ADSI Editの使用についてサポートが必要な場合は、Microsoftテクニカルサポートにお問い合わせください。

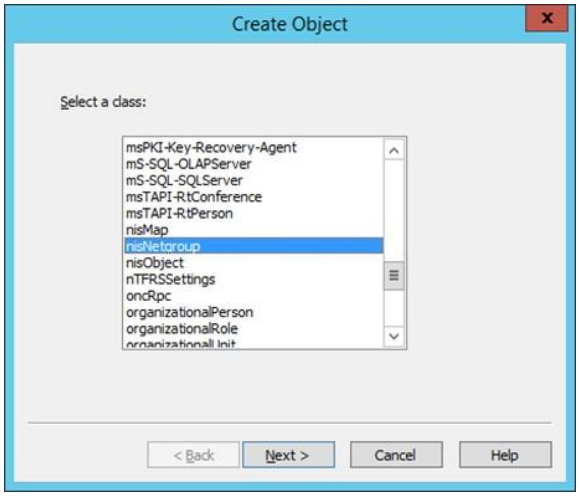
ADSI Editをインストールしたら、ADSI Editコンソールを開き、デフォルトのネーミングコンテキストパスに接続します。図24を参照してください。

図24）デフォルトのネーミングコンテキストへの接続

接続すると、Active Directoryスキーマ全体が表示されます。NISオブジェクトのコンテナが存在しない場合は、組織的な目的でコンテナを作成することを推奨します。

コンテナを作成するには、目的の場所が高輝度表示されたら右クリックし、[新規作成（New）]>[オブジェクト（Object）]を選択します。このステップでは、オブジェクトタイプ（またはオブジェクトクラス）を指定できる新しいダイアログボックスが表示されます。図25を参照してください。

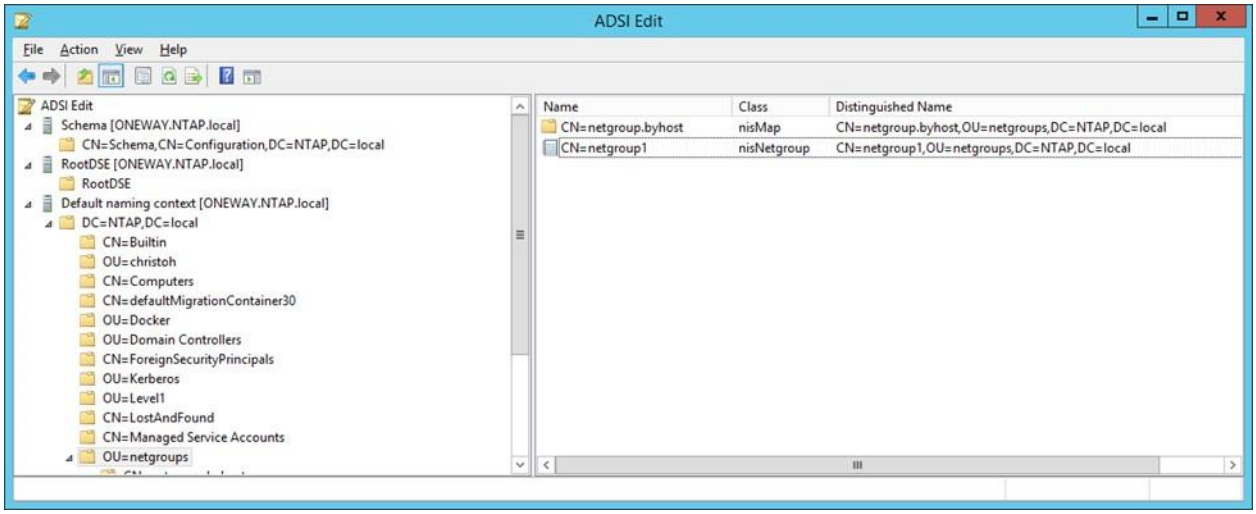
図25）新しいオブジェクトの作成



- **nismap** を使用すると、`netgroup.byhost` マップエントリを作成できます。
- **nisNetgroup** は、従来のネットグループを作成します。
- **nisObject** を使用すると、ネットグループ検索に使用するホストエントリを作成できます。

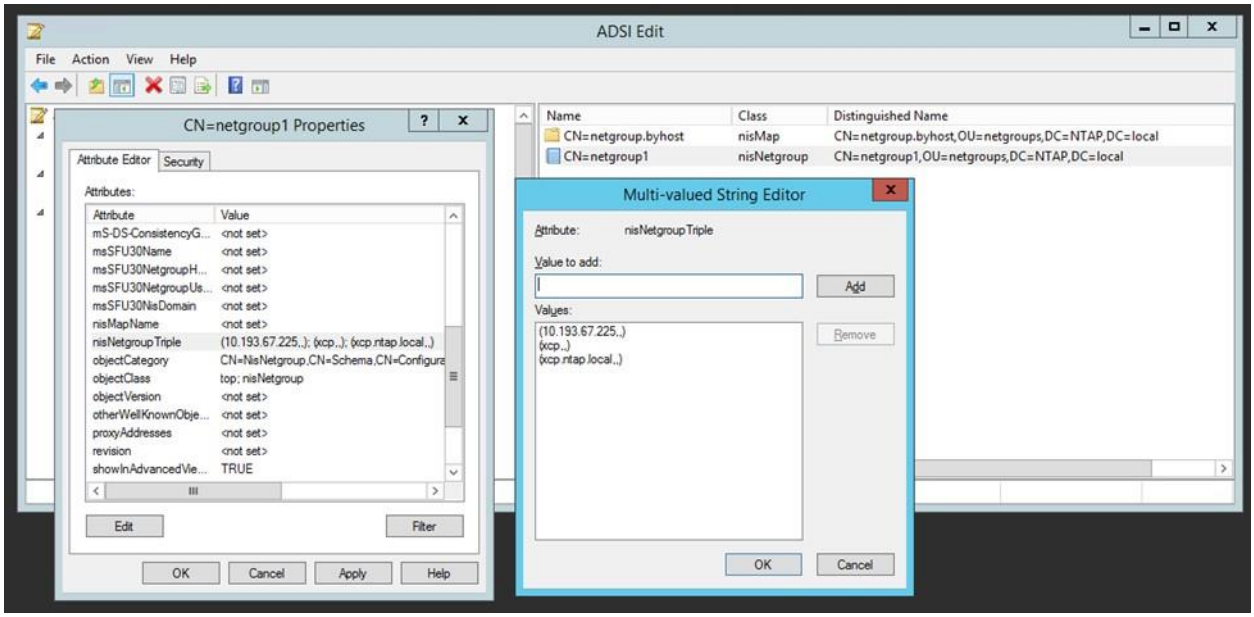
たとえば、図26 のLDAPサーバのネットグループOUには2つのエントリがあります。

図26）Active Directoryのネットグループオブジェクト



上記の例で `netgroup1` は、は通常のネットグループです。`nisNetgroupTriple` ホスト名、-、-などの一般的なロジックを使用します。図27を参照してください。

図27）NetGroup1のエントリ



netgroup.byhostエントリを作成します。

`netgroup.byhost` エントリを作成するには `nisObject`、ホスト名の `.*` 末尾にを付加したを作成します。この手順で、ホストエントリのDNS名が終了し、ホスト名の検索に使用できることをONTAPに通知します。たとえば、という名前のホスト `centos7.ntap.local` `centos7.ntap.local.*` は、`netgroup.byhost` エントリを作成するときにとして作成されます。

次に、`netgroup.byhost` Active Directory LDAPを使用したONTAPでの作業ネットグループクエリを示します。

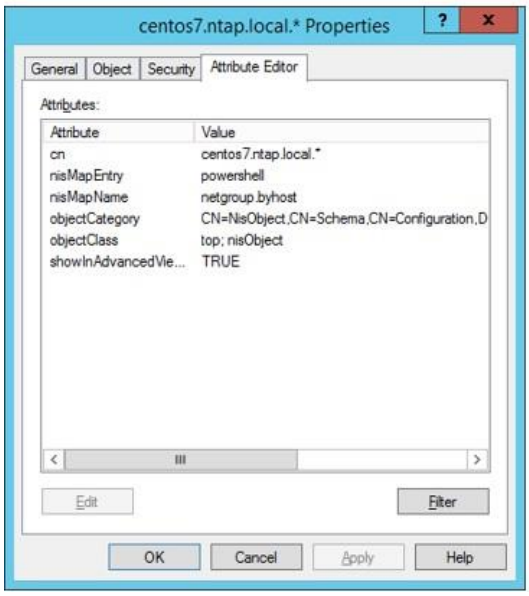
```
cluster::*> getxxbyyy netgrpcheck -node node01 -vserver DEMO -netgroup powershell -clientIP
10.193.67.225 -show-source true
  (vserver services name-service getxxbyyy netgrpcheck)
Success. Client 10.193.67.225 is member of netgroup powershell
Searched using NETGROUP_BYHOST
Source used for lookup: LDAP
```

`nisMap` この属性は、エントリがマップのタイプであることをLDAPサーバおよびクライアントに通知します。NISマップの説明および各種NISマップの例については'NIS マップを参照してくださいONTAPでは、は `netgroup.byhost` NISマップとしてのみサポートされます。

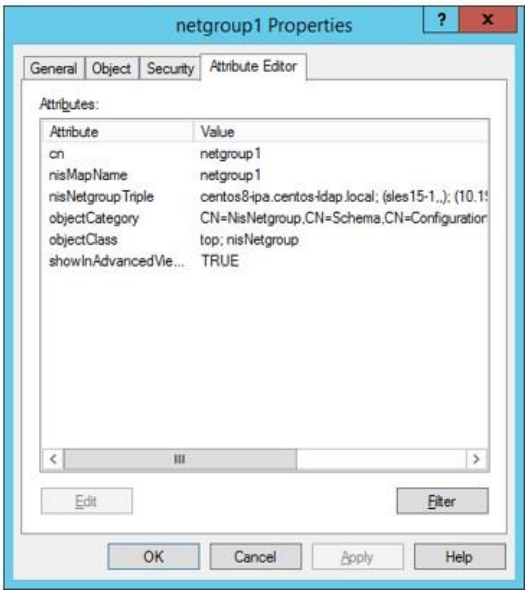
図28 の例は、`netgroup.byhost` Active Directory内のネットグループとオブジェクト、およびそれらに関連付けられている属性を示しています。

図28）Active Directory LDAPのnetgroupエントリとnetgroup.byhostエントリ

netgroup.byhost entry



Netgroup entry



WindowsのGUIを使用したネットグループオブジェクトの管理

ADSI EditまたはいずれかのCLIメソッドを使用してネットグループオブジェクトを作成したあと、Active Directory Users and Computers（ADUC）MMCを使用してエントリを管理できます。ADUCには安全対策があるため、ADSI Editよりもその方法が推奨されます。図28 では、ネットグループクライアントの追加、変更、削除、またはの変更など、CNフィールドを除くすべての項目をGUIで変更できます `nisMapEntry`。CNフィールドを変更するには `Rename-ADObject`、PowerShellでコマンドを使用します。

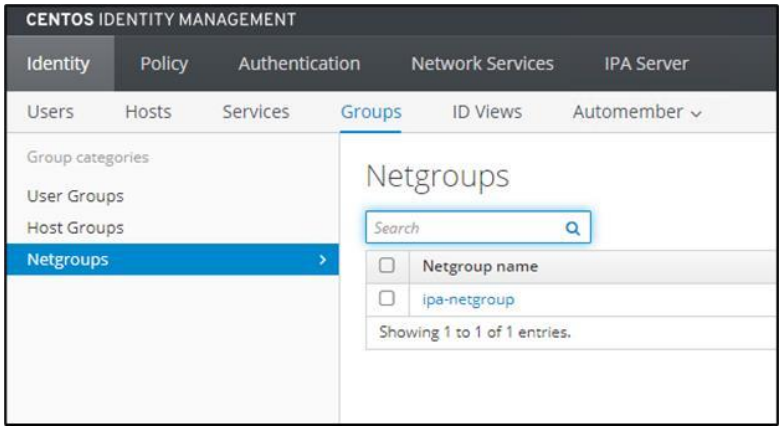
FreeIPA LDAPを使用したネットグループの作成

FreeIPA LDAPを使用して、ネットグループを作成および管理することもできます。最も簡単な方法は、提供されているGUI Webページを使用することです。FreeIPA Webインターフェイスに接続するには、`http://freeipaserver` Webブラウザでに移動します。

FreeIPA LDAPでのネットグループの追加

ネットグループ管理GUIは、FreeIPA GUIの[Identity]>[Groups]にあります。図29を参照してください。

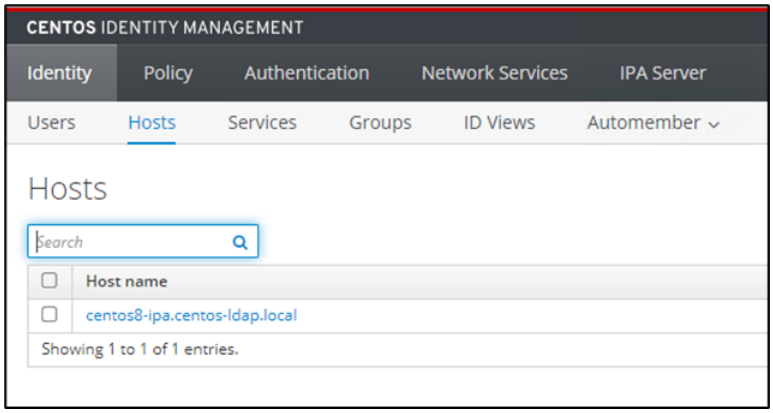
図29）FreeIPAネットグループ



新しいネットグループを作成するには、[Add]をクリックします。既存のネットグループを編集する（ホストまたはIPアドレスを追加または削除する）には、ネットグループ名を選択します。

ホストを追加するには、GUIの[Same Identity]部分の[Hosts]タブを使用します。図30を参照してください。

図30）FreeIPAホスト



ネットグループを作成したら、ONTAP CLIを使用して動作を確認できます。

```
cluster::*> getxxbyyy netgrpcheck -node node1 -vserver NFS -netgroup ipa-netgroup -clientIP
10.193.67.222 -show-source true
  (vserver services name-service getxxbyyy netgrpcheck)
Success. Client 10.193.67.222 is member of netgroup ipa-netgroup
Searched using NETGROUP_BYNAME
Source used for lookup: LDAP
```

ONTAPノネツトクルウフキヤツシユ

ONTAPは、複数のキャッシュを使用して、ホスト名やネットグループなどの情報をローカルに格納します。この方法は、必要になるたびに外部ソースからこの情報を取得する必要がある場合よりも高速です。

エクスポートポリシーとルールは、NFSエクスポートへのアクセスを制御します。各エクスポートポリシーにはルールが含まれ、各ルールにはクライアントアクセスを制御するためのパラメータが含まれています。これらのパラメータの一部では、ドメイン名、ホスト名、ネットグループなどのオブジェクトを解決するために、ONTAPがDNSサーバやNISサーバなどの外部ソースと通信する必要があります。外部ソースとの通信には、負荷やネットワークなどが原因で遅延が発生する可能性があります。パフォーマンスを向上させるために、ONTAPは複数のキャッシュに情報をローカルに格納することで、エクスポートポリシールールオブジェクトの解決にかかる時間を短縮します。

キャッシュを使用して情報をローカルに格納する場合の主な欠点は、ONTAPが外部ネームサーバを取得してローカルに格納したあとに外部ネームサーバに関する情報が変更された場合、キャッシュに古い情報が含まれている可能性があることです。その結果、成功する必要があるクライアントアクセス要求は失敗し、失敗する必要があるクライアントアクセス要求は成功する可能性があります。このような問題を回避するために、ONTAPには一定期間が経過すると自動的にキャッシュがフラッシュされ、一部のエクスポートポリシーキャッシュを表示および手動でフラッシュできるコマンドが用意されています。

キャッシュの表示とフラッシュ、およびタイムアウト値の表示と変更を行うコマンドの詳細については、セクション「ONTAP CLIコマンドによるLDAPトラブルシューティング」を参照してください。

NIS netgroup strict（nfs.netgroup.strict）

ONTAP 7-Modeでは `nfs.netgroup.strict`、オプションを使用して、Data ONTAPがネットグループをネットグループとして認識するようにネットグループエントリで@記号を必要とするかどうかを制御できました。

ONTAPには現在、この `nfs.netgroup.strict` オプションに相当するものはありません。エクスポートポリシールール内のすべてのネットグループをネットグループとして認識するには、@記号を指定する必要があります。@記号が指定されていない場合、ONTAPはエントリをホスト名として扱い、DNSまたはローカルホストで名前の解決を試みます。

netgroup.byhostのサポート

`netgroup.byhost` エントリを使用すると、ネットグループエントリの検索速度が大幅に向上します。を使用すると `netgroup.byhost`、クラスタはネットグループ内のすべてのエントリにアクセスを照会する必要がなくなり、代わりにホストごとのLDAP検索を使用してネットグループを取得できます。エントリが多数あるネットグループを含む大規模な環境では、この方法を使用すると検索にかかる時間が大幅に短縮され、LDAPクエリのタイムアウトによるアクセスの問題を回避できます。`netgroup.byhost` バージョン8.3以降では、のサポートがONTAPに追加されました。

netgroup.byhostの例

「Active Directory LDAPを使用したネットグループの作成」セクションでは、Windows Active Directoryを使用してネットグループを作成する方法を説明しました。作成されたネットグループの1つにはという名前が付けられ `netgroup1`、もになります `nisMapEntry`。したがって、スタンドアロンのネットグループとして機能すること`-is-netgroup-byhost- enabled false`も（）、ホストによって実行されるネットグループクエリをネットグループにマッピングする方法として機能することもできます（`-is- netgroup-byhost-enabled true`）。

前述のセクションでは、で使用できるホストエントリの例も示しています `netgroup.byhost`。

たとえば、`netgroup.byhost` オブジェクトにホストが設定されているとします。そのホストは、`centos8-ipa`IPアドレス10.193.67.222のフリーIPAサーバーです。図31 では`.*`、DNSで検索する名前の一部がなくなったことをONTAPに通知するために、名前の末尾にあることに注意してください。

図31）netgroup.byhostオブジェクト内のホスト

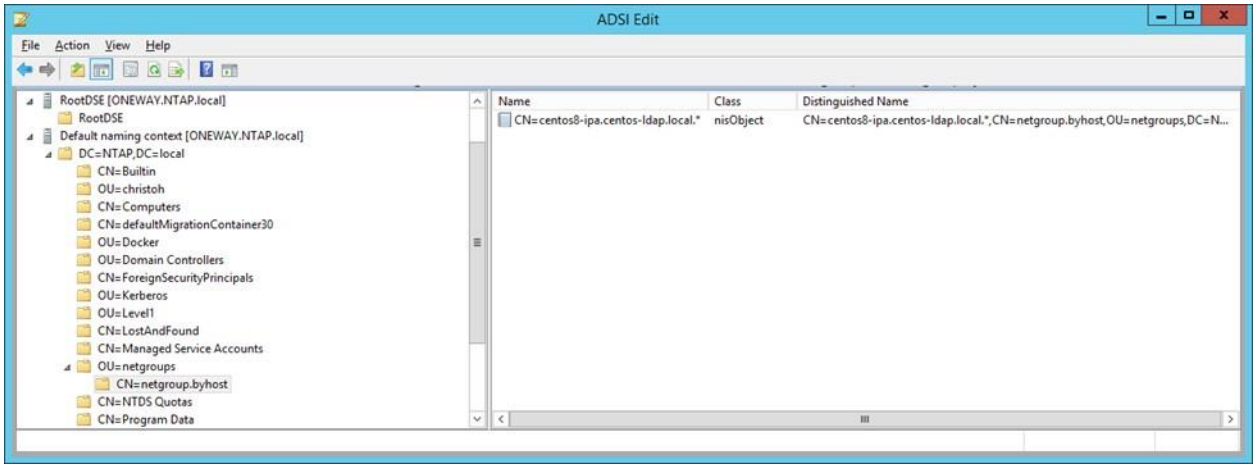
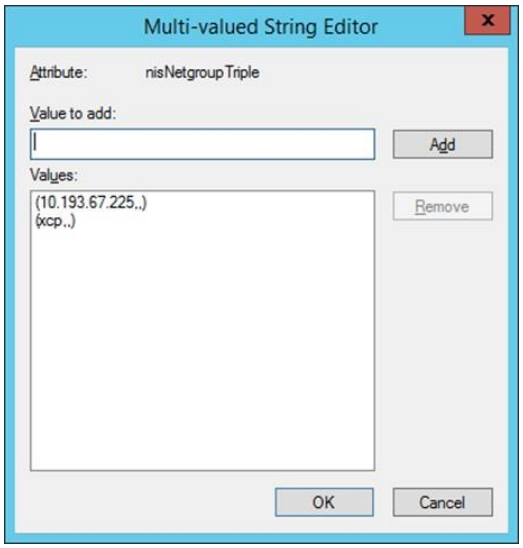


図32）NetGroup1のnisNetgroupTripleエントリ



に関するNetAppのドキュメントを参照してください。

図32 に示すように、に netgroup1 は次のもののみがあります。nisNetgroupTriple エントリ。

そのため、次の点に注意してください。

- netgroup.byhost サポートを有効にすると、centos8-ipa netgroup1 が定義されている唯一のホストであるため、割り当てられたエクスポートにのみアクセスできます。
- netgroup.byhost サポートを無効にすると centos8-ipa アクセスが拒否され、nisNetgroupTriple フィールド内のホストがアクセス権を取得します。

この情報は、コマンドを使用して確認できます export-policy check-access。（このコマンドの詳細については、「export-policy」セクションを参照してください）。

netgroup.byhostが無効になっている例

この例では netgroup.byhost、が無効になっているため、centos8-ipa クライアントはネットグループエクスポートポリシーを使用してボリュームにアクセスできませんが、nisNetgroupTriple フィールド（10.193.67.225 と xcp）のクライアントはアクセスできます。

```
cluster::*> ldap client show -client-config DEMO -fields is-netgroup-byhost-enabled
vserver client-config is-netgroup-byhost-enabled
---------- ----------------- ----------------------------------
DEMO       DEMO              false

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.222 -
authentication-method sys -protocol nfs3 -access-type read-write
                                          Policy    Policy       Rule
Path                                Policy     Owner     Owner Type  Index Access
----------------------------------- ---------- --------- ----------- ----- ------------
/                                   default    vsroot    volume          2 read
/netgrpvol                          netgroup   netgrpvol volume          0 denied
```

```
cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.225 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type Index Access
----------------------------- ---------- --------- ---------- ------ ------------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          1 read-write

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.233 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type  Index Access
----------------------------- ---------- --------- ---------- ------ ------------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          1 read-write
```

ネットグループキャッシュを表示すると、成功したクライアントが使用した netgroup_byname （または netgrp_byname)アクセスを取得した）ことを確認できます。失敗したアクセスには、のソースが表示され noneます。つまり、ネガティブキャッシュ内にあることを示します。

netgroup.byhostが有効になっている例

この例では、キャッシュがクリアされ、netgroup.byhost LDAPクライアントでサポートが有効になっています。この操作を実行すると、結果が逆になります。 centos8-ipa はアクセス権を持ち、他のクライアントはアクセス権を持ちません。

```
cluster::*> name-service cache netgroups ip-to-netgroup delete-all -vserver DEMO
  (vserver services name-service cache netgroups ip-to-netgroup delete-all)
Notice: This operation may take some time to complete.

cluster::*> name-service cache netgroups ip-to-netgroup show -vserver DEMO
  (vserver services name-service cache netgroups ip-to-netgroup show)
There are no entries matching your query.

cluster::*> ldap client modify -client-config DEMO -vserver DEMO -is-netgroup-byhost-enabled true

Warning: For the netgroup.byhost feature to work correctly, ensure that the values for the "nis-
object-class", "nis-mapname-attribute" and "nis-mapentry-attribute" parameters in the associated
schema match your LDAP schema using the "vserver services name-service ldap client schema"
commands.

cluster::*> ldap client show -client-config DEMO -fields is-netgroup-byhost-enabled
vserver client-config is-netgroup-byhost-enabled
------- ------------- ------------------------------------
DEMO    DEMO          true

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.222 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type  Index Access
----------------------------- ---------- --------- ---------- ------ ------------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          0 denied

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.225 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type Index Access
----------------------------- ---------- --------- ---------- ------ ------------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          1 read-write

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.233 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type  Index Access
----------------------------- ---------- --------- ---------- ------ ------------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          1 read-write
```

```
cluster::*> name-service cache netgroups ip-to-netgroup show -vserver DEMO
  (vserver services name-service cache netgroups ip-to-netgroup show)
Vserver     IP Address Netgroup      Source Create Time
----------- ---------- ------------- ------ ---------------
DEMO        10.193.67.222
                       netgroup1     none   2/20/2020 22:09:18
DEMO        10.193.67.225
                       netgroup1     netgrp_byname
                                     2/20/2020 22:09:25
DEMO        10.193.67.233
                       netgroup1     netgrp_byname
                                     2/20/2020 22:09:31
```

ONTAPでnetgroup.byhostのサポートを有効にする

`netgroup.byhost` ONTAPでは、サポートはデフォルトでは有効になっていません。有効にするには、LDAPクライアント設定の次のオプションを変更する必要があります。

```
-is-netgroup-byhost-enabled
-netgroup-byhost-dn
-netgroup-byhost-scope
```

当然のことながら、`-is-netgroup-byhost-enabled` を使用できるようにするには有効にする必要があります。`netgroup.byhost` 機能性：

DNとスコープは `netgroup.byhost`、機能するフィルタを指定します。詳細については、使用しているONTAPリリースのアドミニストレーションガイドを参照してください。この機能のサポートはONTAP 8.3以降のバージョンにのみ適用されることに注意してください。

外部LDAPクライアントの設定

ONTAP SVMは、LDAPサーバと通信してユーザやグループを照会できるLDAPクライアントです。同じLDAPサーバへのLDAPクエリを使用するようにクライアントOSを設定することもできます。この構成では、ONTAPクライアントとLinux / NFSクライアントがユーザとグループに同じソースを使用できるため、最小限のファイル管理で一貫したアクセス権限が提供されます。

このセクションでは、SSSD LDAPモジュールについて説明します。他のLDAPクライアントについてはこのセクションでは説明しませんが、同じ一般的な概念が適用されます。

一般に、次の手順を実行します。

1. LDAPクライアントがインストールまたは更新されていない場合は、インストールまたは更新します。
2. Active Directory LDAPを使用しており、LDAPバインドにKerberosを使用する場合は、クライアントをActive Directoryドメインに参加させます。
3. DNSがクライアントで正しく設定されていることを確認します。
4. `nsswitch.conf sss` passwd、group、およびnetgroupに使用するファイルを設定します（必要な場合）。

   注意: initgroupsは補完的なGIDルックアップを壊す可能性があるため、コメントアウトしてください。
5. で使用するLDAPクライアントを設定し `LDAP id_provider`ます。
6. 必要なLDAPクライアントスキーマオプションを使用するようにLDAPクライアントを設定します。

SSSDの詳細な手順については、次のセクションを参照してください。

注：その他のLDAPクライアント設定については、ベンダーのドキュメントを参照してください。

SSSD–Linux LDAPクライアント

SSSDはRed HatとFedoraがPADL、Samba Winbind、およびその他のActive DirectoryベースのPAMと `nss` モジュールの代替として開発したシステムデーモンである。SSSDは、さまざまなIDおよび認証プロバイダへのアクセスを提供します。新しいLDAPインターフェイスを使用するために、という名前の新しいPAMモジュール `pam_sss` が作成されました。SSSDにはActive Directoryプロバイダタイプが含まれているため、Windows Active Directory 2003、2008、および2012と簡単に統合できます。SSSDは、GSSAPIを使用してTLS暗号化とLDAPを活用します。これにより、より安全なLDAPバインディングとネットワーク経由のルックアップが可能になります。

このドキュメントの手順では、認証されたLDAPバインドにGSSAPI (Kerberos)を使用するようにSSSDを設定する方法について説明します。SSSDは、クライアントとActive Directoryドメインコントローラでサポートされている最も強力なKerberos暗号化タイプを使用します。

SSSD設定では、`/etc/sssd/sssd.conf` SSSDをサポートするクライアント上のファイルを使用します。設定を変更するたびに、SSSDを再起動する必要があります。

クライアントでネームデータベースをキャッシュするようにSSSDを設定できます。NetAppでは、パフォーマンス上の理由から、この手順を実行することを推奨しています。ただし、キャッシュはトラブルシューティングで原因の混乱を招く可能性があるため、トラブルシューティング中にサービスを再起動するときは、次の手順を使用してキャッシュをクリアします。

```
[client] # service sssd stop
[client] # rm -f /var/lib/sss/db/*
[client] # service sssd start
```

SSSDもデフォルトでは大文字と小文字を区別します。Microsoft Active Directoryでは大文字と小文字が区別されないため、NetAppでは、大文字と小文字の区別を無視するようにSSSDを設定することを推奨します。

RHEL、CentOS、Fedoraのクライアント設定

以下は、実行中のカーネルがSSSD LDAPパッケージをサポートしていることを前提としています。一部の新しいバージョンのLinuxには、基本的なインストールにデフォルトでSSSDが含まれています。SSSDがインストールされていない場合は、インストールします。

アプリケーションを確認するには、次のコマンドを実行します。

```
[client] # yum list | grep sssd
```

インストールするには、次のコマンドを実行します。

```
[client] # yum install -y sssd
```

アプリケーションがすでにインストールされている場合は、次のコマンドを実行してアップグレードすることをお勧めします。

```
[client] # yum update -y sssd
```

Active Directory LDAP環境の場合は、セットアップと使用を簡単にするために、Linuxクライアントをドメインに参加させます。この手順を使用すると、クライアントは追加のセットアップ手順なしでActive Directoryドメインの KDC機能を使用できます。これにより、Kerberosを使用したセキュアなバインドが提供され、SSSDと `krb5.conf` Active Directoryユーザ検索用のファイルが自動的に設定されます。UNIXのID検索には若干の追加設定が必要ですが、作業の大部分は `realmd` アプリケーションによって実行されます。

```
[client] # yum install -y realmd
```

古いクライアントでは、手動でKerberos設定を行うか、`net ads` コマンドを使用する必要があります。詳細については、TR-4616またはクライアントOSのドキュメントを参照してください。

アプリケーションをインストールしたら、設定プロセスを開始できます。

DNSを設定

DNSは、KerberosやLDAPなど、さまざまな機能に必要です。具体的には、DNSはホスト名の解決に使用され、SPNの照会に使用されます。また、DNSはLDAP SRVレコードを照会します。

DNSは、クライアント固有のコマンドユーティリティウィザードのいずれかを使用するか、または `/etc/resolv.conf` ファイルの基本的な編集を使用して設定できます。適用するDNSサーバと検索ドメインは、クライアントが使用しているホスト名とSPNを照会できる必要があります。

RHELおよびCentOSでDNSを設定する方法については 、Red Hatカスタマーポータルで「ドメインDNS設定の変更」を参照してください。

キー配布センターに参加

Key Distribution Center（KDC；キー配布センター）は、Kerberos認証サービスを環境に提供します。SSSDなどのLDAPアプリケーションは、「バインド」と呼ばれるログインを通じてLDAPサーバを使用します。 バインドには匿名パスワードを使用することも、プレーンテキストパスワードを使用することもできますが、理想的には、バインドにはできるだけ多くのセキュリティが使用されます。バインドにKerberosとKDCの相互作用を使用することは、このような広範なセキュリティを促進する1つの方法です。

SSSDは、Kerberos SPNを介してLDAPにバインドする方法を提供し、利用可能な最も強力なKerberos暗号化タイプ（現在、新しいKDCではAES-256）でバインドを暗号化します。`sssd.conf` ファイルを使用して手動で実行することも、などのドメイン参加ツールを使用して自動的に実行することもできます `realm`。

使用可能な `realm` コマンドは次のとおりです。

```
# realm
 realm discover -v [realm-name]
   Discover available realm

 realm join -v [-U user] realm-name
   Enroll this machine in a realm

 realm leave -v [-U user] [realm-name]
   Unenroll this machine from a realm

 realm list
   List known realms

 realm permit [-ax] [-R realm] user ...
   Permit user logins

 realm deny --all [-R realm]
   Deny user logins
```

`realm discover -v [realm-name]` コマンドを使用すると、DNSが処理を実行していることを確認したり、アプリケーションの依存関係を確認したりできます。

```
# realm discover -v NTAP.LOCAL
 * Resolving: _ldap._tcp.ntap.local
 * Performing LDAP DSE lookup on: 10.193.67.236
 * Successfully discovered: NTAP.LOCALNTAP.LOCAL
NTAP.LOCALNTAP.LOCAL
  type: kerberos
  realm-name: NTAP.LOCAL
  domain-name: NTAP.LOCALNTAP.LOCAL
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
ntap.local
  type: kerberos
  realm-name: NTAP.LOCAL
  domain-name: ntap.local
  configured: no
```

`realm join` コマンドを実行する前に、`krb5.conf` ファイルを確認してください。この例では、何も設定されていません。

```
# cat /etc/krb5.conf
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
 default =  FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
```

```
[libdefaults]
# default_realm = EXAMPLE.COM

[realms]
# EXAMPLE.COM = {
# kdc = kerberos.example.com
# admin_server = kerberos.example.com
# }

[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
```

今KDCレルムに参加してください。パッケージの依存関係がない場合は、自動的にインストールされます。

```
# realm join NTAP.LOCAL
Password for Administrator:
 * Installing necessary packages: adcli sssd-tools
```

次に、を確認できます `realm list`。

```
# realm list
NTAP.LOCALNTAP.LOCAL
  type: kerberos
  realm-name: NTAP.LOCAL
  domain-name: ntap.local
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@ntap.local
  login-policy: allow-realm-logins
```

レルムが結合されると' `krb5.conf` ファイルは新しいレルム情報を含むように変更されます

```
default_realm = NTAP.LOCAL
[realms]
# EXAMPLE.COM = {
# kdc = kerberos.example.com
# admin_server = kerberos.example.com
# }

 NTAP.LOCAL = {
 }

[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
 ntap.local = NTAP.LOCAL
 .ntap.local = NTAP.LOCAL
```

また `sssd.conf`、Active Directory情報も取得します。

```
[domain/NTAP.LOCALNTAP.LOCAL]
ad_domain = NTAP.LOCALNTAP.LOCAL
krb5_realm = NTAP.LOCAL
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
```

/etc/sssd/sssd.confファイルの設定

を使用してドメインに参加する場合 `realm`、SSSD設定では `id_provider` のが使用され `ad`ます。このアプローチでは、このドキュメントで後述するSSSD UID/GIDアルゴリズム（SSSD Active Directoryプロバイダ）方式を使用します。このメソッドが提供するUNIX IDはONTAPではサポートされていません。そのため、にLDAPを含む2番目の設定セクションをSSSD設定に追加する必要があります `id_provider`。

次に、環境によって異なる設定例を示します。

```
[domain/DOMAIN]
auth_provider = krb5
chpass_provider = krb5
id_provider = ldap
ldap_search_base = dc=ntap,dc=local
ldap_schema = rfc2307bis
ldap_sasl_mech = GSSAPI
ldap_user_object_class = user
ldap_group_object_class = group
ldap_user_home_directory = unixHomeDirectory
ldap_user_principal = userPrincipalName
ldap_account_expire_policy = ad
ldap_force_upper_case_realm = true
ldap_user_search_base = cn=Users,dc=ntap,dc=local
ldap_group_search_base = cn=Users,dc=ntap,dc=local
ldap_sasl_authid = CENTOS7$@NTAP.LOCAL
krb5_server = ntap.local
krb5_realm = NTAP.LOCAL
krb5_kpasswd = ntap.local
use_fully_qualified_names = false
```

上記の例では、

- Kerberosは `ldap_sasl_mech` とを使用してバインド `ldap_sasl_authid`
- `ldap_sasl_authid` SPNとしてのマシンアカウント
- LDAPを `id_provider`
- lookups`use_fully_qualified_names = false`()の短縮名

この `realm` コマンドでは、デフォルトで完全修飾名（など `user@REALM.COM`）を使用するようにSSSDが設定されているため、LDAP検索は名前検索の発行方法によって異なります。

たとえば、を検索する `prof1@NTAP.LOCAL`と、SSSDはActive Directoryプロバイダを使用し、Active Directoryセキュリティ識別子(SID)に基づいてUIDを生成します。

```
# id prof1@NTAP.LOCAL
uid=1587401110(prof1@NTAP.LOCALNTAP.LOCAL) gid=1587400513(domainusers@NTAP.LOCALNTAP.LOCAL)
groups=1587400513(domainusers@NTAP.LOCALNTAP.LOCAL),1587401106(group2@NTAP.LOCALNTAP.LOCAL),15874
01122(sharedgroup@NTAP.LOCALNTAP.LOCAL),1587401111(profgroup@NTAP.LOCALNTAP.LOCAL),1587401105(gro
up1@NTAP.LOCALNTAP.LOCAL),1587401107(group3@NTAP.LOCALNTAP.LOCAL)
```

を検索する `prof1`と、SSSDによってUIDが生成されるのではなく、LDAPからUNIX属性が取得されます。

```
# id prof1
uid=1100(prof1) gid=1101(ProfGroup)
groups=1101(ProfGroup),1201(group1),1203(group3),1202(group2),1220(sharedgroup)
```

この構成は、両方のタイプのユーザ検索を使用する環境に柔軟性を提供します。

SSSD UID/GIDアルゴリズム（SSSD Active Directoryプロバイダ）

Red Hatが提供するLDAPクライアントであるSSSDでは、ユーザとグループのIDを提供する2つの方法があります。IDプロバイダーとしてLDAPを使用するようにSSSDを設定すると、SSSDは、ユーザーとグループの検索にRFC 2307ベースのスキーマ標準を使用する通常のLDAP検索クエリを実行します。たとえば、という名前のユーザを `user` LDAPプロバイダを使用して検索すると、SSSDは、`uid=user` UID番号、ホームディレクトリパス、グループメンバーシップなどのユーザ認証に関連する情報を検索し、検索します。

SSSDは Active Directory統合解決策(IDプロバイダAD)もサポートしています。この解決策は、ユーザとグループに既存のWindows SIDを使用してUNIX ID管理用のUIDとGIDの数値を作成するアルゴリズムに基づいてUNIX IDを提供します。その目的は、ユーザとグループごとにUNIX属性を作成する必要をなくし、その作業をSSSDに依存させることです。

たとえば、次のSSSDクライアントの例では LDAP、SSSDは AD IDプロバイダーに対してとの両方を使用するように設定されています。

```
[domain/DOMAIN]
auth_provider = krb5
chpass_provider = krb5
id_provider = ldap
ldap_search_base = dc=ntap,dc=local
ldap_schema = rfc2307bis
ldap_sasl_mech = GSSAPI
ldap_user_object_class = user
ldap_group_object_class = group
ldap_user_home_directory = unixHomeDirectory
ldap_user_principal = userPrincipalName
ldap_account_expire_policy = ad
ldap_force_upper_case_realm = true
ldap_user_search_base = cn=Users,dc=ntap,dc=local
ldap_group_search_base = cn=Users,dc=ntap,dc=local
ldap_sasl_authid = CENTOS7$@NTAP.LOCAL
krb5_server = ntap.local
krb5_realm = NTAP.LOCAL
krb5_kpasswd = ntap.local
use_fully_qualified_names = false

[domain/NTAP.LOCALNTAP.LOCAL]
ad_domain = NTAP.LOCALNTAP.LOCAL
krb5_realm = NTAP.LOCAL
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
```

上記の設定では、FQDNが指定されていない場合にLDAPが照会され、ユーザにFQDNが割り当てられている場合はActive Directoryが使用されます。この方法では、同じユーザに対して2つの異なるUIDが提供されます。

FQDNを指定しない場合は、次のように返されます。

```
# id prof1
uid=1100(prof1) gid=1101(ProfGroup)
groups=1101(ProfGroup),1201(group1),1203(group3),1202(group2),1220(sharedgroup)
```

FQDNを指定すると、そのユーザは次の情報を取得します。

```
# id prof1@NTAP.LOCAL
uid=1587401110(prof1@NTAP.LOCALNTAP.LOCAL) gid=1587400513(domainusers@NTAP.LOCALNTAP.LOCAL)
groups=1587400513(domainusers@NTAP.LOCALNTAP.LOCAL),1587401107(group3@NTAP.LOCALNTAP.LOCAL),15874
01111(profgroup@NTAP.LOCALNTAP.LOCAL),1587401105(group1@NTAP.LOCALNTAP.LOCAL),1587401122(sharedgr
oup@NTAP.LOCALNTAP.LOCAL),1587401106(group2@NTAP.LOCAL)
```

数値UIDは 1587401110、ユーザのSIDとSSSDアルゴリズムに基づいて生成されます。

```
cluster::*> vserver services access-check authentication translate -vserver DEMO -win-name prof1
S-1-5-21-3552729481-4032800560-2279794651-1110
```

ONTAPでは現在、この方法によるUNIXユーザIDの作成はサポートされていません。生成されたUIDは、ONTAPが照会できる物理的な場所には格納されません。また、ONTAPは現在、このアルゴリズムを使用してUNIXのユーザIDとグループIDを作成しません。

ONTAPでSSSDを使用する場合は、IDプロバイダとしてLDAPを使用してLDAPサーバにUNIX属性を入力するか、`passwd group` SSSDアルゴリズムが使用するのと同じUIDおよびGID情報を使用してSVMにローカルおよびのエントリを作成します。

SSSDを使用する場合のDNSに関する考慮事項

SSSDでは、セキュアなLDAPバインドにKerberos認証を使用できます。そのため、SSSD設定で使用されるLDAPのUniversal Resource Identifier（URI）に関する情報が含まれるように、DNSを適切に設定する必要があります。SSSDでは、フェールオーバー用のラウンドロビンDNSエントリの使用はサポートされていません。フェールオーバーが正常に機能するには、各エントリが一意で、DNS内にある必要があります。詳細については、SSSDのドキュメントを参照してください。

SSSDのもう1つの制限は、フェールオーバーがのエントリの順序に依存する `/etc/resolv.conf`ことです。ファイル内の最初のDNSサーバにアクセスできない場合、SSSDはDNSサーバが利用可能になるか `/etc/resolv.conf` ファイルが変更されるまで、試行をブラックホールします。この問題の詳細については、Red Hatのバグ966757を参照してください。

クラスタ管理用のLDAP認証

また、LDAPサーバを使用して、CLI、API、およびONTAP System Managerへのアクセス（ユーザのみ）のクラスタログインと認証に使用するユーザとグループをホストすることもできます。

この使用方法は、Active Directoryドメイントンネリングとは異なります。Active Directoryドメイントンネリングを使用する手順については、製品マニュアルを参照してください。

このセクションでは、CentOS 8のネームサービスとKDC機能にFreeIPAを使用するLDAPについて説明します。ここで説明する手順は、ファイルアクセス用のユーザ名およびグループに対してLDAPを設定するためのものではありません。代わりに、管理のためにクラスタにログインします。ただし、手順の多くは、ファイルアクセス用にUNIXユーザおよびグループ用にLDAPを設定する場合と同じです。

基本手順

次の手順の概要は、クラスタログイン用にONTAPで使用するLDAPを設定する方法を示しています。次の手順は、データをホストしているSVMではなく、クラスタ管理SVMで実行します。

1. LDAPサーバがサポートするパスワードハッシュが、ONTAPでサポートされている方法の1つであることを確認します。
   - Crypt（すべてのタイプ）、SHA、SSHA
2. クラスタSVMでDNSをセットアップします。
3. テンプレートからLDAPクライアントスキーマを作成します。
   - クライアントスキーマがLDAPサーバと一致していることを確認してください。
4. クラスタSVMが所有するLDAPクライアントを作成します。
   - クライアントスキーマで、パスワードハッシュを表示する権限を持つバインドユーザが設定されていることを確認してください。
   - 必ずバインドパスワードを設定してください。
   - ベース、ユーザ、またはグループDNが適切な場所に設定されていることを確認します。
5. クラスタSVMでLDAPを有効にします。
6. `ns-switch` LDAPを使用するようにデータベースを変更します。
7. LDAPルックアップを確認します。
8. を `nsswitch` 認証方式として使用し、目的のユーザまたはグループのセキュリティログインアカウントを作成します。

9. ログインをテストします。

詳細な手順

次のセクションでは、クラスタ管理用にONTAPへのユーザおよびグループログイン用にLDAPを設定する方法について詳しく説明します。

CentOS 8でFreeIPAサーバーを作成する手順については、次のリンクを参照してください。

https://kifarunix.com/install-and-setup-freeipa-server-on-centos-8/

FreeIPAの考慮事項

FreeIPAでは、パスワードハッシュ交換を介したLDAP認証にFreeIPAを使用する際に考慮すべき点がいくつかあります。

FreeIPAスキーマ–compat

FreeIPAはデフォルトで、ユーザーを含む2つの異なるCN領域を作成します。1つはと呼ばれ `compat`、古いLDAPおよびNIS環境との下位互換性を提供することを目的としています。このCNはユーザおよびグループの検索には問題ありませんが、`userPassword` ONTAPのLDAP認証で使用するために必要なフィールドは含まれていません。

たとえば `ldapsearch CN=compat`、とのユーザからの出力を次に示します `CN=accounts`。`userPassword` にはユーザの属性がないことに注意してください `CN=compat`。

```
# ldapsearch -D "cn=Directory Manager" -W -p 389 -h 10.193.67.222 -b "dc=centos-ldap,dc=local" -s
sub "(uid=idm-ldap)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=centos-ldap,dc=local> with scope subtree
# filter: (uid=idm-ldap)
# requesting: ALL
#

# idm-ldap, users, compat, centos-ldap.local
dn: uid=idm-ldap,cn=users,cn=compat,dc=centos-ldap,dc=local
objectClass: posixAccount
objectClass: ipaOverrideTarget
objectClass: top
gecos: IDM LDAP
cn: IDM LDAP
uidNumber: 1971600001
gidNumber: 1971600000
loginShell: /bin/sh
homeDirectory: /home/idm-ldap
ipaAnchorUUID:: OklQQTpjZW50b3MtbGRhcC5sb2NhbDowYzA2OGMxYS00N2EwLTExZWEtOWZhNS
0wMDUwNTY5ZWM0N2Q=
uid: idm-ldap

# idm-ldap, users, accounts, centos-ldap.local
dn: uid=idm-ldap,cn=users,cn=accounts,dc=centos-ldap,dc=local
givenName: IDM
sn: LDAP
uid: idm-ldap
cn: IDM LDAP
displayName: IDM LDAP
initials: IL
gecos: IDM LDAP
krbPrincipalName: idm-ldap@CENTOS-LDAP.LOCAL
gidNumber: 1971600000
userClass: user
objectClass: top
objectClass: person
objectClass: organizationalperson
```

```
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: ipauser
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
objectClass: ipauserauthtypeclass
loginShell: /bin/sh
homeDirectory: /home/idm-ldap
mail: idm-ldap@centos-ldap.local
krbCanonicalName: idm-ldap@CENTOS-LDAP.LOCAL
userPassword:: cGFzc3dvcmQ=
ipaUniqueID: 0c068c1a-47a0-11ea-9fa5-0050569ec47d
krbPrincipalKey:: MIHeoAMCAQGhAwIBAaIDAgEOowMCAQGkgccwgcQwaKAbMBmgAwIBBKESBBBf
V1MkWEtbaWJHIzUoPT8koUkwR6ADAgESoUAEPiAAyXz46+O9PYO29Jp9jtSsjzBmRfP807GukpwDF
4UuPueLD5N+alOaMeh32YUfBe4DsyRNWo17VMw4sE3UMFigGzAZoAMCAQShEgQQdkR6KVVIU3hZXn
gnXSpQX6E5MDegAwIBEaEwBC4QANcX45dw98u/gynzQDKQ02dTvcOOp6uTE5wgJyzZZVaEON2l2hW
Dow8i/2Fo
uidNumber: 1971600001
krbPasswordExpiration: 20200206034103Z
krbLastPwdChange: 20200206034103Z
krbExtraData:: AALPijtecm9vdC9hZG1pbkBDRU5UT1MtTERBUC5MT0NBTAA=
mepManagedEntry: cn=idm-ldap,cn=groups,cn=accounts,dc=centos-ldap,dc=local
memberOf: cn=ipausers,cn=groups,cn=accounts,dc=centos-ldap,dc=local
krbLastFailedAuth: 20200205022117Z
krbLoginFailedCount: 0
krbTicketFlags: 128
ipaUserAuthType: password
```

クラスタSVMでONTAP LDAPクライアントをセットアップするときは base-dn、フィールドを指定します。通常、このフィールドは最上位ドメインです。ただし、FreeIPAでは原因 compat、ユーザとグループの情報をLDAPに適切に照会できても、CN内のユーザとグループが最初に検出され、その後LDAPログインが失敗する可能性があります。

この問題を回避するには、user-dn group-dn パスワード情報が格納された適切なユーザDNを使用するように、LDAPクライアントのオプションとオプションをadvanced権限で設定します。

FreeIPAを使用した認証のLDAPクライアントの例：

```
cluster::*> ldap client show -client-config IDM

Client Configuration Name: IDM
LDAP Server List: 10.x.x.x
(DEPRECATED)-LDAP Server List: -
Active Directory Domain: -
Preferred Active Directory Servers: -
Bind Using the Vserver's CIFS Credentials: false
Schema Template: IPA
LDAP Server Port: 389
Query Timeout (sec): 3
Minimum Bind Authentication Level: simple
Bind DN (User): uid=ONTAPLDAP,cn=sysaccounts,cn=etc,dc=centos-ldap,dc=local
Base DN: dc=centos-ldap,dc=local
Base Search Scope: subtree
User DN: cn=accounts,dc=centos-ldap,dc=local
User Search Scope: subtree
Group DN: cn=accounts,dc=centos-ldap,dc=local
Group Search Scope: subtree
Netgroup DN: -
Netgroup Search Scope: subtree
Vserver Owns Configuration: false
Use start-tls Over LDAP Connections: false
Enable Netgroup-By-Host Lookup: false
Netgroup-By-Host DN: -
Netgroup-By-Host Scope: subtree
```

```
Client Session Security: none
LDAP Referral Chasing: false
Group Membership Filter:
```

FreeIPA：LDAPクエリでのパスワードハッシュの表示

FreeIP LDAPスキーマは、「ディレクトリマネージャ」と呼ばれる管理ユーザを使用して変更できます。このユーザは、パスワードハッシュも表示できます。デフォルトでは、LDAPサーバ内の他のユーザはパスワードハッシュを表示できません。これは、ONTAPなどのパスワードハッシュの比較を必要とするLDAP認証の設定に問題があります。

その結果、匿名バインドにはパスワードハッシュを表示する権限がないため、LDAPクライアントの作成時に匿名バインドが機能しません。また、シンプルバインドまたはSASLバインドを設定した場合、ディレクトリマネージャや適切なアクセス権を持つ新規ユーザなど、パスワードハッシュを表示するアクセス権を持つユーザを指定した場合にのみ機能します。FreeIPA のベストプラクティスには、リモートサービスでDirectory Managerを使用しないことが記載されています。ベストプラクティスリンクページには、代わりにシステムアカウントを作成すると記載されています。ここでの主な目標は同じです。 `userPassword` クエリのフィールドを見ることができるバインドユーザーを持つことです。

フィールドを表示できるユーザと表示できないユーザのLDAPクエリの例を次に示します。

非動作バインドの例 `userPassword`：入力なし：

```
cluster::*> ldap client show -client-config IDM -fields bind-dn
vserver client-config bind-dn
---------- ----------------- --------------------------
DEMO    IDM           idm-ldap

cluster::*> getxxbyyy getpwbyname -vserver cluster -username idm-ldap
  (vserver services name-service getxxbyyy getpwbyname)
pw_name: idm-ldap
pw_passwd:
pw_uid: 1971600001
pw_gid: 1971600000
pw_gecos:
pw_dir:
pw_shell: /bin/sh
```

作業バインドの例`userPassword` ：入力済み：

```
cluster::*> ldap client show -client-config IDM -fields bind-dn
vserver client-config bind-dn
---------- ----------------- --------------------------
DEMO    IDM           CN=Directory Manager

cluster::*> getxxbyyy getpwbyname -vserver cluster -username idm-ldap
  (vserver services name-service getxxbyyy getpwbyname)
pw_name: idm-ldap
pw_passwd:
{crypt} $6$Z7$P4yQSiVYP513mNeH2PJLqOPUSOXLyh /
nGUWtFclPsEUj7tHU5y4eu6SRH1XijBgycZnAQHMCdpmJikWFkajp4 0
pw_uid: 1971600001
pw_gid: 1971600000
pw_gecos:
pw_dir:
pw_shell: /bin/sh
```

新しく作成したシステムアカウントを指定するときは、必ず完全DNパスを使用してください。たとえば次のように指定できます。

```
-bind-dn uid=ONTAPLDAP,cn=sysaccounts,cn=etc,dc=centos-ldap,dc=local
```

必要に応じて、`-min-bind-level -bind-dn` オプションの変更中にオプションをanonymousにドロップします。または、`-skip-configuration-validation true` バインドパスワードを変更するか、または最初にバインドパスワードを変更できるまで、オプションを使用できます。

パスワードを表示できるディレクトリマネージャ以外のユーザの作成

自分のバインドDNに使用するパスワードも表示できるディレクトリマネージャ以外のシステムアカウントを作成する場合は `bind-auth.update`、次の形式のファイルを作成します。

```
dn: uid=bind-auth,cn=sysaccounts,cn=etc,dc=example,dc=com
add: objectClass: account
add: objectClass: simplesecurityobject
add: uid: bind-auth
add: userPassword:  REALPASSWORDGOESHERE
add: passwordExpirationTime: 20380119031407Z
add: nsIdleTimeout: 0

dn: cn=users,cn=accounts,dc=example,dc=com
add: aci:(targetattr="userPassword")(targetfilter="(objectClass=posixAccount)")(version 3.0; acl
"Allow bind user to read password hashes for authentication"; allow(read, search, compare)
userdn="ldap:///uid=bind-auth,cn=sysaccounts,cn=etc,dc=example,dc=com";)
```

コマンドを使用して適用する `ipa-ldap-updater bind-auth.update` か、を使用して `ldapmodify`、新しいサービスアカウントをバインドDNとして使用してONTAP SVMからパスワードを表示できるかどうかをテストします。

FreeIPA Schema-パスワードハッシュ暗号化レベル

ユーザがONTAPの認証方式としてLDAPでログインすると、ログインプロセスの一環としてパスワードハッシュの比較が実行されます。パスワードハッシュ暗号化方式がONTAPでサポートされていない場合、LDAP認証は失敗します。デフォルトでは、FreeIPAは可能な限り最も安全なパスワードハッシュアルゴリズムssha512を使用します。

ただし、ONTAPで現在サポートされているパスワードハッシュの長さは次のとおりです。

- crypt（すべてのタイプ）
- SHA1/SHA2
- SSHA1/SSHA2

SSHまたはWebログインでLDAP認証を使用するには、認証用のユーザを作成するときに、パスワードハッシュを上記のいずれかの長さにする必要があります。

FreeIPAのパスワードハッシュの長さを変更する必要がある場合：

```
# ldapmodify -D "cn=Directory Manager" -W -p 389 -h centos8-ipa -x
Enter LDAP Password:
dn: cn=config
changetype: modify
replace: passwordStorageScheme
passwordStorageScheme: CRYPT-SHA512

modifying entry "cn=config"


# ldapsearch -D "cn=Directory Manager" -W -p 389 -h centos8-ipa -b "cn=config" | grep
passwordStorageScheme
Enter LDAP Password:
passwordStorageScheme: CRYPT-SHA512
```

注： ONTAP 9.7P8以前では、ONTAPでサポートされるパスワードハッシュの長さがCRYPT-SHA512で最も強力でした。ONTAP 9.7P9以降では、バグ1264152によるSHA/SSHA-512暗号化がサポートされています。そのため、これらのリリースではFree IPAでパスワードスキームを変更する必要はありません。

ただし、すべてのユーザのパスワードハッシュを変更する必要はない場合があります。そのため、回避策では `passwordStorageScheme`、値を変更し、必要なユーザとパスワードを作成（または既存のパスワードを変更）`passwordStorageScheme`してから、`passwordStorageScheme` 元の値に戻すことができます。新しい `passwordStorageScheme` ハッシュの長さは、新しいユーザまたは変更されたパスワードだけになります。

FreeIPA：LDAPグループ

場合によっては、単一のユーザではなくLDAPグループを使用することもできます。グループを使用すると、クラスタでログインユーザを作成する際のオーバーヘッドを回避できます。一元化された場所を提供することで、ユーザーを追加または削除するときのログインの管理も簡素化されます。ONTAPクラスタ管理におけるLDAPグループの制限の1つとして、HTTPまたはSystem Managerで使用するLDAPグループを指定できない点が挙げられます。

LDAPグループとONTAPログインを連携させるには、まずグループメンバーシップがONTAPクラスタから正しく認識されている必要があります。`getxxbyyy` コマンドセットを使用してテストできます。を参照してください。getXXbyYY FreeIPAはグループメンバーシップにmember LDAP scheme属性を使用するため、RFC 2307bisを使用するだけでなく、その側面を反映するようにONTAP LDAPクライアントスキーマを変更する必要があります。

次のスキーマテンプレートは、FreeIPAで使用するカスタムスキーマを示しています。RFC 2307bisスキーマに基づいています。テンプレートとのスキーマ属性の違いは黄色で強調表示されます。スキーマテンプレートの変更内容は異なる場合があります。詳細については、LDAP管理者にお問い合わせください。

無料のIPA LDAPスキーマテンプレートの例：

```
                                  Schema Template: IPA
                                          Comment:
               RFC 2307 posixAccount Object Class: person
                 RFC 2307 posixGroup Object Class: posixgroup
                RFC 2307 nisNetgroup Object Class: nisNetgroup
                           RFC 2307 uid Attribute: uid
                        RFC 2307 uidNumber Attribute: uidNumber
                        RFC 2307 gidNumber Attribute: gidNumber
               RFC 2307 cn (for Groups) Attribute: cn
             RFC 2307 cn (for Netgroups) Attribute: cn
                  RFC 2307 userPassword Attribute: userPassword
                           RFC 2307 gecos Attribute: gecos
                 RFC 2307 homeDirectory Attribute: homeDirectory
                    RFC 2307 loginShell Attribute: loginShell
                     RFC 2307 memberUid Attribute: member
              RFC 2307 memberNisNetgroup Attribute: memberHost
              RFC 2307 nisNetgroupTriple Attribute: nisNetgroupTriple
              Enable Support for Draft RFC 2307bis: true
       RFC 2307bis groupOfUniqueNames Object Class: posixgroup
            RFC 2307bis uniqueMember Attribute: member
Data ONTAP Name Mapping windowsToUnix Object Class: posixAccount
  Data ONTAP Name Mapping windowsAccount Attribute: windowsAccount
   Data ONTAP Name Mapping windowsToUnix Attribute: windowsAccount
   No Domain Prefix for windowsToUnix Name Mapping: false
                              Vserver Owns Schema: false
 Maximum groups supported when RFC 2307bis enabled: 256
                RFC 2307 nisObject Object Class: ipahost
                  RFC 2307 nisMapName Attribute: cn
                 RFC 2307 nisMapEntry Attribute: cn
```

次に、グループメンバーシップを照会するgetxxbyyyコマンドの例を示します。

```
cluster::*> getxxbyyy getgrlist -node node1 -vserver cluster -username ipa-user
(vserver services name-service getxxbyyy getgrlist)
pw_name: ipa-user
Groups: 1971600000 1971600004


cluster::*> getxxbyyy getgrbygid -node node1 -vserver cluster -groupID 1971600000
(vserver services name-service getxxbyyy getgrbygid)
name: admins
gid: 1971600000
gr_mem: admin uid=admin cn=users cn=accounts dc=centos-ldap dc=local

cluster::*> getxxbyyy getgrbygid -node node1 -vserver cluster -groupID 1971600004
(vserver services name-service getxxbyyy getgrbygid)
name: ontap-ldap
```

```
gid: 1971600004
gr_mem: idm-ldap ipa-user uid=idm-ldap cn=users cn=accounts dc=centos-ldap dc=local uid=ipa-user
cn=users cn=accounts dc=centos-ldap dc=local
```

LDAPグループメンバーシップクエリで想定されるユーザが入力されていることを確認したら、LDAPグループのセキュリティログインを作成できます。ログイン用にLDAPユーザアカウントを作成する場合との違いの1つは、作成するアカウントが `- is-ns-switch-group yes` オプションを使用したLDAPグループであることをONTAPに通知する必要があることです。

```
cluster::*> security login create -user-or-group-name ontap-ldap -application ssh -
authentication-method nsswitch -role admin -is-ns-switch-group yes -second-authentication-method
none -vserver cluster

cluster::*> security login create -user-or-group-name ontap-ldap -application ontapi -
authentication-method nsswitch -role admin -is-ns-switch-group yes -second-authentication-method
none -vserver cluster

cluster::*> security login show -vserver cluster -user-or-group-name ontap-ldap -fields is-ns-
switch-group
vserver          user-or-group-name application authentication-method is-ns-switch-group
---------------- ------------------ ----------- ------------------------ ------------------
cluster          ontap-ldap         ontapi      nsswitch                 yes
cluster          ontap-ldap         ssh         nsswitch                 yes
```

LDAPグループ認証キャッシュ

認証にLDAPグループが使用されると、ONTAPにキャッシュされます。キャッシュをフラッシュする必要がある場合は、次のコマンドを使用します。

```
cluster::*> security login group-authentication cache clear -vserver cluster -user ipa-user -
application ssh
```

一般的な問題とトラブルシューティング手順

次の情報では、NetApp ONTAPのLDAPの問題を解決するための一般的な問題とトラブルシューティング手順について説明します。このセクションでは、できるだけ多くのシナリオと問題を含めようとしていますが、すべてを網羅しているわけではありません。ここで説明していない問題が発生した場合は、「NetAppサポートに連絡する前にどのような情報を収集する必要があるか」のセクションに記載されている情報を収集してください。関連する情報をすべて入手したら、NetAppテクニカルサポートにお問い合わせください。

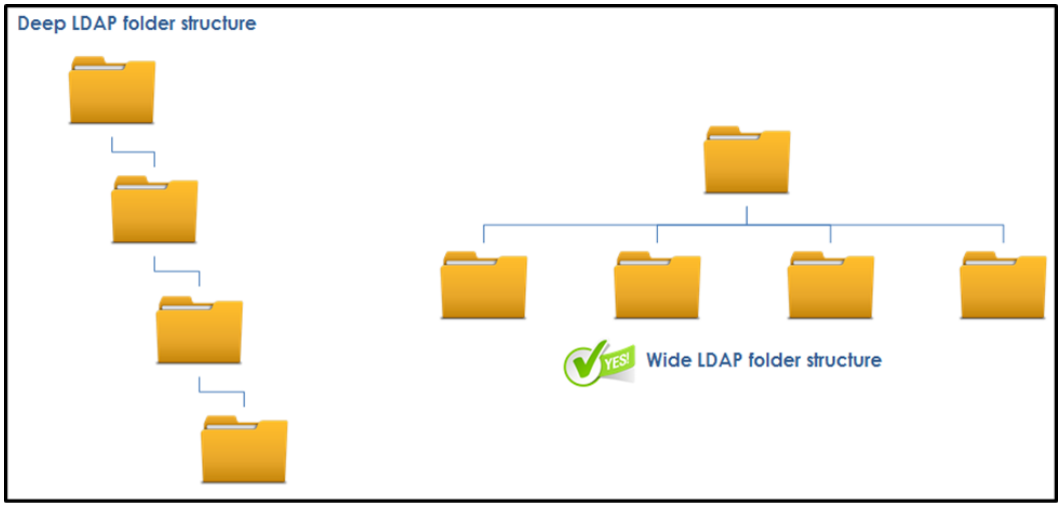
LDAP検索の最適化

エンタープライズNASのLDAPクライアントとしてONTAPを使用する場合は、アクセスの遅延を解消するために、LDAP検索ができるだけ早く実行されるようにする必要があります。ONTAP for NASには大量のキャッシュがありますが、初期ルックアップには依然としてコストがかかります。LDAPのパフォーマンスを最適化するには、ここで説明するベストプラクティスに従う必要があります。ネームサービスのベストプラクティスの一覧については、TR-4668：『Name Services Best Practice Guide：

- LDAPサーバおよび関連するネームサービスサーバ（DNSなど）が低レイテンシのネットワークリンク上にあることを確認します。
- LDAPサーバとDNSサーバはONTAPクラスタに対してローカルに配置するのが理想的です。
- LDAPサーバが過負荷状態（CPU使用率など）になっていないことを確認します。過負荷のLDAPサーバは、クエリへの応答に時間がかかります。LDAPサーバには、Active Directoryパフォーマンステストツール（ADTest.exe）など、パフォーマンスを測定するための特定のツールが用意されていることがよくあります。LDAPのパフォーマンステストの詳細については、LDAPサーバベンダーにお問い合わせください。
- 検索の問題をトラブルシューティングするには `ldapsearch`、やなどのLDAPクエリツールを使用し `ldp.exe`ます。
- ロードバランシングと冗長性を有効にするには、任意のクライアント設定に複数のLDAPサーバを含めます。
- LDAPスキーマを維持して、使用されなくなった古いレコードを削除します。

LDAPスキーマ構造と識別名（DNS）を、詳細な設計ではなくワイドな設計で構築します。ワイドスキーマでは、短いDNSを使用できます。例については、図33を参照してください。

図33）LDAPスキーマ構造の例



障害ポイント

ONTAPを使用してLDAPクエリを取得する場合は、ONTAP SVMが、UNIXまたはWindows OSと同様に、LDAPサーバに接続するLDAPクライアントとして機能していることに注意してください。したがって、問題が発生した場合は、複数の障害点を調査する必要があります。

ネットワーク

LDAPサーバ接続は、ネットワークで開始および終了します。ONTAP SVMは、データ LIF（クラスタノードの物理ネットワークポートに存在する仮想IPアドレス）を使用してIPアドレスを提供します。ネットワーク障害はさまざまな理由で発生する可能性があります。これらはすべて、TCP/IPに依存するアプリケーションの一般的なネットワークトラブルシューティングシナリオです。次に例を示します。

- ネットワークケーブルに障害が発生しました。
- ネットワークポートで障害が発生しました。
- データLIFがSVMに存在しません。
- SVM用のネットワークルートが設定されていません。
- ファイアウォールがトラフィックをブロックしています。
- データLIFは、LDAPサーバのネットワークにアクセスできないネットワークポートに配置されます。
- LDAPサーバのネットワークがダウンしています。

基本的なpingを介してLDAPサーバに到達できない場合、ONTAPはLDAP設定の適用を阻止します。ネットワークの問題を特定する方法の詳細については、本レポートの「トラブルシューティングツール」を参照してください。

DNS

LDAPサーバリストでLDAPホスト名が指定されている場合、Active Directoryドメインが指定されている場合、またはLDAP SRVレコードを照会する必要がある場合に、LDAPの障害にDNSが関与します。DNS設定はLDAPで使用する場合は必須ではありませんが、NetAppではこの設定を強く推奨しています。DNS障害は、次のようなさまざまな理由で発生する可能性があります。

- ネットワーク接続に問題があります

- DNSクエリのタイムアウト
- 見つからないホスト
- DNS設定が正しくない

基本的なpingを介してDNSサーバに到達できない場合、ONTAPはDNS設定が適用されないようにします。DNSの問題を見つける方法の詳細については、「トラブルシューティングツール」セクションを参照してください。

ネームサービススイッチ（ns-switch）の設定

ネームサービススイッチは、さまざまなネームサービスの検索先と検索順序をクライアントに指示します。ONTAP SVMにはそれぞれ、`ns-switch` ユーザ、グループ、ネットグループ、およびホスト名検索用に外部ネームサービスまたはローカルファイルを指定するための独自の設定があります。

ONTAP SVMがLDAPサーバと通信できるようにするには、ns-switchを設定する必要があります。「SVMネームサービススイッチ（ns-switch）の変更」を参照してください。

LDAPポート

LDAPポート設定は、ONTAP SVMがLDAPサーバとの通信に使用するネットワークポートを認識する方法です。ポート389は標準のLDAPポートですが、環境によってはLDAPサーバの設定に基づいてLDAPポートが異なる場合があります。たとえば、LDAP over SSLを使用するには、多くの場合ポート636が必要です。また、難読化によるセキュリティ上の考慮事項のために、LDAPポートを非標準のLDAPポートに変更する場合もあります。ONTAP SVMでは、LDAP over SSLを使用する場合はポート636のみがサポートされ、StartTLSでLDAPを使用する場合はポート389のみがサポートされます。標準LDAP呼び出しでは、サーバおよびクライアントで設定されている任意のポートを使用できます。LDAP通信に使用されているポートを確認するには、LDAP管理者に問い合わせてください。

LDAPバインド

LDAPバインドは、LDAPクライアントがLDAPサーバにログインして、名前およびグループ検索の読み取り専用クエリを実行する方法です。ほとんどの場合、LDAPのすべてのユーザがLDAPサーバにバインドしてスキーマ属性を読み取ることができます。ユーザパスワードフィールドの場合、特権LDAPユーザ（LDAPログインを使用してクラスタを管理するLinuxベースのLDAPのDirectory Managerなど）が必要になることがあります。

バインドは3つの方法で設定できますが、LDAPサーバは特定のバインド方法のみをサポートするように設定できます。

- **匿名**（誰でもLDAPスキーマを読み取ることができます）
- **Simple**（基本的なユーザ名とパスワードのバインド）
- **SASLは** 最も安全なバインディング形式であり、KerberosやNTLMなどのさまざまな暗号化方式を使用して実行できます。

LDAPバインドが失敗すると、ユーザとグループの検索も失敗します。LDAPバインドが失敗した場合、ONTAPは、LDAPサーバと同様にイベントログにメッセージを記録します。LDAPバインドの問題を検出する方法の詳細については、「トラブルシューティングツール」を参照してください。

LDAP DN検索設定

DN検索設定とは、LDAPクライアント設定で指定するスキーマの場所を指します。これにより、LDAP検索で最も効率的な場所を検索できるようになります。ベースDNは主な検索を指示するように指定されますが、ユーザ、グループ、およびネットグループDNのフィルタを使用すると、クエリをさらに絞り込んでオブジェクトの検索にかかる時間を短縮できます。

LDAP DNが正しく設定されていない場合や間違ったDNが指定されている場合は、ユーザとグループの検索は成功しますが、想定される結果（または結果）は返されません。例えると、電話帳の「R」セクションで「スミス」という名前の人を探しています。

LDAP DNの設定に関する問題は、追跡が困難な場合があります。以外にエラーはない `object not found` ので、トラブルシューティングにはもう少し掘り下げる必要があります。LDAP DNの問題を検出する方法の詳細については、「トラブルシューティングツール」セクションを参照してください。

LDAPクライアントスキーマ設定

ONTAPには 、LDAPクライアント設定で使用するデフォルトの読み取り専用LDAPスキーマテンプレートがいくつか用意されています。使いやすいように、これらのテンプレートには共通のスキーマ属性値が用意されています。ただし、LDAPサーバがテンプレートと一致しないスキーマ設定を使用している場合もあります。このような場合は、スキーマテンプレートを新しい書き込み可能なテンプレートにコピーして変更できます。

これらのスキーマ属性は、ONTAPがユーザおよびグループ検索用に生成するLDAP検索クエリの作成に役立ちます。間違ったスキーマ属性が指定されている場合、ONTAPは間違った値を送信し、LDAPサーバから適切な結果を取得しません。その結果、ONTAPは受信するクライアント要求に基づいてユーザを識別できず、ユーザに適切な権限を適用できないため、ファイルアクセスの問題が発生します。

スキーマが正しく設定されていないと、セカンダリグループメンバーシップが正しく設定されないこともあります。スキーマ属性を正しく取得するには、このレポートの「LDAPスキーマ構成」セクションに記載されている手順に従ってください。

LDAPスキーマ構成の問題を検出する方法の詳細については、「トラブルシューティングツール」を参照してください。

トラブルシューティングツール

このセクションでは、環境内のLDAPの問題のトラブルシューティングに使用できる特定のツールとコマンドについて説明します。

サードパーティのツールとユーティリティ

場合によっては、LDAPの問題のトラブルシューティングにサードパーティのユーティリティが必要になることがあります。このセクションでは、これらのツールのいくつかについて説明します。

基本的なネットワークトラブルシューティング：ping、nslookup、dig、telnet、nmap

LDAPの基本的なトラブルシューティングでは、通常、ネットワーク接続を確認する必要があります。pingでは、LDAPサーバ、クライアント、およびONTAP間のネットワークが適切に接続されているかどうかを確認できます。ただし、基本的なpingはネットワークでブロックされることがあるため、telnetやnmapなどのユーティリティを使用してポート接続をチェックすると便利です。また、一部のLDAP構成ではDNSによる名前解決のチェックが重要になるため、nslookupやdigなどのツールを使用してDNSをテストできます。

`nmap` Windows 2012 R2を実行しているLDAPサーバへののの例：

```
# nmap x.x.x.x

Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-14 23:34 EST
Nmap scan report for oneway.ntap.local (x.x.x.x)
Host is up (0.00023s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
```

```
636/tcp   open ldapssl
2049/tcp open nfs
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
```

nslookup との例 dig：

```
# nslookup ntap.local
Server:         x.x.x.x
Address:        x.x.x.x#53

Non-authoritative answer:
Name:   ntap.local
Address: x.x.x.x

# dig ntap.local

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> ntap.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9482
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ntap.local.                    IN      A

;; ANSWER SECTION:
ntap.local.             590     IN      A       x.x.x.x

;; Query time: 1 msec
;; SERVER: x.x.x.x#53(x.x.x.x)
;; WHEN: Fri Feb 14 23:37:57 EST 2020
;; MSG SIZE rcvd: 55
```

を使用し dig てSRVレコードを照会します。

```
# dig SRV ldap/oneway.ntap.local

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> SRV ldap/oneway.ntap.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31583
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ldap/oneway.ntap.local.                IN      SRV

;; AUTHORITY SECTION:
ntap.local.             900     IN      SOA     oneway.ntap.local. hostmaster.ntap.local. 2399
900 600 86400 3600

;; Query time: 1 msec
;; SERVER: x.x.x.x#53(x.x.x.x)
;; WHEN: Fri Feb 14 23:39:09 EST 2020
;; MSG SIZE rcvd: 105

# dig SRV _ldap._tcp.ntap.local

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> SRV _ldap._tcp.ntap.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62440
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;_ldap._tcp.ntap.local.          IN      SRV

;; ANSWER SECTION:
_ldap._tcp.ntap.local. 600      IN      SRV     0 100 389 oneway.ntap.local.

;; ADDITIONAL SECTION:
oneway.ntap.local.      3600    IN      A       x.x.x.x

;; Query time: 1 msec
;; SERVER: x.x.x.x#53(x.x.x.x)
;; WHEN: Fri Feb 14 23:40:08 EST 2020
;; MSG SIZE rcvd: 103
```

sss_cache

Linuxクライアントで SSSDを使用する場合は、ss_cacheコマンドを使用してSSSDキャッシュをフラッシュできます。このプロセスは、以下を使用してグローバルに実行できます。

```
# sss_cache -E
```

または、ユーザまたはグループ単位で、次の機能を使用します。

```
# sss_cache -u usernamre
# sss_cache -g groupname
```

パケット トレース

多くの場合、パケットトレースは、基本的な接続、バインドの問題、LDAP検索の問題など、LDAPのさまざまな問題を切り分けるのに非常に役立ちます。tcpdumpからWiresharkまで、任意のパケットトレースユーティリティを使用できます。LDAPトラフィックがSSLまたは証明書を介して暗号化されている場合、パケットトレースはそれほど有用ではありませんが、証明書キーを使用してトレースを復号化することができます。次のリンクは、このアプローチの例を示しています。

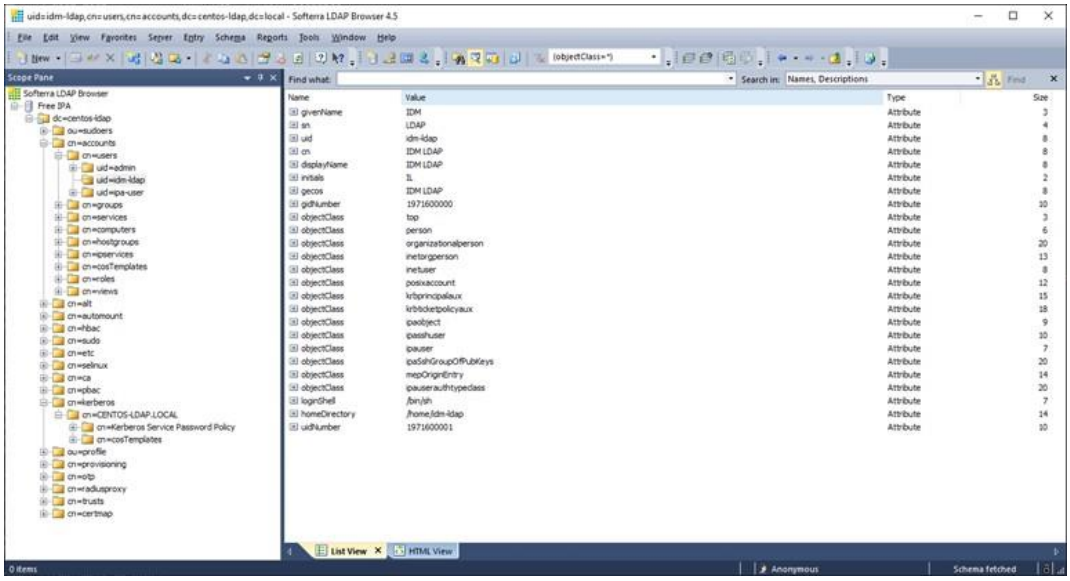
- IDMWORKS:Active DirectoryへのLDAPSトラフィックの復号化
- Microsoft ドキュメント：NetMon 3.4およびNMDecryptを使用したLDAP SSLネットワークトラフィックの読み取り
- Wireshark：LDAP over SSLのデコードに問題がある

パケットキャプチャによるLDAP通信の例については、セクション「パケットトレースから見たLDAPトラフィック」を参照してください。

LDAPブラウザ：Softerra

Softerraは、LDAPスキーマの表示、バインドのテスト、クエリなどを可能にする無料のLDAPブラウザアプリケーションを提供しています。このブラウザでは、SSL証明書など、ONTAPが使用するバインドと同じタイプのバインドをすべて使用でき、カスタムLDAPクライアントスキーマに必要な属性を特定するのに役立ちます。図34を参照してください。

図34）Softerra LDAPブラウザ



LDP

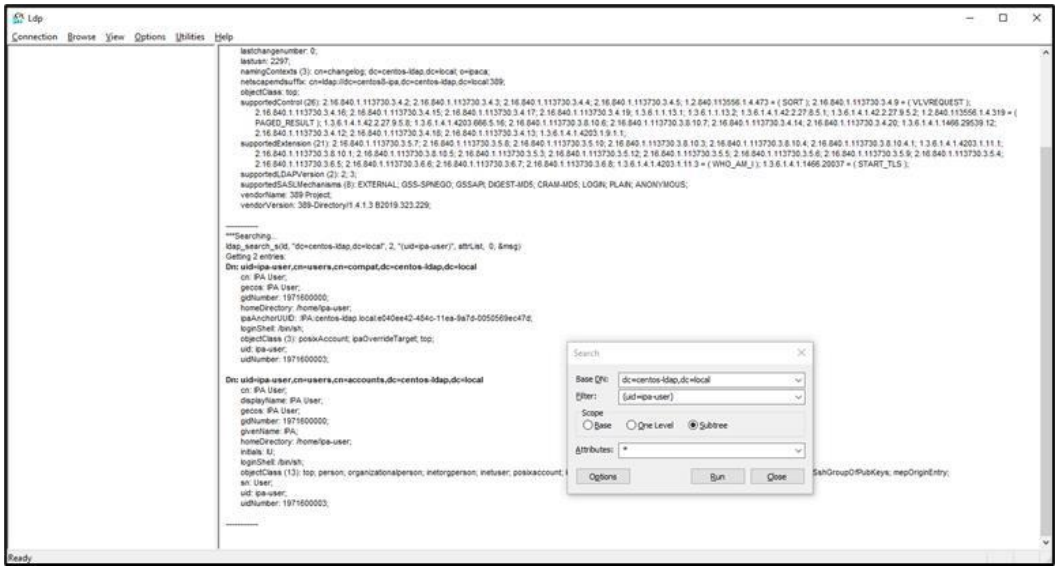
LDPは、Microsoft Windowsが提供するLDAPクライアントです。このユーティリティには、Softerra LDAPブラウザに似た機能がありますが、GUIの操作はあまり行われません。このツールは通常、Active Directoryドメインコントローラにありますが、Windowsクライアントにもインストールできます。

LDPでは、次のことが可能です。

- 接続
- バインド
- SSL経由でStartTLSまたはLDAP（あるいはその両方）を使用
- 参照
- 検索クエリの実行

この機能を使用すると、ONTAPの外部でLDAP機能をテストできます。これにより、LDAPサーバが正常に動作しており、検索クエリが適用されていることを確認できます。検索例については、図35を参照してください。

図35）LDPを使用したLDAP検索の例



ldapsearch

ldapsearch は、LDAPサーバとコマンドラインでやり取りして標準のLDAP検索を実行できる、Linuxベースの標準ユーティリティです。このコマンドを使用すると、バインドレベル、使用する証明書、検索フィルタ、およびLDAPサーバおよびスキーマのトラブルシューティングに役立つその他の便利なメカニズムを指定できます。

例 `ldapsearch`：

```
# ldapsearch -h x.x.x.x -p 389 -x -b 'dc=centos-ldap,dc=local' -s sub '(uid=ipa-user)'
# extended LDIF
#
# LDAPv3
# base <dc=centos-ldap,dc=local> with scope subtree
# filter: (uid=ipa-user)
# requesting: ALL
#

# ipa-user, users, accounts, centos-ldap.local
dn: uid=ipa-user,cn=users,cn=accounts,dc=centos-ldap,dc=local
givenName: IPA
sn: User
uid: ipa-user
cn: IPA User
displayName: IPA User
initials: IU
gecos: IPA User
gidNumber: 1971600000
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: ipauser
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
loginShell: /bin/sh
homeDirectory: /home/ipa-user
```

```
uidNumber: 1971600003
```

PowerShell

UNIX LDAP環境でActive Directoryを使用している場合は、PowerShellを使用してユーザとグループの属性をダンプできます。ユーザとグループの属性のリストは、LDAPクライアントスキーマの問題の作成やトラブルシューティングに非常に役立ちます。

PowerShellを使用したUNIXユーザおよびグループの属性ダンプの例：

```
PS C:\> Get-ADUser prof1 -properties *


AccountExpirationDate                :
accountExpires                       : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 132146010015585937
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : NTAP.LOCAL/Users/prof1
Certificates                         : {}
City                                 :
CN                                   : prof1
codePage                             : 0
Company                              :
CompoundIdentitySupported            : {}
Country                              :
countryCode                          : 0
Created                              : 1/14/2017 12:23:19 PM
createTimeStamp                      : 1/14/2017 12:23:19 PM
Deleted                              :
Department                           :
Description                          :
DisplayName                          : prof1
DistinguishedName                    : CN=prof1,CN=Users,DC=NTAP,DC=local
Division                             :
DoesNotRequirePreAuth                : False
dSCorePropagationData                : {12/31/1600 7:00:00 PM}
EmailAddress                         :
EmployeeID                           :
EmployeeNumber                       :
Enabled                              : True
Fax                                  :
gecos                                : Prof1
gidNumber                            : 1101
GivenName                            : prof1
HomeDirectory                        :
HomedirRequired                      : False
HomeDrive                            :
HomePage                             :
HomePhone                            :
Initials                             :
instanceType                         : 4
isDeleted                            :
KerberosEncryptionType               : {}
LastBadPasswordAttempt               : 10/3/2019 2:30:01 PM
LastKnownParent                      :
lastLogoff                           : 0
lastLogon                            : 132255810960575467
LastLogonDate                        : 2/13/2020 3:27:30 PM
lastLogonTimestamp                   : 132260992500117213
LockedOut                            : False
loginShell                           : /bin/sh
logonCount                           : 142
```

```
LogonWorkstations                    :
Manager                              :
MemberOf                             : {CN=sharedgroup,CN=Users,DC=NTAP,DC=local,
CN=ProfGroup,CN=Users,DC=NTAP,DC=local, CN=group3,CN=Users,DC=NTAP,DC=local,
CN=group2,CN=Users,DC=NTAP,DC=local...}
MNSLogonAccount                      : False
MobilePhone                          :
Modified                             : 2/13/2020 3:27:30 PM
modifyTimeStamp                      : 2/13/2020 3:27:30 PM
msDS-User-Account-Control-Computed   : 0
Name                                 : prof1
nTSecurityDescriptor                 : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                       : CN=Person,CN=Schema,CN=Configuration,DC=NTAP,DC=local
ObjectClass                          : user
ObjectGUID                           : 0973b3f1-da85-499c-80b4-a210e0d0fb2f
objectSid                            : S-1-5-21-3552729481-4032800560-2279794651-1110
Office                               :
OfficePhone                          :
Organization                         :
OtherName                            :
PasswordExpired                      : False
PasswordLastSet                      : 1/23/2018 10:18:37 AM
PasswordNeverExpires                 : True
PasswordNotRequired                  : False
POBox                                :
PostalCode                           :
PrimaryGroup                         : CN=Domain Users,CN=Users,DC=NTAP,DC=local
primaryGroupID                       : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                          :
ProtectedFromAccidentalDeletion      : False
pwdLastSet                           : 131611943171895803
SamAccountName                       : prof1
sAMAccountType                       : 805306368
ScriptPath                           :
sDRightsEffective                    : 15
ServicePrincipalNames                : {}
SID                                  : S-1-5-21-3552729481-4032800560-2279794651-1110
SIDHistory                           : {}
SmartcardLogonRequired               : False
State                                :
StreetAddress                        :
Surname                              :
Title                                :
TrustedForDelegation                 : False
TrustedToAuthForDelegation           : False
uid                                  : {prof1}
uidNumber                            : 1100
unixHomeDirectory                    : /home/prof1
UseDESKeyOnly                        : False
userAccountControl                   : 66048
userCertificate                      : {}
UserPrincipalName                    : prof1@NTAP.LOCAL
uSNChanged                           : 832283
uSNCreated                           : 12924
whenChanged                          : 2/13/2020 3:27:30 PM
whenCreated                          : 1/14/2017 12:23:19 PM

PS C:\> Get-ADGroup profgroup -properties *


CanonicalName                   : NTAP.LOCAL/Users/ProfGroup
CN                              : ProfGroup
Created                         : 1/14/2017 12:24:31 PM
createTimeStamp                 : 1/14/2017 12:24:31 PM
Deleted                         :
Description                     :
DisplayName                     :
DistinguishedName               : CN=ProfGroup,CN=Users,DC=NTAP,DC=local
dSCorePropagationData           : {12/31/1600 7:00:00 PM}
gidNumber                       : 1101
```

```
GroupCategory                   : Security
GroupScope                      : Global
groupType                       : -2147483646
HomePage                        :
instanceType                    : 4
isDeleted                       :
LastKnownParent                 :
ManagedBy                       :
member                          : {CN=quota user,CN=Users,DC=NTAP,DC=local,
CN=prof1,CN=Users,DC=NTAP,DC=local, CN=student2,CN=Users,DC=NTAP,DC=local,
CN=Administrator,CN=Users,DC=NTAP,DC=local}
MemberOf                        : {}
Members                         : {CN=quota user,CN=Users,DC=NTAP,DC=local,
CN=prof1,CN=Users,DC=NTAP,DC=local, CN=student2,CN=Users,DC=NTAP,DC=local,
CN=Administrator,CN=Users,DC=NTAP,DC=local}
Modified                        : 8/30/2019 3:38:12 PM
modifyTimeStamp                 : 8/30/2019 3:38:12 PM
Name                            : ProfGroup
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  : CN=Group,CN=Schema,CN=Configuration,DC=NTAP,DC=local
ObjectClass                     : group
ObjectGUID                      : e2fae6f6-e682-4c37-b998-d0e2215e8e66
objectSid                       : S-1-5-21-3552729481-4032800560-2279794651-1111
ProtectedFromAccidentalDeletion : False
SamAccountName                  : ProfGroup
sAMAccountType                  : 268435456
sDRightsEffective               : 15
SID                             : S-1-5-21-3552729481-4032800560-2279794651-1111
SIDHistory                      : {}
uSNChanged                      : 680730
uSNCreated                      : 12933
whenChanged                     : 8/30/2019 3:38:12 PM
whenCreated                     : 1/14/2017 12:24:31 PM
```

ネットグループ属性の検索には `Get-AdObject`、次のコマンドを使用します。

```
PS C:\> Get-ADObject -LDAPFilter "(objectClass=nisNetgroup)" -Properties *


CanonicalName                   : NTAP.LOCAL/netgroups/netgroup1
CN                              : netgroup1
Created                         : 3/1/2017 3:04:00 PM
createTimeStamp                 : 3/1/2017 3:04:00 PM
Deleted                         :
Description                     :
DisplayName                     :
DistinguishedName               : CN=netgroup1,OU=netgroups,DC=NTAP,DC=local
dSCorePropagationData           : {12/31/1600 7:00:00 PM}
instanceType                    : 4
isDeleted                       :
LastKnownParent                 :
Modified                        : 2/20/2020 9:43:17 PM
modifyTimeStamp                 : 2/20/2020 9:43:17 PM
Name                            : netgroup1
nisNetgroupTriple               : {(10.193.67.225,,), (xcp,,)}
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  : CN=NisNetgroup,CN=Schema,CN=Configuration,DC=NTAP,DC=local
ObjectClass                     : nisNetgroup
ObjectGUID                      : 3cb36ede-668c-4e5c-a9b0-a6d927dfdec7
ProtectedFromAccidentalDeletion : False
sDRightsEffective               : 15
showInAdvancedViewOnly          : True
uSNChanged                      : 834544
uSNCreated                      : 24423
whenChanged                     : 2/20/2020 9:43:17 PM
whenCreated                     : 3/1/2017 3:04:00 PM
```

LDAPトラブルシューティング用のONTAP CLIコマンド

ONTAPには、LDAPの問題のトラブルシューティングに使用できるコマンドとログファイルがいくつか用意されています。このセクションでは、これらのコマンドについて説明します。

ネットワークping

ONTAPでは、任意のデスティネーションホスト名またはアドレスに対してネットワークpingを実行できます。これには、特定のデータLIFおよびSVMからトラフィックを強制的に送信する方法も含まれます。

```
cluster::*> network ping ?
   { -node <nodename>                    Node
   |  -lif <lif-name> }                  Logical Interface
    -vserver <vserver>                   Vserver
  [ -use-source-port {true|false} ]      *(DEPRECATED)-Use Source Port of Logical Interface
   [-destination] <Remote InetAddress>   Destination
  [ -show-detail|-s [true] ]             Show Detail Output
  [ -record-route|-R [true] ]            Record Route
  [ -verbose|-v [true] ]                 Show All ICMP Packets
  [ -packet-size <integer> ]             Packet Size
  [ -count <integer> ]                   Count
  [ -wait <integer> ]                    Packet Send Wait Time (secs)
  [ -flood [true] ]                      *Flood Ping
  [ -disallow-fragmentation|-D [true] ]  Disallow Packet Fragmentation (default: false)
  [ -wait-response <integer> ]           Packet Response Wait Time (ms) (default: 10000)
```

getXXbyYY

ONTAPには、advanced権限（`getxxbyyy`）のコマンドが用意されています。このコマンドを使用すると、`ns-switch` SVMからSVMのファイルに設定されているネームサービスへの検索を実行できます。

使用可能なコマンドは次のとおりです。

```
cluster::*> getxxbyyy ?
  (vserver services name-service getxxbyyy)
  getaddrinfo                 *Gets the IP address information by using the host name.
  getgrbygid                  *Gets the group members by using the group identifier or GID.
  getgrbyname                 *Gets the group members by using the group name.
  getgrlist                   *Gets the group list by using the user name.
  gethostbyaddr               *Gets the host information from the IP address.
  gethostbyname               *Gets the IP address information from host name.
  getnameinfo                 *Gets the name information by using the IP address.
  getpwbyname                 *Gets the password entry by using the user name.
  getpwbyuid                  *Gets the password entry by using the user identifier or UID.
  netgrpcheck                 *Check if a client is part of a netgroup using combined API
```

`getxxbyyy` は、LDAP、NIS、またはローカルファイルでユーザ、グループ、グループメンバーシップ、およびネットグループを照会できます。また、DNSまたはローカルファイルでホスト名を照会できます。また、コマンドでは、結果の元となるネームサービスソースを指定したり（`-show-source true`）、コマンド（隠しオプション）から詳細なエラーを提供したりできます `-show-granular-err true`。キャッシュをバイパスして、を使用してネームサービスから検索が行われたかどうかを確認することもできます `-use-cache false`。

`getxxbyyy` UNIXユーザを検索する例：

```
cluster::*> getxxbyyy getpwbyname -vserver NFS -node node1 -username ipa-user -show-source true -
show-granular-err true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name:  ipa-user
pw_passwd:
{crypt}$6$GX$kUwi9EhRKmzY8RQwvYwzNW0as5xFPV12i9B5PNZa3.soXLnQFmmTCuojtZ/H9dqt6vjUBHS4V2IFKZZE5Pk9
c.
pw_uid: 1971600003
pw_gid: 1971600000
pw_gecos:
pw_dir: /home/ipa-user
```

```
pw_shell: /bin/sh

NIS:
Error code:    NS_ERROR_NONE
Error message: No error
LDAP:
Error code:    NS_ERROR_NONE
Error message: No error
DNS:
Error code:    NS_ERROR_NONE
Error message: No error
FILES:
Error code:    NS_ERROR_NONE
Error message: No error
Deterministic Result: Success
```

getxxbyyy グループメンバーシップを取得する例：

```
cluster::*> getxxbyyy getgrlist -node node1 -vserver DEMO -username seventeengids
  (vserver services name-service getxxbyyy getgrlist)
pw_name: seventeengids
Groups: 1201 12348 123411 123415 12345 12344 123414 12349 12341 12347 123417 1234 12346 123416
123410 123413 12343 123412 12342 1202 1203 1204 1220 1205 1206 1207 1208 1209 1210 1211 1212 1213
1214 1215 1216 1217
```

getxxbyyy以下を使用したホスト名検索の例：

```
cluster::*> getxxbyyy gethostbyname -node node1 -vserver DEMO -hostname centos8 -show-source true
  (vserver services name-service getxxbyyy gethostbyname)
Source used for lookup: DNS
Host name: centos8
Canonical name: centos8.NTAP.LOCAL
IPv4: x.x.x.x
```

ネットグループメンバーチェックの例：

```
cluster::*> getxxbyyy netgrpcheck -node node1 -vserver DEMO -netgroup netgroup1 -clientIP
10.193.67.225 -show-source true
  (vserver services name-service getxxbyyy netgrpcheck)
Success. Client 10.193.67.225 is member of netgroup netgroup1
Searched using NETGROUP_BYNAME
Source used for lookup: LDAP
```

vserver services access-check

ONTAP 9.3以降のバージョンでは、次のようなネームサービスとやり取りするためのコマンドが用意されています。

- 認証
- DNS
- ネーム マッピング
- サーバ検出

これらのコマンドは、`vserver services access-check` コマンドセットの下にあります。`access-check` コマンドは、基本的には `diag secd` advanced権限に移植されたコマンドです。

認証

ストレージ管理者は、認証コマンドを使用して、マルチプロトコルNAS環境のユーザ、グループ、グループメンバーシップ、数値ID、およびネームマッピングを確認できます。これらのコマンドは、ユーザとIDが想定した結果と一致することを確認したり、グループメンバーシップ情報がSMBプロトコルとNFSプロトコルの両方で機能しているかどうかを確認したりする場合に役立ちます。

より詳細なコマンドの1つは、show-creds コマンドです。このコマンドは、SVMにNFSとSMBが設定されている場合にのみ機能しますが、数値ID、SID、ネームマッピングなど、照会中のユーザに関する幅広い情報が提供されます。

show-creds コマンドの例：

```
cluster::*> vserver services access-check authentication show-creds -vserver DEMO -win-name prof1
-list-id true -list-name true

 UNIX UID: 1100 (prof1) <> Windows User: S-1-5-21-3552729481-4032800560-2279794651-1110
(NTAP\prof1 (Windows Domain User)) <<ネームマッピング

 GID: 1101 (ProfGroup) <<プライマリUNIXグループ
 Supplementary GIDs: << UNIXグループメンバーシップ
  1101 (ProfGroup)
  1201 (group1)
  1202 (group2)
  1203 (group3)
  1220 (sharedgroup)

 Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows
Domain group)

 Windows Membership: << Windows SMBグループメンバーシップ
  S-1-5-21-3552729481-4032800560-2279794651-1106   NTAP\group2 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1122   NTAP\sharedgroup (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1105   NTAP\group1 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1107   NTAP\group3 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1111   NTAP\ProfGroup (Windows Domain group)
  S-1-18-2   Service asserted identity (Windows Well known group)
  S-1-5-32-551   BUILTIN\Backup Operators (Windows Alias)
  S-1-5-32-545   BUILTIN\Users (Windows Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users

 Privileges (0x2086): << Windows権限
  SeBackupPrivilege
  SeRestorePrivilege
  SeChangeNotifyPrivilege
```

DNS

このaccess-check コマンドでは、DNSにフォワードルックアップまたはSRVルックアップを照会することもできます。または、getxxbyyy コマンドを使用することもできます。

ネーム マッピング

ONTAPでは、マルチプロトコルNAS環境のユーザに対してネームマッピングが実行されます。ファイルまたはフォルダのACL形式に基づいてアクセス権を決定するには、有効なユーザが存在する必要があるため、アクセス対象のボリュームまたはqtreeのセキュリティ形式に基づいてユーザを認証することが目的です。（「セキュリティ形式」を参照してください）。たとえば、NTFSセキュリティ形式では、UNIXユーザを有効なWindowsユーザにマッピングする必要があります。LDAPを使用すると、ユーザとグループを一元化して、マルチプロトコルNAS環境のシームレスなネームマッピングを実現できます。

access-check name-mapping コマンドを使用すると、ストレージ管理者は、UNIXユーザとWindowsユーザのネームマッピングが正しいこと、およびKerberos NFSアクセス用のKerberos SPNマッピングが正しいことを確認できます。

access-check name-mapping コマンドの例：

```
cluster::*> access-check name-mapping show -vserver DEMO -direction win-unix -name NTAP\prof1
  (vserver services access-check name-mapping show)
'NTAP\prof1' maps to 'prof1'
```

vserver services name-service

LDAPおよびNASのトラブルシューティングに役立つコマンドのもう1つのセットは `vserver services name-service`、コマンドです。advanced権限で使用できるコマンドは次のとおりです。

```
cluster::*> vserver services name-service ?
  cache>                      *The cache directory
  dns>                        Manage DNS service
  getxxbyyy>                  *Execute getXXbyYY for the given command.
  ldap>                       Manage LDAP configuration
  netgroup>                   Manage local netgroups
  nis-domain>                 Manage Network Information Service domains
  ns-switch>                  Manage Name Services Switch ordering
  unix-group>                 Manage local UNIX group accounts
  unix-user>                  Manage local UNIX user accounts
  ypbind>                     *The ypbind directory
```

このセクションでは、これらのコマンドと、LDAPおよびNASのトラブルシューティングに適した場所について説明します。

キャッシュ

ネットワークとネームサーバの全体的な負荷を軽減するために、ONTAPは多数のネームサービス要求をキャッシュします。これらのキャッシュの詳細については、TR-4668を参照してください。これらのコマンドを使用すると、キャッシュの有効期間を確認、フラッシュ、および設定できます。

管理可能な使用可能なキャッシュは次のとおりです。

```
cluster::*> name-service cache
    group-membership hosts            netgroups        settings
    show-count       unix-group       unix-user
```

`group-membership` キャッシュの例：

```
cluster::*> name-service cache group-membership show -vserver DEMO -user prof1
  (vserver services name-service cache group-membership show)
                                Number of
Vserver    User        Group    Groups    Groups       Create Time     Is Partial
---------- ----------- -------- --------- ------------ ------------------- ----------
DEMO       prof1       1101     5         1101, 1201, 1202, 1203, 1220
                                                      2/13/2020 15:32:00
                                                                          False
```

SVMのグループメンバーシップキャッシュはユーザ単位で削除することもできます。この機能は、ユーザが最近グループに対して追加または削除され、その変更がキャッシュに正確に反映されない場合に便利です。

キャッシュビューとフラッシュは、DNSホスト名、UNIXユーザおよびグループ、およびネットグループにも適用できます。

DNSホスト名キャッシュの例：

```
cluster::*> name-service cache hosts forward-lookup show -vserver DEMO -host *
  (vserver services name-service cache hosts forward-lookup show)
                  IP       Address IP                      Create
Vserver   Host    Protocol Family Address          Source  Time        TTL(sec)
--------- ------- -------- ------- ---------------- ------- ----------- ----------
DEMO      oneway.ntap.local
                  Any      Any     xx.xxx.xx.xxx dns       2/13/2020 3600
                                                           15:39:27
DEMO      oneway.ntap.local
                  Any      Ipv4    xx.xxx.xx.xxx dns       2/13/2020 3600
                                                           15:51:03
```

`unix-user` キャッシュの例：

```
cluster::*> name-service cache unix-user user-by-name show -vserver DEMO -pw-name prof1
  (vserver services name-service cache unix-user user-by-name show)

            Vserver: DEMO
      pw_name field: prof1
       pw_uid field: 1100
       pw_gid field: 1101
        Create Time: 2/13/2020 15:27:30
Source of the Entry: ldap
```

単一のホストに対してネットグループクエリを実行すると、ONTAPはネットグループのすべてのホストをキャッシュに取り込みます。これにより、クラスタの負荷が軽減されます。キャッシュを確認すると、`ip-to-netgroup` 照会された特定のホストのキャッシュを確認できます。

```
cluster::*> name-service cache netgroups ip-to-netgroup show -vserver DEMO
  (vserver services name-service cache netgroups ip-to-netgroup show)
Vserver     IP Address Netgroup      Source Create Time
----------- ---------- ------------- ---------- --------------
DEMO        10.193.67.222
                       netgroup1     ldap    2/20/2020 21:21:21
DEMO        10.193.67.225
                       netgroup1     none    2/20/2020 21:21:28
DEMO        10.193.67.233
                       netgroup1     netgrp_byname
                                             2/20/2020 21:14:12
```

また、照会されたかどうかに関係なく、メンバーの完全なリストを表示することもできます。

```
cluster::*> name-service cache netgroups members show -vserver DEMO
  (vserver services name-service cache netgroups members show)
Vserver     Netgroup     Hosts         Source Create Time
----------- ------------ ------------- ---------- --------------
DEMO        netgroup1    10.193.67.225,xcp.ntap.local,xcp
                                       ldap    2/20/2020 21:08:58
```

すべてのキャッシュには特定のタイムアウト時間（Time-To-Live、TTL）が設定されています。この時間が経過すると、古いエントリが残らないようにエントリが期限切れになります。負のTTL値もあります。負のTTL値では、存在しない可能性のあるオブジェクトでシステムがオーバーランするのを防ぐために、失敗した検索が実行されます。キャッシュタイムアウト値は `settings`、キャッシュタイプごとにコマンドを使用して調整できます。キャッシュを有効または無効にすることもできます。

表13 に、ONTAP 9.7の各キャッシュのデフォルトのキャッシュタイムアウト値を示します。

表13）ONTAP 9.7以降のデフォルトのキャッシュタイムアウト値

キャッシュ	デフォルトタイムアウト
グループメンバーシップリスト	24時間TTL
ホスト	24時間TTL、1分間の負のTTL
ネットグループ	24時間TTL、30分負TTL
UNIXグループ	24時間TTL、1分間の負のTTL
UNIXユーザ	24時間TTL、1分間の負のTTL

注： キャッシュタイムアウト値は、ONTAPのリリースによって変わる場合があります。ONTAPリリースのキャッシュ設定を確認してください。

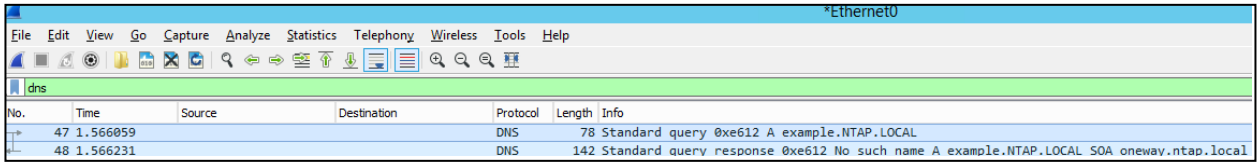
また、ネームサービスキャッシュもデフォルトでは4時間ごとに合計キャッシュ削除されますが、この期間はグローバル `name-service cache settings` コマンドを使用して制御できます。このコマンドでは `name-service`、ノード間でキャッシュをレプリケートして `name- service` SVMにグローバルキャッシュを提供するかどうかを制御することもできます。

DNS

name-service dns コマンドを使用すると、DNSまたはローカルホストファイルエントリを設定したり、動的DNS更新を有効にしたり、DNSサーバのステータスを確認したりできます。

トラブルシューティングの目的で、で dns check は、接続および要求の速度に関する情報を提供できます。このコマンドを実行すると、example.dnsdomain.com 図36に示すように、設定されたDNSサーバに対しての標準の「A」レコードクエリが実行されます。

図36）設定済みのDNSサーバ



例 dns check：

```
cluster::*> name-service dns check -vserver DEMO
  (vserver services name-service dns check)
                                Name Server
Vserver        Name Server      Status        Status Details
-------------- ---------------- ------------- ----------------------------------------------------------------
DEMO           xx.xxx.xx.xxx    up            Response time (msec): 1
```

注: デフォルトでは、dns check はDNS設定が作成されたときに実行されます。dns check いずれかのテスト中にが失敗した場合、-skip-config-validation がに設定されていないかぎり、設定の変更は失敗します true。

getXXbyYY

このコマンドについては前のセクションで説明しましgetXXbyYYた。このコマンドは name-service、ユーザ、グループ、およびDNSルックアップのチェックに使用します。

ldap

name-service ldap コマンドを使用すると、LDAPクライアントおよびスキーマを設定したり、LDAPサーバのステータスを確認したりできます。

トラブルシューティングの目的で、で ldap check は、接続および要求の速度に関する情報を提供できます。このコマンドを実行すると、次の処理が実行されます。

- LDAPサーバへの基本的な接続がチェックされます。
  - でホスト名が設定されている場合は -ldap-servers、DNSが照会されてIPアドレスに解決されます。
  - IPアドレスが設定されている場合、DNSは使用されません。
  - この -ad-domain 設定が構成されている場合、DNSはLDAP SRVレコードを検索します。
- LDAPバインドはLDAPクライアント設定に基づいて実行されます。
  - 最小バインドレベルは、許可される最小バインドレベルです。SASLから始めて、より安全なバインド方法を先に試行します。
- バインドが成功すると、設定されているDNSがチェックされます。
  - ベース、ユーザ、グループ、ネットグループのDNSが設定されている場合は、クエリが実行されます。
  - クエリは基本的な wholeSubtree もので、DNSが存在すると応答するLDAPサーバだけが検索されます。

注： デフォルトでは、ldap check はLDAPクライアント設定の作成時に実行されます。ldap check いずれかのテスト中にが失敗した場合、-skip-config- validation がに設定されていないかぎり、設定の変更は失敗します true。

例 `ldap check`：

```
cluster::> name-service ldap check -vserver DEMO
  (vserver services name-service ldap check)

                  Vserver: DEMO
Client Configuration Name: DEMO
              LDAP Status: up
      LDAP Status Details: Successfully connected to LDAP server "x.x.x.x".
   LDAP DN Status Details: All the configured DNs are available.
```

netgroup

`netgroup` コマンドを使用すると、ネットグループファイルを外部ソースからURIを使用してローカルSVM上のキャッシュにロードし、アクセスを高速化できます。ファイルはFTPまたはHTTP経由でロードされます。

例 `netgroup load`：

```
cluster::*> netgroup load -vserver NFS -source http://x.x.x.x/files/netgroupfile.txt
[Job 25720] Job succeeded: Netgroup Load Job Success
cluster::*> netgroup file show -vserver NFS
                    Member
Vserver    Netgroup Netgroup    Host           User          Domain
---------- -------- ----------- -------------- ------------- --------------------------
NFS
           netgroupfile
                    -           centos8        ipa-user     ,
```

NISドメイン

このコマンドセットはLDAPとは関係がなく、NISとのやり取りに使用されます。

NSスイッチ

このコマンドセットは `ns-switch`、ユーザとグループの検索のソースとしてLDAPを指定するなど、SVMの設定を管理するために使用します。

unix-userおよびunix-group

これらのコマンドセットを使用して、ローカルユーザとローカルグループを管理したり、ユーザとグループに対してファイルのみモードを有効にしたりできます。ファイル専用モードの詳細については、「ONTAPでのローカルファイルの使用」を参照してください。

ypbind

このコマンドは、NISサーバへの接続をテストするための標準のNISコマンドです。LDAPには適用されません。

エクスポートポリシー

ONTAPのエクスポートポリシーは、NFS（必要に応じてSMB）共有アクセス用のエクスポートルールのコンテナです。共有やファイルの権限とは異なり、アクセスはクライアントIPアドレス、ホスト名、ネットグループ、またはサブネットによって制御されます。エクスポートポリシールールは初期のゲートオプションであり、NFSを保護する唯一の方法とは考えないでください。Kerberos、暗号化、ユーザ権限など、他の方法も使用する必要があります。

このセクションでは、`export-policy` LDAP機能に関連する一連のコマンドについて説明します。これは、LDAPがネットグループをクラスタに提供し、クラスタをエクスポートに適用できるためです。

チェック-アクセス

check-access コマンドを使用すると、ボリューム、qtree、およびクライアントIPアドレスを指定して、エクスポートに許可されるアクセスレベルを確認できます。ONTAPは、DNSホスト名を解決し、LDAPでネットグループを検索し、テスト処理をエクスポートに送信します。

コマンドでは、次のオプションを使用できます。

```
cluster::*> export-policy check-access ?
  [ -instance | -fields <fieldname>, ... ]
   -vserver <vserver name>                            Vserver Name
  [-volume] <volume name>                             Volume Name
  [-client-ip] <IP Address>                           Client IP Address
  [-authentication-method] <authentication method>    Authentication Method
  [-protocol] <Client Access Protocol>                Protocol
  [-access-type] {read|read-write}                    Access Rights to Check for
  [ -qtree <qtree name> ]                              Name of the Qtree
  [ -path <text> ]                                     Path
  [ -policy <text> ]                                   Export Policy
  [ -policy-owner <text> ]                             Export Policy Owner
  [ -policy-owner-type {volume|qtree} ]                Type of Export Policy Owner
  [ -rule-index <integer> ]                            Export Policy Rule Index
  [ -access {read|read-write} ]                        Access Rights
  [ -partial-rule-match {true|false} ]                 Did a Subset of the Rules Match?
  [ -clientmatch <text> ]                              Client Match Spec
```

この例では、ルールセットにネットグループが含まれているエクスポートポリシーをテストします。

```
cluster::*> vol show -vserver DEMO -volume netgrpvol -fields policy
vserver volume    policy
---------- ------------ -----------
DEMO    netgrpvol netgroup

cluster::*> export-policy rule show -vserver DEMO -policyname netgroup
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
---------------- -------------------- --------- ------------ ------------------------------ ------------
DEMO         netgroup                any      @netgroup1            any

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.222 -
authentication-method sys -protocol nfs3 -access-type read-write
                                       Policy    Policy       Rule
Path                            Policy     Owner     Owner Type  Index Access
------------------------------------------ ---------------- ---------------- ---------- ------------
/                               default    vsroot    volume          2 read
/netgrpvol                      netgroup   netgrpvol volume          1 read-write
```

コマンドの実行後にネットグループキャッシュにデータが読み込まれたことを確認できます。

```
cluster::*> cache netgroups ip-to-netgroup show -vserver DEMO
  (vserver services name-service cache netgroups ip-to-netgroup show)
Vserver    IP Address Netgroup      Source  Create Time
---------- ---------------------------------------- ---------- ---------------
DEMO       10.193.67.222
                      netgroup1    ldap    2/21/2020 09:10:27
```

qtreeを照会すると、パス全体を照会します。

```
cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.222 -
authentication-method sys -protocol nfs3 -access-type read-write -qtree tree
                                       Policy    Policy       Rule
Path                            Policy     Owner     Owner Type  Index Access
------------------------------------------ ---------------- ---------------- ---------- ------------
/                               default    vsroot    volume          2 read
/netgrpvol                      netgroup   netgrpvol volume          1 read
/netgrpvol/tree                 netgroup   tree      qtree           1 read-write
```

エクスポートポリシールールを書き込み拒否に変更すると、次のようになります。

```
cluster::*> export-policy rule modify -vserver DEMO -policyname netgroup -ruleindex 1 -rorule
never

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.222 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type  Index Access
----------------------------- ---------- --------- ----------- ----- ------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          1 denied
```

キャッシュフラッシュ

エクスポートポリシーではキャッシュも使用されるため、IPアドレス、ホスト名、ネットグループなどの検索にかかる時間が短縮されます。このアプローチにより、NFSエクスポートのマウントとトラバースに必要な時間を短縮できます。

ネットグループを削除またはクライアントを追加するために変更した場合や、クライアントのアクセスレベルが変更された場合など、キャッシュが古くなり、フラッシュが必要になることがあります。キャッシュは export-policy、このセクションに記載されている他のコマンドを使用して表示できます。

次のコマンドでは、個々のキャッシュまたはすべてのキャッシュを一括でフラッシュできます。

```
cluster::*> export-policy cache flush ?
   [-vserver] <vserver name>                                    Vserver
  [[-node] <nodename>]                                          Node
  [ -cache {all|access|host|id|name|netgroup|showmount|ip} ] Cache Name
```

注： すべてのキャッシュを再取り込みする必要がないように、可能な場合は個々のキャッシュのみをフラッシュするか、このセクションの他のコマンドを使用して個々のエントリをフラッシュします。

キャッシュのフラッシュには、次のキャッシュを使用できます。

```
cluster::*> export-policy cache flush -vserver DEMO -cache ?
  all                         All
  access                      Access Cache in the Nblade
  host                        Host Name to IP Cache in the Mgwd
  id                          ID to Credential Cache in the Mgwd
  name                        Name to ID Cache in the Mgwd
  netgroup                    Netgroup cache in the Mgwd
  showmount                   Showmount Caches in the Mgwd and the Nblade
  ip                          IP to Host Name Cache in the Mgwd
```

アクセスキャッシュ

access-cache コマンドを使用すると、エクスポートポリシーのアクセスキャッシュを表示および管理できます。このコマンドでは、NFS経由でボリュームにアクセスしたポリシーとホストを指定できます。

次の例では、2つのクライアントがネットグループエクスポートポリシーを使用してボリュームへのアクセスを試みます。アクセスできるのは1つだけです。

```
cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.225 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type  Index Access
----------------------------- ---------- --------- ----------- ----- ------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          0 denied

cluster::*> export-policy check-access -vserver DEMO -volume netgrpvol -client-ip 10.193.67.222 -
authentication-method sys -protocol nfs3 -access-type read-write
                                    Policy    Policy       Rule
Path                          Policy     Owner     Owner Type  Index Access
----------------------------- ---------- --------- ----------- ----- ------
/                             default    vsroot    volume          2 read
/netgrpvol                    netgroup   netgrpvol volume          1 read-write
```

.225 クライアントがマウントしようとすると、クライアントは拒否されます。

```
[root@centos7 ~]# mount -o nfsvers=3 DEMO:/netgrpvol /netgrpvol
mount.nfs: access denied by server while mounting DEMO:/netgrpvol
```

.222 クライアントがマウントするときに許可されます。

```
[root@centos8-ipa ~]# mount -o nfsvers=3 DEMO:/netgrpvol /netgrpvol
[root@centos8-ipa ~]# mount | grep netgrp
DEMO:/netgrpvol on /netgrpvol type nfs
(rw,relatime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec
=sys,mountaddr=10.193.67.219,mountvers=3,mountport=635,mountproto=udp,local_lock=none,addr=10.193
.67.219)
```

この結果はに反映されます access-cache。Positive はアクセスに成功した negative ことを示し、はアクセスに失敗したことを示します。キャッシュはノード単位で、クライアントが接続されているデータLIFを所有するノードによって異なります。

```
cluster::*> export-policy access-cache show -node node2 -vserver DEMO -policy netgroup -address
10.193.67.222 -instance

                                      Node: node2
                                   Vserver: DEMO
                                Policy Name: netgroup
                                 IP Address: 10.193.67.222
                     Access Cache Entry Flags: has-usable-data
                                Result Code: 0
                  First Unresolved Rule Index: -
                       Unresolved Clientmatch: -
               Number of Matched Policy Rules: 1
         List of Matched Policy Rule Indexes: 1
                               Age of Entry: 83s
                  Access Cache Entry Polarity: positive
Time Elapsed since Last Use for Access Check: 83s
      Time Elapsed since Last Update Attempt: 83s
                Result of Last Update Attempt: 0
                 List of Client Match Strings: @netgroup1

cluster::*> export-policy access-cache show -node node2 -vserver DEMO -policy netgroup -address
10.193.67.225 -instance

                                      Node: node2
                                   Vserver: DEMO
                                Policy Name: netgroup
                                 IP Address: 10.193.67.225
                     Access Cache Entry Flags: has-usable-data
                                Result Code: 0
                  First Unresolved Rule Index: -
                       Unresolved Clientmatch: -
               Number of Matched Policy Rules: 0
         List of Matched Policy Rule Indexes: -
                               Age of Entry: 41s
                  Access Cache Entry Polarity: negative
Time Elapsed since Last Use for Access Check: 41s
      Time Elapsed since Last Update Attempt: 41s
                Result of Last Update Attempt: 0
                 List of Client Match Strings: -
```

netgroup

この export-policy netgroup コマンドには、次のオプションがあります。

```
cluster::*> export-policy netgroup ?
  cache>                      The cache directory
  check-membership            Check to see if the client is a member of the netgroup
  queue>                      The queue directory
```

ONTAP 9.3以降ではグローバルネームサービスキャッシュが追加され（ 詳細についてはTR-4668を参照）、 netgroup cache コマンドが vserver services name-service netgroup コマンドに移動されました。ただし、を使用してネットグループのメンバーシップを確認することはできます check-membership。このコマンドが成功するかどうかは、照会対象のネットグループを含むエクスポートポリシールールが存在するかどうかによって異なります。

```
cluster::*> export-policy rule show -vserver DEMO -policyname netgroup
Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
---------------- ---------- -------- ----------- ---------------------------- ------------
DEMO         netgroup        1       any      @netgroup1             any


cluster::*> export-policy netgroup check-membership -vserver DEMO -netgroup netgroup1 -client-ip
10.193.67.222
Client 10.193.67.222 is a member of netgroup "netgroup1" for Vserver "DEMO" with state "name
service cache".
```

check-membership コマンドの詳細については、マニュアルページを参照してください。

CIFSドメイン

Active Directoryドメインは他のドメインを信頼できます。LDAPユーザが信頼できるドメインに属している場合、ONTAPはどちらのドメインにも同じバインドクレデンシャルを使用して照会できます。場合によっては、ドメインの信頼が正常に機能していないため、次のコマンドを使用して問題を検索する必要があります。

CIFSドメインの信頼

このコマンドは、参加しているActive Directoryドメインのドメイン信頼を照会したときにONTAPが認識する内容を確認し、信頼を再検出するオプションを提供します。信頼できるドメインが正しく表示されないと、ドメイン間のLDAP通信が機能しません。

```
NAME
     vserver cifs domain trusts -- Manage discovered trusted domains

DESCRIPTION
     Manage discovered trusted domains

COMMANDS
     rediscover - Reset and rediscover trusted domains for a Vserver

     show - Display discovered trusted domain information
```

CIFSドメインを検出-サーバ

このコマンドを使用すると、ストレージ管理者は、ONTAPによるActive Directoryドメインの認識を確認して、サーバからドメインコントローラへの接続が適切に機能しているかどうかを確認できます。

```
cluster::*> cifs domain discovered-servers ?
  discovery-mode>             *The discovery-mode directory
  reset-servers               Reset and rediscover servers for a Vserver
  show                        Display discovered server information
```

event log show

ONTAPで問題が発生すると、イベントログサブシステムに記録されます。これらのログは一定期間オンボックスで維持され、イベントログ履歴の以前の段階で問題を確認する必要がある場合は、NetApp Active IQ®デジタルアドバイザから入手できます。

イベントログメッセージは、次のコマンドオプションに示すように、日付、時刻、重大度、メッセージ名など、さまざまな方法でフィルタリングできます。

```
cluster::*> event log show ?
```

```
  [ -detail | -detailtime | -instance | -fields <fieldname>, ... ]
  [[-node] <nodename>]                          Node
  [[-seqnum] <Sequence Number>]                 Sequence#
  [ -time <"MM/DD/YYYY HH:MM:SS"> ]             Time
  [ -severity {EMERGENCY|ALERT|ERROR|NOTICE|INFORMATIONAL|DEBUG} ]
  Severity (default: <=ERROR)
  [ -ems-severity {NODE_FAULT|SVC_FAULT|NODE_ERROR|SVC_ERROR|WARNING|NOTICE|INFO|DEBUG|VAR} ]
  *EMS Severity
  [ -source <text> ]                            Source
  [ -message-name <Message Name> ]              Message Name
  [ -event <text> ]                             Event
  [ -kernel-generation-num <integer> ]          *Kernel Generation Number
  [ -kernel-sequence-num <integer> ]            *Kernel Sequence Number
  [ -action <text> ]                            Corrective Action
  [ -description <text> ]                       Description
  [ -filter-name <text> ]                       Filter Name
```

注： これらのコマンドの詳細については、ONTAPリリースのマニュアルページを参照してください。

LDAP接続などのネームサービスの問題については、メッセージ名の特定のサブセットを使用してイベントログをフィルタリングし、問題を迅速に検出できます。以下のリストは包括的なものではありませんが、始めることができます。

注意： メッセージ名では大文字と小文字が区別されます。

LDAPの場合：

```
cluster::*> event route show -message-name *ldap*
                                                                Freq    Time
Message                              Severity       Destinations Threshd Threshd
-----------------------------------------------------------------------------------
ldap.false.configs.removed           NOTICE         -            0       0
netgroup.ldap.byhost.missing         INFORMATIONAL -             0       0
netgroup.ldap.config                 ERROR          -            0       0
secd.ldap.connectFailure             ALERT          -            0       0
secd.ldap.hostnames.not.resolved     ERROR          -            0       0
secd.ldap.hostnames.resolved.partially
                                     ERROR          -            0       0
secd.ldap.noServers                  EMERGENCY      -            0       0
secd.ldap.query.timed.out            ERROR          -            0       0
secd.ldap.referralError              INFORMATIONAL  -            0       0
secd.ldap.slowServer                 ERROR          -            0       0
secd.netgroup.ldap.badFilter         ERROR          -            0       0
```

エクスポートの場合：

```
cluster::*> event route show -me sage-name *expo t*
                                                                Freq    Time
Message                              Severity       Destinations Threshd Threshd
-----------------------------------------------------------------------------------
Nblade.exportAccessChkFailed         ERROR          -            0       0
Nblade.exportAccessIndeterm          ERROR          -            0       0
crypto.export.failed                 ALERT          -            0       0
exports.anon.noCredForId             ERROR          -            0       0
exports.dns.config                   ERROR          -            0       0
exports.dom.notFound                 ERROR          -            0       0
exports.dom.transient                ERROR          -            0       0
exports.hostname.notFound            INFORMATIONAL  -            0       0
exports.hostname.transient           ERROR          -            0       0
exports.netgroup.dnsNoPtrRec         ERROR          -            0       0
exports.netgroup.notFound            ERROR          -            0       0
exports.netgroup.partial             ERROR          -            0       0
exports.ngbh.allFailed               ERROR          -            0       0
exports.nsdb.anonNameToId            ERROR          -            0       0
exports.policy.empty                 NOTICE         -            0       0
exports.policy.last.rule             ERROR          -            0       0
```

NFS許可の場合：

```
cluster::*> event route show -message-name *nfsAuth*
                                                                Freq     Time
Message                                 Severity        Destinations   Threshd Threshd
--------------------------------------- --------------- ------------- ------- -------
secd.nfsAuth.noCifsCred                 ERROR           -             0       0
secd.nfsAuth.noCifsSid                  ERROR           -             0       0
secd.nfsAuth.noCifsUser                 ERROR           -             0       0
secd.nfsAuth.noNameMap                  ERROR           -             0       0
secd.nfsAuth.noUnixCreds                ERROR           -             0       0
secd.nfsAuth.problem                    ERROR           -             0       0

cluster::*> event route show -message-name *unix*
                                                                Freq     Time
Message                                 Severity        Destinations   Threshd Threshd
--------------------------------------- --------------- ------------- ------- -------
secd.unixLookupFailure                  ERROR           -             0       0
```

ネットグループの場合：

```
cluster::*> event route show -message-name *netgroup*
                                                                Freq     Time
Message                                 Severity        Destinations   Threshd Threshd
--------------------------------------- --------------- ------------- ------- -------
exports.netgroup.dnsNoPtrRec            ERROR           -             0       0
exports.netgroup.notFound               ERROR           -             0       0
exports.netgroup.partial                ERROR           -             0       0
netgroup.files.missing                  ERROR           -             0       0
netgroup.ldap.byhost.missing            INFORMATIONAL   -             0       0
netgroup.ldap.config                    ERROR           -             0       0
netgroup.nis.byhost.decode              ERROR           -             0       0
netgroup.nis.byhost.missing             INFORMATIONAL   -             0       0
netgroup.nis.config                     ERROR           -             0       0
secd.netgroup.ldap.badFilter            ERROR           -             0       0
```

名前変換の場合：

```
cluster::*> event route show -message-name *nameTrans*
                                                                Freq     Time
Message                                 Severity        Destinations   Threshd Threshd
--------------------------------------- --------------- ------------- ------- -------
secd.nameTrans.groupNotFound            ERROR           -             0       0
secd.nameTrans.invalidConfig            ERROR           -             0       0
secd.nameTrans.invalidUser              ERROR           -             0       0
secd.nameTrans.noNameMapping            ERROR           -             0       0
secd.nameTrans.unknownUser              ERROR           -             0       0
secd.nameTrans.userNotFound             ERROR           -             0       0
```

統計

ONTAPには統計サブシステムがあり、パフォーマンスの問題を追跡したり、増分エラーを検索したりできます。

これらの統計はオンデマンドで表示され、`statistics start` コマンドを使用して開始されます。オブジェクトとカウンタでフィルタを使用できます。

マニュアルページのエントリは次のとおりです。

```
cluster::*> man statistics start
statistics start               Data ONTAP 9.7               statistics start

NAME
statistics start -- Start data collection for a sample

AVAILABILITY
This command is available to cluster and Vserver administrators at the advanced privilege level.

DESCRIPTION
```

```
This command starts the collection of performance data. Use the statistics stop command to stop
the collection. You view the sample of performance data by using the statistics show command. You
can collect more than one sample at a time.

PARAMETERS
 [-object <text>] - Object
Selects the objects for which you want to collect performance data. This parameter is required.
To view a list of valid object names, type statistics catalog object show at the command prompt.
To specify multiple objects, use "|" between each object.

Caution: You should limit the scope of this command to only a few objects at a time to avoid a
potentially significant impact on the performance of the system.

 [-instance <text>] - Instance
Selects the instances for which you want to collect performance data. If you do not specify this
parameter, the command collects statistics for all of the instances associated with the specified
objects. To specify multiple instances, use "|" between each instance.

For example, if you want to collect disk object statistics, you can use this parameter to specify
the name of a specific disk whose statistics you want to view. If you do not specify this
parameter, the command will collect statistics for all disks in the system.

 [-counter <text>] - Counter
Selects the counters for which you want to collect performance data. If you do not specify this
parameter, the command collects statistics for all of the counters in the specified objects.

To specify multiple counters, use "|" between each counter.

 [-preset <text>] - Preset
If this parameter is specified, the command displays statistics for the specified preset.

 [-sample-id <text>] - Sample Identifier
Specifies an identifier for the sample. Identifiers must be unique and are restricted to the
characters 0-9, a-z, A-Z, and "_". If you do not specify this parameter, the command generates a
sample identifier for you and defines this sample as the default sample for the CLI session. When
you run the statistics show command without specifying the -sample-id parameter, data from the
default sample displays. If you run this command during the same CLI session and do not specify
the -sample-id parameter, the command overwrites the previous sample. The command does not delete
the default sample when you close your session.

 [-vserver <vserver name>] - Vserver
Selects the vserver for which you want to collect performance data. If you do not specify this
parameter, the command collects statistics for all of the Vservers in the cluster.

 [-node {<nodename>|local}] - Node
Selects the node for which you want to collect performance data. If you do not specify this
parameter, the command collects statistics for all of the nodes in the cluster.

 [-filter <text>] - Filter
Selects performance data for the instance that matches the specified filter criteria. For
example, to display the instances from node1, specify -filter "node_name=node1".

 [-duration <integer>] - Sample Duration in Minutes
If this parameter is specified, the command will collect the closing sample after the time
specified. Duration can be specified in minutes.

 [-sample-type {User|System}] - Sample Type (privilege: diagnostic)
If this parameter is specified, the command will set the sample owner type to user or system. The
default sample type is user.

 [-max <integer>] - Tracker Size
Specifies the number of most active instances of an active object to display. The default setting
is to display all of the instances.

 [-sort-key <text>] - Counter Used For Sorting
If this parameter is specified, the command displays statistics sorted by the specified counter.
Only one counter can be specified.

 [-sort-order {ascending|descending}] - Sort Order
```

```
This parameter may be used in conjunction with the -sort-key parameter. This parameter changes
the order in which statistics are sorted. Possible values are ascending and descending. The
default setting is descending.
```

ネームサービスおよびLDAP統計の場合、-object オプションで次のオブジェクトを指定できます。これは、潜在的な問題やトラブルシューティングに役立ちます。

```
accesscache*
credstore
external_service*
nfs_credstore
nfs_exports_access_cache
nfs_exports_cache
secd*
```

pipe()|値を指定して、1つの統計コマンドで複数のオブジェクトを指定できます。

例：

```
cluster::*> statistics start -object
accesscache*|credstore|external_service*|nfs_credstore|secd*|nfs_exports_access_cache|nfs_exports
_cache
Statistics collection is being started for sample-id: sample_235
```

キャッシュの統計情報には、キャッシュエントリの数、キャッシュにヒットした回数、キャッシュエントリが失われた回数などの情報が表示されます。

外部サービスの統計には、レイテンシ、処理数、使用中のサーバなど、DNSクエリとLDAPクエリに関する情報が表示されます。

次の例では、SVM / SVM、オブジェクト、およびインスタンス名でフィルタして、LDAPサーバのIPアドレスまで、外部サービスカウンタを詳細に表示できます。ここでのユースケースは、このSVMから発生した匿名バインドの数を調べるためです。

```
cluster::*> statistics show -vserver NFS -object external_service* -instance
*LDAP*AnonymousBind:10.193.67.222 -counter num*

Object: external_service_op
Instance: NFS:LDAP (NIS & Name Mapping):AnonymousBind:10.193.67.222
Start-time: 3/3/2020 15:16:43
End-time: 3/3/2020 15:25:32
Elapsed-time: 529s
Scope: NFS

    Counter                                                     Value
    -------------------------------------------- ----------------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               0
    num_responses_received                                          0
    num_successful_responses                                        0
    num_timeouts                                                    0
```

次の例は、ユーザが何回検索されたかを調べる方法を示しています。

```
cluster::*> statistics show -vserver NFS -object external_service* -instance
*LDAP*GetUserInfoFromName:10.193.67.222 -counter num*

Object: external_service_op
Instance: NFS:LDAP (NIS & Name Mapping):GetUserInfoFromName:10.193.67.222
Start-time: 3/3/2020 15:16:43
End-time: 3/3/2020 15:27:40
Elapsed-time: 657s
Scope: NFS

    Counter                                                     Value
    -------------------------------------------- ----------------------------------------
    num_not_found_responses                                         0
```

```
    num_request_failures                                          1
    num_requests_sent                                             2
    num_responses_received                                        2
    num_successful_responses                                      1
    num_timeouts                                                  0
    num_not_found_responses                                       0
    num_request_failures                                          0
    num_requests_sent                                             0
    num_responses_received                                        0
    num_successful_responses                                      0
    num_timeouts                                                  0
```

secd* オブジェクトの場合、統計が開始されてからエラーが発生した回数を確認できます。特定のオブジェクトは secd_rpc_error次のとおりです。

```
cluster::*> statistics show -vserver NFS -object secd_rpc_error -instance *ERROR* -counter count

Object: secd_rpc_error
Instance: NFS:secd_rpc_check_ldap_config:RESULT_ERROR_SECD_NO_SERVER_AVAILABLE
Start-time: 3/3/2020 15:16:43
End-time: 3/3/2020 15:31:49
Elapsed-time: 906s
Scope: NFS

    Counter                                                     Value
    -------------------------------------------- ----------------------------------------
    count                                                           0
    count                                                           0

Object: secd_rpc_error
Instance: NFS:secd_rpc_ldap_get_netgroup_match_by_host:RESULT_ERROR_SECD_GROUP_NOT_FOUND
Start-time: 3/3/2020 15:16:43
End-time: 3/3/2020 15:31:49
Elapsed-time: 906s
Scope: NFS

    Counter                                                     Value
    -------------------------------------------- ----------------------------------------
    count                                                           1

Object: secd_rpc_error
Instance:
NFS:secd_rpc_ldap_get_netgroup_match_by_host:RESULT_ERROR_SECD_NETGROUP_BYHOST_NOT_ENABLED
Start-time: 3/3/2020 15:16:43
End-time: 3/3/2020 15:31:49
Elapsed-time: 906s
Scope: NFS

    Counter                                                     Value
    -------------------------------------------- ----------------------------------------
    count                                                           0

Object: secd_rpc_error
Instance: NFS:secd_rpc_ldap_get_passwd:RESULT_ERROR_SECD_USER_NOT_FOUND
Start-time: 3/3/2020 15:16:43
End-time: 3/3/2020 15:31:49
Elapsed-time: 906s
Scope: NFS

    Counter                                                     Value
    -------------------------------------------- ----------------------------------------
    count                                                           0
    count                                                           0
6 entries were displayed.
```

必要な期間だけ統計を実行したら、クラスタの負荷を軽減し、統計ファイルを小さくするために、統計を無効にする必要があります。

```
cluster::*> statistics stop
```

```
Statistics collection is being stopped for sample-id: sample_235
```

既存の統計サンプルを表示または削除することもできます。

```
cluster::*> statistics samples
    delete show
```

vserver security file-directory show

ストレージ管理者がファイルシステム内のファイルやフォルダの権限を簡単に表示できるように、ONTAPにはコマンドが用意されて `vserver security file-directory show`います。このコマンドは、権限やアクセスに関する問題のトラブルシューティングに役立ちます。

このコマンドを実行するには、SVMとボリューム内のファイルまたはフォルダの完全パスを使用します。コマンドの詳細については、を `man vserver security file-directory show`参照してください。

次の例は、オブジェクトのセキュリティ形式と適用されるACLの形式に基づくコマンドの出力を示しています。

NTFSセキュリティ形式の例：

```
cluster::> vserver security file-directory show -vserver DEMO -path /data/Windows.iso

               Vserver: DEMO
             File Path: /data/Windows.iso
      File Inode Number: 15770
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 20
 DOS Attributes in Text: ---A----
Expanded Dos Attributes: -
           UNIX User Id: 0
          UNIX Group Id: 0
         UNIX Mode Bits: 777
 UNIX Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:NTAP\DomainUsers
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff-(Inherited)
```

UNIXセキュリティ形式の例–モードビット権限：

```
cluster::> vserver security file-directory show -vserver DEMO -path /flexgroup_16/newfile1

               Vserver: DEMO
             File Path: /flexgroup_16/newfile1
      File Inode Number: 3358476
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 20
 DOS Attributes in Text: ---A----
Expanded Dos Attributes: -
           UNIX User Id: 0
          UNIX Group Id: 0
         UNIX Mode Bits: 644
 UNIX Mode Bits in Text: rw-r--r--
                   ACLs: -
```

mixedセキュリティ形式の例- NFSv4.x ACL

```
cluster::> vserver security file-directory show -vserver DEMO -path /home/student2

               Vserver: DEMO
             File Path: /home/student2
      File Inode Number: 97
```

```
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           UNIX User Id: 0
          UNIX Group Id: 0
         UNIX Mode Bits: 775
 UNIX Mode Bits in Text: rwxrwxr-x
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         DACL - ACEs
                           ALLOW-OWNER@-0x1601ff
                           ALLOW-user-student2-0x1601ff
                           ALLOW-user-prof1-0x21
                           ALLOW-user-admin-0x1601ff
                           ALLOW-GROUP@-0x1201ff-IG
                           ALLOW-EVERYONE@-0x1200a9
```

mixedセキュリティ形式–NTFS対応のセキュリティの例：

```
cluster::> vserver security file-directory show -vserver DEMO -path /mixed/nfs3

               Vserver: DEMO
             File Path: /mixed/nfs3
     File Inode Number: 32636
         Security Style: mixed
        Effective Style: ntfs
         DOS Attributes: 20
 DOS Attributes in Text: ---A----
Expanded Dos Attributes: -
           UNIX User Id: 1100
          UNIX Group Id: 1101
         UNIX Mode Bits: 777
 UNIX Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:NTAP\prof1
                         Group:NTAP\DomainUsers
                         DACL - ACEs
                           ALLOW-NTAP\Administrator-0x1201ff
                           ALLOW-NTAP\prof1-0x1f01ff
                           ALLOW-Everyone-0x1201ff
```

セキュリティ形式は、ONTAPでのネームマッピングの実行方法に影響します。アクセスを試行するユーザは、オブジェクトに設定されている権限構造に適合するユーザ名に解決する必要があります。

NetAppサポートに連絡する前に収集する情報

LDAP問題が発生して手動で解決できない場合は、NetAppサポートにご相談ください。サポートケースをオープンした場合、テクニカルサポートエンジニアは問題のトラブルシューティングを行うためにデータを収集する必要があります。このプロセスを円滑に進めるために、回答で回答できる質問と、サポートケースを迅速に解決するために役立つ情報を以下に示します。このリストはすべてを網羅しているわけではありません。テクニカルサポートエンジニアからさらにデータを要求される場合がありますが、ここから始めましょう。

- 問題が発生した日時
- 使用されているLDAPサーバのタイプとOS
- 使用されているLDAPクライアント
- 影響を受けるユーザまたはグループ
- 問題はまだ発生していますか？間欠的ですか？
- テクニカルサポートエンジニアがLDAPサーバからの追加情報を必要とした場合に、LDAP管理者が電話に出ることはできますか。
- LDAPサーバで何らかの暗号化が使用されているか。

- 問題はすべてのノードで実行されますか。いくつかのノード？特定のIPアドレス
- ONTAPからネットワーク経由でLDAPサーバにアクセスできますか。
- `-type all（autosupport invoke * -type all）`を使用して新しいAutoSupportレポートを生成します。
  - このコマンドは、LDAPクライアント、クライアントスキーマ、DNS、ネットワーク、イベントログ、など。
- 「ONTAP CLI commands for LDAP troubleshooting」セクションの手順に従って、トラブルシューティングコマンドの出力を確認しましたか。
- ONTAP以外の他のクライアントは、「サードパーティのツールとユーティリティ」セクションに記載されているコマンドを使用してLDAPに適切に照会できますか。
- LDAPクエリの問題（ユーザが見つかりません）またはLDAP設定の問題については、ユーザおよびグループのLDAPスキーマから出力を収集します。この出力は、正しいスキーマが使用されていることを確認するのに役立ちます。
- クライアント、LDAPサーバ、およびONTAPシステムからの問題実行中のパケットトレース。
- ネームサービスおよびキャッシュの統計キャプチャ情報を提供します。「統計」セクションを参照してください。

ONTAPでのパケットトレースの収集については、次のNetAppナレッジベースの記事を参照してください。

- ONTAP 9.2+システムでパケットトレース（tcpdump）をキャプチャする方法
- ONTAP 9.1以下のシステムでpkttを使用してローリングパケットトレースを収集する方法

ベストプラクティス

このセクションでは、NetApp ONTAPでLDAPを使用する場合の特定のシナリオのベストプラクティスについて説明します。これらのベストプラクティスは難しい要件ではなく、成功のための単なるガイドラインです。ベストプラクティスは、単純な問題の防止には役立ちますが、環境内で問題が発生しないことを保証するものではありません。このリストは完全なものではありませんが、複数のシナリオに対応しようとしています。

LDAPサーバノベストプラクティス

LDAPサーバのベストプラクティスの概要を次に示します。

- 複数のLDAPサーバを使用して、単一のサーバの過負荷を防止します。
- LDAPサーバを最新のOSリリースおよびパッチリリースに更新します。
- 可能な場合は、バインドとLDAP検索に暗号化を使用します（クエリにはSASL BINDとStartTLS、SMB署名など）。
- LDAP over SSL（LDAPS）の代わりにStartTLSを使用します。LDAPSは標準として廃止されました。
- で使用するサービスアカウントを作成し、管理者またはディレクトリマネージャのユーザではなく、ONTAPのLDAPクライアントにバインドします。
- LDAPサーバで匿名バインドを無効にします。
- フォレスト内の複数のドメインにUNIX属性があるWindows Active Directory LDAPでは、UNIX ID管理のために属性をグローバルカタログにレプリケートすることを検討してください。「UNIX ID管理にActive Directoryを使用するLDAP」および「Active Directoryグローバルカタログ検索」サブセクションを参照してください。
- 同じ名前（など `ldap.ntap.local`）を使用して複数のLDAPサーバのDNS Aレコードを作成し、DNSロードバランシングを提供するか、外部のネットワークロードバランサを使用してサーバ間でネットワーク接続を分散します。
- 可能であれば、LDAPサーバにUNIX属性が自動的に入力されるように、ユーザおよびグループの作成の自動化を設定します。このベストプラクティスは、主にWindowsアカウントとUNIXアカウントを使用するマルチプロトコルNAS環境に関連しています。

- マルチプロトコルNAS環境でUNIXユーザ名を作成する場合は、明示的なネームマッピングルールが不要になるように、Windows名と同じユーザ名を使用してください。

DNSサーバのベストプラクティス

次に、DNSサーバのベストプラクティスの概要を示します。TR-4523では、DNSロードバランシングについて詳しく説明しています。

- 冗長性とロードバランシングを実現するには、相互に情報を複製する複数のDNSサーバを使用します。
- ホストがDNSにフォワードルックアップとリバースルックアップのレコードを持っていることを確認します。
- LDAPでDNSで使用可能なSRVレコードがあることを確認します。
- 冗長性を確保するために、ONTAP SVMのDNS設定で複数のDNSサーバを指定します。

キャッシュ管理のベストプラクティス

このセクションでは、ONTAPでのキャッシュ管理のベストプラクティスの概要について説明します。

キャッシュタイムアウト設定

ネームサービスキャッシュには、エントリが古くなる状況を回避するために時間の経過とともにキャッシュが期限切れになるため、デフォルトで特定のタイムアウト設定があります。表14に、ONTAP 9.7以降のデフォルトのキャッシュ設定を示します。

ONTAPのキャッシュタイムアウト値の多くは変更可能です。キャッシュのタイムアウト設定には、次のベストプラクティスが適用されます。

- ほとんどの場合、キャッシュタイムアウトはデフォルトのままにしておいてください。キャッシュ内の古いエントリを削除するには、
  `cache flush` コマンド。
- チャーン率が高い環境（ユーザがグループに対して頻繁に追加または削除される、ネットグループがホストを追加または削除するなど）では、キャッシュタイムアウト値を小さくしてより頻繁に更新することを検討してください。
- お客様の環境でチャーンが少ない（ユーザがほとんど変更されず、ネットグループがほとんど変更されない）場合は、キャッシュを長く維持するためにタイムアウト値を大きくすることを検討してください。
- キャッシュタイムアウト値を小さくすると、ONTAPとネームサービスの間のネットワークトラフィックが増加し、ONTAPとネームサービスのCPUの負荷が増大し、パフォーマンスが低下する可能性があることに注意してください。キャッシュタイムアウト値を大きくすると、古いエントリが頻繁に生成され、ユーザに誤ってアクセスが許可または拒否される可能性があります。
- ネームサービスサーバに関する統計を監視するには、次の手順を実行します。

```
cluster::> set diag
cluster::*> statistics start -object external_service_server
cluster::*> statistics show -object external_service_server
```

手動キャッシュフラッシュに関する考慮事項

キャッシュを手動でフラッシュすると、次の理由で古くなっている可能性がある情報がキャッシュから削除されます。

- エクスポート ポリシー ルールが最近変更された
- ユーザ情報またはグループメンバーシップの最近の変更
- ネーム サーバでホスト名のレコードが最近変更された
- ネーム サーバでネットグループ エントリが最近変更された
- ネットグループのフルロードを妨げていたネットワーク停止からのリカバリ

キャッシュをフラッシュすると、古い情報が削除され、ONTAPは適切な外部リソースから現在の情報を取得するように強制されます。

注: キャッシュの再取り込みは、リソースを大量に消費する可能性があります。キャッシュのフラッシュは、特定の問題を解決しようとしている場合にのみ実行し、可能であれば問題のあるエントリのみをフラッシュします。

キャッシュによっては、個々のエントリが削除されることがあります。他のキャッシュは一括でフラッシュする必要があります。表14 に、ONTAP 9.7以降でフラッシュできるキャッシュのレベルを示します。キャッシュをフラッシュできるレベルも、表示できるレベルに対応していることがよくあります。

表14）ONTAP 9.7以降での手動キャッシュフラッシュの操作性

キャッシュ	キャッシュフラッシュの操作性
ネットグループメンバーキャッシュ	個々のクライアントまたはすべてのクライアント
ネットグループIPホスト間キャッシュ	個々のクライアントまたはすべてのクライアント
LDAPグループ認証	個人名
エクスポートポリシーキャッシュ	個々のキャッシュまたはすべてのキャッシュ
ネームサービス:グループメンバーシップ	コベツノユーザオヨビグループ
ネームサービス:ホスト	個別のフォワードDNSルックアップとリバースDNSルックアップ
ネームサービス：UNIXユーザおよびグループ	個々のユーザとグループ、またはすべてのユーザとグループ
エクスポートポリシーアクセスキャッシュ	個々のクライアント/ポリシー

エクスポートポリシーのベストプラクティス

このセクションでは、ONTAPでのエクスポートポリシーとルールのベストプラクティスの概要について説明します。

エクスポートポリシーとルールは、アクセスを要求しているクライアントに基づいてNFSエクスポートへのアクセスを制御するのに役立ちます。最も一般的なエクスポートポリシーのベストプラクティスについては、TR-4067を参照してください。LDAPサーバに関連するエクスポートポリシーとルールには、次のベストプラクティスが適用されます。

- エクスポートポリシーで同じアクセス権限を持つ多数のクライアントを指定する場合は、ストレージ管理の複雑さを軽減するために、ネットグループの使用を検討してください。
- SVMのDNS設定が適切に機能しており、フォワードルックアップとリバースルックアップによってホストを解決できることを確認します。
- エクスポートポリシールールでは、ルールインデックスの順序によって、最初に適用されるエクスポートポリシールールが決まります。サブネット全体に対してより限定的なポリシーを設定し、特定のクライアントにマウントへのルートアクセスを許可する場合は、リストの上位にある管理クライアントのルールインデックスを設定して、最初に処理されるようにします。より制限の厳しいポリシールールを最初に指定すると、ルールインデックスでルートアクセスが許可されていても、クライアントはそのポリシーに基づいてアクセスを拒否されます。
- エクスポートポリシールールでネットグループを指定する場合は、`@netgroup` 構文を使用します。指定しない場合、ONTAPはネットグループをホスト名として解釈します。たとえば、`netgroup1` ルールでを指定する場合は、を使用し `@netgroup1`ます。

ネットグループノベストプラクティス

次に、ONTAPでのネットグループのベストプラクティスの概要を示します。

- ネットグループに追加したホストがDNSに存在することを確認します。
- @記号を使用して、エクスポートポリシールールでネットグループを指定します。
- を使用する場合は `netgroup.byhost`、次の点を考慮して、ホストに必要なアクセス結果を有効にしてください。
  - ホスト名のDNSレコードのフォワードおよびリバース。
  - ネットグループファイル内のホストの三重エントリ。
  - ホストの `netgroup.byhost` エントリのネットグループ仕様。

- 大文字と小文字の区別の問題を回避するために、常に小文字のホストを使用する必要があります。
- `netgroup.byhost` 大文字と小文字の区別を含む、DNSとエントリの同期。
- `netgroup.byhost` NISでを使用する場合は-、エントリにダッシュ（）が使用されないように3つの値が設定されていることを確認してください。たとえば、エントリは()`host,,`not()のようになります`host,-,-`。ONTAPは、トリプルのホスト部分のみをサポートします。NISは、トリプルの他の部分のエントリを試行エントリとして扱います。

- `netgroup.byhost` ネットグループが非常に大きい大規模な環境では、NetAppの機能を使用することを強く推奨します。アクセスが正常に機能するため `netgroup.byhost` には、ネットグループエントリとネットグループエントリが同期されている必要があります。

LDAPクライアントのベストプラクティス

次に、LDAPクライアント（LDAPクライアントでもあるONTAPを含む）のベストプラクティスの概要を示します。

- 使用可能な最も安全な方法でバインドおよび検索するようにLDAPクライアントを設定します。ONTAPの場合は、CIFSサーバとしてのバインド（存在する場合）、SMB署名でのバインド、LDAPSまたはStartTLSの使用が含まれます。
- Linuxクライアントの場合、NetAppは設定とセットアップを容易にするためにSSSDを推奨しています。
- LDAPにSSSDを使用する場合は、LDAPアイデンティティプロバイダのみがサポートされます。Active Directory IDプロバイダは、Active Directory SIDに基づいて一意のUID数値を生成します。現在のONTAPではサポートされていません。詳細については、「SSSD UID/GIDアルゴリズム（SSSD Active Directoryプロバイダ）」を参照してください。
- `ldapsearch` およびONTAP CLIコマンドを使用して、すべてのLDAPクライアントが同じユーザおよびグループ情報（グループメンバーシップを含む）を返すことを確認します。
- 名前や数値IDが競合しているクライアントでローカルユーザやローカルグループを使用しないでください。この状況により、ファイルやフォルダへのアクセスで原因が予期しない動作をする可能性があります。

付録A：コマンド例およびその他の情報

このセクションでは、このドキュメントの前のセクションには当てはまらなかったコマンド例やその他の情報を示します。

ONTAPでのローカルファイルの使用

場合によっては、ユーザ、グループ、ネットグループなどにネームサービスサーバを使用できない（外部ネームサービスにアクセスできない）ことや、必要な（LDAPの設定を正当化できるユーザが不足している）ことがあります。

このような場合、NetApp ONTAPには、これらのオブジェクトのローカルファイルエントリを作成するためのいくつかの方法が用意されています。管理は一元化され、クライアント間で一貫性があるため、外部ネームサービスを使用することを推奨します。

ONTAPでローカルファイルを使用するには、主に次の2つの方法があります。

- System ManagerまたはCLIを使用して、ユーザ、グループ、ホストなどのエントリを個別に作成します。
- `the load-from-uri` コマンドを使用してONTAP SVMにファイルをインポートします。ファイルをプルするには、HTTPサーバまたはFTPサーバへのアクセスが必要です。

ユーザ、グループ、グループメンバーシップ、ホスト、NISデータベース、およびネットグループ：ローカ

ルユーザとローカルグループの作成方法の詳細については、製品ドキュメントを参照してください。

拡張モード/ファイル専用モード

環境には数千のユーザとグループが存在し、LDAPサーバが存在しない場合があります。ただし、デフォルトでは、SVMごとに作成できるローカルユーザとローカルグループの数に制限があります。

ONTAP 9.1でローカルユーザとローカルグループの拡張モード/ファイル専用モードを使用すると、ストレージ管理者はローカルユーザとローカルグループの制限を拡張できます。そのためには、diagレベルのネームサービスオプションを有効にし、`load-from-uri` 機能を使用してファイルをクラスタにロードしてより多くのユーザとグループを提供します。拡張モード/ファイルのみモードでは、ネームサービスサーバやネットワークなどに対する外部の依存関係が不要になるため、ネームサービス検索のパフォーマンスも向上します。ただし、ファイル管理によってストレージ管理のオーバーヘッドが増大し、人為的ミスの可能性が高まるため、このパフォーマンスにはネームサービスの管理が容易になりません。さらに、ローカルファイル管理はクラスタごとに実行する必要があるため、複雑さが増します。

ユーザとグループに対してこのオプションを有効にするには、`vserver services name-service unix-user file-only` コマンドと `vserver services name-service unix-group file-only` コマンドを使用します。

```
NAME
vserver services name-service unix-user file-only modify -- Change configuration for UNIX-user
file download

AVAILABILITY
This command is available to cluster and Vserver administrators at the diagnostic privilege
level.

DESCRIPTION
The vserver services name-service unix-user file-only modify command enables you to load UNIX
user files with large number of UNIX users beyond the maximum configurable limit of 65536 for the
cluster. Once it is enabled, individual operations on UNIX users are not allowed, and the users
can only be managed using the vserver services name-service unix-user load-from-uri command.


PARAMETERS
-vserver <vserver name> - Vserver
Use this parameter to specify the Vserver for which you want to modify the file-only mode.

[-is-enabled {true|false}] - Is File-Only Download Enabled?
Use this parameter with value true to enable the file-only mode. This field is set to false by
default.
```

モードを有効にしたら、次のコマンドを使用して、URIからユーザファイルとグループファイルをロードします。

```
cluster::*> vserver services name-service unix-user load-from-uri
```

メモ： ユーザの場合は10MB、グループの場合は25MBを超えるファイルをロードする場合は、`-skip-file-size- check` オプションを使用します。

ファイルのみモードを使用する場合、ユーザおよびグループに対する個々の操作は許可されません。この構成は、現在、NetApp MetroCluster™またはSVMディザスタリカバリ（SVM DR）のシナリオではサポートされていません。

このコマンドを使用すると、いくつかの警告が発行されます。

```
cluster::*> vserver services name-service unix-user file-only modify -vserver SVM1 -is-enabled
true

Warning: Do not enable the file-only configuration if you are using, or plan to use, MetroCluster
or Vserver Async DR.
         If you enable the file-only configuration:
         - Modifying individual user entries will not be possible.
         - Local Unix-users must be managed by downloading a file using the "vserver services
name-service unix-user load-from-uri" command.
```

```
         - Downloading the users will replace all existing users. The standard set of users must
be present in the file. If the users "root", "pcuser" and "nobody" are not defined, a data
serving interruption might occur.
         This command may take some time to complete.
Do you want to continue? {y|n}: y
```

ローカルユーザおよびローカルグループファイルのステータスを確認するには、次のコマンドを使用します。

```
cluster::*> vserver services unix-user file status
Vserver   Node            Load Time           Hash Value
--------- --------------- ------------------- ----------------------------------------
Hash Value DB                      File Size
---------------------------------- ---------------
SVM1
          node-01
                          10/11/2016 10:55:27 6b617f426b0646df581fe94b0d20b7cc
1e0e62ca1bd18174174e9f562f1aea88 75B
          node-02
                          10/11/2016 10:55:27 6b617f426b0646df581fe94b0d20b7cc
1e0e62ca1bd18174174e9f562f1aea88 75B
```

外部ネームサービスは引き続き使用できますか。

ファイルのみモードでは、LDAPまたはNISをネームサービスとして使用できないわけではありません。つまり、ローカルユーザとローカルグループの管理はファイルのみで実行されます。次の例では、SVMでファイルのみモードが有効になっていますが、LDAPを使用して引き続き名前検索を実行できます。

```
cluster::*> name-service ns-switch show -vserver SVM1
  (vserver services name-service ns-switch show)
                                Source
Vserver         Database        Order
--------------- ----------------  ------------
SVM1            hosts           files,
                                dns
SVM1            group           files,
                                ldap
SVM1            passwd          files,
                                ldap
SVM1            netgroup        files
SVM1            namemap         files
5 entries were displayed.

cluster::*> vserver services unix-user file-only show -vserver SVM1

                      Vserver: SVM1
Is File-Only Download Enabled?: true

cluster::*> getxxbyyy getpwbyname -node ontap9-tme-8040-01 -vserver SVM1 -username ldapuser
-show-source true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name:  ldapuser
pw_passwd:
pw_uid: 1108
pw_gid: 513
pw_gecos:
pw_dir: /home/ldapuser
pw_shell: /bin/sh
```

file-only が有効になっている場合、root、pcuser、nobody ロードされているファイルにこれらのユーザが含まれていないと、およびのデフォルトのローカルユーザが削除されることに注意してください。passwd group を使用する場合は、ファイルとファイルにローカルユーザとローカルグループを含めてfile-onlyください。

```
cluster::*> unix-user show -vserver SVM1

Error: show failed: File-only configuration is enabled. Use the command "vserver services name-
service unix-user file show" instead.

cluster::*> vserver services name-service unix-user file show -vserver SVM1
```

```
   Line No File content
-------------  ----------------------
         1 nobody:*:65535:65535::::::
         2 pcuser:*:65534:65534::::::
         3 root:*:0:1::::::
```

制限

このセクションでは、ONTAPのローカルユーザとローカルグループに関する制限について説明します。表15に概要を示します。これらの制限はクラスタ全体に適用されます。

表15）ONTAPクラスタでのローカルユーザとローカルグループの制限

ローカルUNIXユーザ/グループの制限	フアイルノミノユウサトクルウフノセイケン
32,768（デフォルト） 65、536（最大）	passwd ファイルサイズ（ユーザ）：10MB group ファイルサイズ：25MB **注：** passwd との group ファイルサイズはで上書きできます - skip- file-size-checkが、それより大きいファイルサイズはテストされていません。 ユーザ数：400,000 グループ：15,000 グループメンバーシップ：30万 SVM：6

ローカルUNIXユーザとローカルグループの最大数はクラスタ全体で表示され、複数のSVMを含むクラスタに影響します。したがって、クラスタにSVMが4つある場合は、各SVMの最大ユーザ数の合計が、クラスタの最大数に達している必要があります。

例：

- SVM1 ローカルUNIXユーザ数：2、000
- SVM2 ローカルUNIXユーザ数が40、000
- SVM3 20人のローカルUNIXユーザが含まれます。
- SVM4 その後、23、516人のローカルUNIXユーザを作成できます。

制限を超えてUNIXユーザまたはグループを作成しようとすると、エラーメッセージが表示されます。

例：

```
cluster::> unix-group create -vserver NAS -name test -id 12345

Error: command failed: Failed to add "test" because the system limit of {limit number}
       "local unix groups and members" has been reached.
```

制限は、advanced権限レベルで次のコマンドで制御します。

```
cluster::*> unix-user max-limit
    modify show
```

デフォルトのローカルユーザ

vserver setupまたはSystem Managerを使用してSVMを作成すると、デフォルトのローカルUNIXユーザおよびグループが、デフォルトのUIDおよびGIDとともに作成されます。

次に、これらのユーザとグループを示します。

```
cluster::> vserver services unix-user show -vserver vs0
                User             User    Group  Full
Vserver         Name             ID      ID     Name
------------------ -------------------- -------- -------- ----------------------------------------
```

```
nfs             nobody          65535 65535 -
nfs             pcuser          65534 65534 -
nfs             root            0      0      -

cluster::> vserver services unix-group show -vserver vs0
Vserver         Name                 ID
--------------- -------------------- -----------------
nfs             daemon               1
nfs             nobody               65535
nfs             pcuser               65534
nfs             root                 0
```

ファイル専用モードを使用する場合は、クラスタの管理に使用されているファイルに上記のユーザが存在していることを確認してください。file-onlyを有効にすると、アップロードされたファイルにデフォルトのユーザが含まれていない場合、デフォルトのユーザは削除されます。

diag secdとvserver security access-check

SecDとは、ONTAPのシステムシェルにあるユーザ認証アプリケーションのことです。このアプリケーションは、クラスタモードでONTAPを実行した初期の頃から、ドメインコントローラ、LDAPサーバ、DNSなどと対話してきました。何年にもわたってONTAPのリリースを通して、SecDの役割は少し変わっており、LDAPの機能はFreeBSD `libc` モジュールに移されたなど、より多くの操作が他の領域に移されました。

これらの変更は、ネームサービスキャッシュをSVMレベルで保持し、要求を受信したクラスタ内のノードに関係なく使用されるグローバルキャッシュにできるようにNetAppで行われています。SecDは、これまでONTAP 9.3よりも前のバージョンで各ノードにローカライズされたキャッシュを使用していましたが、クラスタ間でキャッシュに違いが生じることがありました。グローバルネームサービスキャッシュの詳細については、TR-4668：『Name Services Best Practices Guide』を参照してください。

グローバルキャッシュに加えて、次のようないくつかの目的を達成するための新しいコマンドが作成されました。

- ネームサービスクエリを簡易化します。
- diag権限を必要としないコマンドを指定します（ただし、トラブルシューティングの必要に応じてノードレベルのクエリを使用することもできます）。
- コマンドを実行するためのノード要件を削除します。

ONTAP 9.6以降では、`diag secd` コマンドの名前検索機能を模倣した新しいコマンドセットが導入されています。可能な場合は、ではなく、これらのコマンドを使用して `diag secd`ください。

```
cluster::*> vserver services access-check ?
  authentication>             *Check Authentication Information
  dns>                        *Check DNS Lookups
  name-mapping>               *Check Name Mapping Operations
  server-discovery>           *Check Server Discovery Information
```

LDAPクエリの例

LDAPクエリの例を次に示します。

LDAPユーザ属性ダンプの例：Active Directory

PowerShellクエリは一連の属性値を返します。この属性値を使用して、構成に適用する適切なLDAPスキーマテンプレートを特定できます。次の例は、`-Properties` 必要な属性を見つけやすくするためににフィルタが適用されたActive Directory LDAPからのユーザダンプを示しています。

```
PS C:\Users\Administrator> Get-ADUser -Identity prof1 -Properties
Name,gecos,gidNumber,HomeDirectory,ObjectClass,sAMAccountName,uid,uidNumber,unixHomeDirectory


DistinguishedName : CN=prof1,CN=Users,DC=NTAP,DC=local
```

```
Enabled           : True
gecos             : Prof1
gidNumber         : 1101
GivenName         : prof1
HomeDirectory     :
Name              : prof1
ObjectClass       : user
ObjectGUID        : 0973b3f1-da85-499c-80b4-a210e0d0fb2f
SamAccountName    : prof1
SID               : S-1-5-21-3552729481-4032800560-2279794651-1110
Surname           :
uid               : {prof1}
uidNumber         : 1100
unixHomeDirectory : /home/prof1
UserPrincipalName : prof1@NTAP.LOCAL
```

PowerShellクエリは、クエリをサポートするバージョンのWindowsでのみ機能することに注意してください。古いバージョンのWindowsまたはLinux/UNIXベースのLDAPサーバでは `ldapsearch`、コマンドを使用できます。

LDAPユーザ属性ダンプの例：ldapsearch

一般的な `ldapsearch` 例については、「一般的なLDAP検索の例」を参照してください。

`ldapsearch` クエリからの出力を次に示します。

```
# ldapsearch -D "cn=Directory Manager" -W -p 389 -h 10.193.67.222 -b "dc=centos-ldap,dc=local" -s
sub "(uid=ipa-user)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=centos-ldap,dc=local> with scope subtree
# filter: (uid=ipa-user)
# requesting: ALL
#

# ipa-user, users, compat, centos-ldap.local
dn: uid=ipa-user,cn=users,cn=compat,dc=centos-ldap,dc=local
objectClass: posixAccount
objectClass: ipaOverrideTarget
objectClass: top
gecos: IPA User
cn: IPA User
uidNumber: 1971600003
gidNumber: 1971600000
loginShell: /bin/sh
homeDirectory: /home/ipa-user
ipaAnchorUUID:: OklQQTpjZW50b3MtbGRhcC5sb2NhbDplMDQwZWU0Mi00ODRjLTExZWEtOWE3ZC
 0wMDUwNTY5ZWM0N2Q=
uid: ipa-user

# ipa-user, users, accounts, centos-ldap.local
dn: uid=ipa-user,cn=users,cn=accounts,dc=centos-ldap,dc=local
givenName: IPA
sn: User
uid: ipa-user
cn: IPA User
displayName: IPA User
initials: IU
gecos: IPA User
krbPrincipalName: ipa-user@CENTOS-LDAP.LOCAL
gidNumber: 1971600000
userClass: user
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
```

```
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: ipauser
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
loginShell: /bin/sh
homeDirectory: /home/ipa-user
mail: ipa-user@centos-ldap.local
krbCanonicalName: ipa-user@CENTOS-LDAP.LOCAL
userPassword:: e2NyeXB0fSQ2JEdYJGtVd2k5RWhSS216WThSUXd2WXd6TlcwYXM1eEZQVjEyaTl
 CNVBOWmEzLnNvWExuUUZtbVRDdW9qdFovSDlkcXQ2dmpVQkhTNFYySUZLWlpFNVBrOWMu
ipaUniqueID: e040ee42-484c-11ea-9a7d-0050569ec47d
krbPrincipalKey:: MIHeoAMCAQGhAwIBAaIDAgEDowMCAQGkgccwgcQwaKAbMBmgAwIBBKESBBB7
 THspfXM9YGZpJ3lrKXtSoUkwR6ADAgESoUAEPiAANeN6Uh1meVExph7lENHLlCq26i8B4To8XooBv
 XDw8MEGNTzEDqlCDI03zyZgTsLaPAaoTR44pIHBqN4AMFigGzAZoAMCAQShEgQQX3UgejBoUURoYk
 8lXnQgUaE5MDegAwIBEaEwBC4QAPUeyAwJ3gYB99nPbnGG8ZsMuuB963O3GLmaJzCOiydzaBcLfvT
 Bz3mN82Ye
uidNumber: 1971600003
krbPasswordExpiration: 20200206144442Z
krbLastPwdChange: 20200206144442Z
krbExtraData:: AAJaJjxecm9vdC9hZG1pbkBDRU5UT1MtTERBUC5MT0NBTAA=
mepManagedEntry: cn=ipa-user,cn=groups,cn=accounts,dc=centos-ldap,dc=local
memberOf: cn=ipausers,cn=groups,cn=accounts,dc=centos-ldap,dc=local
memberOf: cn=trust admins,cn=groups,cn=accounts,dc=centos-ldap,dc=local
memberOf: cn=ontap-ldap,cn=groups,cn=accounts,dc=centos-ldap,dc=local
krbTicketFlags: 128
krbLoginFailedCount: 0
```

クレデンシャルダンプの例

次のコマンドは、設定されているネームサービスとプロトコルサービスからユーザに関するすべての情報を取得します。このコマンドは、マルチプロトコル環境のONTAPでネームマッピングと権限の問題をトラブルシューティングする場合に特に役立ちます。Windowsクレデンシャルを取得するにはActive Directory通信が必要なため、このコマンドはCIFS / SMBが設定されている場合にのみ機能することに注意してください。

```
cluster::*> diag secd authentication show-creds -node ontap9-tme-8040-01 -vserver DEMO -unix-
user-name prof1 -list-id true -list-name true

 UNIX UID: 1100 (prof1) <> Windows User: S-1-5-21-3552729481-4032800560-2279794651-1110
(NTAP\prof1 (Windows Domain User))

 GID: 1101 (ProfGroup)
 Supplementary GIDs:
  1101 (ProfGroup)
  1201 (group1)
  1202 (group2)
  1203 (group3)
  1220 (sharedgroup)

 Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows
Domain group)

 Windows Membership:
  S-1-5-21-3552729481-4032800560-2279794651-1106   NTAP\group2 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1122   NTAP\sharedgroup (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1105   NTAP\group1 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1107   NTAP\group3 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1111   NTAP\ProfGroup (Windows Domain group)
  S-1-18-2   Service asserted identity (Windows Well known group)
  S-1-5-32-551   BUILTIN\Backup Operators (Windows Alias)
  S-1-5-32-545   BUILTIN\Users (Windows Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users

 Privileges (0x2086):
```

```
  SeBackupPrivilege
  SeRestorePrivilege
  SeChangeNotifyPrivilege
```

LDAPスキイマテンフレエト

次に、ONTAPで使用可能なスキーマテンプレートを示します。この出力は、ONTAP 9.6を実行している ONTAPシステムから取得したものです。

AD-IDMU

```
                                  Schema Template: AD-IDMU
                                          Comment: Schema based on Active Directory Identity
Management for UNIX (read-only)
                RFC 2307 posixAccount Object Class: User
                  RFC 2307 posixGroup Object Class: Group
                 RFC 2307 nisNetgroup Object Class: nisNetgroup
                             RFC 2307 uid Attribute: uid
                       RFC 2307 uidNumber Attribute: uidNumber
                       RFC 2307 gidNumber Attribute: gidNumber
                  RFC 2307 cn (for Groups) Attribute: cn
              RFC 2307 cn (for Netgroups) Attribute: name
                    RFC 2307 userPassword Attribute: unixUserPassword
                            RFC 2307 gecos Attribute: name
                   RFC 2307 homeDirectory Attribute: unixHomeDirectory
                      RFC 2307 loginShell Attribute: loginShell
                       RFC 2307 memberUid Attribute: memberUid
               RFC 2307 memberNisNetgroup Attribute: memberNisNetgroup
               RFC 2307 nisNetgroupTriple Attribute: nisNetgroupTriple
               Enable Support for Draft RFC 2307bis: false
       RFC 2307bis groupOfUniqueNames Object Class: groupOfUniqueNames
                 RFC 2307bis uniqueMember Attribute: uniqueMember
Data ONTAP Name Mapping windowsToUnix Object Class: User
  Data ONTAP Name Mapping windowsAccount Attribute: msDS-PrincipalName
   Data ONTAP Name Mapping windowsToUnix Attribute: sAMAccountName
   No Domain Prefix for windowsToUnix Name Mapping: true
                                Vserver Owns Schema: true
 Maximum groups supported when RFC 2307bis enabled: 256
                    RFC 2307 nisObject Object Class: nisObject
                      RFC 2307 nisMapName Attribute: nisMapName
                     RFC 2307 nisMapEntry Attribute: nisMapEntry
```

AD-SFU

```
                                  Schema Template: AD-SFU
                                          Comment: Schema based on Active Directory Services for
UNIX (read-only)
                RFC 2307 posixAccount Object Class: User
                  RFC 2307 posixGroup Object Class: Group
                 RFC 2307 nisNetgroup Object Class: msSFU30NisNetGroup
                             RFC 2307 uid Attribute: sAMAccountName
                       RFC 2307 uidNumber Attribute: msSFU30UidNumber
                       RFC 2307 gidNumber Attribute: msSFU30GidNumber
                  RFC 2307 cn (for Groups) Attribute: cn
              RFC 2307 cn (for Netgroups) Attribute: name
                    RFC 2307 userPassword Attribute: msSFU30Password
                            RFC 2307 gecos Attribute: name
                   RFC 2307 homeDirectory Attribute: msSFU30HomeDirectory
                      RFC 2307 loginShell Attribute: msSFU30LoginShell
                       RFC 2307 memberUid Attribute: msSFU30MemberUid
               RFC 2307 memberNisNetgroup Attribute: msSFU30MemberNisNetgroup
               RFC 2307 nisNetgroupTriple Attribute: msSFU30MemberOfNisNetgroup
               Enable Support for Draft RFC 2307bis: false
       RFC 2307bis groupOfUniqueNames Object Class: groupOfUniqueNames
                 RFC 2307bis uniqueMember Attribute: uniqueMember
Data ONTAP Name Mapping windowsToUnix Object Class: User
  Data ONTAP Name Mapping windowsAccount Attribute: windowsAccount
   Data ONTAP Name Mapping windowsToUnix Attribute: windowsAccount
   No Domain Prefix for windowsToUnix Name Mapping: false
```

```
                                Vserver Owns Schema: true
 Maximum groups supported when RFC 2307bis enabled: 256
                   RFC 2307 nisObject Object Class: msSFU30NisObject
                     RFC 2307 nisMapName Attribute: msSFU30NisMapName
                    RFC 2307 nisMapEntry Attribute: msSFU30NisMapEntry
```

MS-AD-BIS

```
                                  Schema Template: MS-AD-BIS
                                          Comment: Schema based on Active Directory Identity
Management for UNIX (read-only)
                RFC 2307 posixAccount Object Class: User
                  RFC 2307 posixGroup Object Class: Group
                 RFC 2307 nisNetgroup Object Class: nisNetgroup
                             RFC 2307 uid Attribute: uid
                          RFC 2307 uidNumber Attribute: uidNumber
                          RFC 2307 gidNumber Attribute: gidNumber
               RFC 2307 cn (for Groups) Attribute: cn
             RFC 2307 cn (for Netgroups) Attribute: name
                   RFC 2307 userPassword Attribute: unixUserPassword
                           RFC 2307 gecos Attribute: name
                  RFC 2307 homeDirectory Attribute: unixHomeDirectory
                     RFC 2307 loginShell Attribute: loginShell
                      RFC 2307 memberUid Attribute: memberUid
              RFC 2307 memberNisNetgroup Attribute: memberNisNetgroup
              RFC 2307 nisNetgroupTriple Attribute: nisNetgroupTriple
              Enable Support for Draft RFC 2307bis: true
       RFC 2307bis groupOfUniqueNames Object Class: group
                RFC 2307bis uniqueMember Attribute: Member
Data ONTAP Name Mapping windowsToUnix Object Class: User
  Data ONTAP Name Mapping windowsAccount Attribute: sAMAccountName
   Data ONTAP Name Mapping windowsToUnix Attribute: sAMAccountName
   No Domain Prefix for windowsToUnix Name Mapping: true
                                Vserver Owns Schema: true
 Maximum groups supported when RFC 2307bis enabled: 256
                   RFC 2307 nisObject Object Class: nisObject
                     RFC 2307 nisMapName Attribute: nisMapName
                    RFC 2307 nisMapEntry Attribute: nisMapEntry
```

RFC 2307

```
                                  Schema Template: RFC-2307
                                          Comment: Schema based on RFC 2307 (read-only)
                RFC 2307 posixAccount Object Class: posixAccount
                  RFC 2307 posixGroup Object Class: posixGroup
                 RFC 2307 nisNetgroup Object Class: nisNetgroup
                             RFC 2307 uid Attribute: uid
                          RFC 2307 uidNumber Attribute: uidNumber
                          RFC 2307 gidNumber Attribute: gidNumber
               RFC 2307 cn (for Groups) Attribute: cn
             RFC 2307 cn (for Netgroups) Attribute: cn
                   RFC 2307 userPassword Attribute: userPassword
                           RFC 2307 gecos Attribute: gecos
                  RFC 2307 homeDirectory Attribute: homeDirectory
                     RFC 2307 loginShell Attribute: loginShell
                      RFC 2307 memberUid Attribute: memberUid
              RFC 2307 memberNisNetgroup Attribute: memberNisNetgroup
              RFC 2307 nisNetgroupTriple Attribute: nisNetgroupTriple
              Enable Support for Draft RFC 2307bis: false
       RFC 2307bis groupOfUniqueNames Object Class: groupOfUniqueNames
                RFC 2307bis uniqueMember Attribute: uniqueMember
Data ONTAP Name Mapping windowsToUnix Object Class: posixAccount
  Data ONTAP Name Mapping windowsAccount Attribute: windowsAccount
   Data ONTAP Name Mapping windowsToUnix Attribute: windowsAccount
   No Domain Prefix for windowsToUnix Name Mapping: false
                                Vserver Owns Schema: true
 Maximum groups supported when RFC 2307bis enabled: 256
                   RFC 2307 nisObject Object Class: nisObject
                     RFC 2307 nisMapName Attribute: nisMapName
                    RFC 2307 nisMapEntry Attribute: nisMapEntry
```

LDAPクライアント設定の例

次の設定は、Windows Server 2012を実行しているActive Directory LDAPサーバを指すLDAPクライアントからのものです。

Active Directory LDAPクライアント

```
                                 Vserver: DEMO
               Client Configuration Name: DEMO
                          LDAP Server List: -
           (DEPRECATED)-LDAP Server List: -
                 Active Directory Domain: NTAP.LOCAL
       Preferred Active Directory Servers: -
Bind Using the Vserver's CIFS Credentials: true
                          Schema Template: DEMO
                         LDAP Server Port: 389
                      Query Timeout (sec): 3
        Minimum Bind Authentication Level: sasl
                           Bind DN (User): ldap-user
                                  Base DN:
                        Base Search Scope: subtree
                                  User DN: -
                       User Search Scope: subtree
                                 Group DN:  -
                      Group Search Scope: subtree
                             Netgroup DN: -
                   Netgroup Search Scope: subtree
              Vserver Owns Configuration: true
     Use start-tls Over LDAP Connections: false
          Enable Netgroup-By-Host Lookup: false
                     Netgroup-By-Host DN: -
                  Netgroup-By-Host Scope: subtree
                 Client Session Security: none
                   LDAP Referral Chasing: false
                 Group Membership Filter: -
```

次の設定は、Red Hat Directory Serverをポイントするクライアントからのものです。

RHEL Directory Server LDAPクライアント

```
               Client Configuration Name: centos7.ntap2016.local
                          LDAP Server List: centos7.ntap2016.local
           (DEPRECATED)-LDAP Server List: -
                 Active Directory Domain: -
       Preferred Active Directory Servers: -
Bind Using the Vserver's CIFS Credentials: false
                          Schema Template: RFC-2307
                         LDAP Server Port: 389
                      Query Timeout (sec): 3
        Minimum Bind Authentication Level: simple
                           Bind DN (User): cn=ldapadm,dc=ntap2016,dc=local
                                  Base DN: dc=ntap2016,dc=local
                        Base Search Scope: subtree
                                  User DN: -
                       User Search Scope: subtree
                                 Group DN:  -
                      Group Search Scope: subtree
                             Netgroup DN: -
                   Netgroup Search Scope: subtree
              Vserver Owns Configuration: false
     Use start-tls Over LDAP Connections: false
          Enable Netgroup-By-Host Lookup: false
                     Netgroup-By-Host DN: -
                  Netgroup-By-Host Scope: subtree
                 Client Session Security: none
                   LDAP Referral Chasing: false
                 Group Membership Filter: -
```

パケットトレースから見たLDAPトラフィック

このセクションでは、ONTAP SVM LDAPクライアントとWindows Active Directoryを実行するLDAPサーバ間のLDAP通信について説明します。このトレースでは、が `getxxbyyy` という名前の特定のユーザのクラスタで実行されました `prof1`。

```
cluster::*> getxxbyyy getpwbyname -node node1 -vserver DEMO -username prof1 -show-source true -
use-cache false
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
pw_name: prof1
pw_passwd:
pw_uid: 1100
pw_gid: 1101
pw_gecos:
pw_dir:
pw_shell: /bin/sh
```

LDAPクライアント設定は次のとおりです。

```
cluster::*> ldap client show -client-config DEMO

                                 Vserver: DEMO
                Client Configuration Name: DEMO
                        LDAP Server List: -
            (DEPRECATED)-LDAP Server List: -
                  Active Directory Domain: ntap.local
       Preferred Active Directory Servers: -
Bind Using the Vserver's CIFS Credentials: true
                          Schema Template: DEMO
                         LDAP Server Port: 389
                     Query Timeout (sec): 3
        Minimum Bind Authentication Level: sasl
                           Bind DN (User): administrator
                                  Base DN: DC=NTAP,DC=local
                       Base Search Scope: subtree
                                 User DN: CN=Users,DC=NTAP,DC=local
                       User Search Scope: subtree
                                Group DN: -
                     Group Search Scope: subtree
                              Netgroup DN: -
                   Netgroup Search Scope: subtree
               Vserver Owns Configuration: true
     Use start-tls Over LDAP Connections: false
          Enable Netgroup-By-Host Lookup: true
                      Netgroup-By-Host DN: -
                   Netgroup-By-Host Scope: subtree
                  Client Session Security: none
                    LDAP Referral Chasing: false
                  Group Membership Filter: -
```

トレースの最初のステップは、LDAP SRVレコードのDNSレコード検索でした。これは `-ad- domain`、クライアント設定で使用された設定に基づいています。

```
10.193.67.237 10.193.67.236 DNS       81     Standard query 0xcbec SRV _ldap._tcp.ntap.local
```

この要求は成功したため、のSRVレコードに対して別のDNS要求が作成されました `Default- First-Site-Name`。

```
10.193.67.236 10.193.67.237 DNS       134    Standard query response 0xcbec SRV
_ldap._tcp.ntap.local SRV 0 100 389 oneway.ntap.local A 10.193.67.236

10.193.67.237 10.193.67.236 DNS       112    Standard query 0x0075 SRV _ldap._tcp.Default-First-
Site-Name._sites.ntap.local

10.193.67.236 10.193.67.237 DNS       165    Standard query response 0x0075 SRV
_ldap._tcp.Default-First-Site-Name._sites.ntap.local SRV 0 100 389 oneway.ntap.local A
10.193.67.236
```

次に、クライアント設定で指定されたLDAPポートが通常のTCPパケットを使用してテストされ、ポートが開いていてリスンしていることが確認されます。

```
10.193.67.237 10.193.67.236 TCP       74      14802 → 389 [SYN] Seq=0 Win=65535 Len=0 MSS=8960
WS=256 SACK_PERM=1 TSval=890800619 TSecr=0
10.193.67.236 10.193.67.237 TCP       74      389 → 14802 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
MSS=1460 WS=256 SACK_PERM=1 TSval=252542599 TSecr=890800619
```

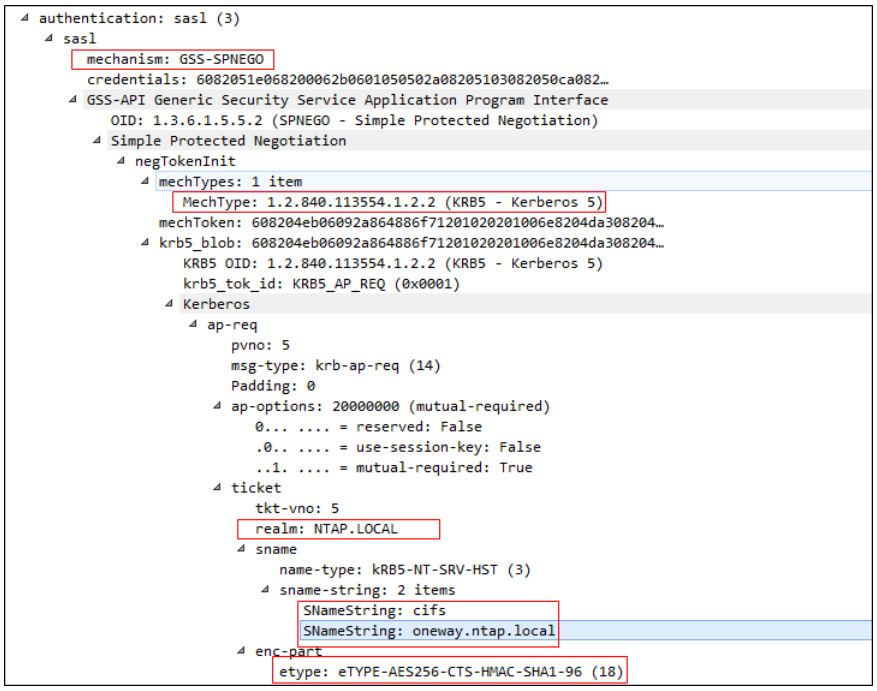
次に、TCPパケットを送信してポートを開き、LDAP通信を実行します。

```
10.193.67.237 10.193.67.236 TCP       66      14802 → 389 [ACK] Seq=1 Ack=1 Win=65792 Len=0
TSval=890800619 TSecr=252542599
```

その後、LDAPバインドが実行されます。

```
10.193.67.237 10.193.67.236 LDAP      1416    bindRequest(1) "<ROOT>" sasl
```

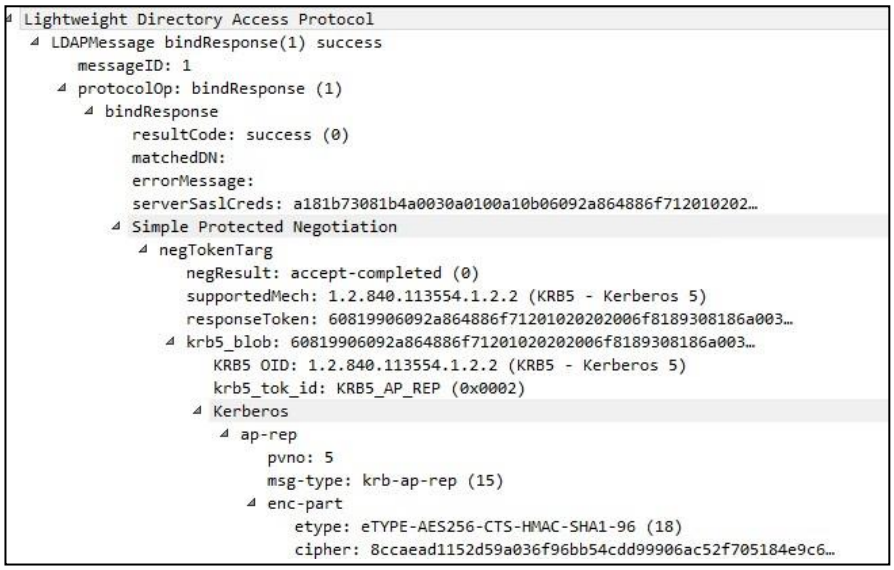
LDAPクライアントオプションがに設定されているため、`-bind-as-cifs-server true`バインド要求ではCIFSマシンアカウントとKerberos認証が使用されます。パケットの詳細に表示されます。



Kerberosが使用されているのは、という名前のCIFSマシンアカウント `DEMO` に有効なDNS Aレコードとリバースネームルックアップレコードがあるためです。何らかの理由でKerberosを使用できない場合は、NTLMにフォールバックします。

次のパケットは、Kerberosでバインドが成功したことを示しています。

```
10.193.67.236 10.193.67.237 LDAP      278     bindResponse(1) success
```

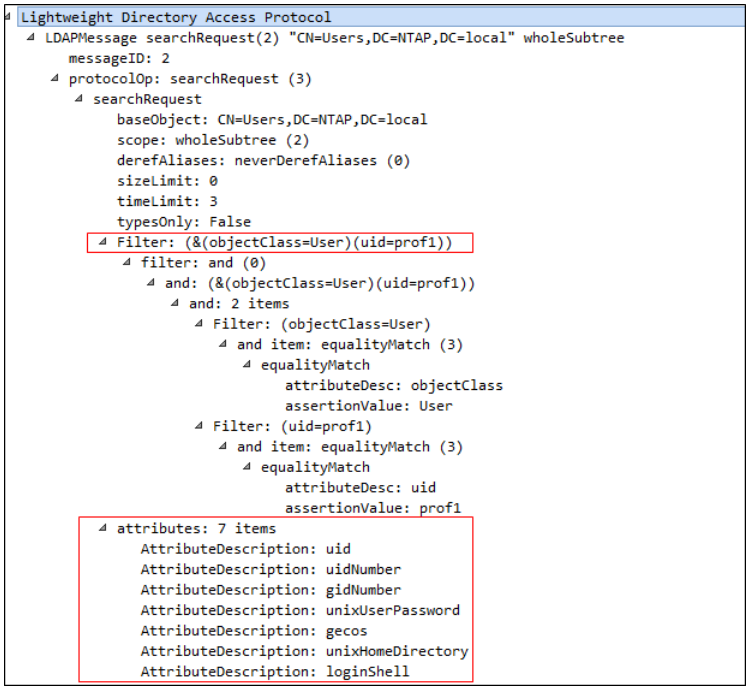


これで、LDAP検索を実行できます。これはユーザ要求であり、`-user-dn` 値が入力されているため、検索に使用されます。ユーザDNが指定されていない場合は、で設定された値にフォールバックし `-base-dn`ます。

```
10.193.67.237 10.193.67.236 LDAP      239     searchRequest(2) "CN=Users,DC=NTAP,DC=local"
wholeSubtree
```

LDAP `searchRequest` パケットは、検索で使用されたフィルタに関する多くの情報を提供します。このLDAP要求がTLSまたはSSLを使用していた場合は暗号化され、トレースを復号化しないかぎり値は表示されませんでした。

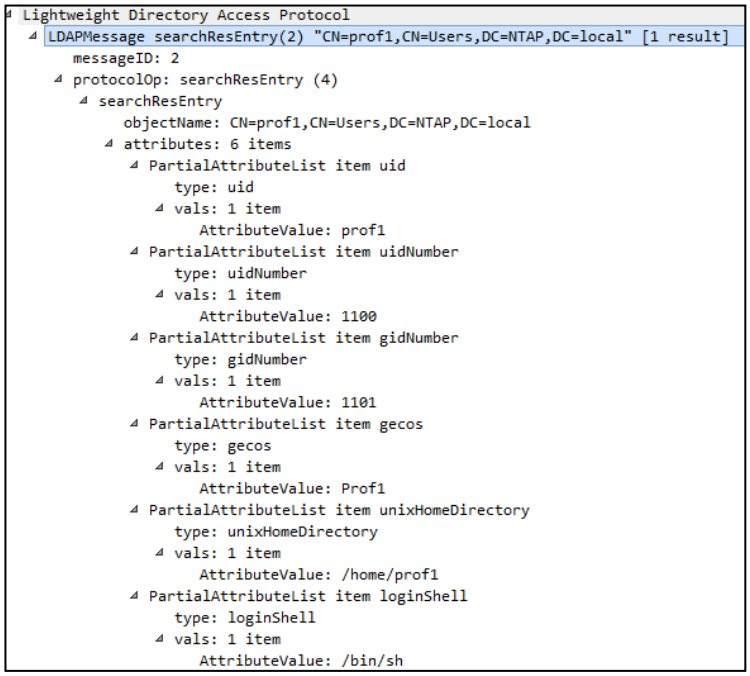
次の例では、ユーザ `objectClass` がUIDの検索に使用されていることがわかります `prof1`。また、ONTAPが検索で7つの異なる属性を要求したこともわかります。この情報を使用して、検索要求のトラブルシューティングを行ったり、`ldapsearch` またはLDPなどのサードパーティツールで使用する独自のLDAP検索フィルタを構築したりできます。



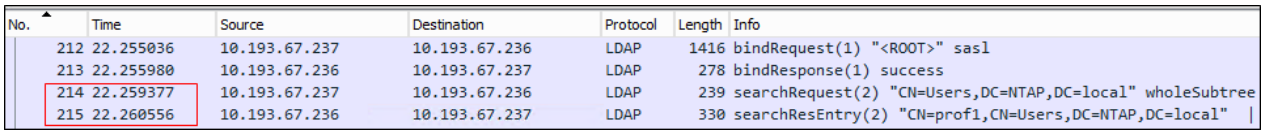
LDAPは `searchRequest` 要求された情報で応答し、1つの結果が返されたことを示します。

```
10.193.67.236 10.193.67.237 LDAP      330     searchResEntry(2)
"CN=prof1,CN=Users,DC=NTAP,DC=local" | searchResDone(2) success [1 result]
```

トレースの詳細には `getXXbyXX`、ONTAP CLIからコマンドを実行した場合と同じ出力が表示されます。



LDAP検索フィルタを表示するだけでなく、に `searchRequest` かかった時間も確認できます。各パケットにはタイムスタンプが付いています。この場合、要求が1秒未満で返されたことがわかります。



No.	Time	Source	Destination	Protocol	Length	Info
212	22.255036	10.193.67.237	10.193.67.236	LDAP	1416	bindRequest(1) "<ROOT>" sasl
213	22.255980	10.193.67.236	10.193.67.237	LDAP	278	bindResponse(1) success
214	22.259377	10.193.67.237	10.193.67.236	LDAP	239	searchRequest(2) "CN=Users,DC=NTAP,DC=local" wholeSubtree
215	22.260556	10.193.67.236	10.193.67.237	LDAP	330	searchResEntry(2) "CN=prof1,CN=Users,DC=NTAP,DC=local"

タイムスタンプ情報を取得すると、LDAPクライアント設定に設定されているLDAPタイムアウト値が原因でLDAPの問題が発生しているかどうかを判断するのに役立ちます。

最後に、要求が完了すると、ONTAPはポート要求を閉じます。

```
10.193.67.237 10.193.67.236 TCP       66      14802 → 389 [ACK] Seq=1524 Ack=477 Win=65792 Len=0
TSval=890800725 TSecr=252542599
```

お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。docfeedback@netapp.comまでお問い合わせください。件名に「TECHNICAL REPORT 4835」と添えてください。

謝辞

`bind-dn` ディレクトリマネージャーではないFreeIPAでユーザーを作成する方法を提供してくれたOliver Brakmannに感謝します。

詳細情報の入手方法

- TR-4067：『ONTAP NFS Best Practice and Implementation Guide』
  www.netapp.com/us/media/tr-4067.pdf
- TR-4523：『ONTAPにおけるDNSロードバランシング』
  www.netapp.com/us/media/tr-4523.pdf
- TR-4616：『NFS Kerberos in ONTAP with Microsoft Active Directory』
  www.netapp.com/us/media/tr-4616.pdf
- TR-4668：『ネームサービスベストプラクティスガイド』（ONTAP 9.3以降）
  www.netapp.com/us/media/tr-4668.pdf
- ONTAP 9ドキュメント センター
  https://docs.netapp.com/ontap-9/index.jsp
- ONTAPおよびONTAP System Managerのドキュメントリソース
  https://www.netapp.com/us/documentation/ontap-and-oncommand-system-manager.aspx

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2020年5月	初版
バージョン1.1	2021年2月	軽微な修正を行いました。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4835-0521-JP