ACS 5.X： LDAP サーバの保護の設定例

目次

概要

Lightweight Directory Access Protocol（LDAP）は、TCP/IP および UDP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。 LDAP は、x.500 ベースのディレクトリ サーバにアクセスするための軽量メカニズムです。 RFC 2251 では LDAP を定義しています。

Access Control Server (ACS) 5.x は、LDAP プロトコルを使用して LDAP 外部データベース（ID ストアとも呼ばれる）と統合します。 LDAP サーバへの接続には、 プレーン テキスト（シンプル）接続と SSL（暗号化）接続という 2 つの方法が使用されます。 ACS 5.x は、この方法の両方を使用して LDAP サーバに接続するように設定できます。 このドキュメントでは、暗号化接続を使用して LDAP サーバに接続するように ACS 5.x が設定されています。

前提条件

要件

このドキュメントでは、ACS 5.x が LDAP サーバに IP 接続し、ポート TCP 636 が空いていることが想定されています。

ポート TCP 636 でセキュア LDAP 接続を容認するように、Microsoft® Active Directory LDAP サーバを設定する必要があります。 このドキュメントでは、Microsoft LDAP サーバにサーバ証明書を発行した認証局（CA）のルート証明書があることが想定されています。 LDAP サーバの設定方法の詳細については、『サードパーティ認証局を使用して SSL で LDAP を有効にする方法』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure ACS 5.x
- Microsoft Active Directory LDAP サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ディレクトリ サービス

ディレクトリ サービスは、コンピュータ ネットワークのユーザおよびネットワーク リソースに関する情報を保存および編成するためのソフトウェア アプリケーション（アプリケーションのセット）です。 ディレクトリ サービスを使用すると、これらのリソースへのユーザ アクセスを管理できます。

LDAP ディレクトリ サービスは、クライアント/サーバ モデルに基づきます。 クライアントは、LDAP サーバに接続することで LDAP セッションを開始し、操作要求をサーバに送信します。 サーバは、応答を送信します。 1 台以上の LDAP サーバに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、ディレクトリを管理します。ディレクトリは、情報を保有するデータベースです。 ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバ間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバ間で分散できます。 各サーバには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前（属性タイプまたは属性の説明）と 1 つ以上の値があります。 属性はスキーマに定義されます。

それぞれのエントリには固有の識別子、 認定者名（DN）があります。 この名前には、エントリ内の属性で構成されている相対識別名（RDN）と、それに続く親エントリの DN が含まれています。 DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

LDAP を使用した認証

ACS 5.x は、ディレクトリ サーバでバインド操作を実行し、プリンシパルを検索および認証することによって、LDAP ID ストアに対してプリンシパルを認証できます。 認証が成功した場合、ACS はプリンシパルに所属するグループおよび属性を取得できます。 取得する属性は、ACS Web インターフェイス（LDAP ページ）で設定できます。 ACS は、これらのグループおよび属性を使用してプリンシパルを認可できます。

ユーザの認証または LDAP ID ストアの問い合わせを行うために、ACS は LDAP サーバに接続し、接続プールを保持します。

LDAP 接続管理

ACS 5.x では、複数の同時 LDAP 接続がサポートされています。 接続は、最初の LDAP 認証時にオン デマンドで開かれます。 最大接続数は、LDAP サーバごとに設定されます。 事前に接続を開いておくと、認証時間が短縮されます。

同時バインディング接続に使用する最大接続数を設定できます。 開かれる接続の数は、LDAP サーバ（プライマリまたはセカンダリ）ごとに異なる場合があり、サーバごとに設定される最大管理接続数によって決まります。

ACS は、ACS で設定されている LDAP サーバごとに、開いている LDAP 接続（バインド情報を含む）のリストを保持します。 認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。

開いている接続が存在しない場合、新しい接続が開かれます。 LDAP サーバが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。

認証プロセスが完了したあと、Connection Manager は Connection Manager への接続を解放します。 詳細については、『ACS 5.X ユーザ ガイド』を参照してください。

設定

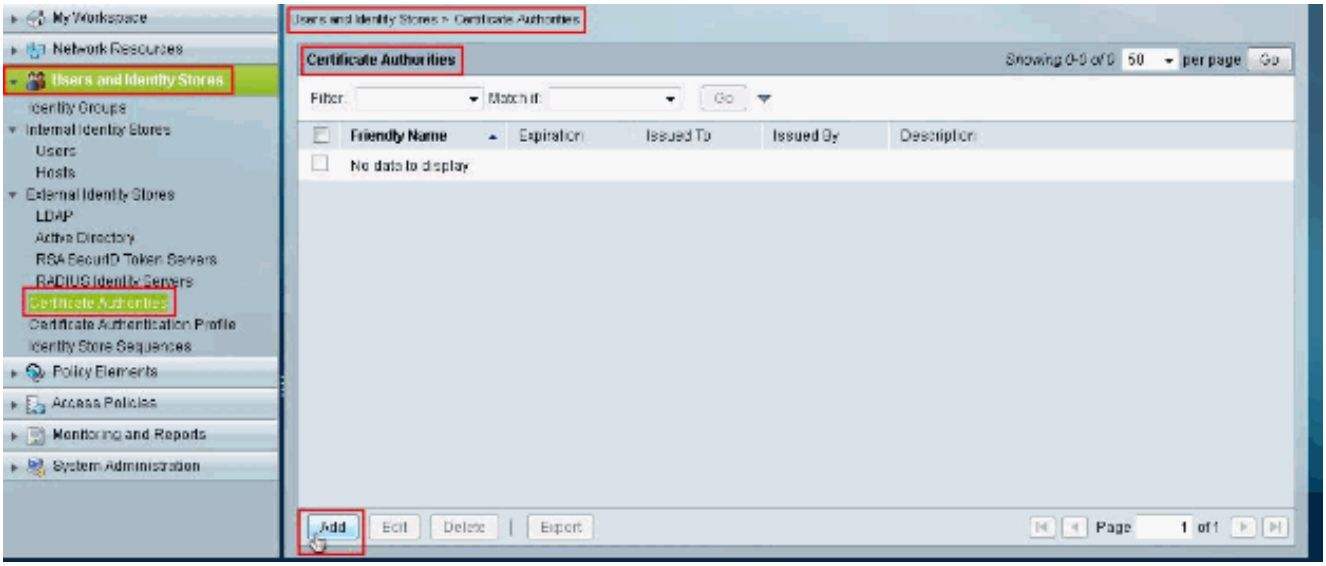
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ACS 5.x でのルート CA 証明書のインストール

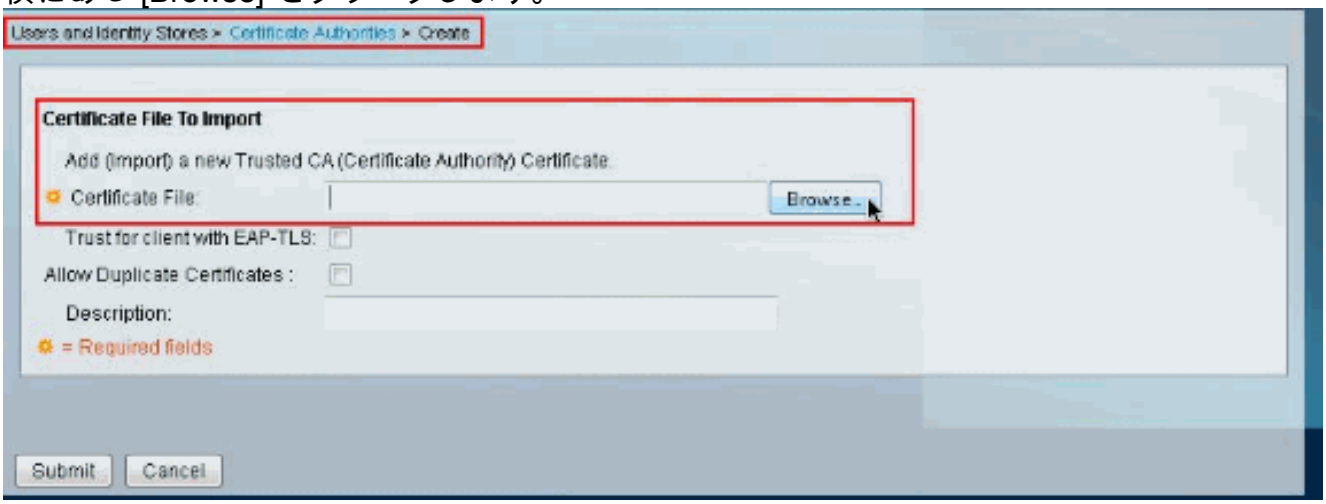
Cisco Secure ACS 5.x にルート CA 証明書をインストールするには、次の手順を実行します。

注: ポート TCP 636 で暗号化接続を容認するように LDAP サーバが事前設定されていることを確認してください。 Microsoft LDAP サーバの設定方法の詳細については、『サードパーティ認証局を使用して SSL で LDAP を有効にする方法』を参照してください。

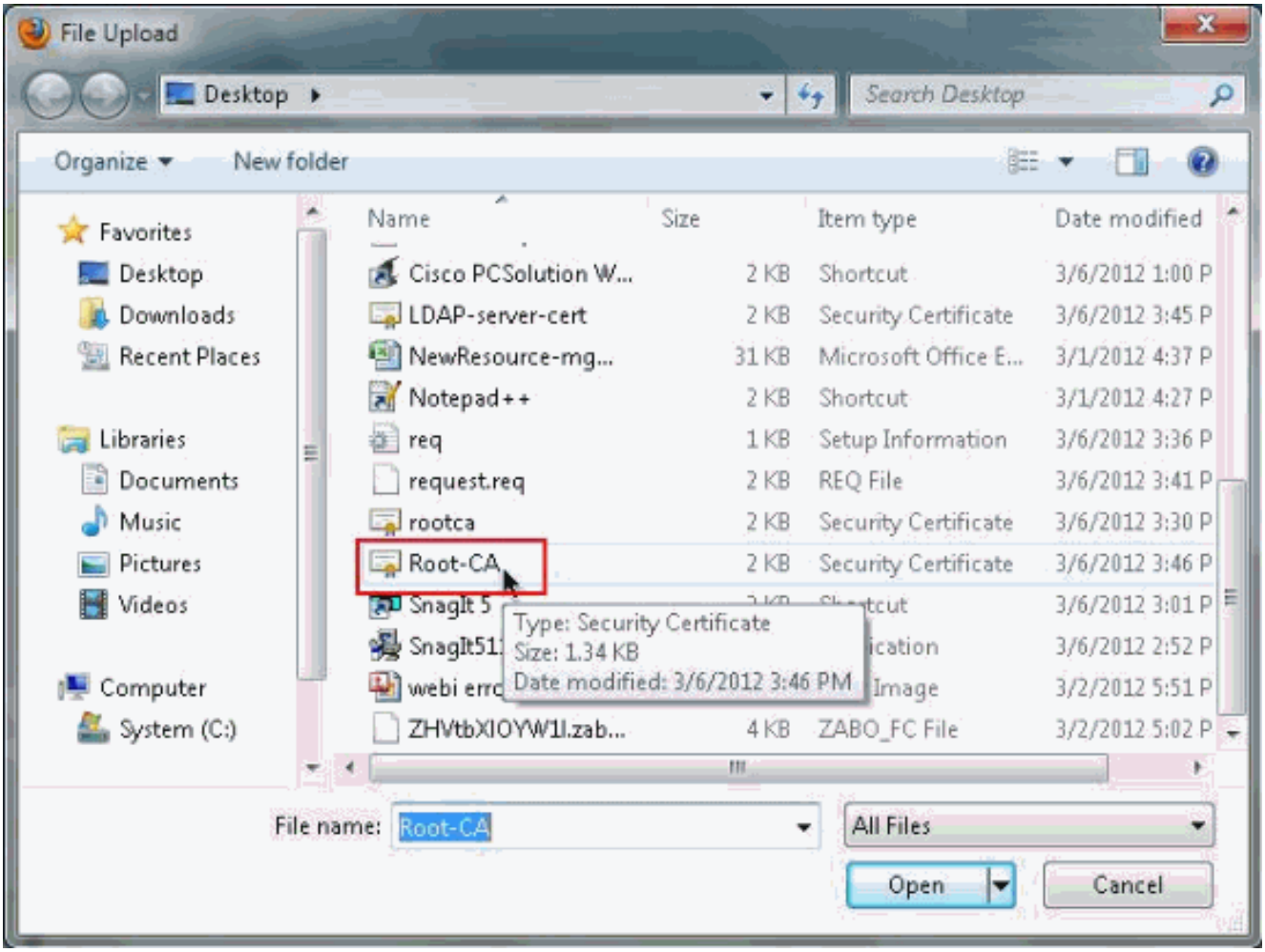
1. Microsoft LDAP サーバにサーバ証明書を発行した CA のルート証明書を追加するには、[Users and Identity Stores] > [Certificate Authorities] を選択し、[Add] をクリックします。



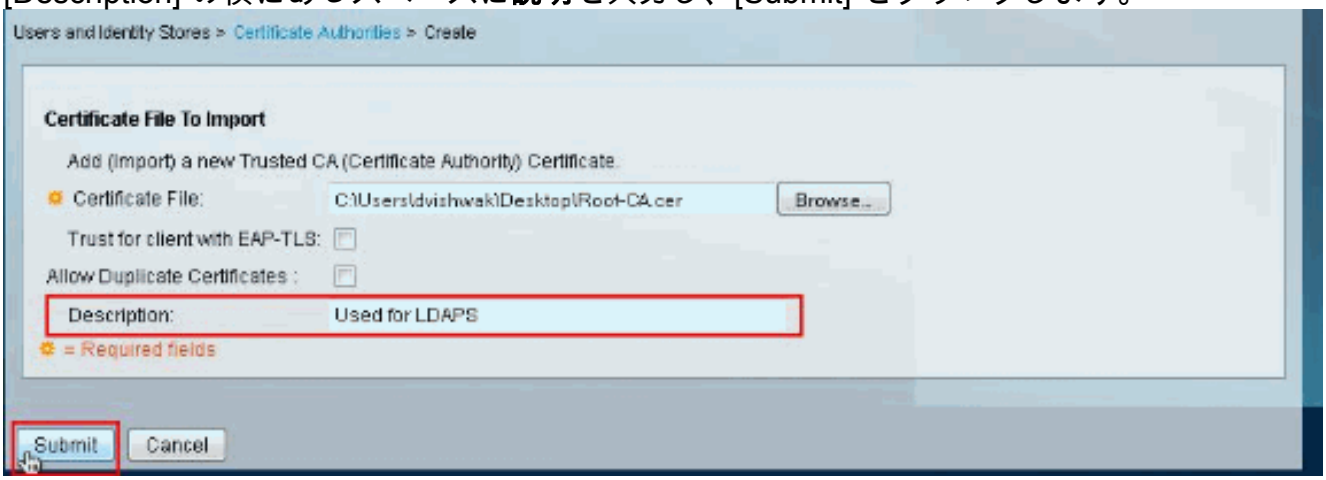
2. 証明書ファイルを検索するには、[Certificate File to Import] セクションで [Certificate File] の横にある [Browse] をクリックします。



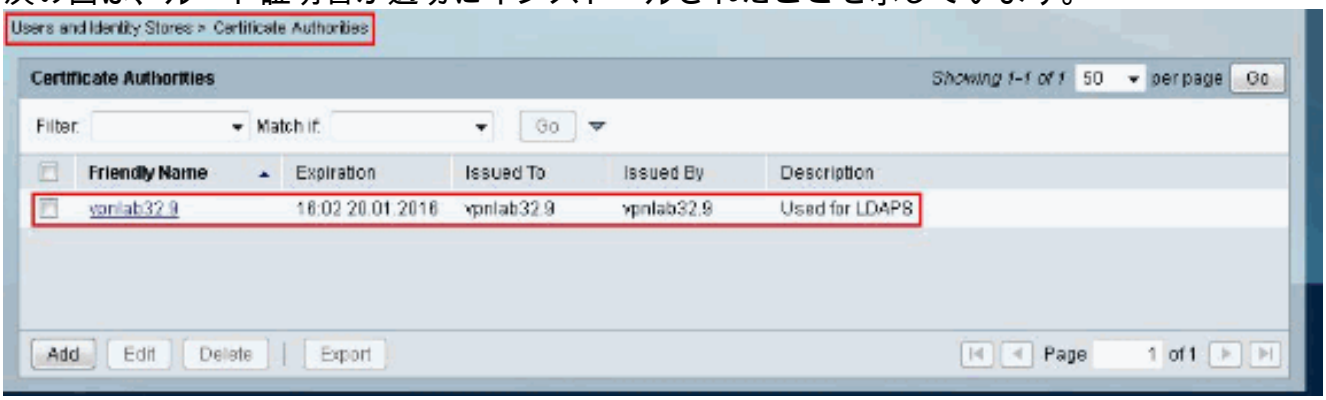
3. 必要な**証明書ファイル**（Microsoft LDAP サーバにサーバ証明書を発行した CA のルート証明書）を選択し、[Open] をクリックします。



4. [Description] の横にあるスペースに**説明**を入力し、[Submit] をクリックします。



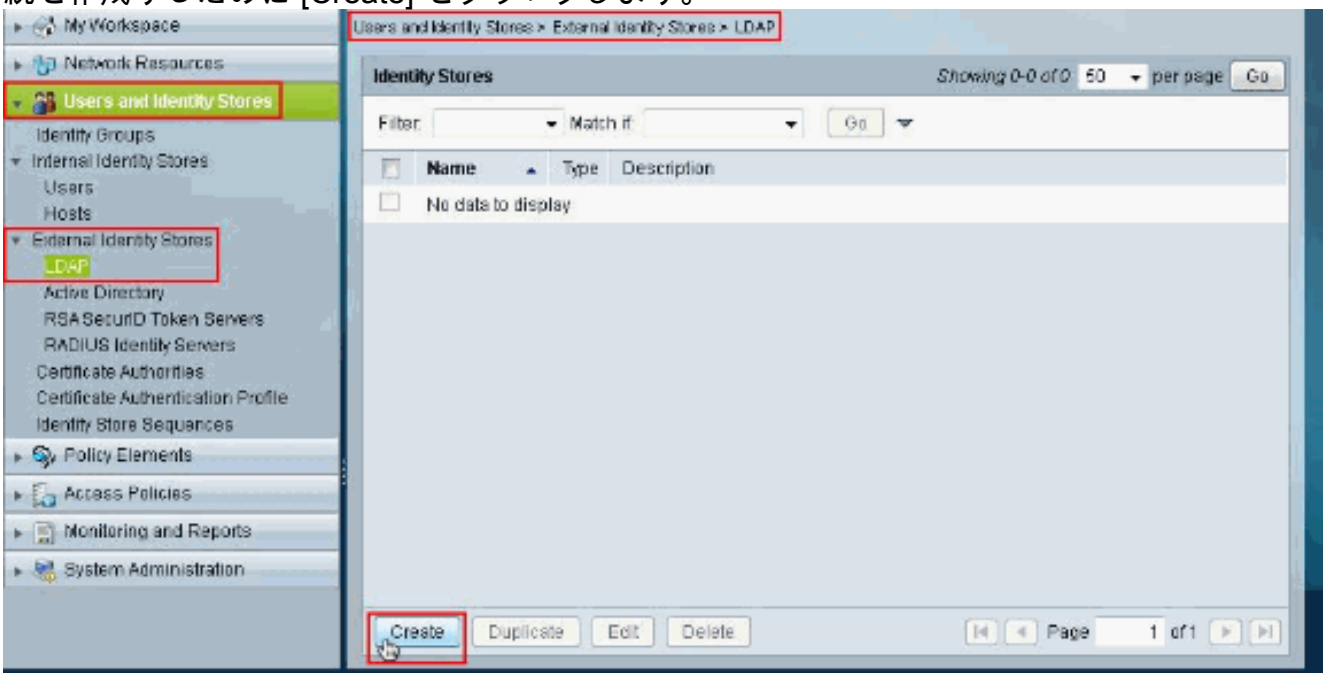
次の図は、ルート証明書が適切にインストールされたことを示しています。



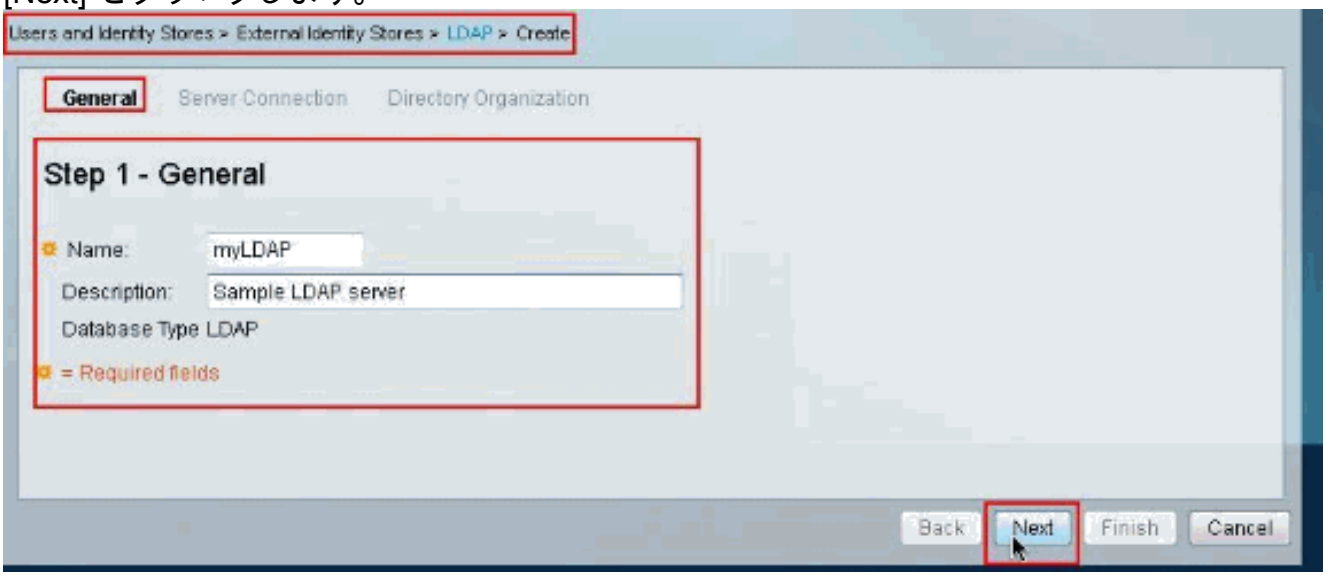
セキュア LDAP 用の ACS 5.X の設定

ACS 5.x をセキュア LDAP 用に設定するには、次の手順を実行します。

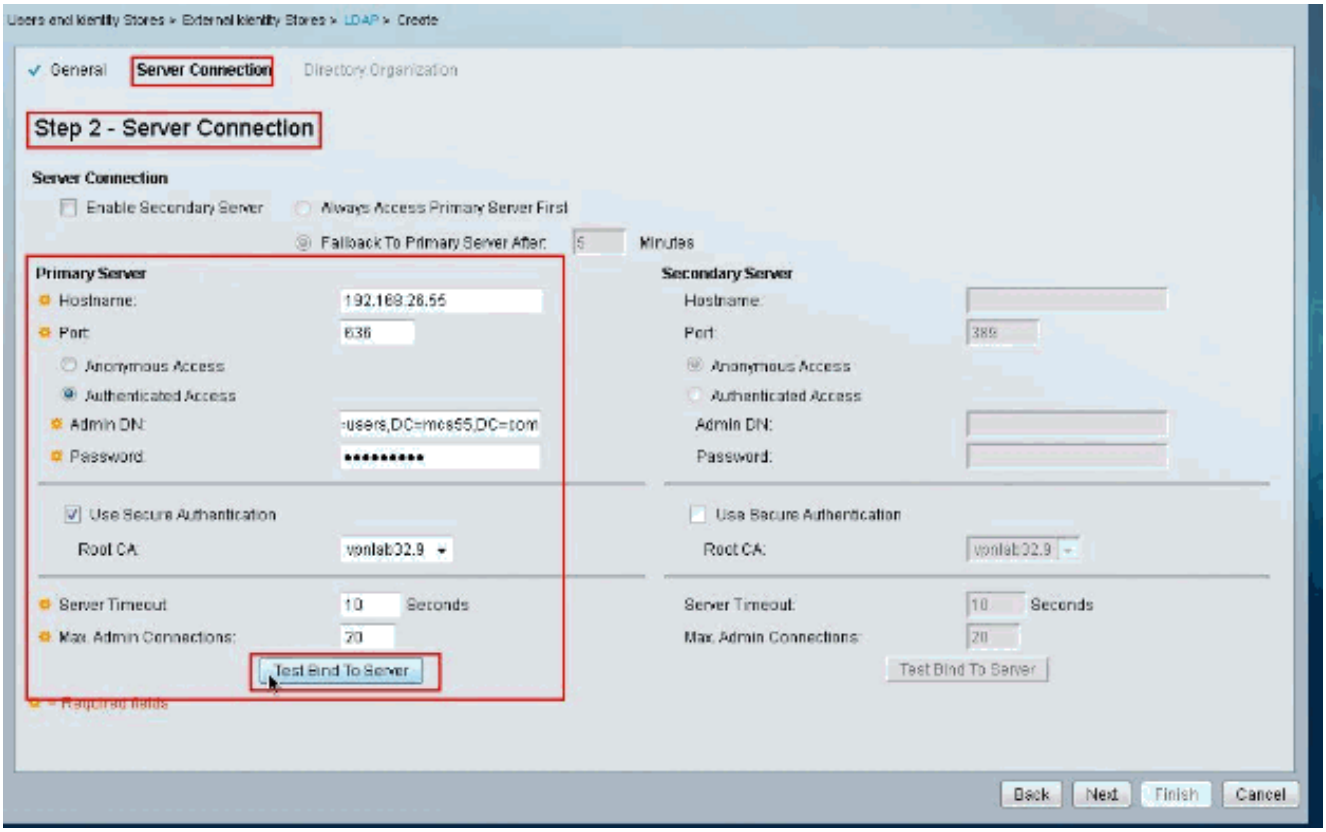
1. [Users and Identity Stores] > [External Identity Stores] > [LDAP] を選択し、新しい LDAP 接続を作成するために [Create] をクリックします。



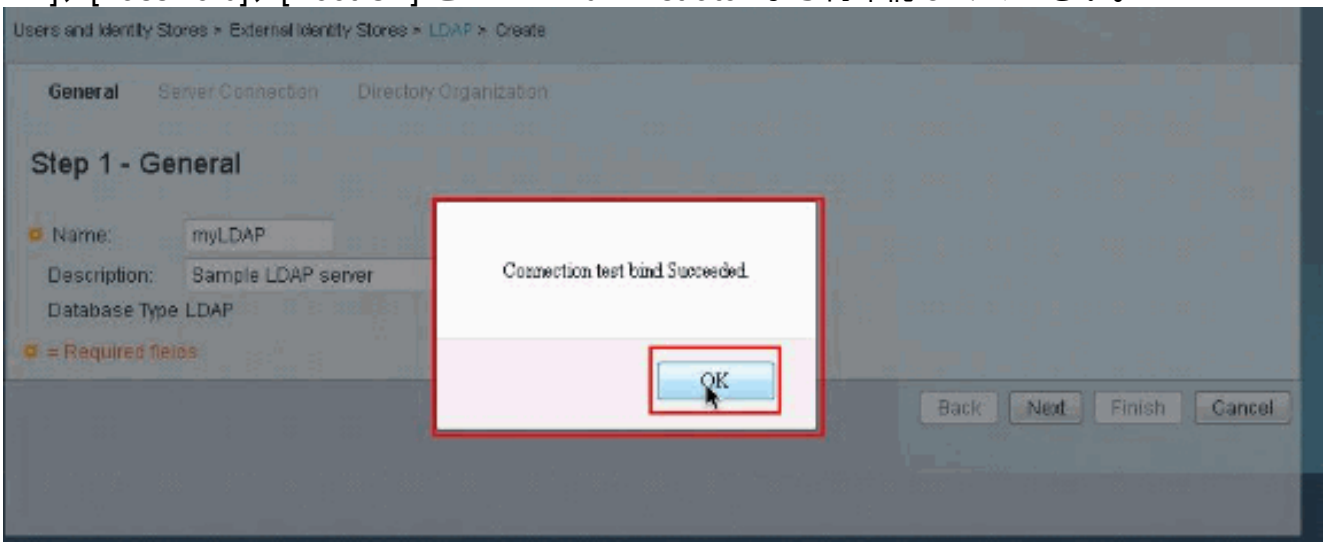
2. [General] タブで、新しい LDAP の [Name] および [Description]（オプション）を指定し、[Next] をクリックします。



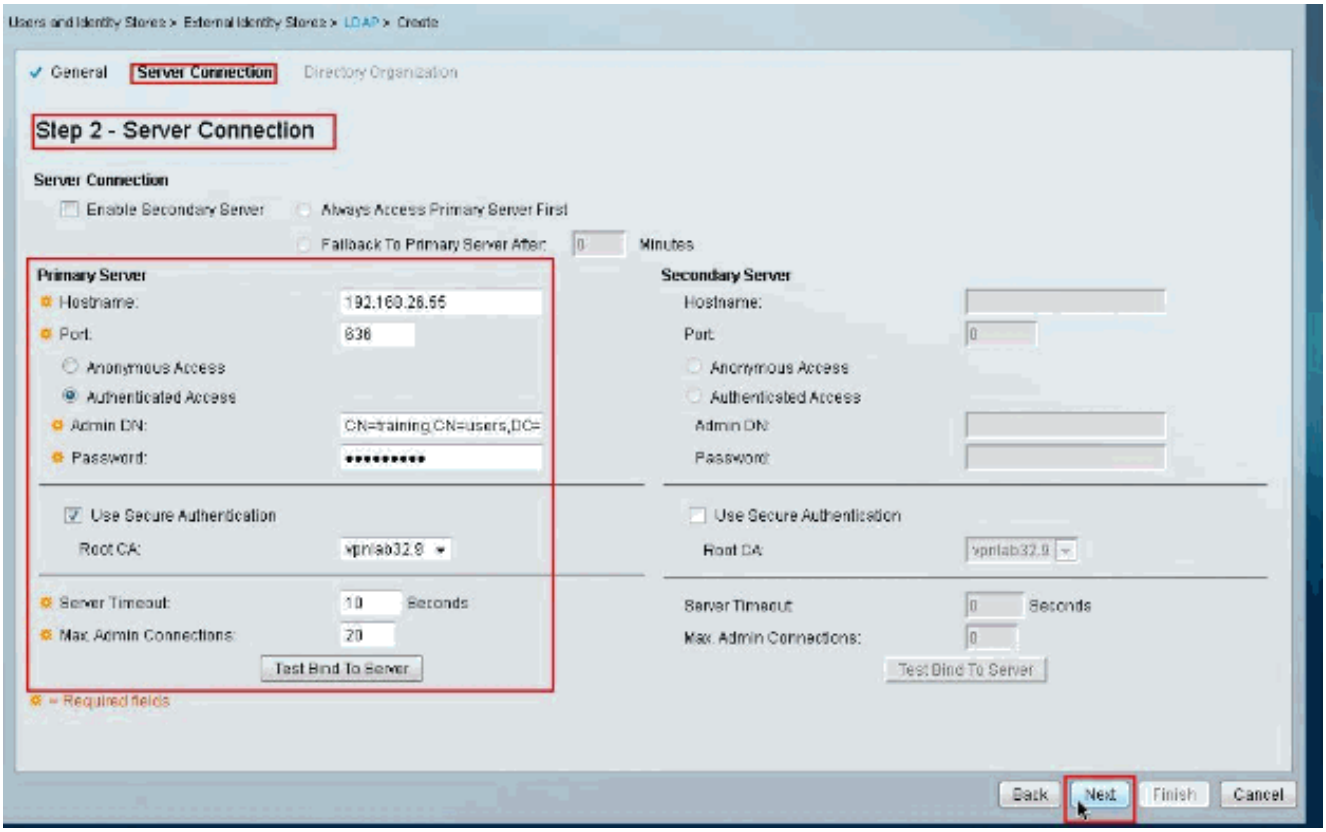
3. [Server Connection] タブの [Primary Server] セクションで、[Hostname]、[Port]、[Admin DN]、[Password] を指定します。 [Use Secure Authentication] チェックボックスがオンになっていることを確認し、最近インストールした**ルート CA 証明書**を選択します。 [Test Bind To Server] をクリックします。**注:** セキュア LDAP の IANA 割り当てポート番号は TCP 636 です。 ただし、LDAP サーバが使用しているポート番号を LDAP Admin から確認してください。**注:** [Admin DN] および [Password] は LDAP Admin によって提供されます。 [Admin DN] は、LDAP サーバのすべての OU に関するすべての権限を読み取る必要があります。



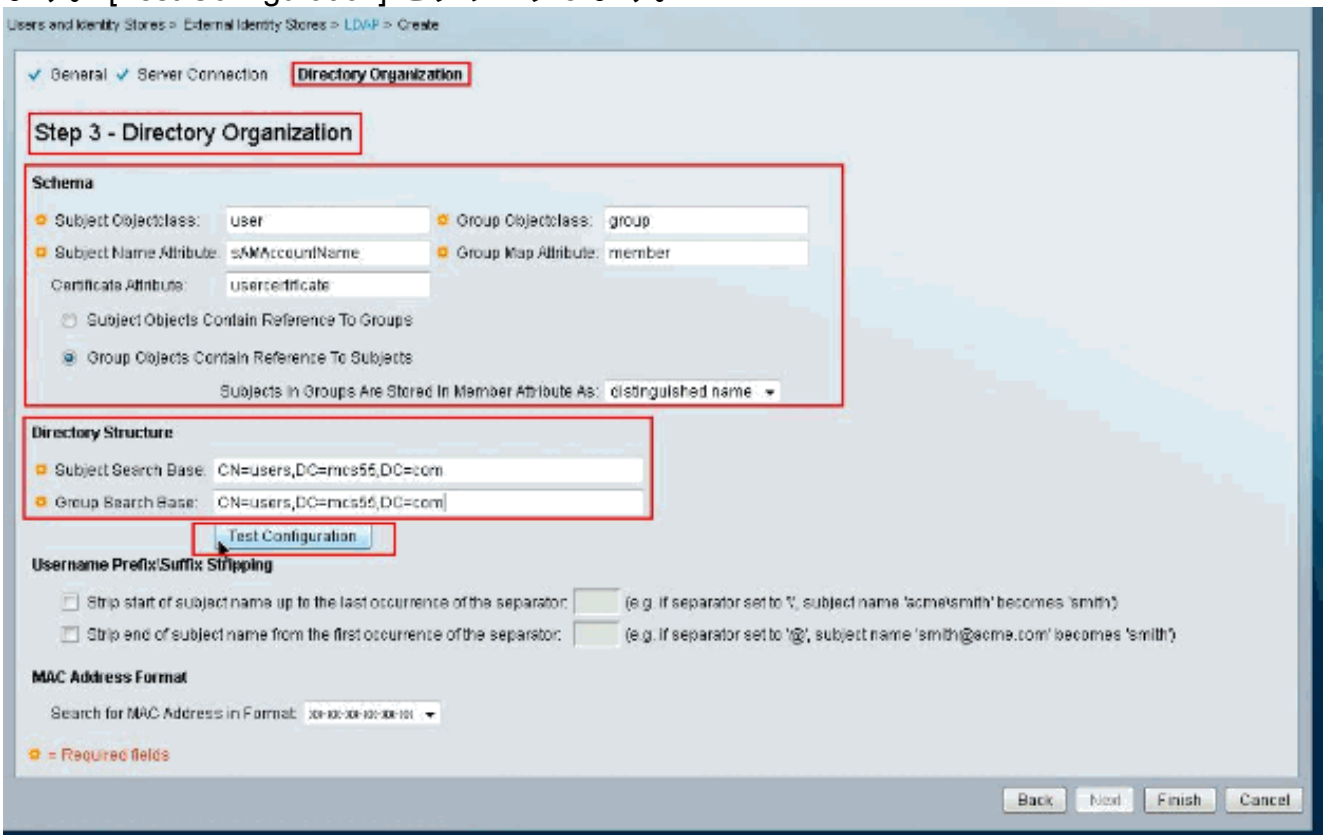
次の図は、**サーバへの接続テスト バインド**が正常に実行されたことを示しています。**注:** テスト バインドが正常に実行されなかった場合は、[Hostname]、[Port number]、[Admin DN]、[Password]、[Root CA] を LDAP Administrator から再確認してください。



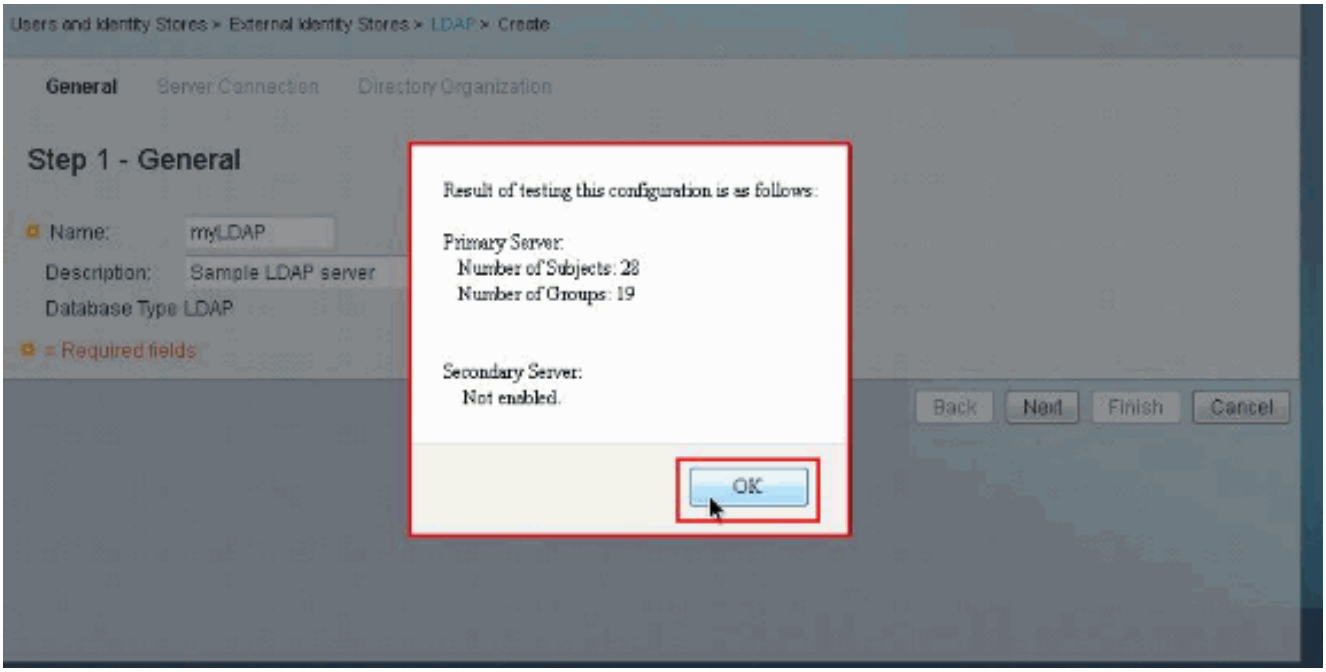
4. [Next] をクリックします。



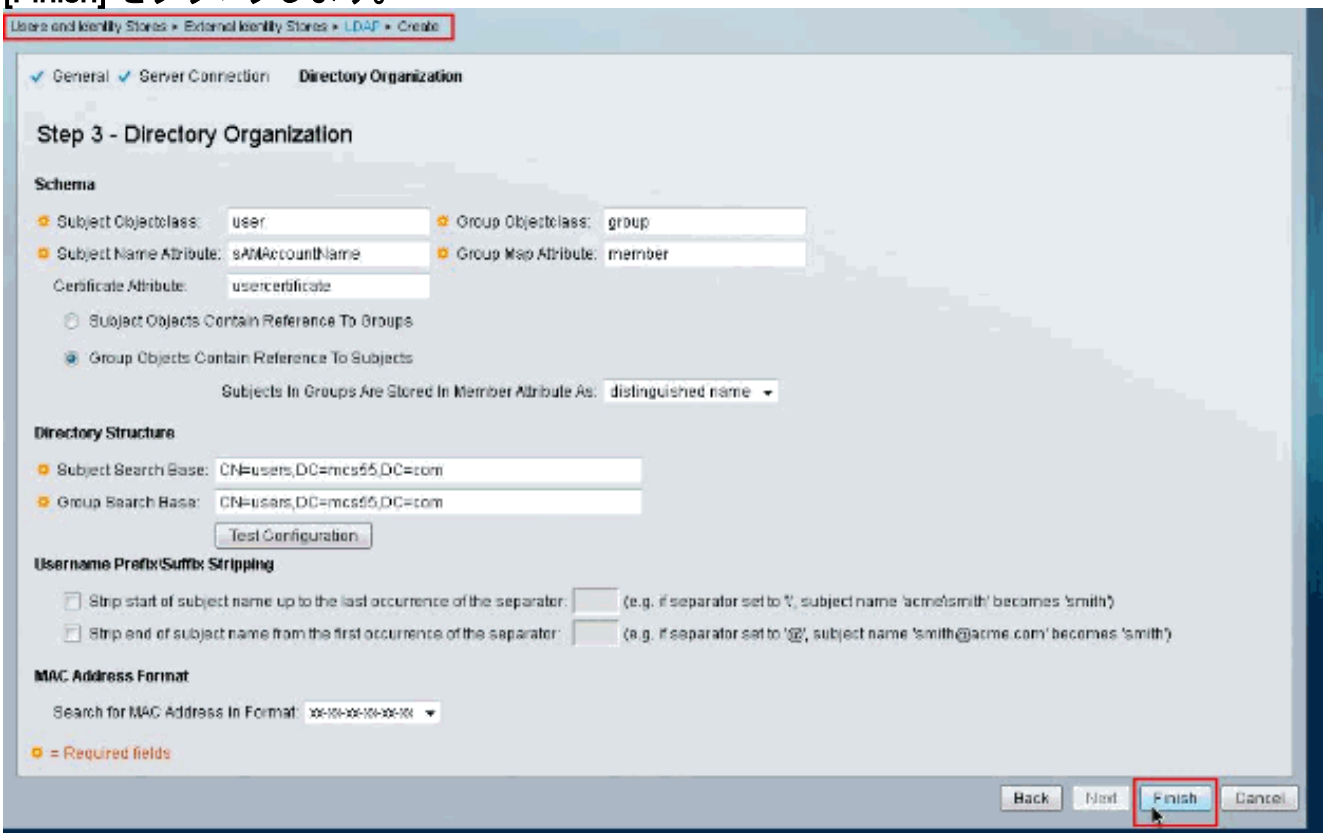
5. [Directory Organization] タブの [Schema] セクションで、必要な詳細を指定します。 LDAP Admin によって提供されるように、[Directory Structure] セクションで必要な情報を指定します。 [Test Configuration] をクリックします。



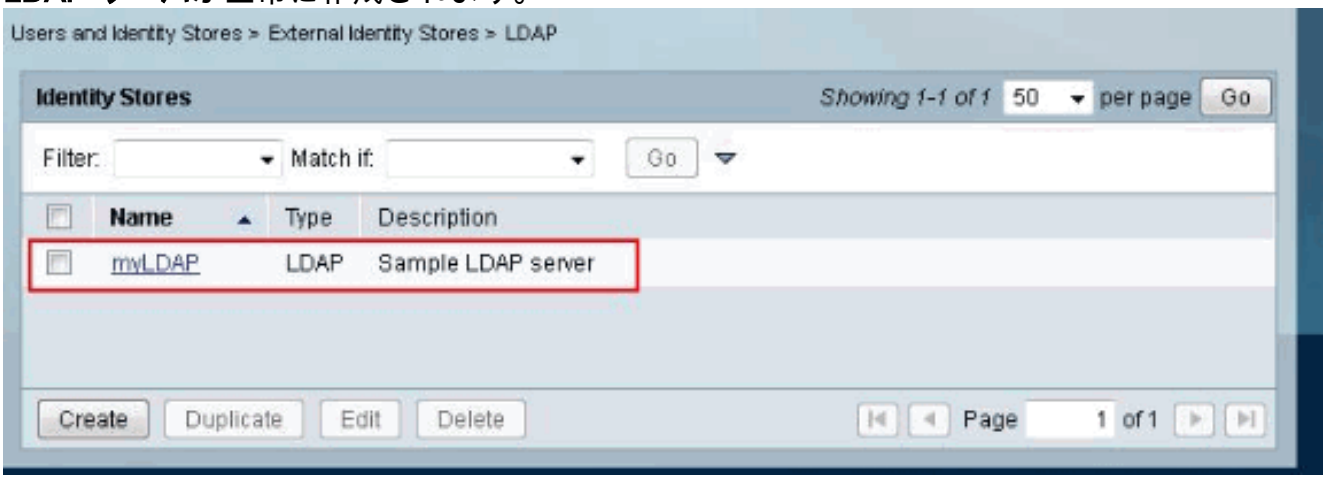
次の図は、**設定テスト**が正常に実行されたことを示しています。**注:** 設定テストが正常に実行されなかった場合は、[Schema] および [Directory Structure] で指定したパラメータを LDAP Administrator から再確認してください。



6. **[Finish] をクリックします。**



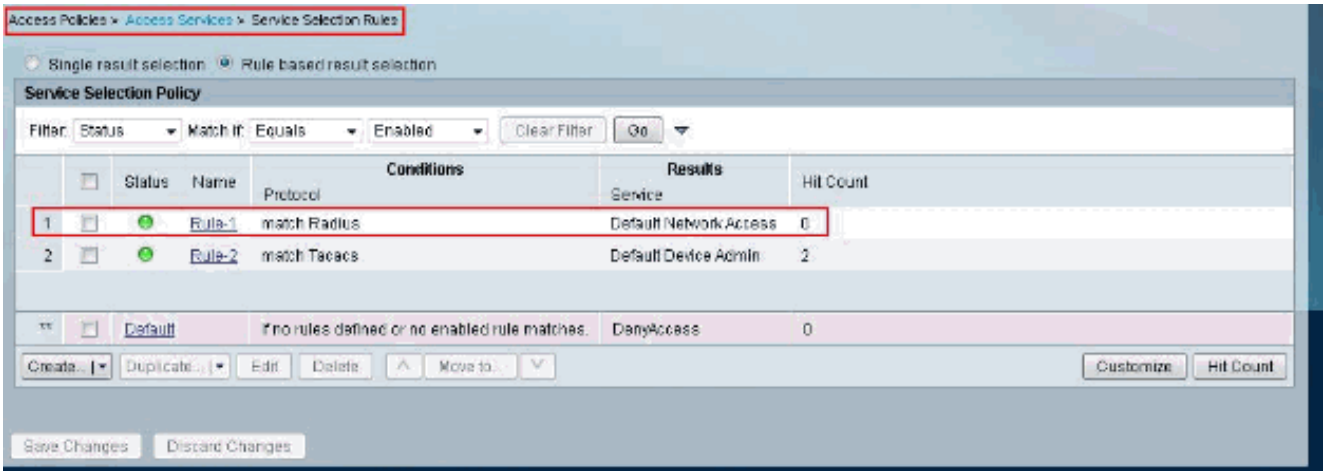
LDAP サーバが正常に作成されます。



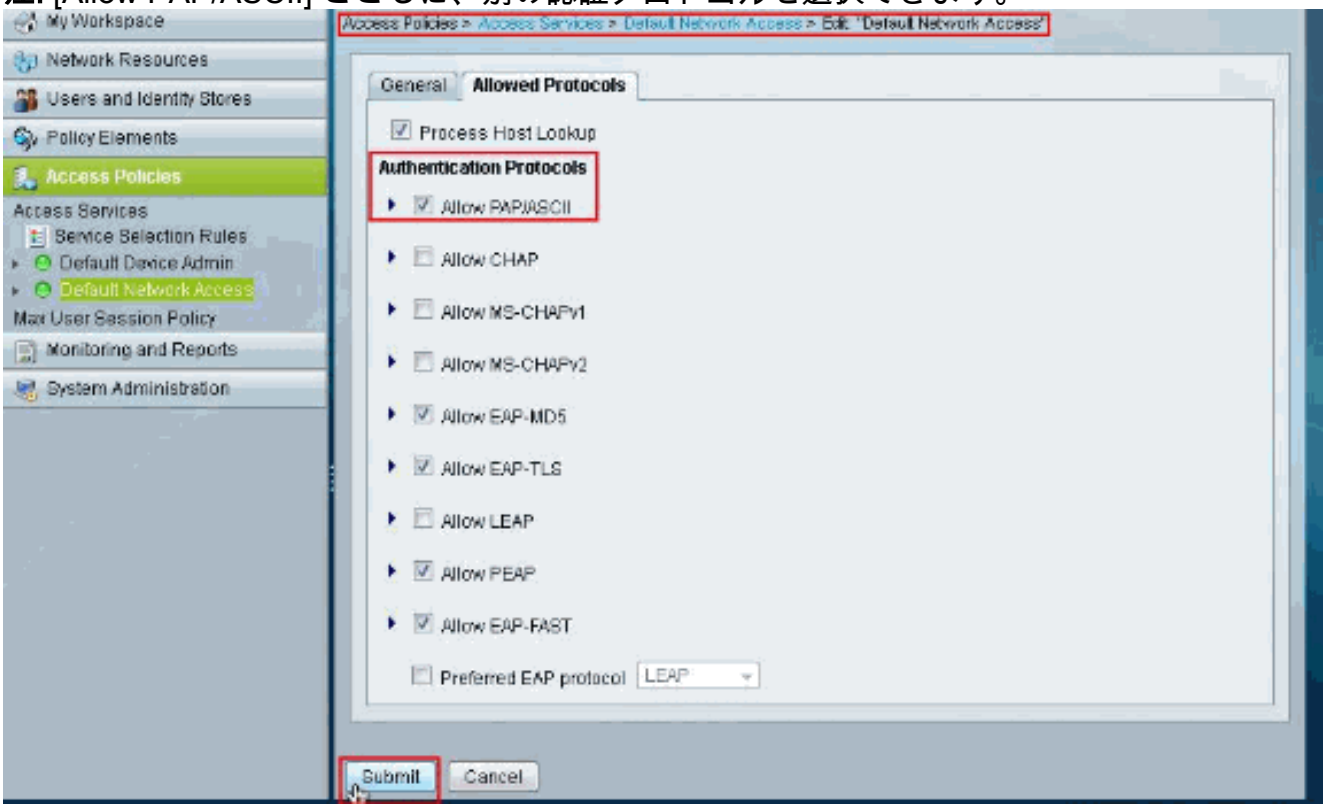
ID ストアの設定

ID ストアを設定するには、次の手順を実行します。

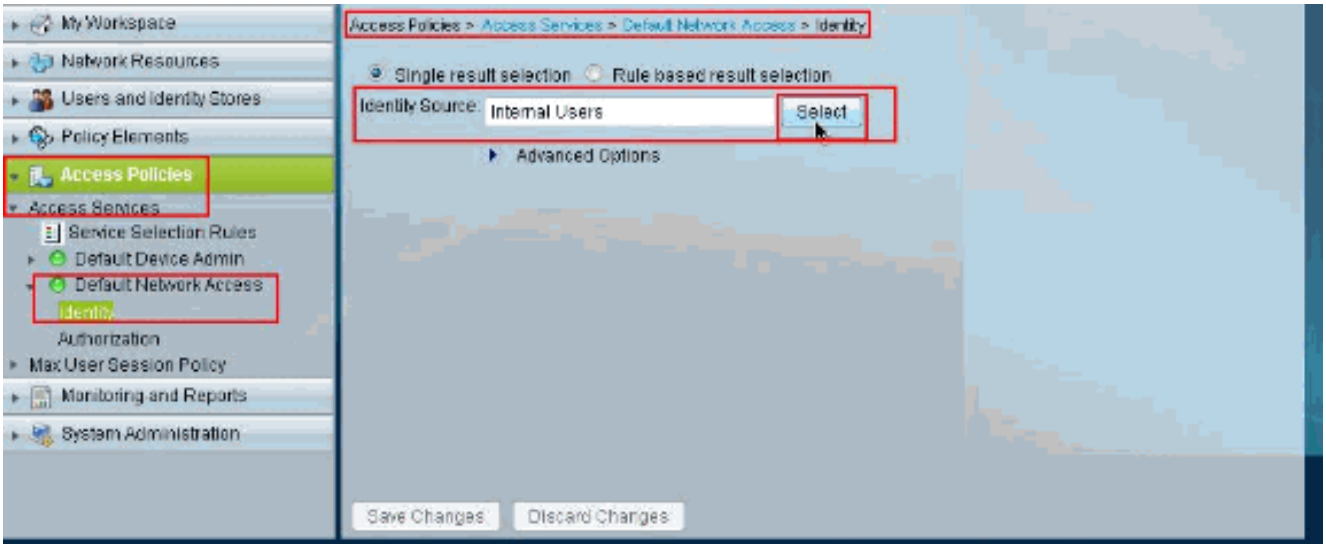
1. [Access Policies] > [Access Services] > [Service Selection Rules] を選択し、どのサーバが認証にセキュア LDAP サーバを使用するかを確認します。 この例のサービスは **Default Network Access** です。



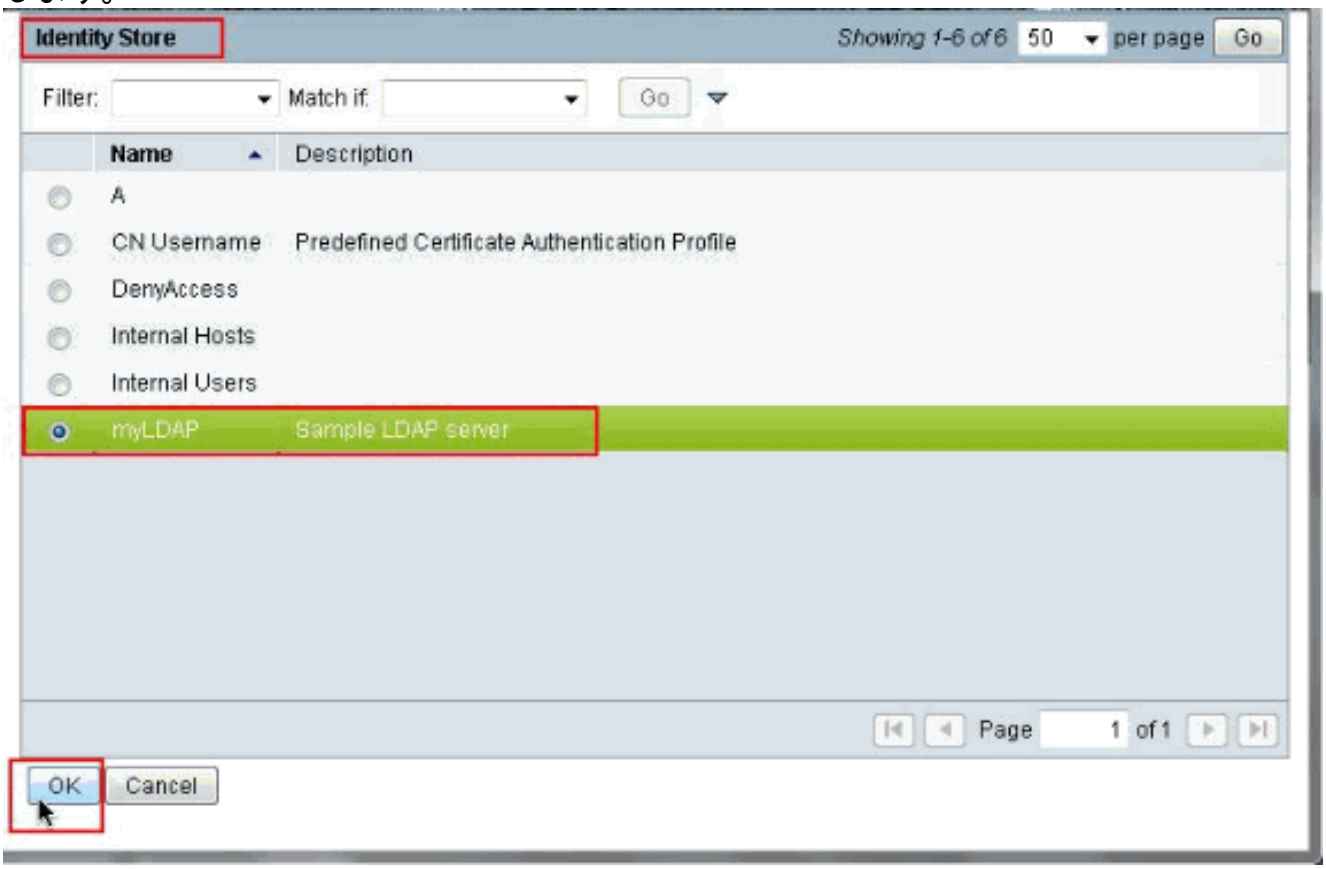
2. 手順 1 でサービスを確認したら、特定のサービスに移動し、[Allowed Protocols] をクリックします。 [Allow PAP/ASCII] が選択されていることを確認し、[Submit] をクリックします。
注: [Allow PAP/ASCII] とともに、別の認証プロトコルを選択できます。



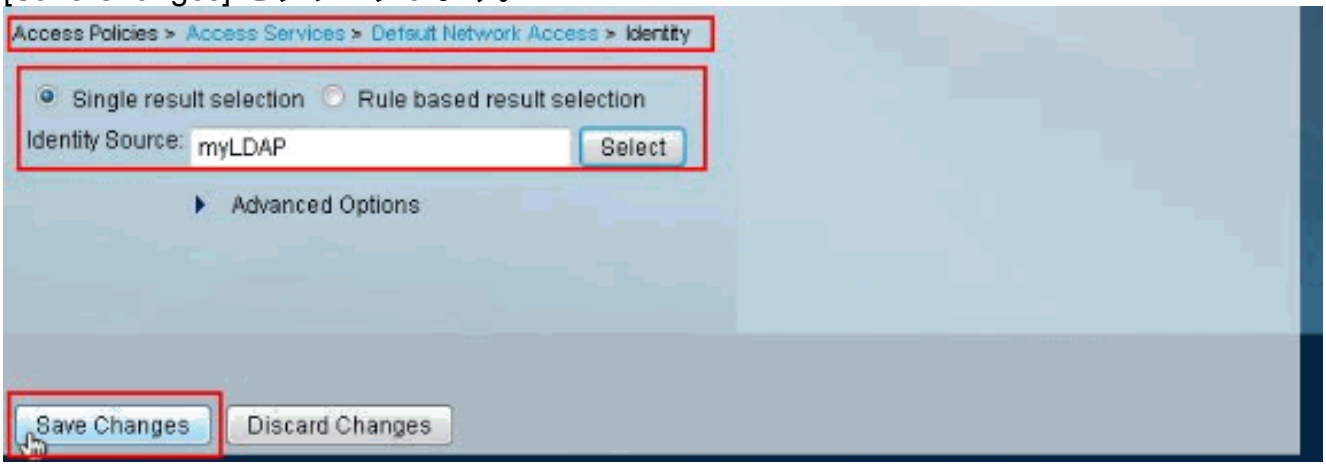
3. 手順 1 で確認したサービスをクリックし、[Identity] をクリックします。 [Identity Source] の横にある [Select] をクリックします。



4. 新しく作成した**セキュア LDAP サーバ**（この例では **myLDAP**）を選択し、[OK] をクリックします。

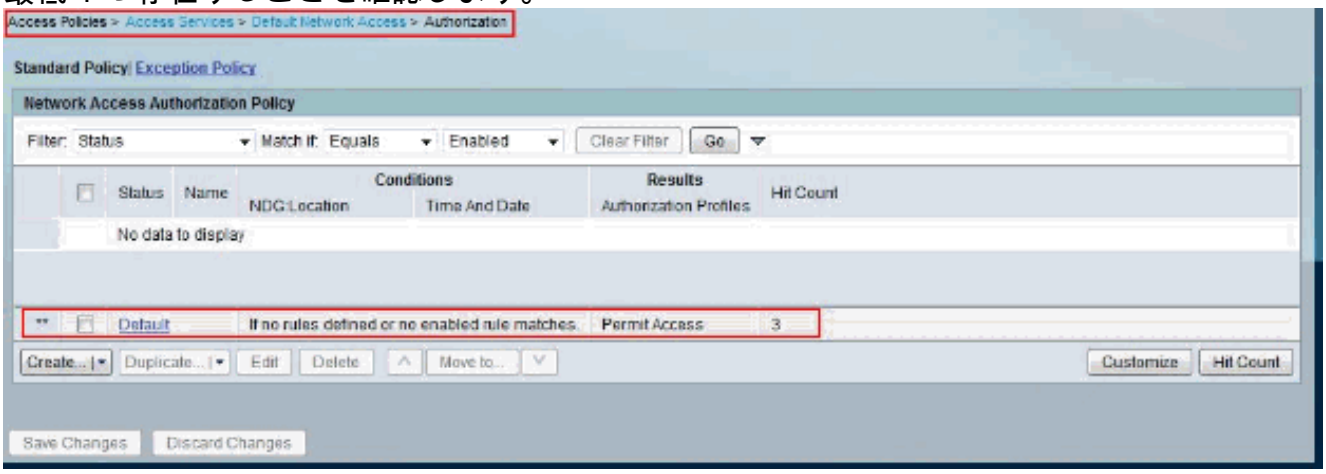


5. [Save Changes] をクリックします。



6. **手順 1** で確認したサービスの [Authorization] セクションに移動し、**認証**を許可するルールが

最低 1 つ存在することを確認します。



トラブルシューティング

ACS は、バインド要求を送信して、LDAP サーバに対してユーザを認証します。 バインド要求には、ユーザの DN およびユーザ パスワードがクリア テキストで含まれています。 ユーザの DN およびパスワードが LDAP ディレクトリ内のユーザ名およびパスワードと一致した場合に、ユーザは認証されます。

- **認証エラー**：ACS は認証エラーを ACS ログ ファイルに記録します。
- **初期化エラー**：LDAP サーバのタイムアウト設定を使用して、LDAP サーバでの接続または認証が失敗したと判断する前に ACS が LDAP サーバからの応答を待つ秒数を設定します。LDAP サーバが初期化エラーを返す理由で考えられるのは、次のとおりです。LDAP がサポートされていないサーバがダウンしているサーバがメモリ不足であるユーザに特権がない間違った管理者クレデンシャルが設定されている
- **バインド エラー**：LDAP サーバがバインド（認証）エラーを返す理由で考えられるのは、次のとおりです。フィルタリング エラーフィルタリング条件を使用した検索の失敗パラメータ エラー無効なパラメータの入力ユーザ アカウントが制限されている（無効、ロックアウト、期限切れ、パスワード期限切れなど）

外部リソース エラーとして次のエラーがロギングされ、LDAP サーバで考えられる問題が示されます。

- 接続エラーが発生した
- タイムアウトが期限切れになった
- サーバがダウンしている
- サーバがメモリ不足である

未知ユーザ エラーとして、エラー A user does not exist in the database が ロギングされます。

無効パスワード エラーとして、エラー An invalid password was entered が ロギングされます。ユーザは存在しますが、送信されたパスワードが無効です。

関連情報

- Cisco Secure Access Control System
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems