UCS Central 向け LDAP 認証の設定例

内容

概要

このドキュメントでは、Cisco Unified Computing System（UCS）Central 用の Lightweight Directory Access Protocol（LDAP）認証の設定例を示します。この設定手順では、UCS Central の GUI を使用し、ドメインを bglucs.com、ユーザ名を testuser としています。

LDAP は、UCS Central ソフトウェアのバージョン 1.0 がサポートする唯一のリモート認証プロトコルです。バージョン 1.0 では、UCS Central 自身に対するリモート認証と LDAP 設定へのサポートが、ごく限られたものになっています。それでも UCS Central を使用すれば、UCS Central が管理する UCS Manager ドメイン用のすべてのオプションを設定することが可能です。

UCS Central のリモート認証へのサポートは、以下の点で制限されています。

- RADIUS と TACACS がサポートされていない。
- 複数のドメイン コントローラに対してロールの割り当てと LDAP プロバイダー グループのマッピングを行う LDAP のグループ メンバシップがサポートされていない。
- ロールを割り当てる際、LDAP は CiscoAVPair の属性または未使用の属性しか使用できない

。割り当てるロールは、UCS Central のローカル データベースで事前に設定されたロールのうちの 1 つである。
- 複数の認証ドメインと認証プロトコルがサポートされていない。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- UCS が導入されている。
- Microsoft Active Directory が導入されている。

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いています。

- UCS Central バージョン 1.0
- Microsoft Active Directory

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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については、『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。

情報の収集

このセクションでは、設定を行う前に知っておくべき情報についてまとめています。

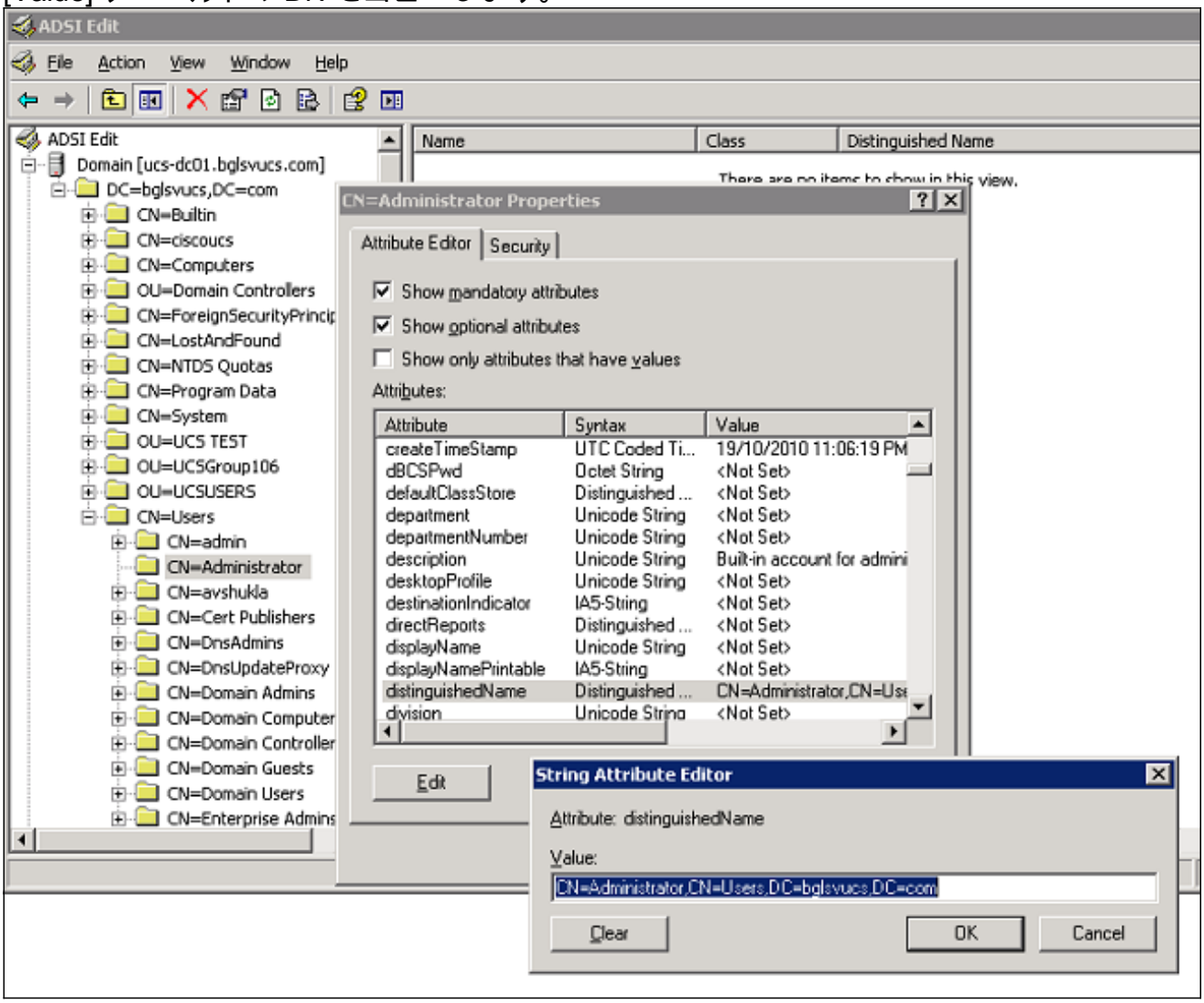
注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

バインド ユーザの詳細

バインド ユーザは、ドメインへの読み取りアクセス権を持つドメイン内のすべての LDAP ユーザに対して指定できます。LDAP 設定にはバインド ユーザが必要です。UCS Central はバインド ユーザのユーザ名とパスワードを使用して、ユーザ認証などの情報について Active Directory（AD）に接続してクエリを行うことができます。ここでは、バインド ユーザに管理者アカウントを使用しています。

この手順では、LDAP 管理者が Active Directory Service Interfaces（ADSI）エディタを使用して DN を検出する方法について説明します。

1. ADSI エディタを開きます。
2. バインド ユーザを検出します。ユーザのパスは、AD のパスと同じです。
3. ユーザを右クリックして [Properties] を選択します。
4. [Properties] ダイアログ ボックスで、[distinguishedName] をダブルクリックします。
5. [Value] フィールドの DN をコピーします。



6. [Cancel] をクリックし、すべてのウィンドウを閉じます。

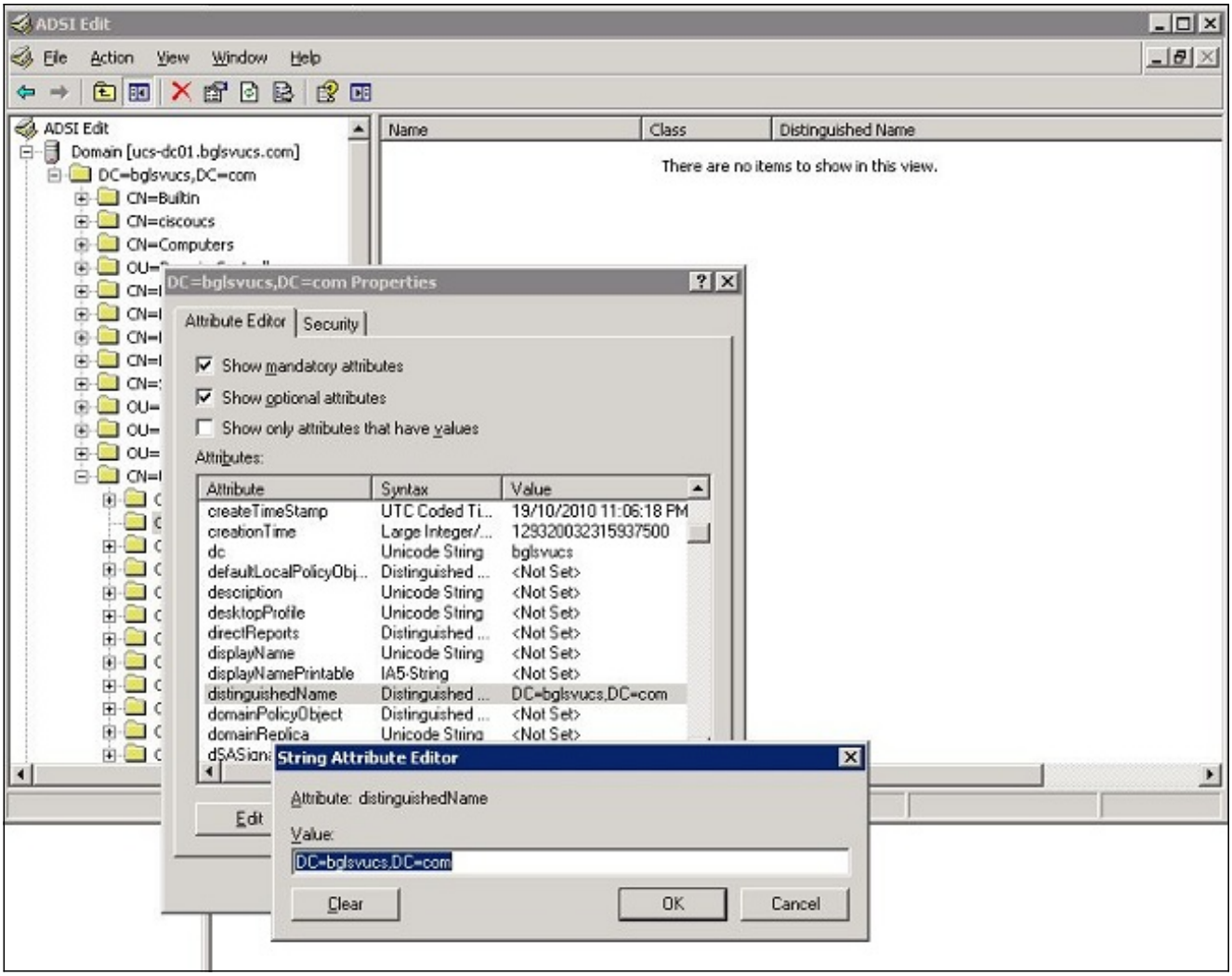
バインド ユーザのパスワードを取得する際は、AD 管理者に連絡してください。

ベース DN の詳細

ベース DN は、ユーザとユーザの詳細情報の検索が開始される Organizational Unit（OU）またはコンテナの DN です。UCS または UCS Central 用の AD に作成された OU の DN を使用できます。ただし、ドメイン ルートの DN を使用した方が簡単な場合もあります。

この手順では、LDAP 管理者が（ADSI）エディタを使用してベース DN を検出する方法について説明します。

1. ADSI エディタを開きます。
2. ベース DN として使用する OU またはコンテナを検出します。
3. OU またはコンテナを右クリックして [Properties] を選択します。
4. [Properties] ダイアログ ボックスで、[distinguishedName] をダブルクリックします。
5. [Value] フィールドの DN をコピーし、他の必要な詳細情報を記録します。



6. [Cancel] をクリックし、すべてのウィンドウを閉じます。

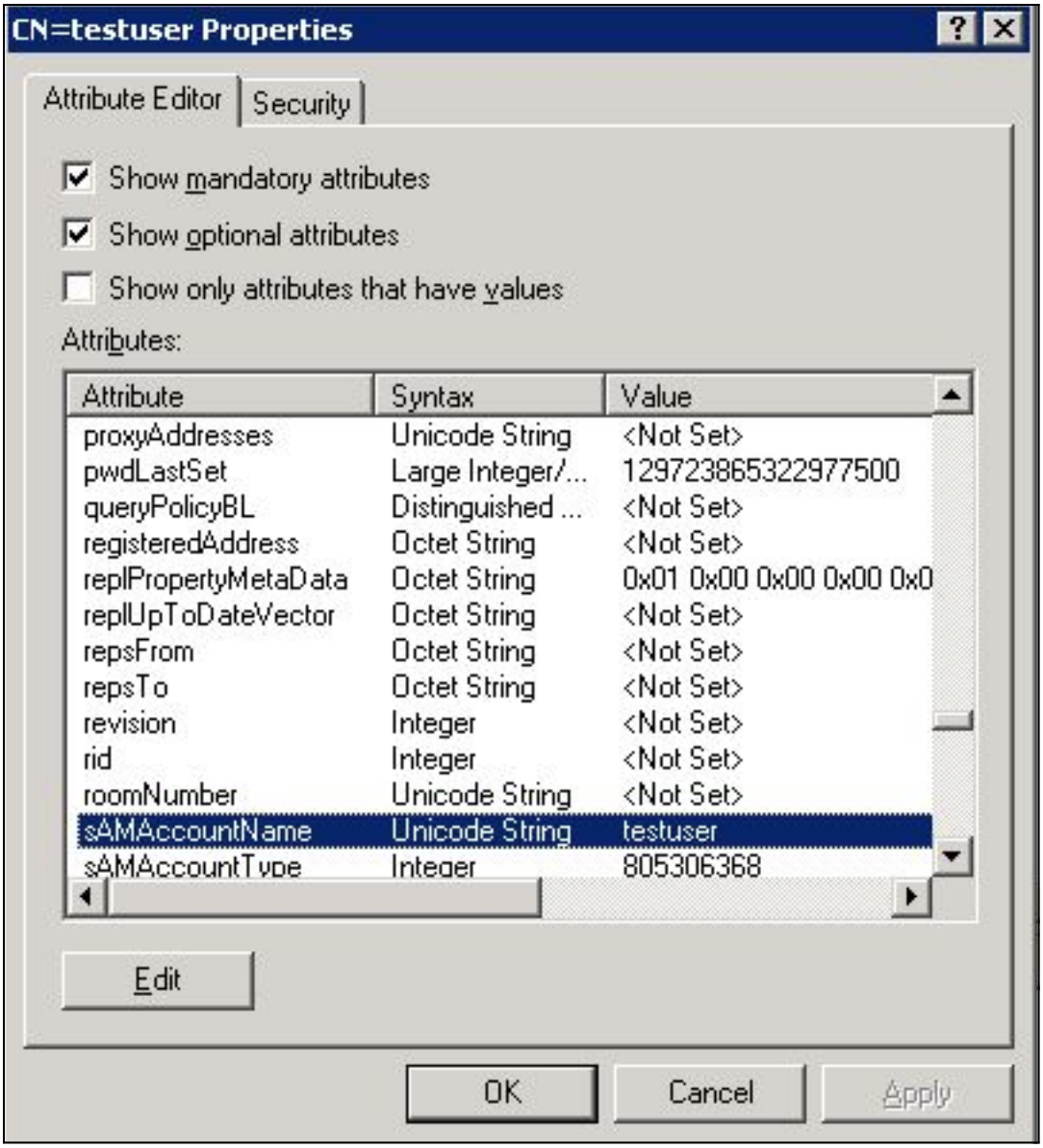
プロバイダーの詳細

プロバイダーの情報は、LDAP 認証や UCS Central での認証を行う際に非常に重要です。プロバイダーは、ユーザの検索や認証を行ったり、ロール情報などのユーザの詳細情報を取得したりするために UCS Central がクエリを行う AD サーバの 1 つです。プロバイダー AD サーバのホスト名や IP アドレスを確実に取得してください。

フィルタのプロパティ

フィルタのフィールドやプロパティは、AD データベースの検索を行う際に使用します。ログイン時に入力されたユーザ ID は AD に返され、フィルタ値と照合されます。

フィルタ値には、sAMAccountName=$userid を使用します。sAMAccountName は AD の属性で、UCS Central GUI へのログイン時に使用する AD のユーザ ID と同じ値になります。



属性の追加と設定

このセクションでは、CiscoAVPair 属性の追加（必要な場合）や更新、または LDAP 設定を行う前の事前設定された属性を更新する際に必要な情報についてまとめています。

属性フィールドでは、ユーザ プロパティ配下にある、ユーザに割り当てるロールを返す AD 属性を指定します。UCS Central ソフトウェアのリリース 1.0a では、カスタムの CiscoAVPair 属性か、AD の未使用属性を統合して、当該ロールを割り当てることができます。

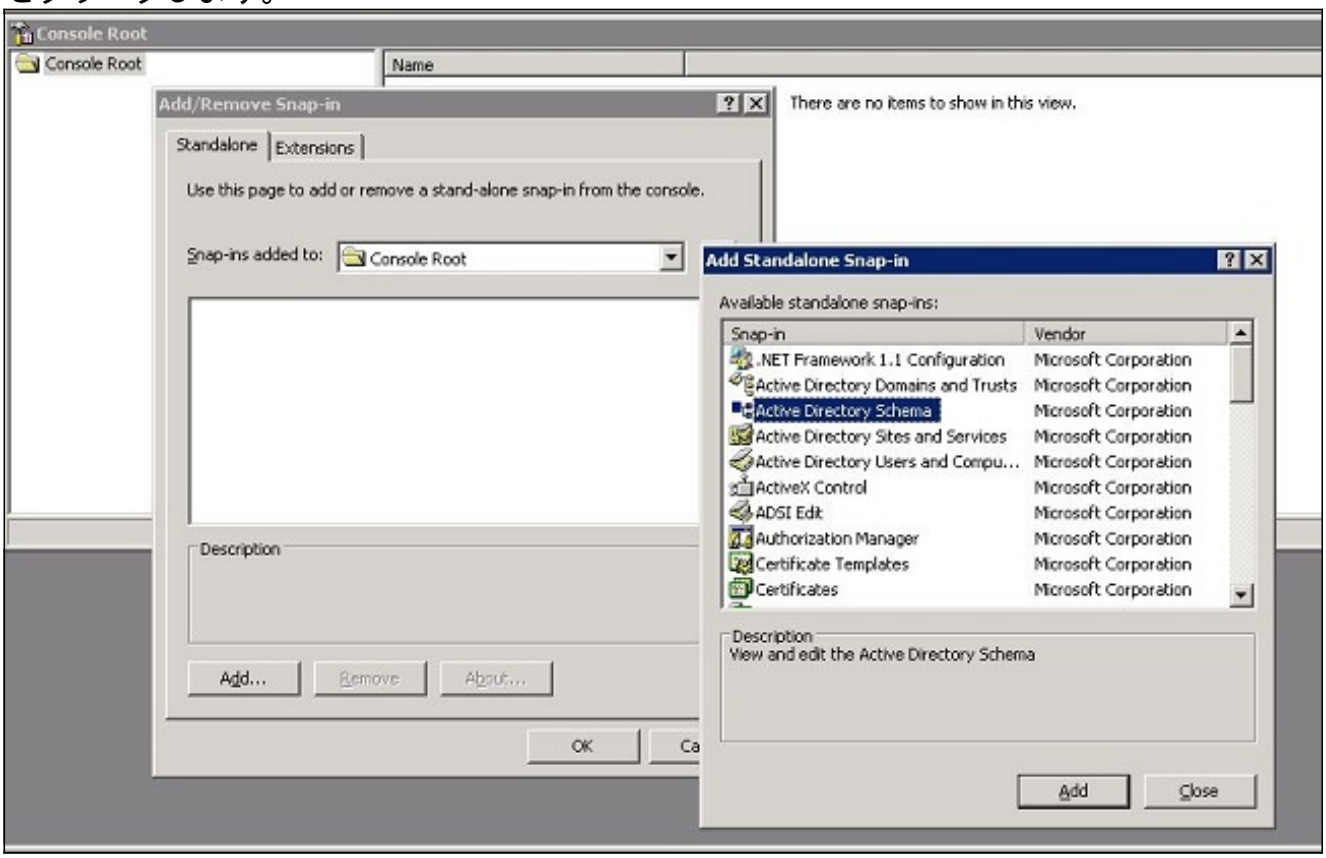
注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

CiscoAVPair 属性の追加

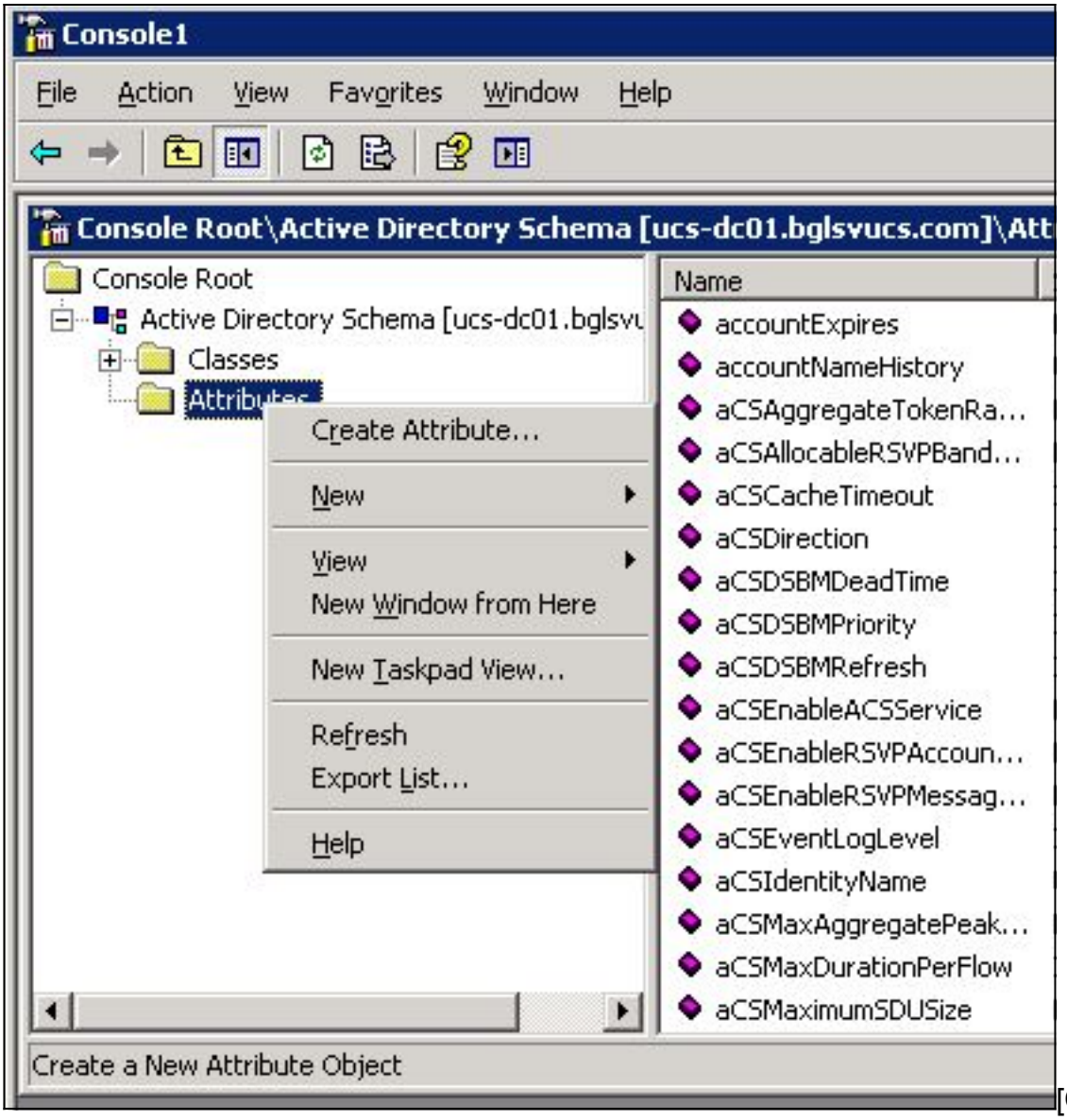
ドメインに新規の属性を追加する場合は、ドメインのスキーマを展開して、属性をクラス（ここではユーザ）に追加します。

この手順では、Windows AD サーバのスキーマを展開し、CiscoAVPair 属性を追加する方法について説明します。

1. AD サーバにログインします。
2. [Start] > [Run] をクリックして **mmc** と入力し、**Enter** キーを押して空の Microsoft Management Console（MMC）を開きます。
3. MMC で、[File] > [Add/Remove Snap-in] > [Add] の順でクリックします。
4. [Add Standalone Snap-in] ダイアログボックスで [Active Directory Schema] を選択し、[Add] をクリックします。

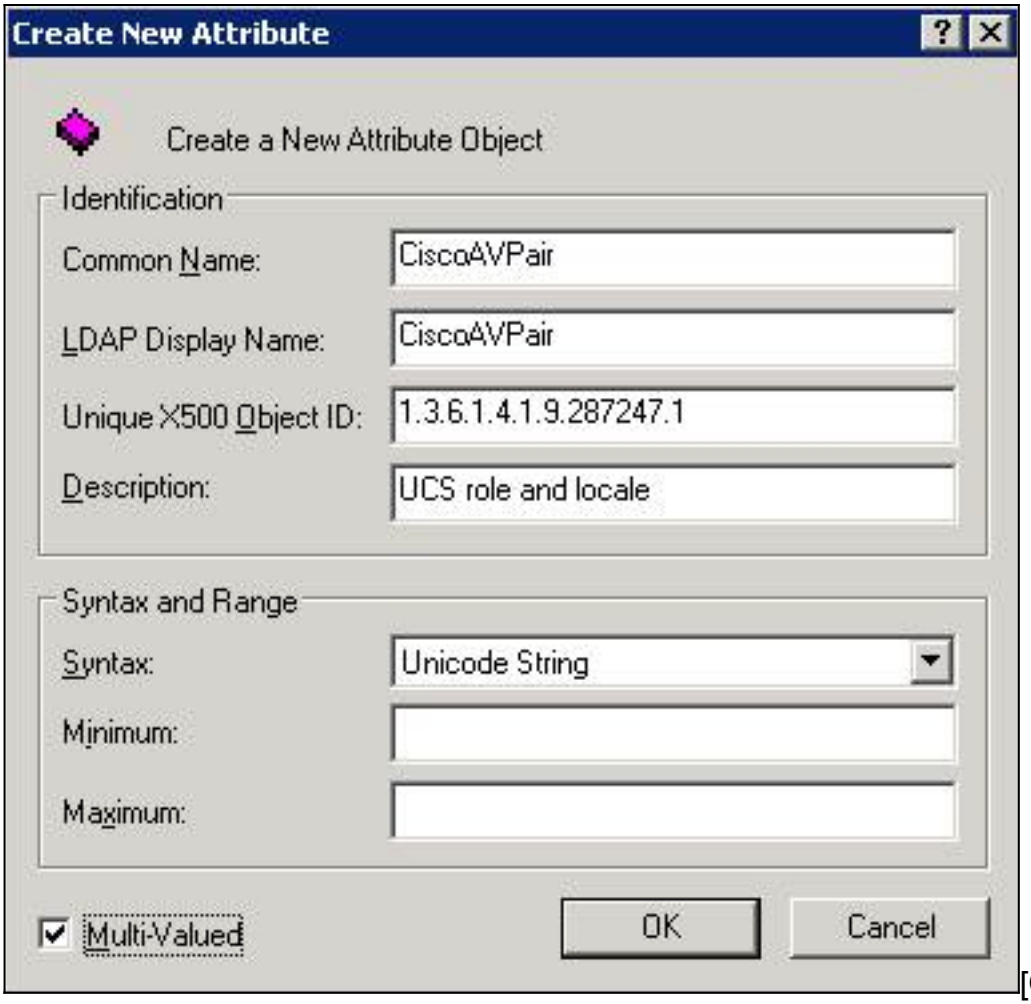


5. MMC で [Active Directory Schema] を展開し、[Attributes] を右クリックして [Create Attribute] を選択します。



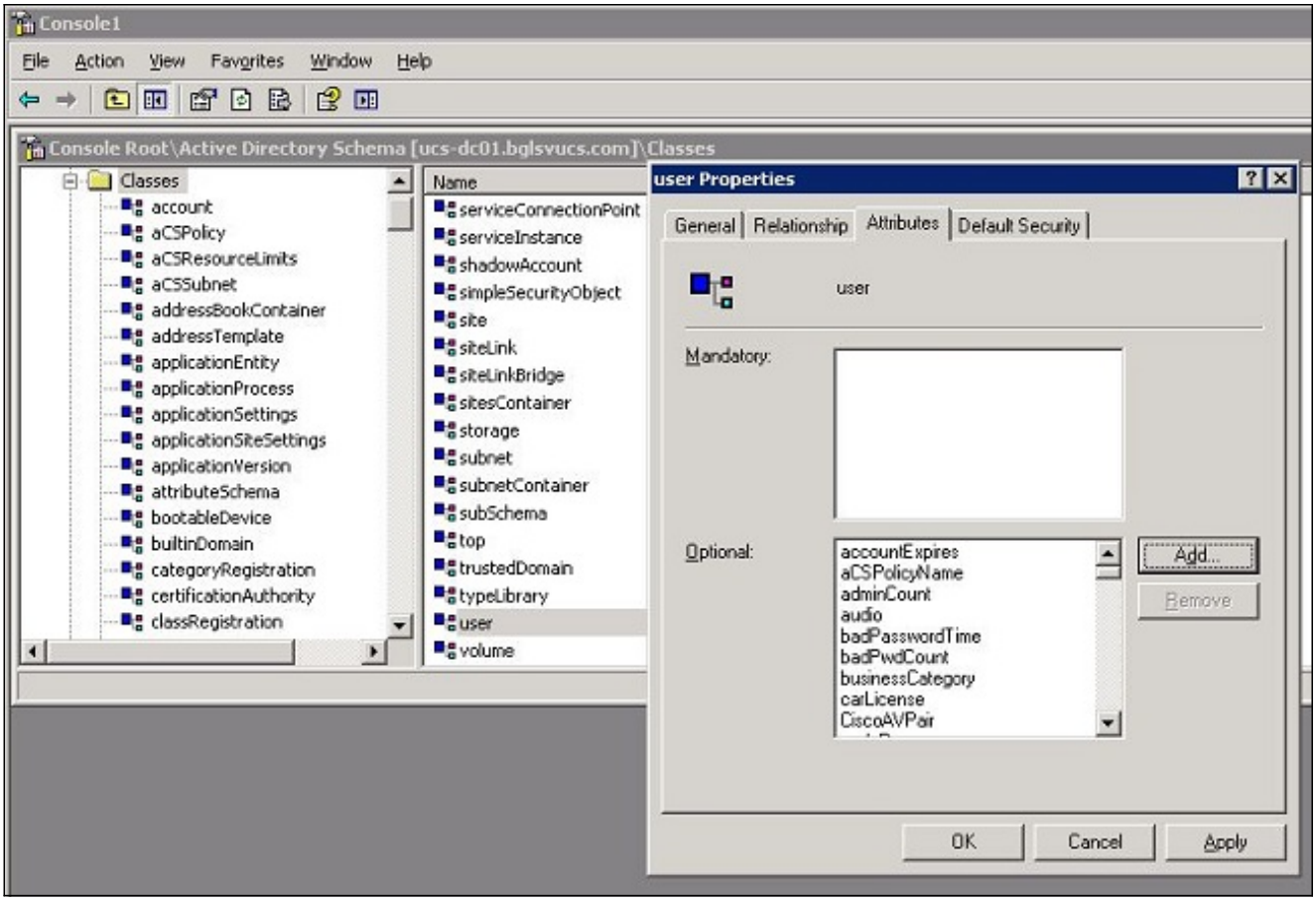
[Create New Attribute] ダイアログボックスが表示されます。

6. リモート認証サービスで、CiscoAVPair という属性を作成します。[Common Name] フィールドと [LDAP Display Name] フィールドで、**CiscoAVPair** と入力します。[Unique 500 Object ID] フィールドで、**1.3.6.1.4.1.9.287247.1** と入力します。[Description] フィールドで、**UCS role and locale** と入力します。[Syntax] フィールドで、ドロップダウン リストから [Unicode String] を選択します。

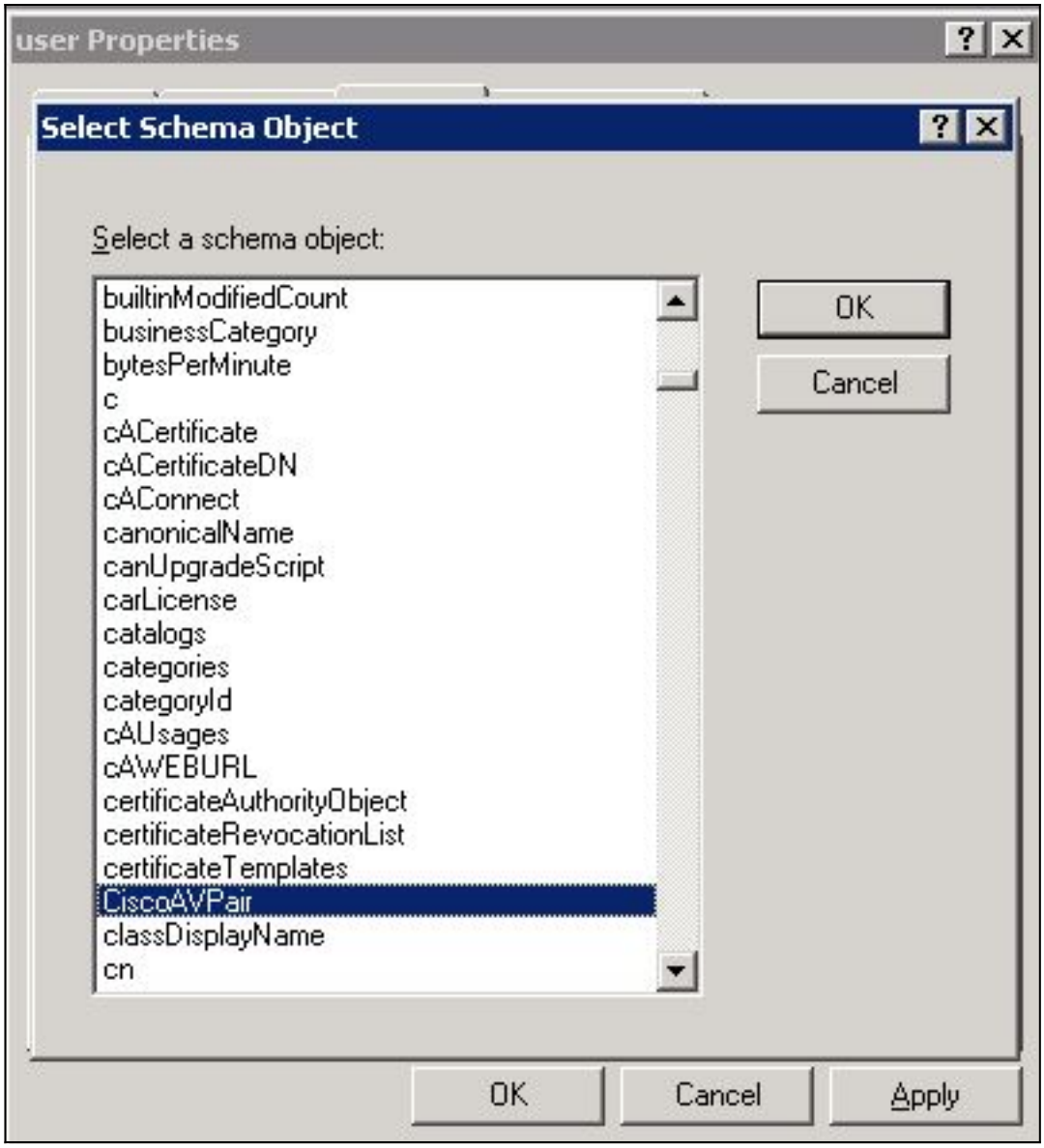


[OK] をクリックし、属性を保存してダイアログボックスを閉じます。属性がスキーマに追加されたら、この属性の対応付けを行うか、この属性をユーザ クラスに追加する必要があります。こうすることで、ユーザ プロパティを編集し、割り当てるロールの値を指定できるようになります。

7. AD スキーマの展開に使用された MMC で [Classes] を展開し、**ユーザ**を右クリックして [Properties] を選択します。
8. [user Properties] ダイアログボックスで [Attributes] タブをクリックし、[Add] をクリックします。

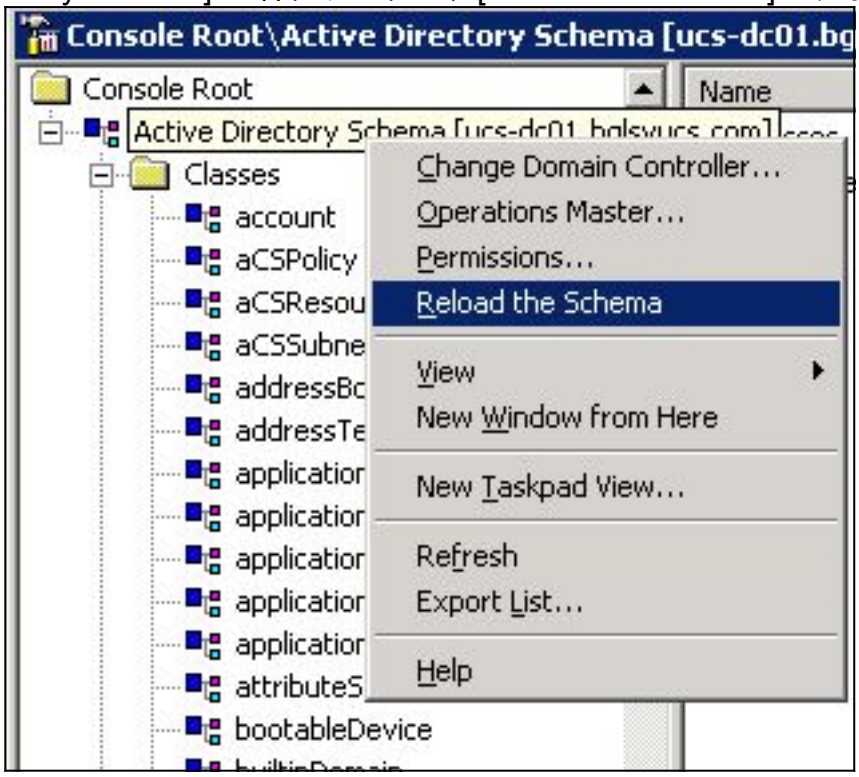


9. [Select Schema Object] ダイアログボックスで [CiscoAVPair] > [OK] の順にクリックします



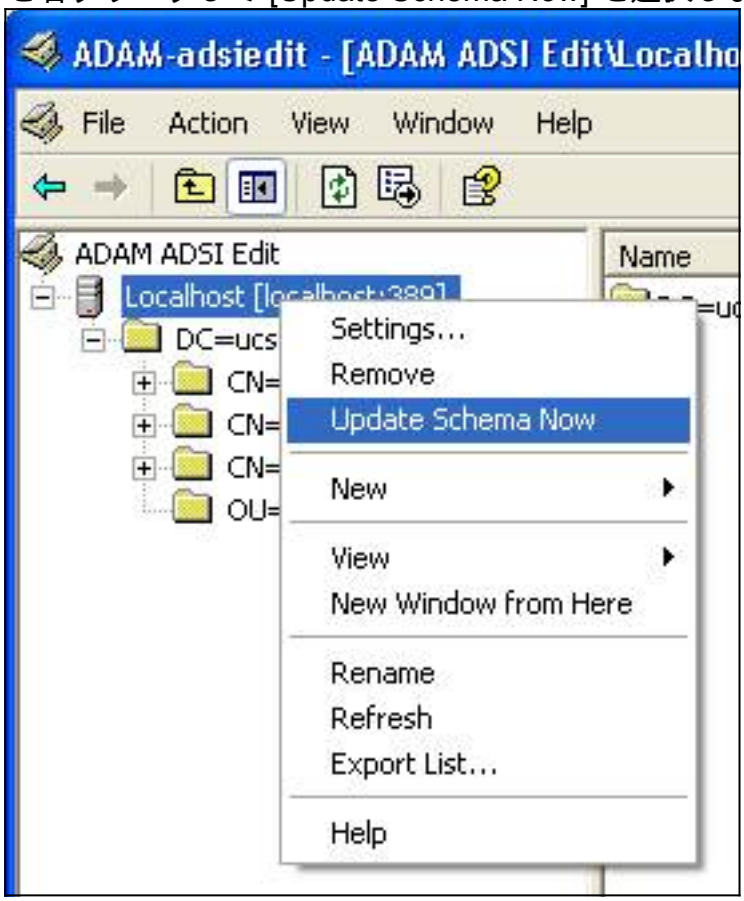
。

10. [user Properties] ダイアログボックスで [Apply] をクリックします。
11. [Active Directory Schema] を右クリックし、[Reload the Schema] を選択して新たな変更を



行います。

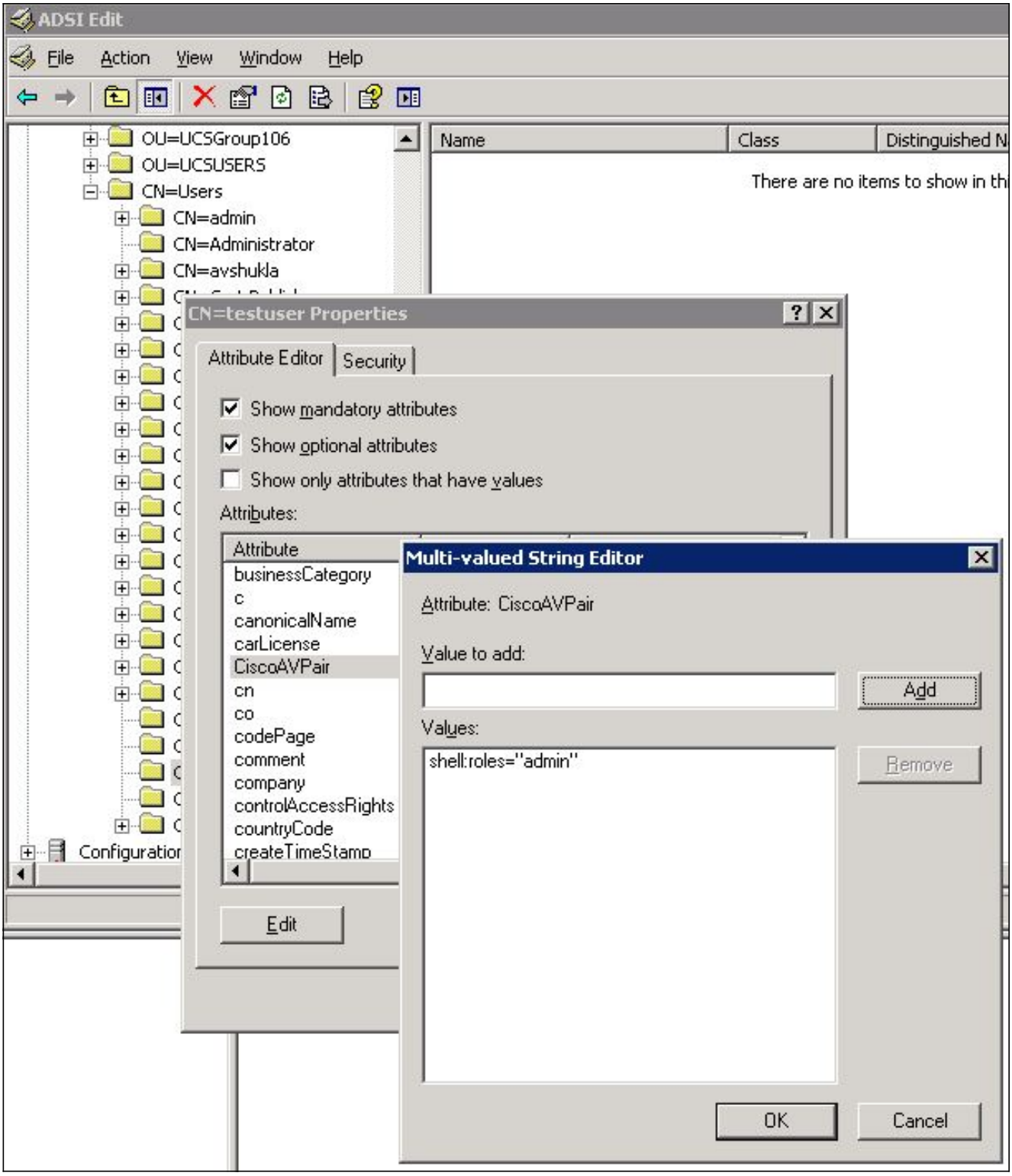
12. 必要に応じて、ADSI エディタを使用してスキーマを更新することもできます。[Localhost] を右クリックして [Update Schema Now] を選択します。



CiscoAVPair 属性の更新

この手順では、CiscoAVPair 属性の更新方法について説明します。入力する値は shell:roles="<role>" です。

1. [ADSI Edit] ダイアログボックスで、UCS Central へのアクセス権が必要なユーザを検索します。
2. ユーザを右クリックして [Properties] を選択します。
3. [Properties] ダイアログボックスで [Attribute Editor] タブをクリックし、[CiscoAVPair] > [Edit] の順にクリックします。
4. [Multi-valued String Editor] ダイアログボックスで、[Values] フィールドに **shell:roles="admin"** と入力して [OK] をクリックします。



5. [OK] をクリックし、変更を保存して [Properties] ダイアログボックスを閉じます。

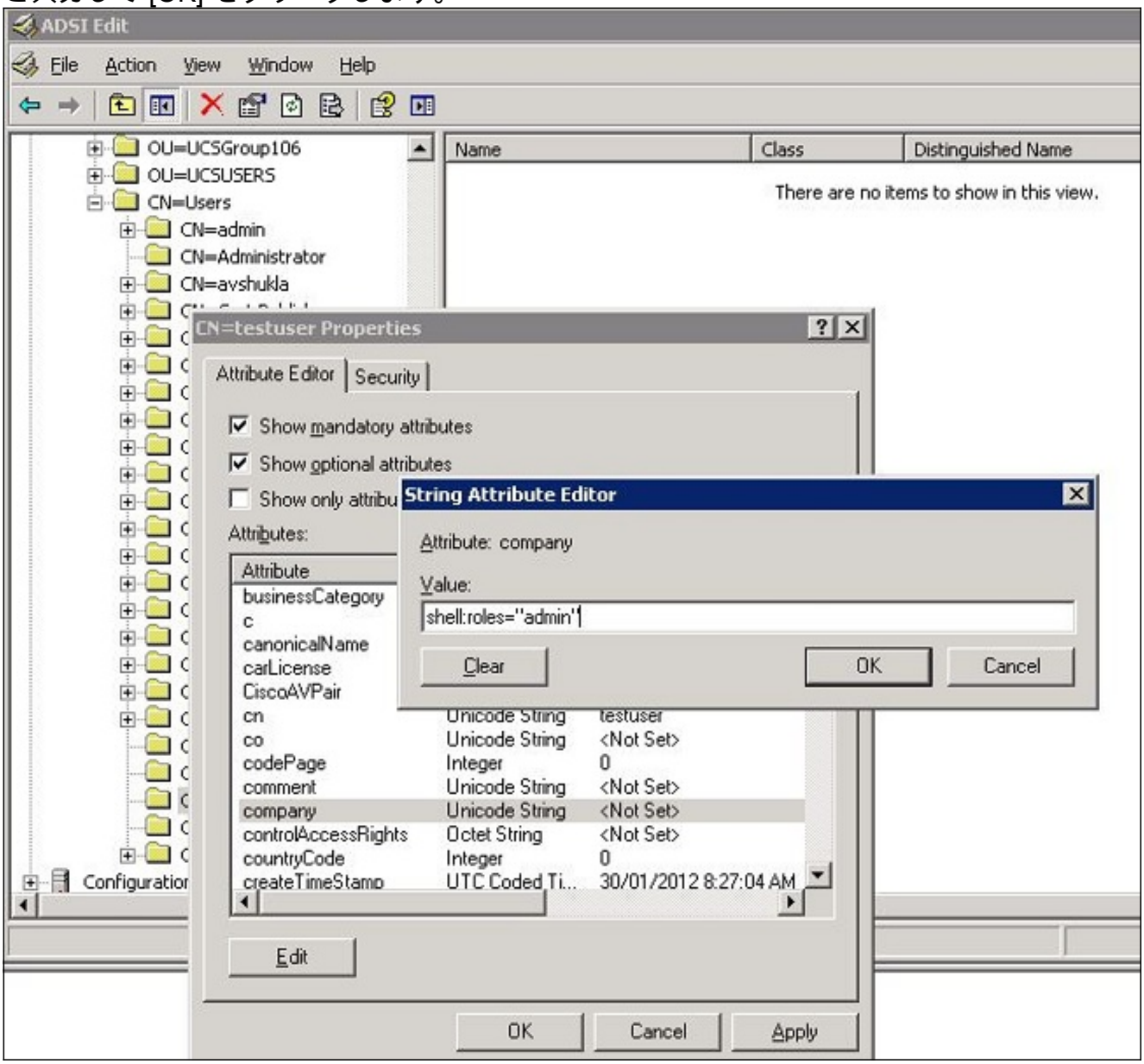
事前設定された属性の更新

この手順では、事前設定された属性の更新方法について説明します。この属性のロールは、UCS Central で事前設定された複数のユーザ ロールのうちの 1 つです。ここでは、属性を *company* としてロールの割り当てを行います。入力する値は shell:roles="<role>" です。

1. [ADSI Edit] ダイアログボックスで、UCS Central へのアクセス権が必要なユーザを検索します。
2. ユーザを右クリックして [Properties] を選択します。
3. [Properties] ダイアログボックスで [Attribute Editor] タブをクリックし、[company] > [Edit]

の順にクリックします。

4. [String Attribute Editor] ダイアログボックスで、[Values] フィールドに **shell:roles="admin"** と入力して [OK] をクリックします。

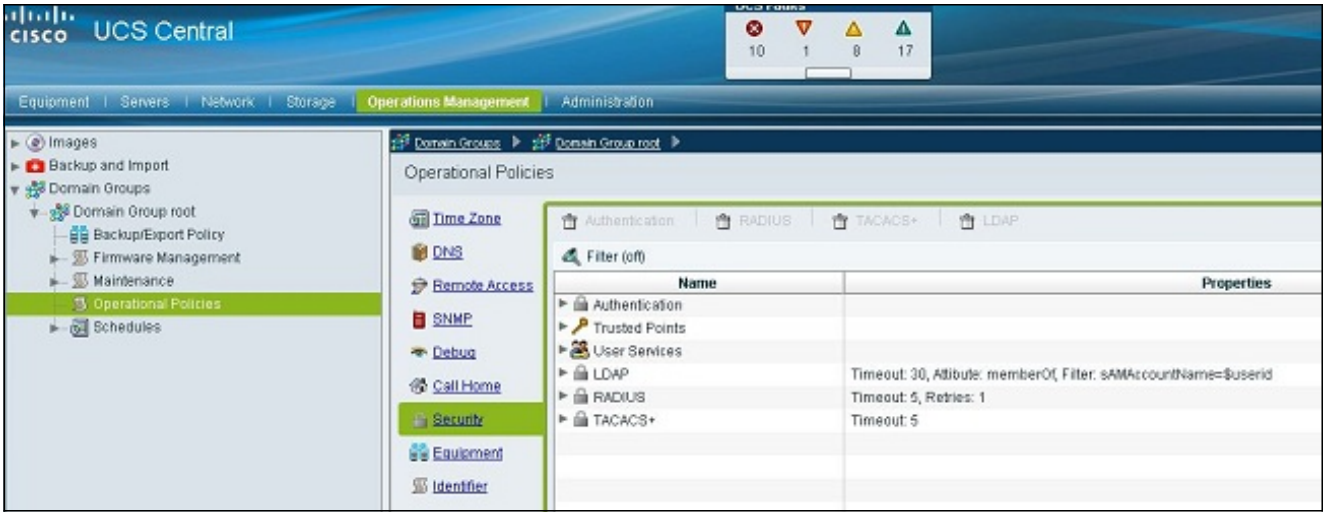


5. [OK] をクリックし、変更を保存して [Properties] ダイアログボックスを閉じます。

UCS Central での LDAP 認証の設定

UCS Central での LDAP 設定は、[Operations Management] 内で完結できます。

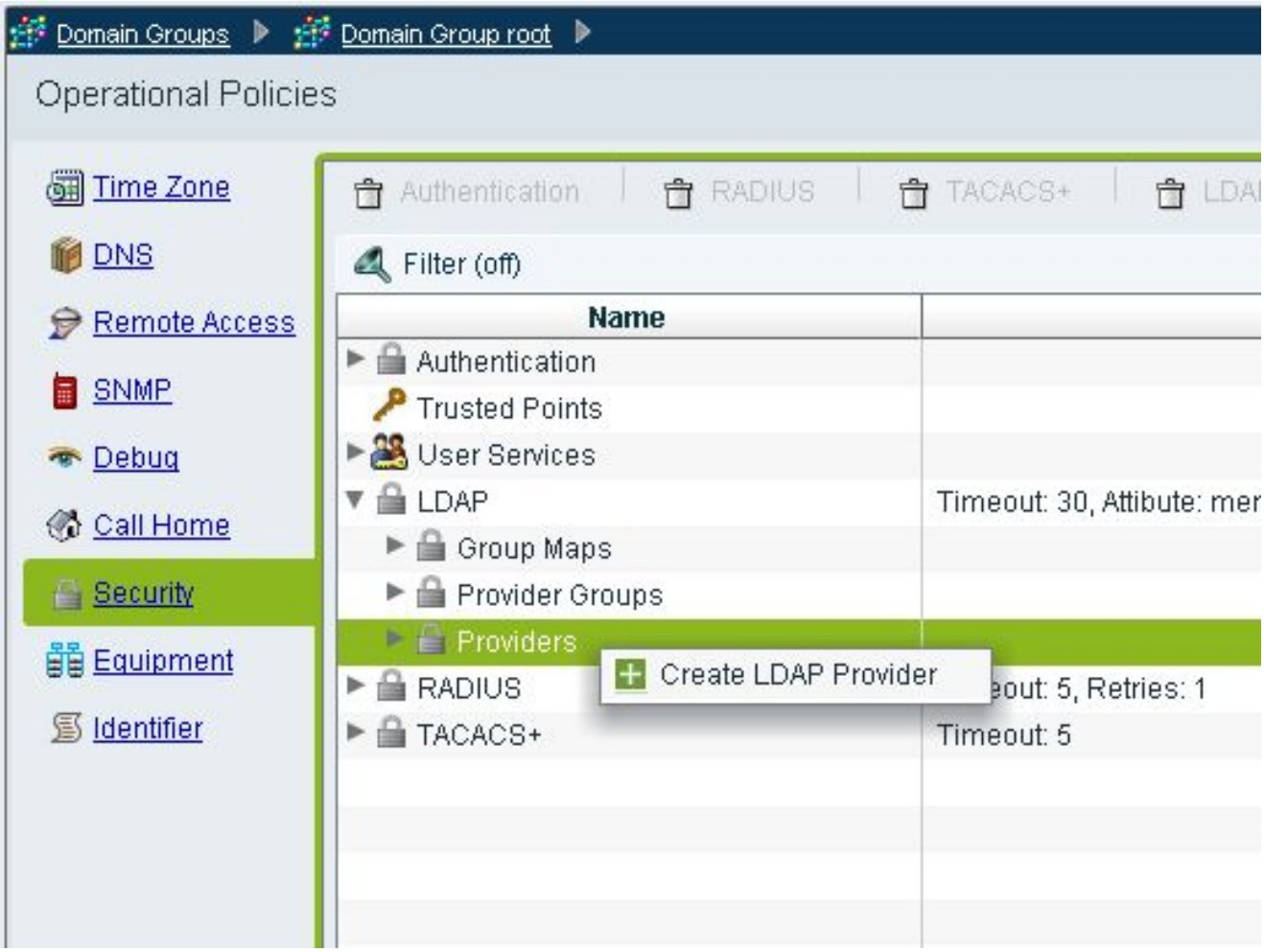
1. ローカル アカウントで UCS Central にログインします。
2. [Operations Management] をクリックし、[Domain Groups] を展開して [Operational Policies] > [Security] の順にクリックします。



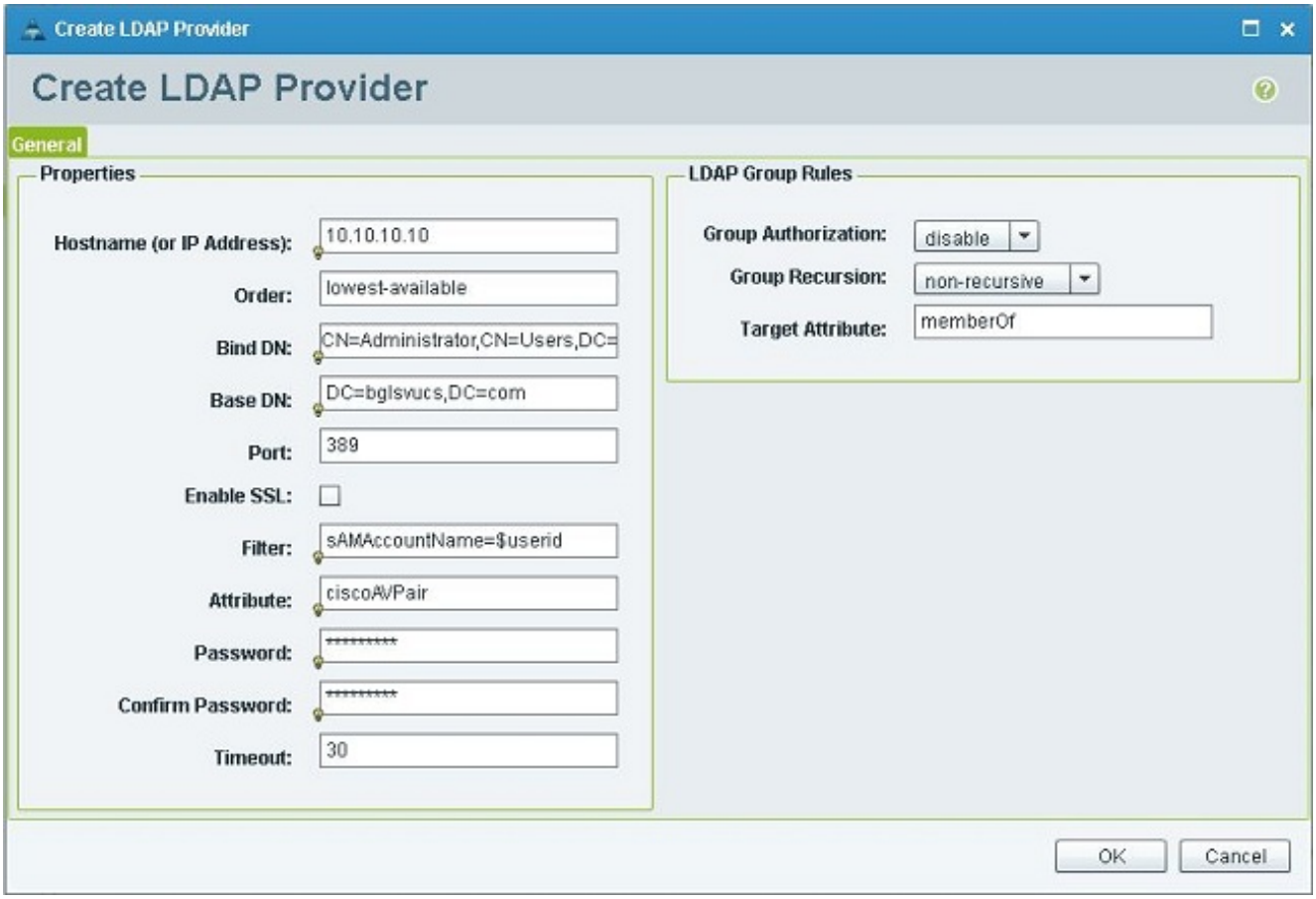
3. LDAP 認証の設定手順は以下のとおりです。LDAP プロバイダーの設定LDAP プロバイダーグループの設定（リリース 1.0a ではサポート対象外）ネイティブ認証ルールの変更

LDAP プロバイダーの設定

1. [LDAP] をクリックし、[Providers] を右クリックして [Create LDAP Provider] を選択します。



2. [Create LDAP Provider] ダイアログボックスで、事前に収集されたこれらの詳細情報を追加します。プロバイダーのホスト名または IP アドレスバインド DNベース DNフィルタ属性（CiscoAVPair、または company などの事前設定された属性）パスワード（バインド DN で使用されているユーザのパスワード
）



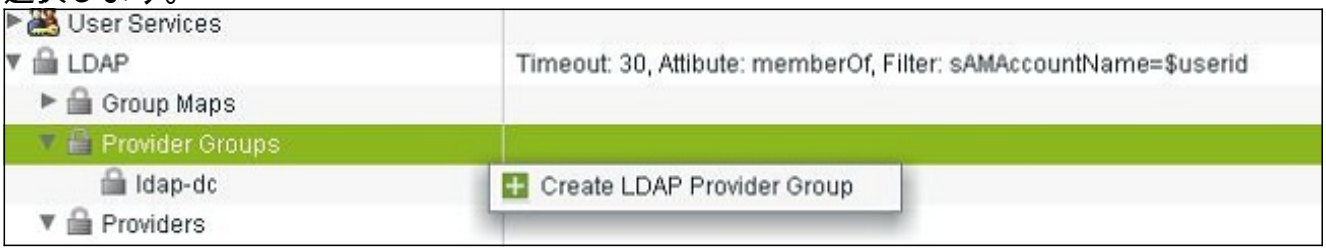
3. [OK] をクリックし、設定を保存してダイアログボックスを閉じます。

注：この画面では、他の値を変更する必要はありません。このリリースでは、UCS Central の認証用の LDAP グループ ルールはサポートされていません。

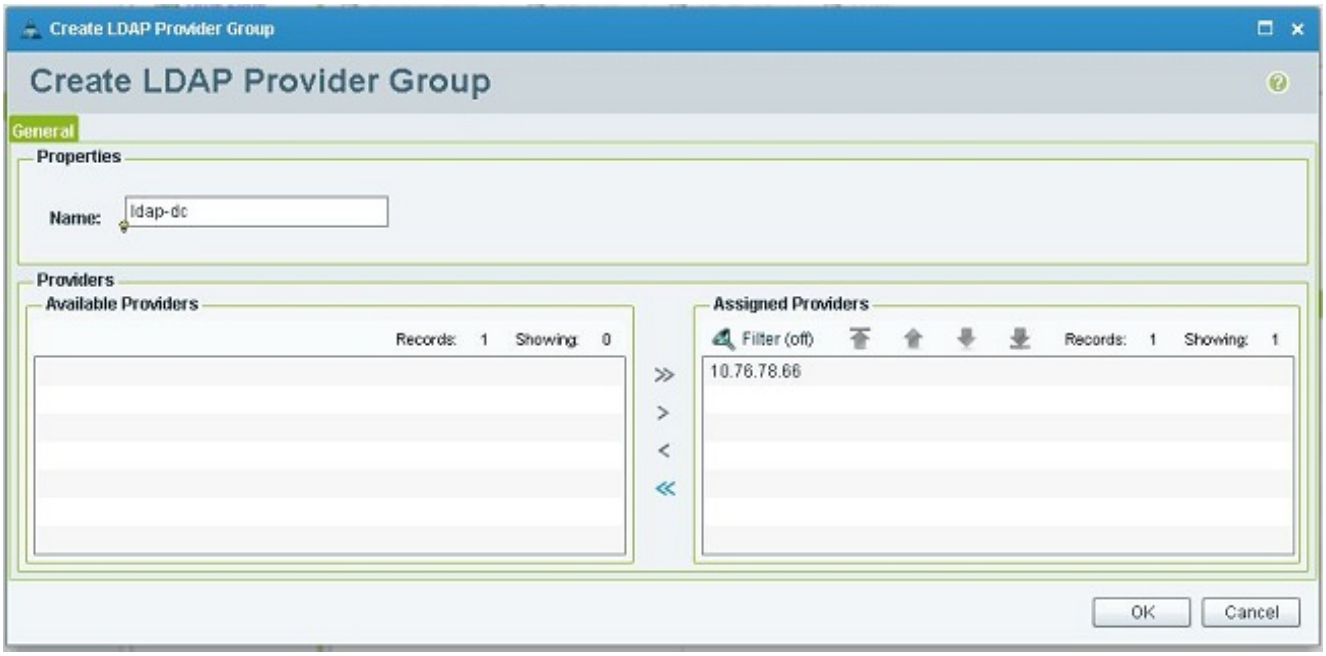
LDAP プロバイダー グループの設定

注：リリース1.0aでは、プロバイダーグループはサポートされていません。この手順では、後の設定で使用するダミーのプロバイダー グループの設定方法について説明します。

1. [LDAP] をクリックし、[Provider Group] を右クリックして [Create LDAP Provider Group] を選択します。



2. [Create LDAP Provider Group] ダイアログボックスで、[Name] フィールドにグループ名を入力します。
3. 左下の [Available Providers] のリストで対象プロバイダーを選択し、[>] をクリックしてこのプロバイダーを右下の [Assigned Providers] に移動します。



4. [OK] をクリックして変更を保存し、画面を閉じます。

ネイティブ認証ルールの変更

UCS Manager の場合と同様、リリース 1.0a では複数の認証ドメインをサポートしていません。この問題を回避するには、ネイティブ認証ルールを変更する必要があります。

ネイティブ認証には、デフォルトのログインまたはコンソールのログインの認証を変更するオプションが備わっています。複数のドメインがサポートされていないため、ローカル アカウントまたは LDAP アカウントのどちらか一方のみを使用できます。レルムの値を変更し、ローカル アカウントか LDAP アカウントを認証用の元データとして使用します。

1. [Authentication] をクリックし、[Native Authentication] を右クリックして [Properties] を選択します。
2. デフォルト認証とコンソール認証のどちらを変更するのか、またはその両方を変更するのかを決めます。GUI と CLI (コマンド ライン インターフェイス) 向けには、デフォルト認証を使用します。 VM (仮想マシン) や KVM (カーネル ベースの仮想マシン) の表示には、コンソール認証を使用します。
3. [Realm] ドロップダウン リストで [ldap] を選択します。認証元データにローカル アカウントを使用するか LDAP アカウントを使用するかは、レルムの値に基づいて決定されます。

4. [OK] をクリックしてウィンドウを閉じます。
5. 必要に応じて [Policies] ページで [Save] をクリックし、変更内容を保存します。

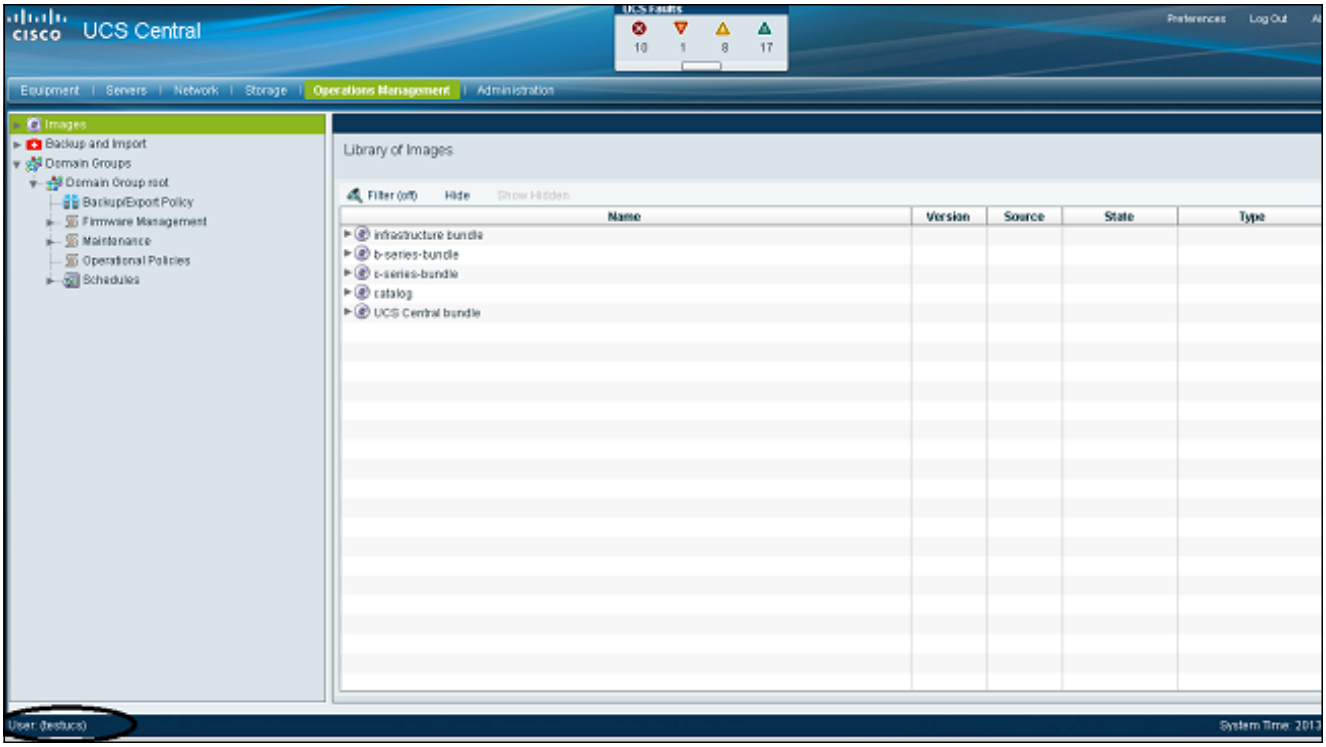
注：LDAP認証が正しく動作することを確認するまで、現在のセッションからログアウトしたり、コンソール認証を変更したりしないでください。コンソール認証では、以前の設定に戻す方法が表示されます。「確認」セクションを参照してください。

確認

この手順では、LDAP 認証のテスト方法について説明します。

1. UCS Central の新規セッションを開き、ユーザ名とパスワードを入力します。ユーザ名の前に、ドメインや文字を含める必要はありません。ここでは、ドメインのユーザ名を testucs としています。

2. UCS Central ダッシュボードが表示されれば、LDAP 認証は成功です。ページの左下隅にユーザ名が表示されます。



トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems