Konfigurationsbeispiel für die LDAP-Authentifizierung in UCS Central

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die LDAP-Authentifizierung (Lightweight Directory Access Protocol) für Cisco Unified Computing System (UCS) Central. Die Verfahren verwenden die grafische Benutzeroberfläche (GUI) von UCS Central, eine Beispieldomäne von bglucs.com und einen Beispielbenutzernamen von testuser.

In Version 1.0 der UCS Central-Software wird LDAP als einziges Remote-Authentifizierungsprotokoll unterstützt. Version 1.0 bietet nur sehr eingeschränkte Unterstützung für Remote-Authentifizierung und LDAP-Konfiguration für UCS Central selbst. Sie können UCS Central jedoch verwenden, um alle Optionen für die von UCS Central verwalteten UCS Manager-Domänen zu konfigurieren.

Die Remote-Authentifizierung in UCS Central unterliegt folgenden Einschränkungen:

- RADIUS und TACACS werden nicht unterstützt.
- Die LDAP-Gruppenzuordnung für die Rollenzuweisung und LDAP-Anbietergruppen für mehrere Domänencontroller werden nicht unterstützt.
- LDAP verwendet nur das CiscoAVPair-Attribut oder ein nicht verwendetes Attribut, um die Rolle zu übergeben. Die übergebene Rolle ist eine der vordefinierten Rollen in der lokalen UCS Central-Datenbank.
- Mehrere Authentifizierungsdomänen/Protokolle werden nicht unterstützt.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- UCS Central wird bereitgestellt.
- Microsoft Active Directory wird bereitgestellt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- UCS Central Version 1.0
- Microsoft Active Directory

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Sammeln von Informationen

In diesem Abschnitt werden die Informationen zusammengefasst, die Sie vor Beginn der Konfiguration sammeln müssen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

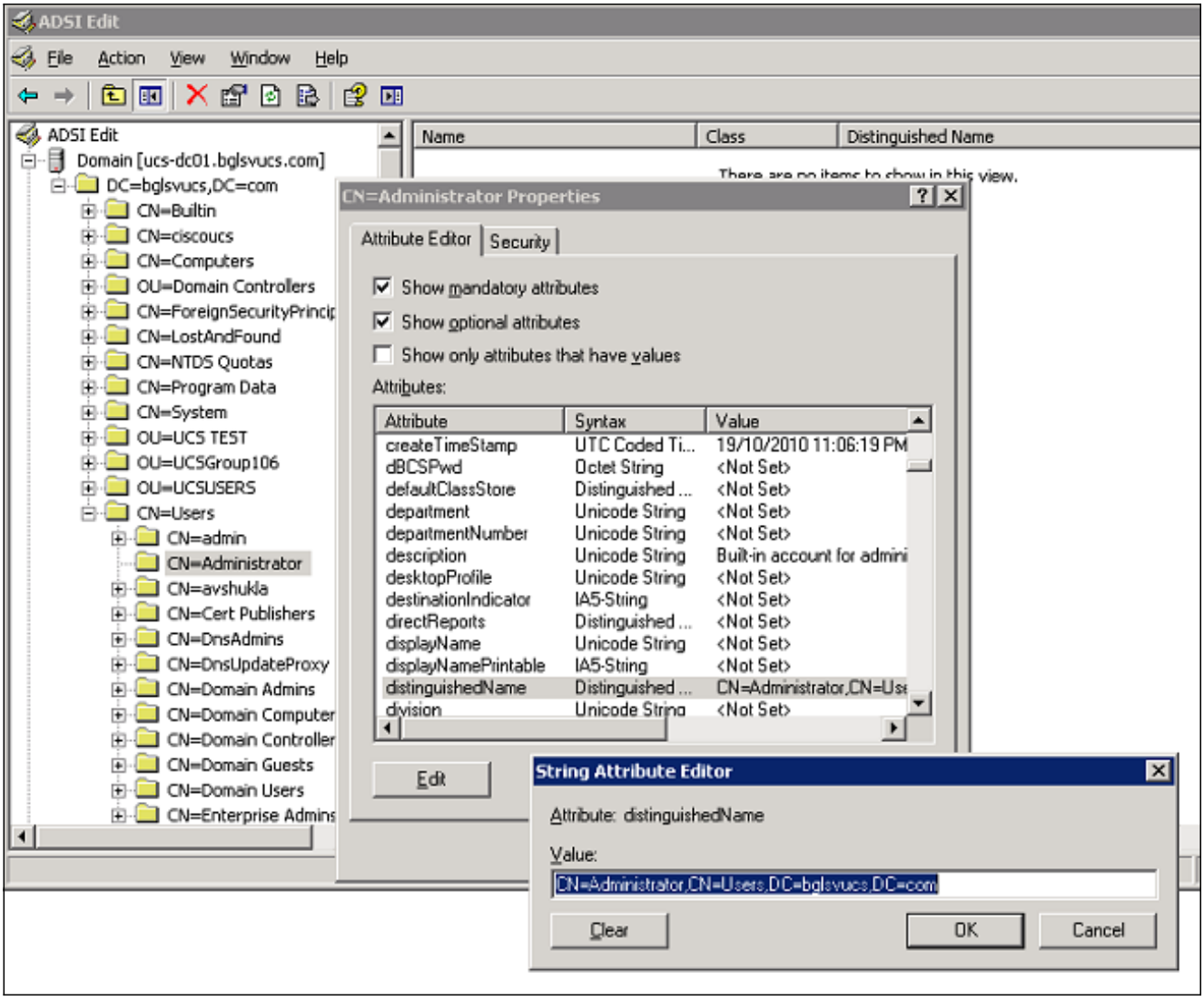
Binden von Benutzerdetails

Bind-Benutzer können ein beliebiger LDAP-Benutzer in der Domäne sein, der über Lesezugriff auf die Domäne verfügt. Für die LDAP-Konfiguration ist ein bindender Benutzer erforderlich. UCS Central verwendet den Benutzernamen und das Kennwort des binden Benutzers, um eine

Verbindung zum Active Directory (AD) herzustellen und diese zur Benutzerauthentifizierung usw. abzufragen. In diesem Beispiel wird das Administratorkonto als binder Benutzer verwendet.

Dieses Verfahren beschreibt, wie ein LDAP-Administrator den ADSI-Editor (Active Directory Service Interfaces) verwenden kann, um die DN zu finden.

1. Öffnen Sie den ADSI-Editor.
2. Suchen Sie den binden Benutzer. Der Benutzer hat denselben Pfad wie im AD.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer, und wählen Sie **Eigenschaften aus**.
4. Doppelklicken Sie im Dialogfeld Eigenschaften auf **DistinguishedName**.
5. Kopieren Sie die DN aus dem Feld
   Wert.



6. Klicken Sie auf **Abbrechen**, um alle Fenster zu schließen.

Um das Kennwort für den binden Benutzer zu erhalten, wenden Sie sich an den AD-Administrator.

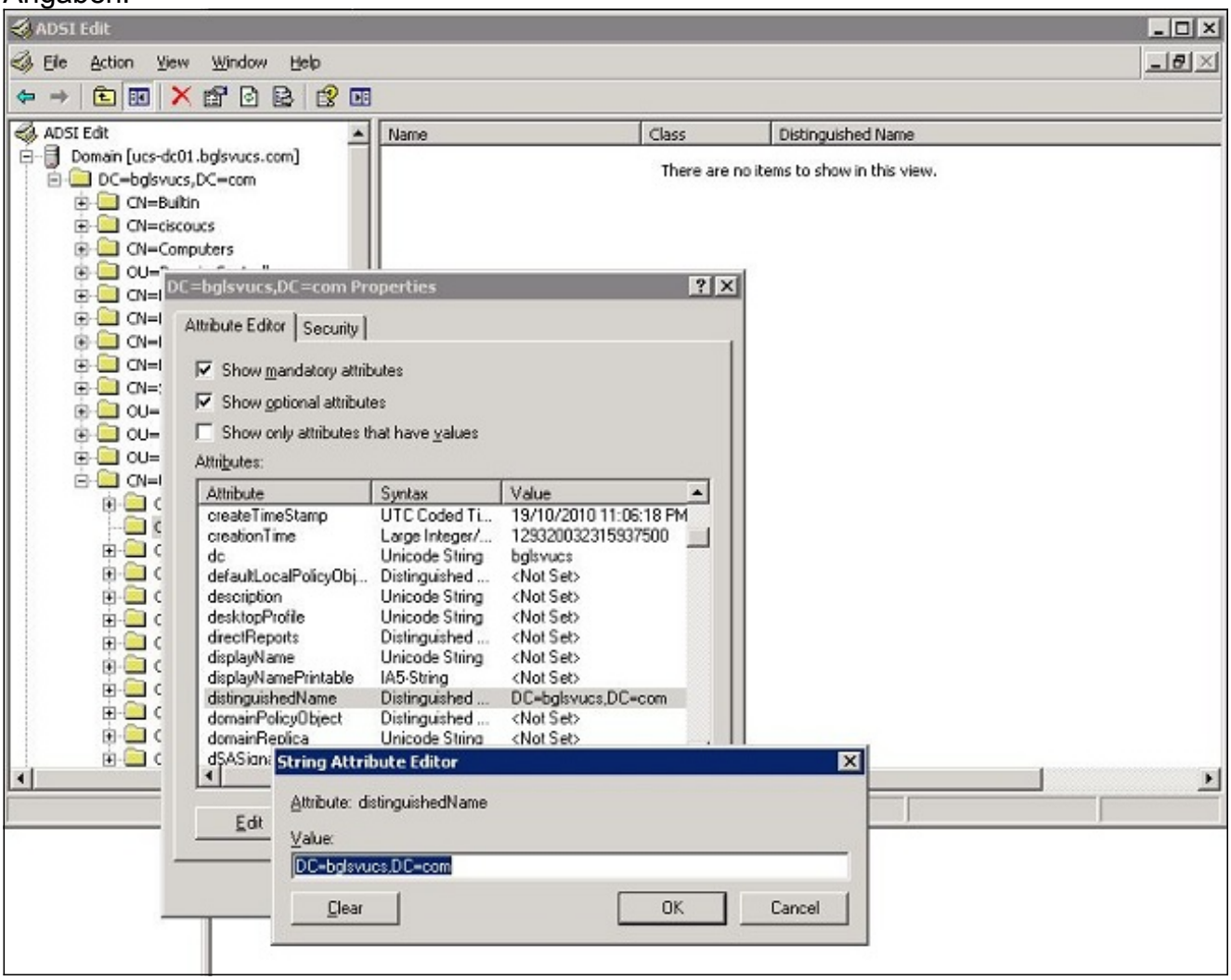
Basis-DN-Details

Basis-DN ist die DN der Organisationseinheit (OU) oder des Containers, in dem die Suche nach Benutzer- und Benutzerdetails beginnt. Sie können die DN einer im AD erstellten OU für das UCS oder UCS Central verwenden. Es ist jedoch möglicherweise einfacher, den DN für den Domänenstamm selbst zu verwenden.

Dieses Verfahren beschreibt, wie ein LDAP-Administrator den ADSI-Editor verwenden kann, um

die Basis-DN zu finden.

1. Öffnen Sie den ADSI-Editor.
2. Suchen Sie die OU oder den Container, der als Basis-DN verwendet werden soll.
3. Klicken Sie mit der rechten Maustaste auf die OU oder den Container, und wählen Sie **Eigenschaften** aus.
4. Doppelklicken Sie im Dialogfeld Eigenschaften auf **DistinguishedName**.
5. Kopieren Sie die DN aus dem Wertefeld, und notieren Sie alle weiteren erforderlichen Angaben.



6. Klicken Sie auf **Abbrechen**, um alle Fenster zu schließen.

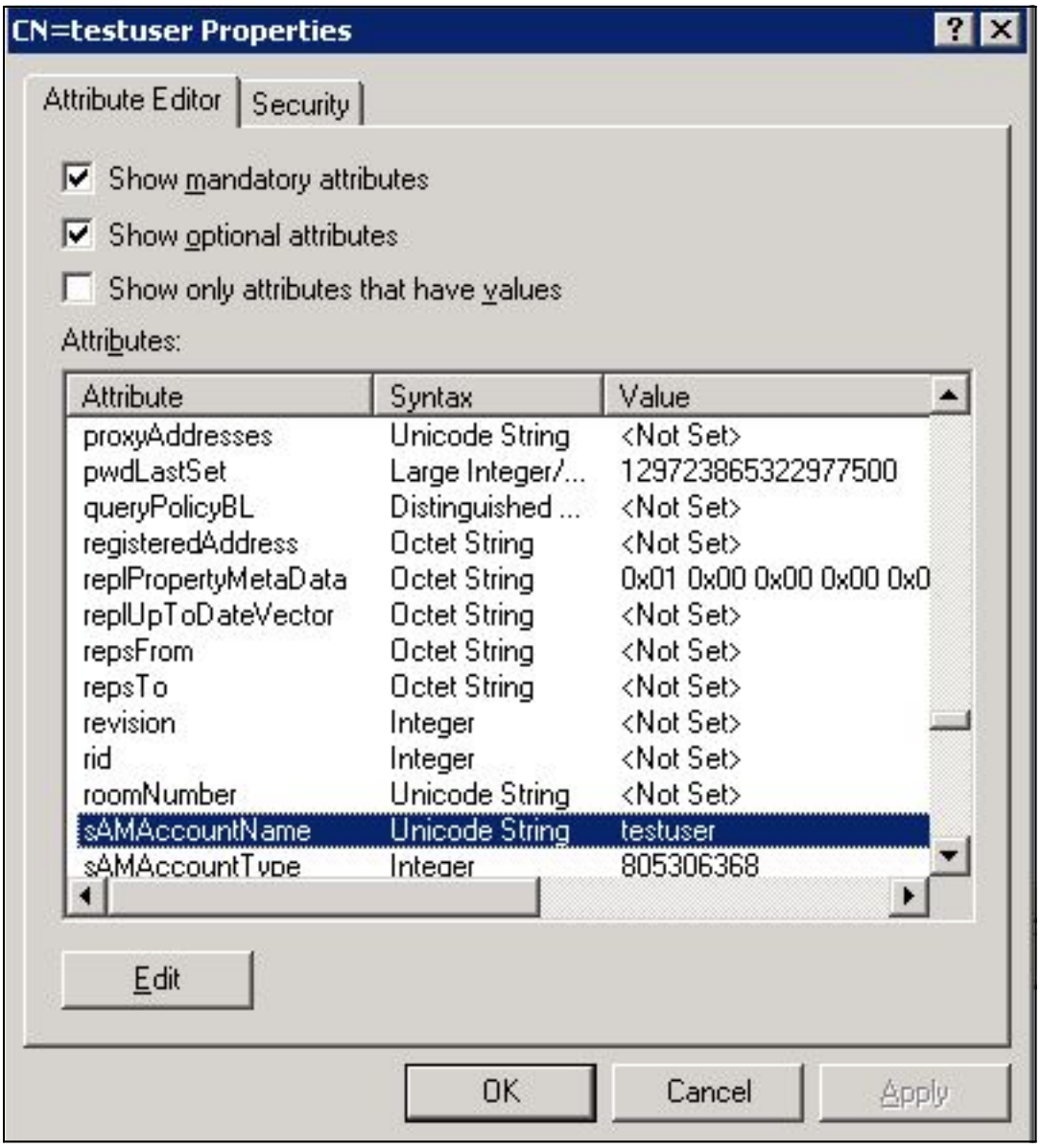
Anbieterdetails

Provider spielt eine Schlüsselrolle bei der LDAP-Authentifizierung und -Autorisierung in UCS Central. Provider ist einer der AD-Server, den UCS Central abfragt, um den Benutzer zu suchen und zu authentifizieren und um Benutzerdetails wie Rolleninformationen abzurufen. Stellen Sie sicher, dass Sie den Hostnamen oder die IP-Adresse des Provider AD-Servers ermitteln.

Filtereigenschaft

Das Filterfeld oder die Filtereigenschaft wird zum Durchsuchen der AD-Datenbank verwendet. Die bei der Anmeldung eingegebene Benutzer-ID wird an das AD zurückgegeben und mit dem Filter verglichen.

Sie können sAMAccountName=$userid als Filterwert verwenden. sAMAccountName ist ein Attribut im AD und hat denselben Wert wie die AD-Benutzer-ID, die für die Anmeldung bei der UCS Central-GUI verwendet wird.



Hinzufügen und Konfigurieren von Attributen

In diesem Abschnitt werden die Informationen zusammengefasst, die Sie benötigen, um das CiscoAVPair-Attribut (falls erforderlich) hinzuzufügen und das CiscoAVPair-Attribut oder ein anderes vordefiniertes Attribut zu aktualisieren, bevor Sie die LDAP-Konfiguration starten.

Das Attributfeld gibt das AD-Attribut (unter der Eigenschaft user) an, das die dem Benutzer zuzuweisende Rolle zurückgibt. In Version 1.0a der UCS Central-Software kann entweder das benutzerdefinierte Attribut CiscoAVPair oder ein anderes nicht verwendetes Attribut im AD vereinheitlicht werden, um diese Rolle zu übergeben.

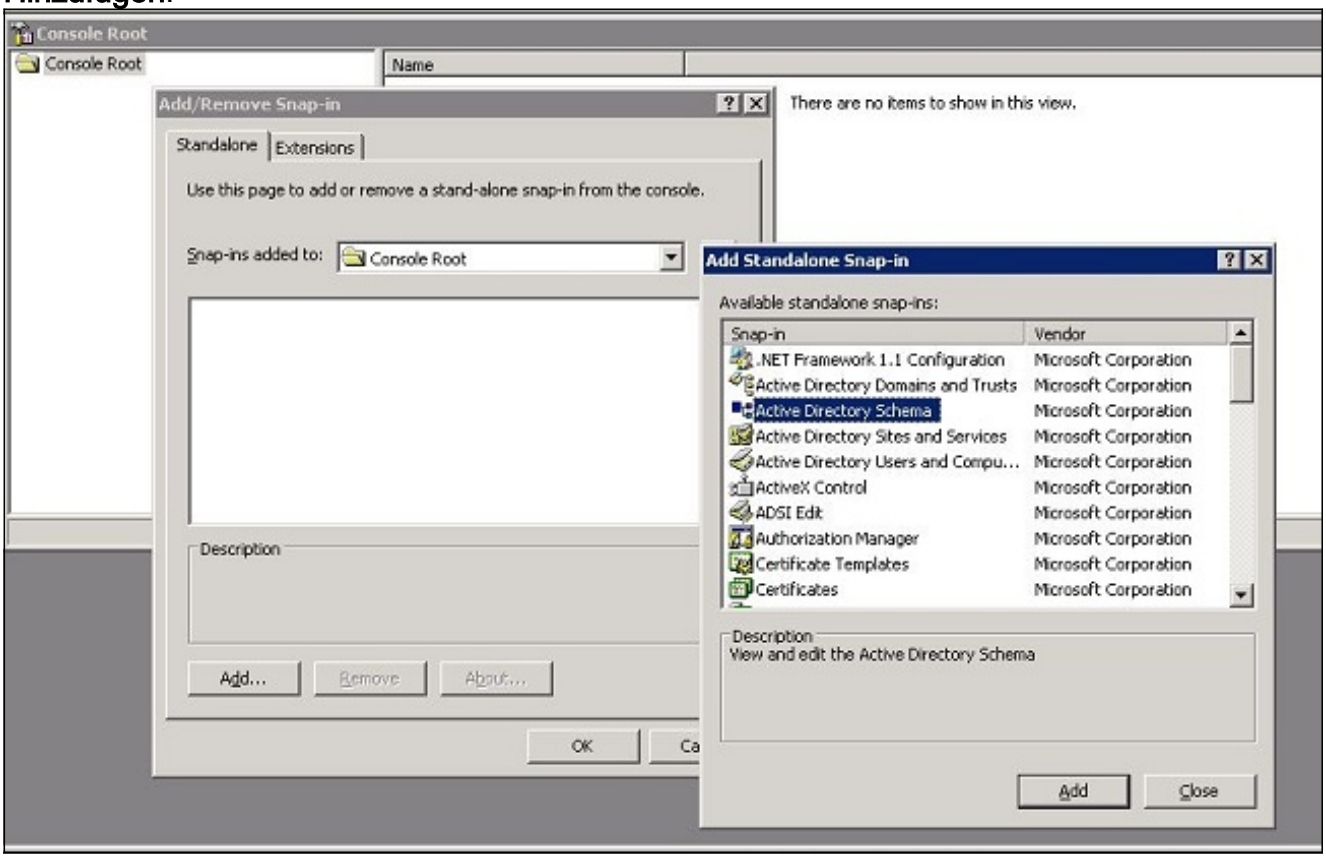
Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

CiscoAVPair-Attribut hinzufügen

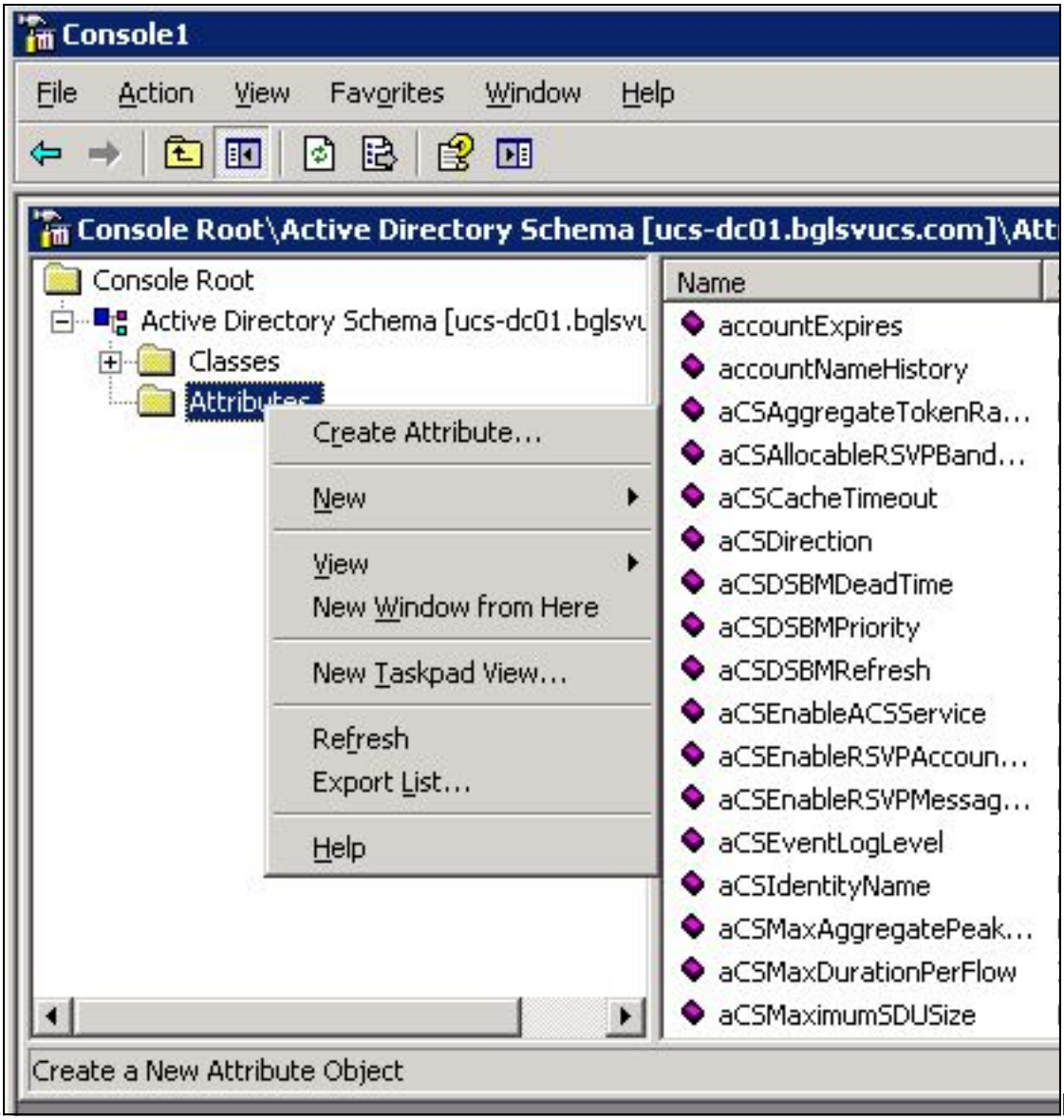
Um der Domäne ein neues Attribut hinzuzufügen, erweitern Sie das Schema der Domäne, und fügen Sie das Attribut der Klasse hinzu (in diesem Beispiel Benutzer).

In diesem Verfahren wird beschrieben, wie Sie das Schema auf einem Windows AD-Server erweitern und das CiscoAVPair-Attribut hinzufügen.

1. Melden Sie sich bei einem AD-Server an.
2. Klicken Sie auf **Start > Ausführen**, geben Sie **mmc ein**, und drücken Sie die **Eingabetaste**, um eine leere Microsoft Management Console (MMC)-Konsole zu öffnen.
3. Klicken Sie in der MMC auf **Datei > Snap-In hinzufügen/entfernen > Hinzufügen**.
4. Wählen Sie im Dialogfeld Standalone Snap-In hinzufügen das **Active Directory-Schema aus**, und klicken Sie auf **Hinzufügen**.

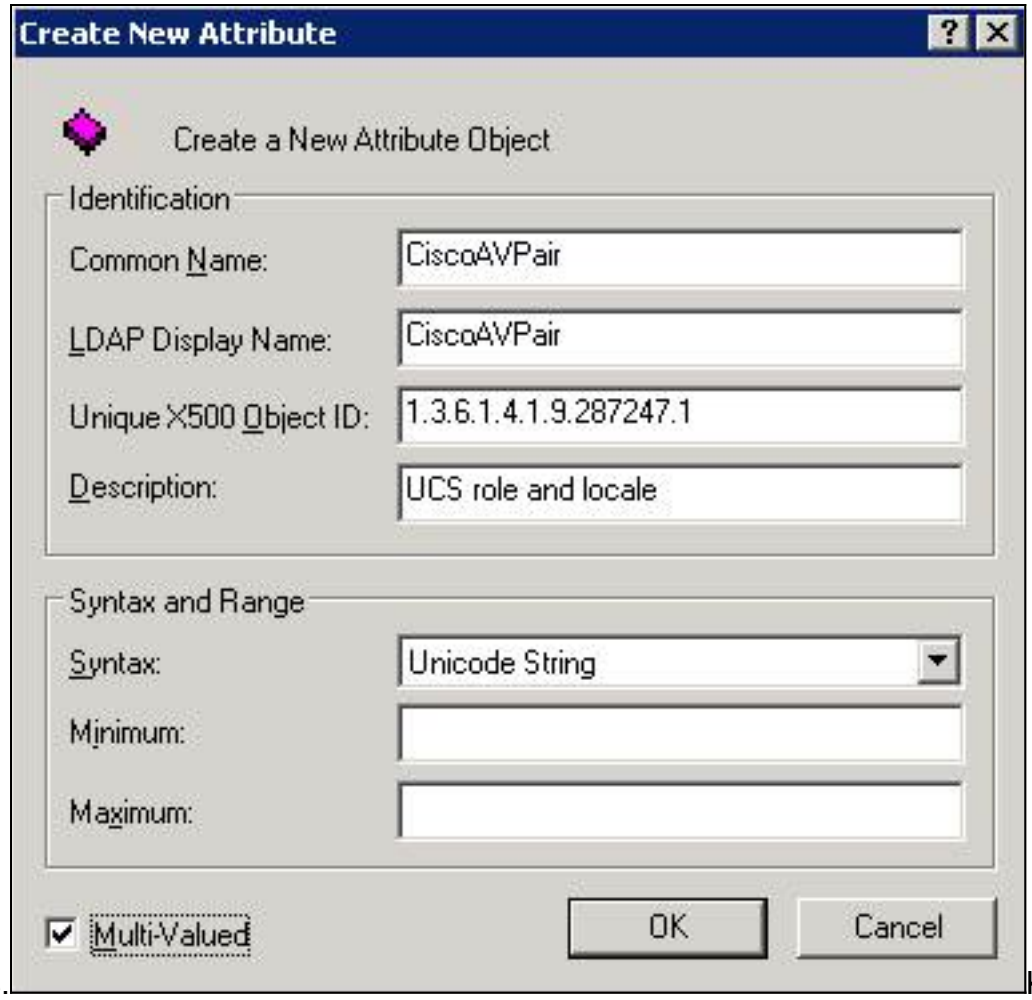


5. Erweitern Sie im MMC das **Active Directory-Schema**, klicken Sie mit der rechten Maustaste auf **Attribute**, und wählen Sie **Create Attribute (Attribut**



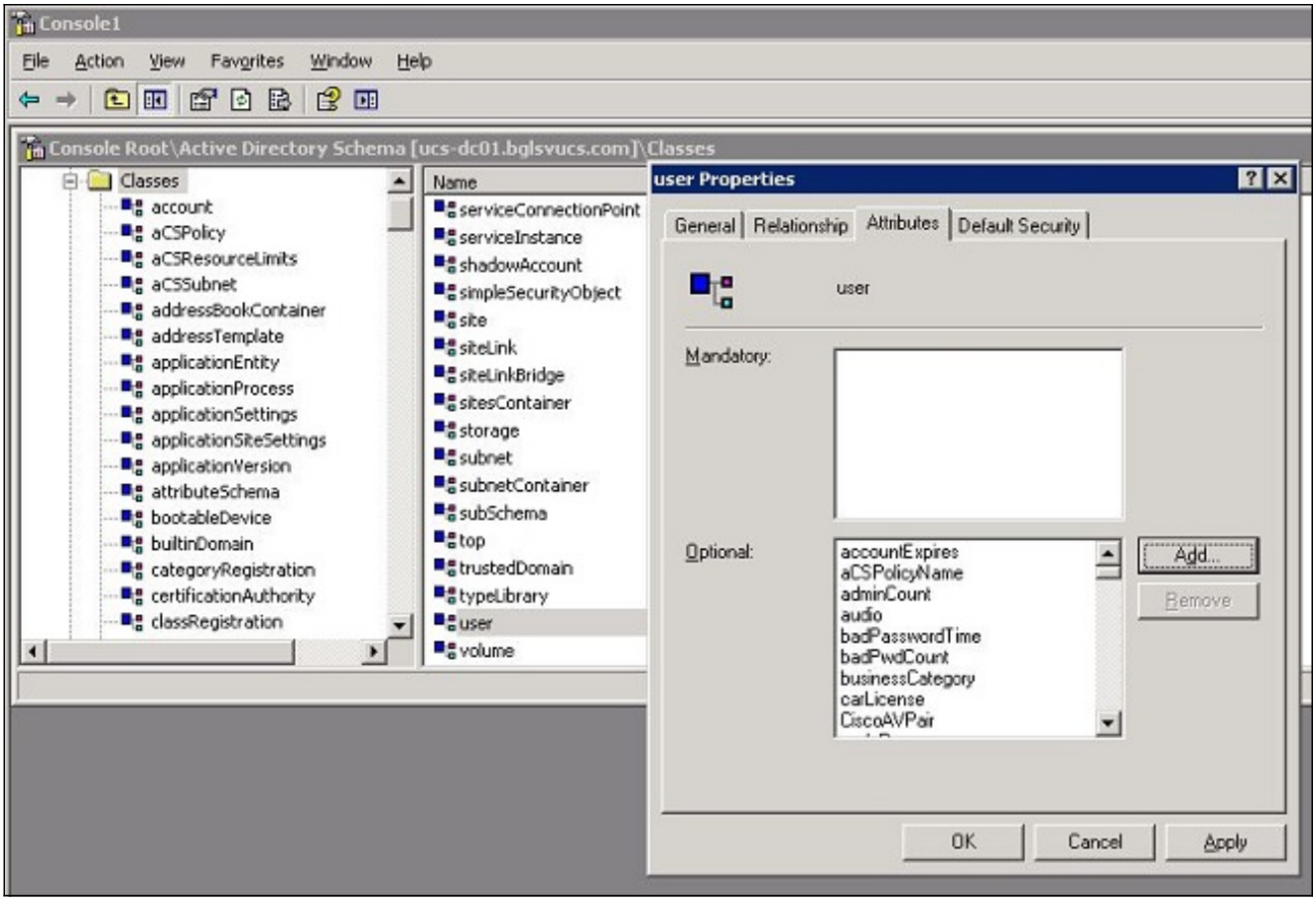
erstellen).Das Dialogfeld Neues Attribut erstellen wird angezeigt.

6. Erstellen Sie im Remote-Authentifizierungsdienst ein Attribut mit dem Namen CiscoAVPair.Geben Sie in die Felder Common Name (Gemeinsamer Name) und LDAP Display Name (LDAP-Anzeigename) **CiscoAVPair ein**.Geben Sie im Feld Unique 500 Object ID (Unique 500-Objekt-ID) **1.3.6.1.4.1.9.287247.1 ein**.Geben Sie im Feld Description (Beschreibung) die **UCS-Rolle und das Gebietsschema ein**.Wählen Sie im Syntaxfeld **Unicode String** aus der Dropdown-Liste

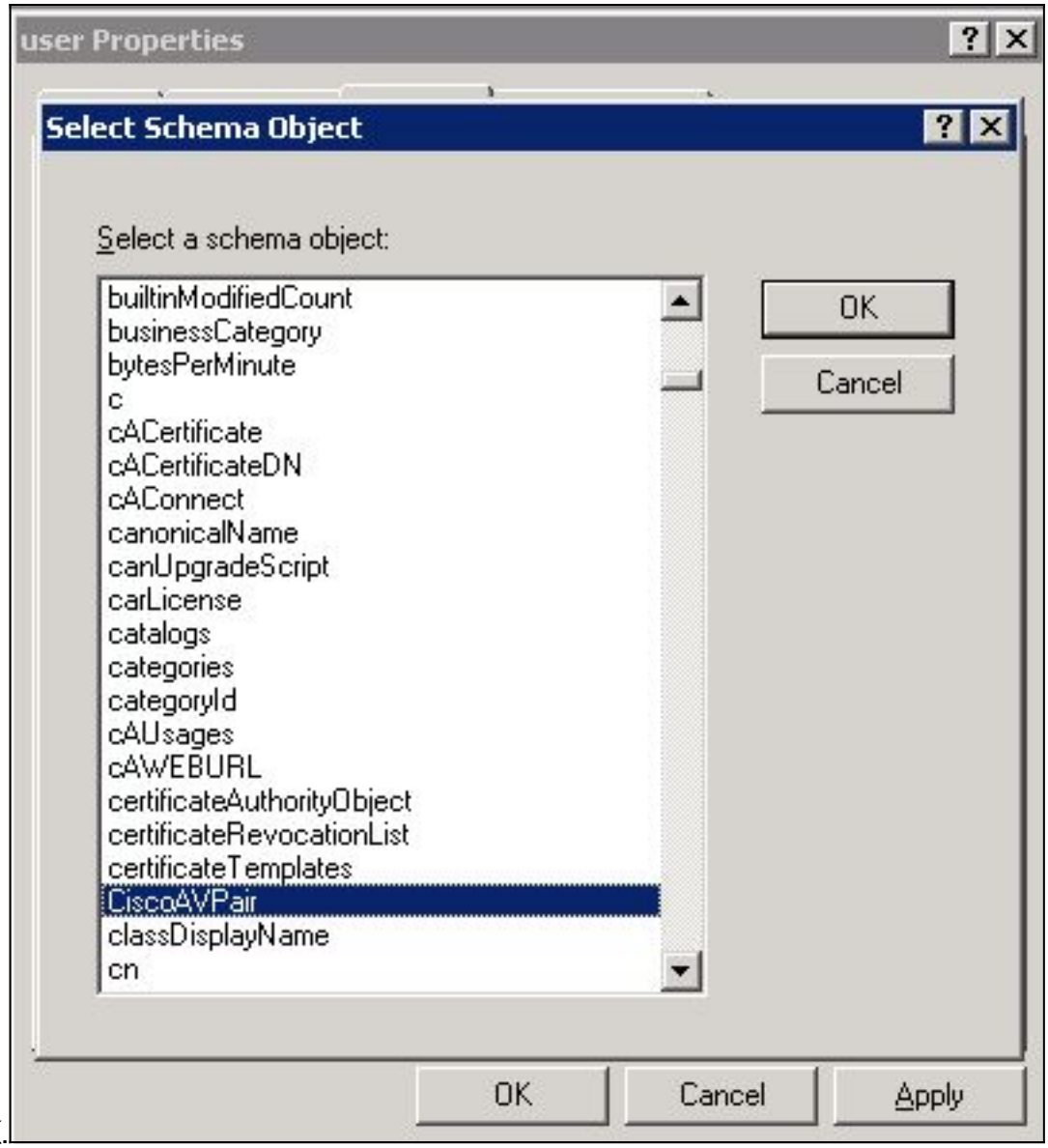


aus.Klicken Sie auf **OK**, um das Attribut zu speichern und das Dialogfeld zu schließen.Nachdem das Attribut dem Schema hinzugefügt wurde, muss es zugeordnet oder in die Benutzerklasse aufgenommen werden. Auf diese Weise können Sie die Benutzereigenschaft bearbeiten und den Wert der übergebenen Rolle angeben.

7. Erweitern Sie in derselben MMC, die für die AD-Schemaerweiterung verwendet wird, **Klassen**, klicken Sie mit der rechten Maustaste auf **Benutzer**, und wählen Sie **Eigenschaften** aus.
8. Klicken Sie im Dialogfeld Benutzereigenschaften auf die Registerkarte **Attribute** und anschließend auf
Hinzufügen.

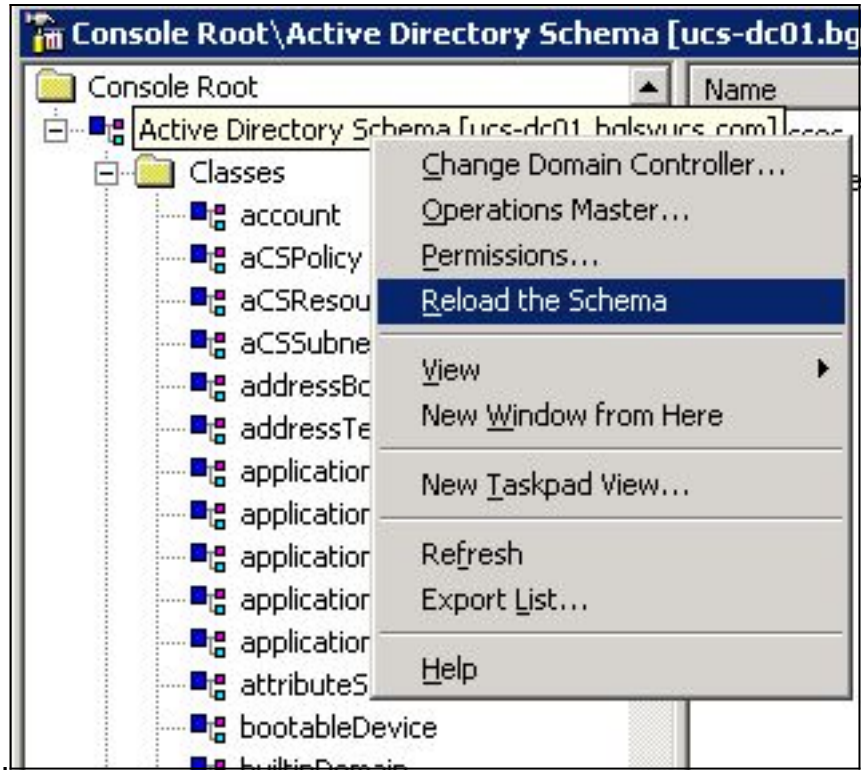


9. Klicken Sie im Dialogfeld Schemaobjekt auswählen auf **CiscoAVPair** und dann auf

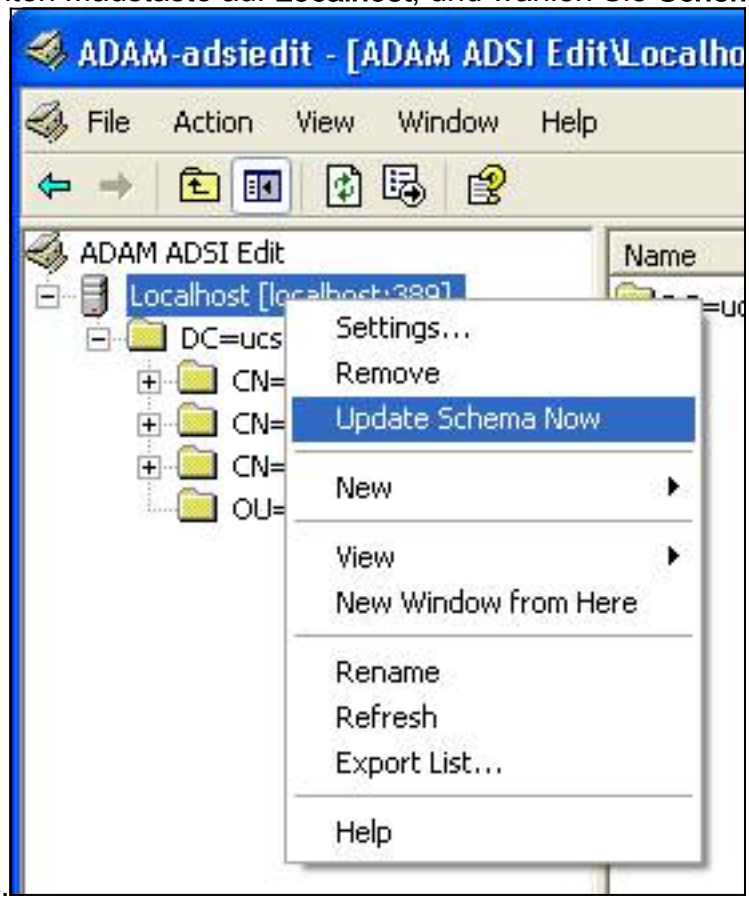


OK.

10. Klicken Sie im Dialogfeld Benutzereigenschaften auf **Übernehmen**.
11. Klicken Sie mit der rechten Maustaste auf **Active Directory-Schema**, und wählen Sie **Schema neu laden aus**, um die neuen Änderungen

einzuschließen. 

12. Verwenden Sie ggf. den ADSI-Editor, um das Schema zu aktualisieren. Klicken Sie mit der rechten Maustaste auf **Localhost**, und wählen Sie **Schema jetzt aktualisieren**



aus.

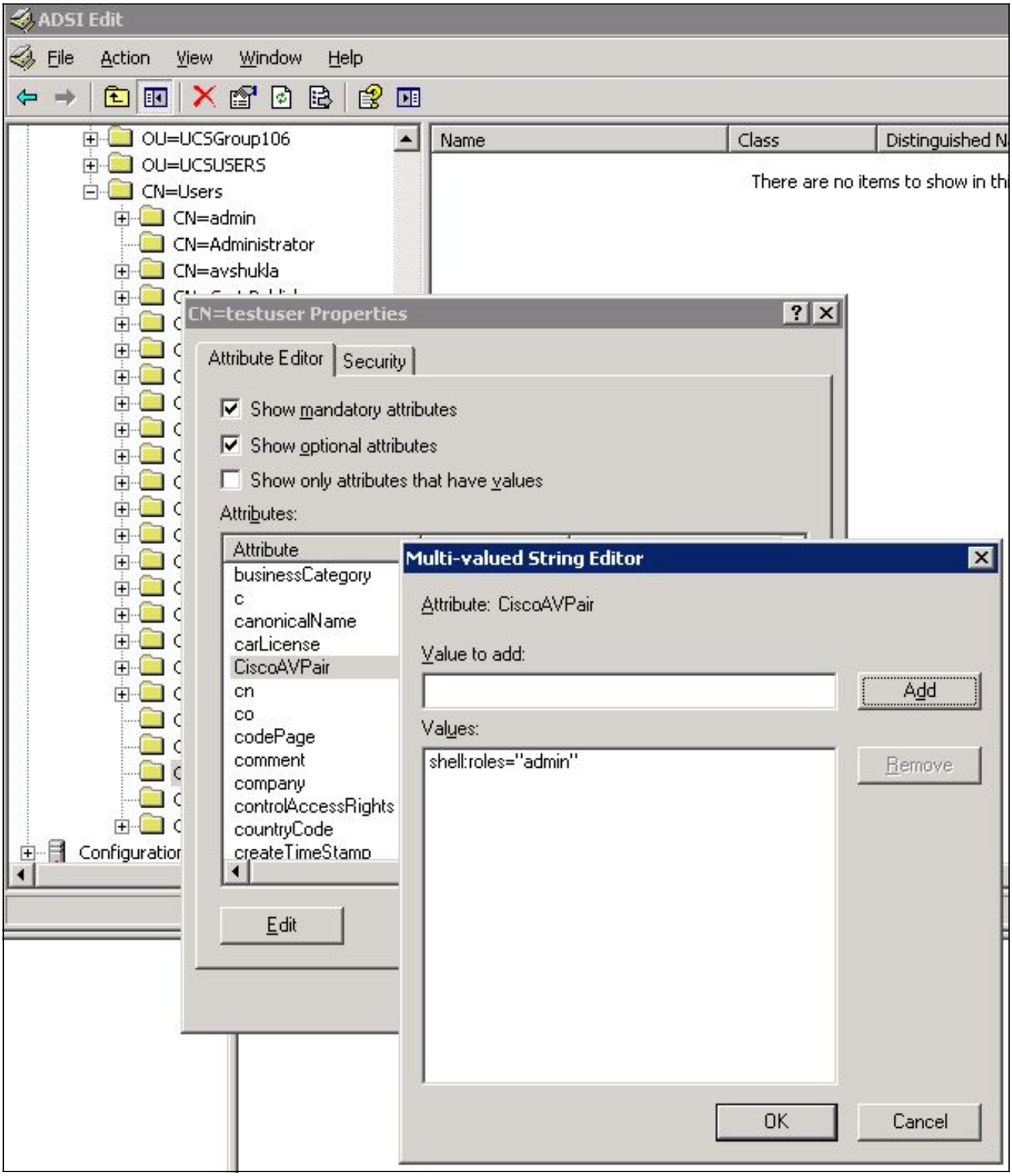
CiscoAVPair-Attribut aktualisieren

In diesem Verfahren wird beschrieben, wie das CiscoAVPair-Attribut aktualisiert wird. Die Syntax lautet `shell:roles="<role>"`.

1. Suchen Sie im Dialogfeld ADSI Edit (ADSI-Bearbeiten) den Benutzer, der Zugriff auf UCS

Central benötigt.

2. Klicken Sie mit der rechten Maustaste auf den Benutzer, und wählen Sie **Eigenschaften aus**.
3. Klicken Sie im Dialogfeld Eigenschaften auf die Registerkarte **Attributeditor**, klicken Sie auf **CiscoAVPair** und klicken Sie auf **Bearbeiten**.
4. Geben Sie im Dialogfeld Mehrwert-Zeichenfolgen-Editor den Wert **shell:roles="admin"** im Feld Werte ein, und klicken Sie auf **OK**.

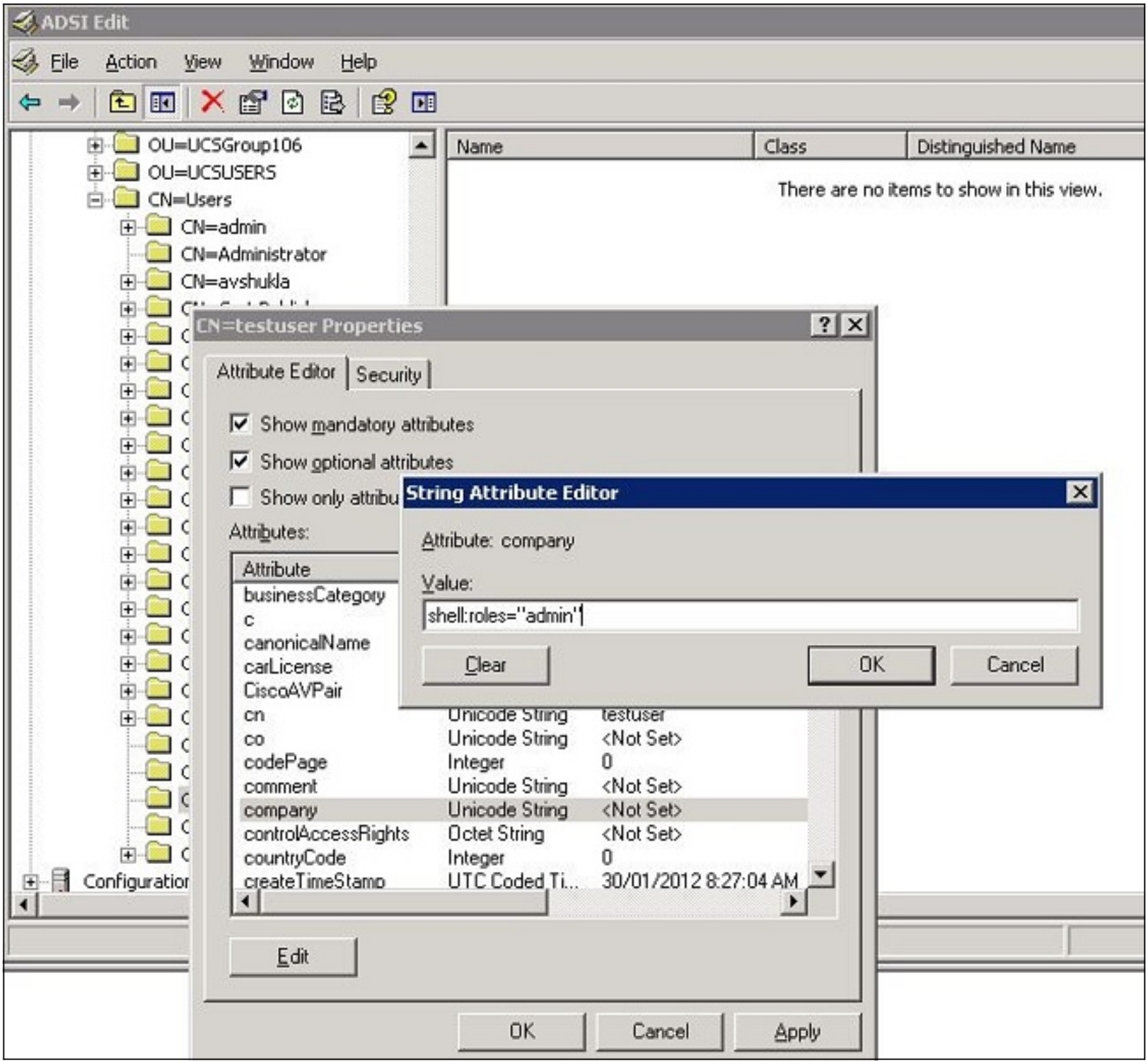


5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld Eigenschaften zu schließen.

Vordefinierte Attribute aktualisieren

In diesem Verfahren wird beschrieben, wie ein vordefiniertes Attribut aktualisiert wird, wobei die Rolle eine der vordefinierten Benutzerrollen in UCS Central ist. In diesem Beispiel wird das Attribut *company* verwendet, um die Rolle zu übergeben. Die Syntax lautet `shell:roles="<role>"`.

1. Suchen Sie im Dialogfeld ADSI Edit (ADSI-Bearbeiten) den Benutzer, der Zugriff auf UCS Central benötigt.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer, und wählen Sie **Eigenschaften aus**.
3. Klicken Sie im Dialogfeld Eigenschaften auf die Registerkarte **Attributeditor**, klicken Sie auf **Firma** und dann auf **Bearbeiten**.
4. Geben Sie im Dialogfeld Zeichenfolgenattribut-Editor den Wert **shell:roles="admin"** im Feld Wert ein, und klicken Sie auf **OK**.

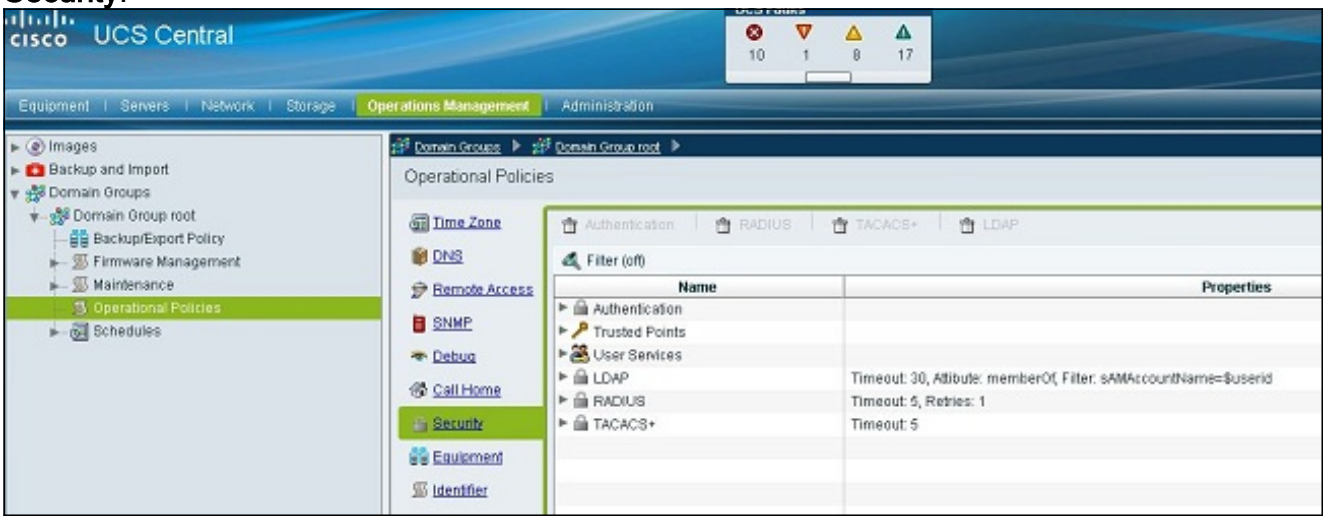


5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld Eigenschaften zu schließen.

Konfigurieren der LDAP-Authentifizierung in UCS Central

Die LDAP-Konfiguration in UCS Central wird unter Operations Management (Betriebsmanagement) abgeschlossen.

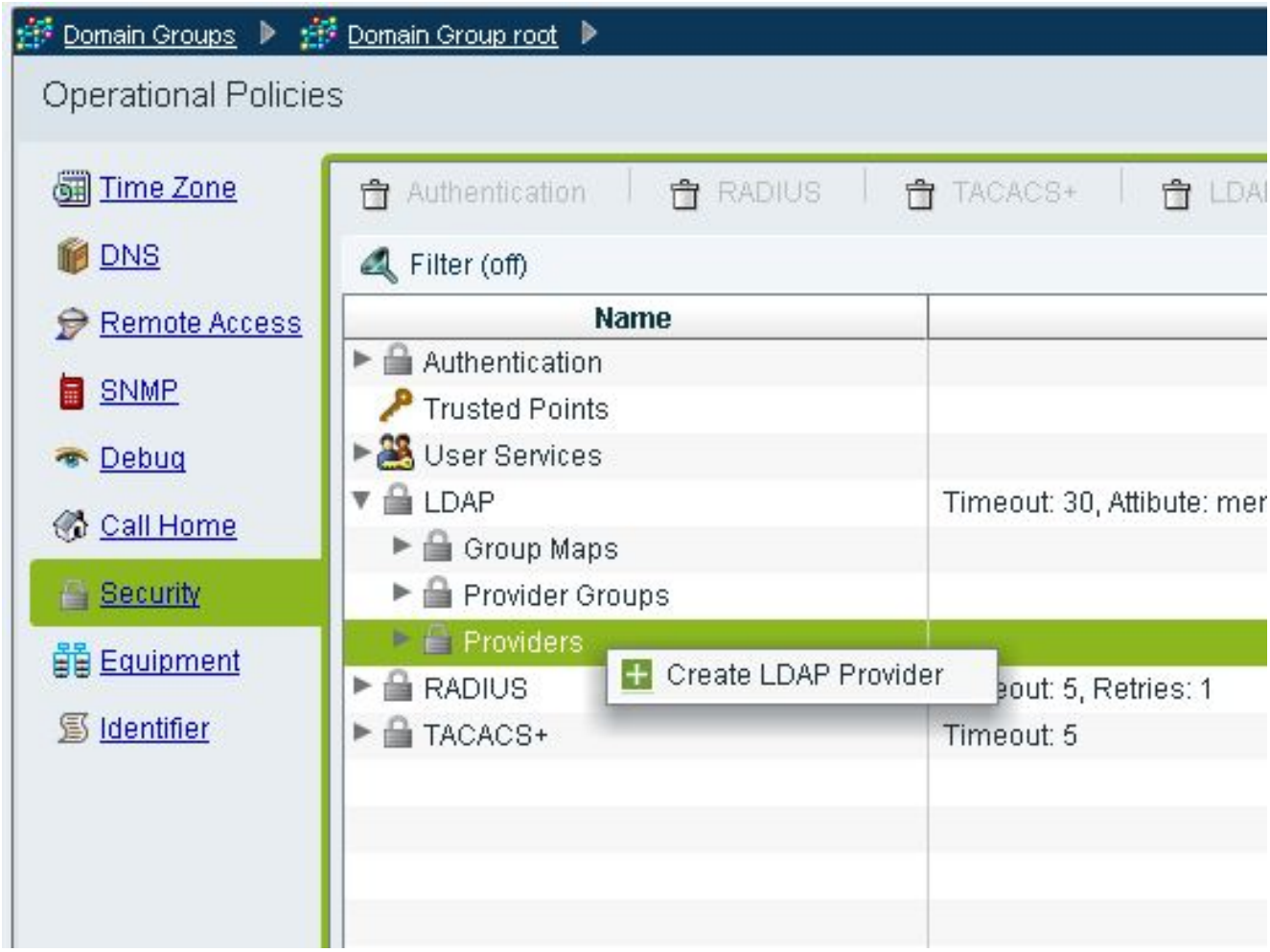
1. Melden Sie sich bei UCS Central unter einem lokalen Konto an.
2. Klicken Sie auf **Operations Management**, erweitern Sie **Domain Groups**, und klicken Sie auf **Operational Policies > Security**.



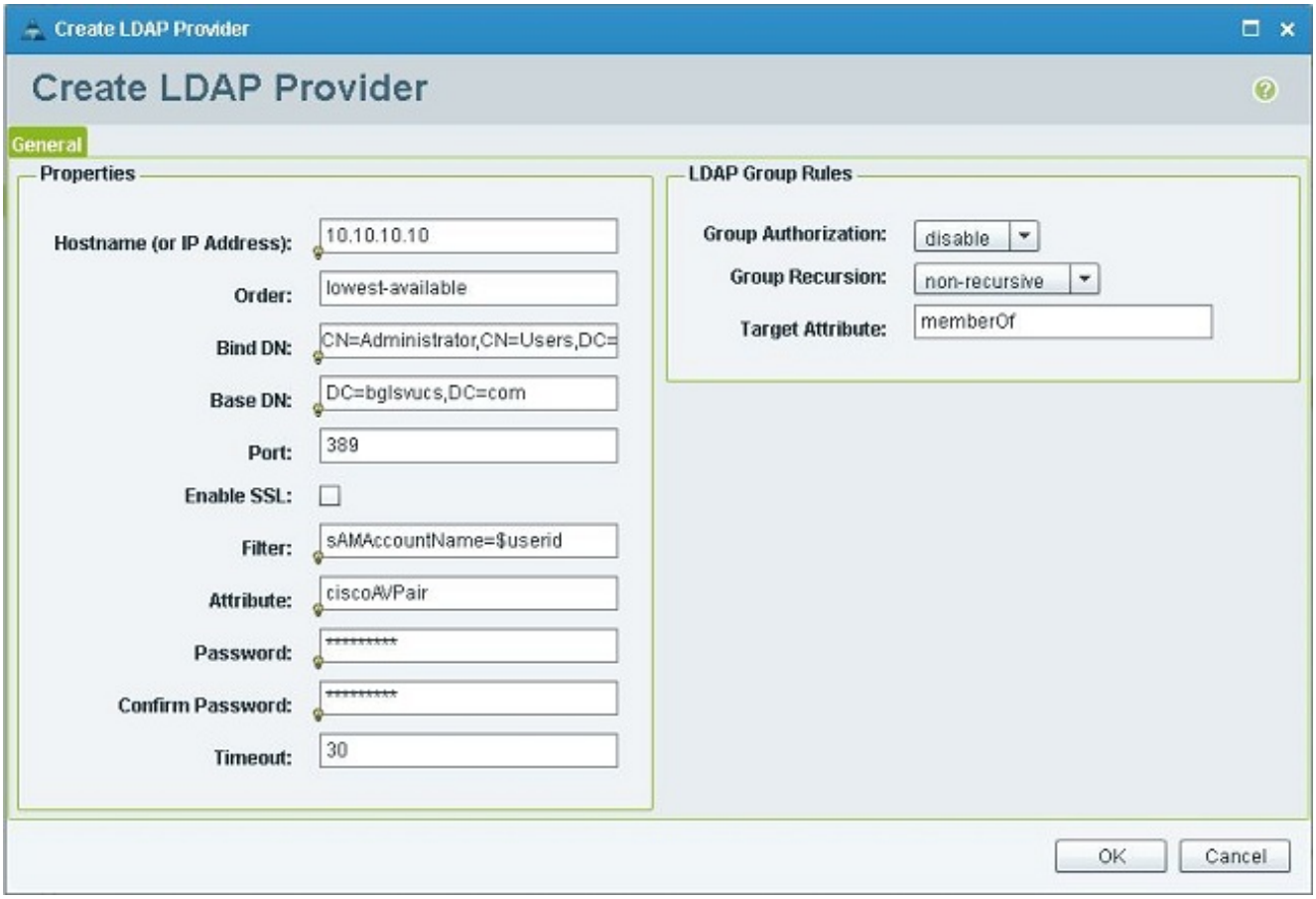
3. Gehen Sie wie folgt vor, um die LDAP-Authentifizierung zu konfigurieren:Konfigurieren Sie den LDAP-Anbieter.Konfigurieren Sie die LDAP-Anbietergruppe (nicht verfügbar in Version 1.0a).Ändern Sie die systemeigene Authentifizierungsregel.

LDAP-Anbieter konfigurieren

1. Klicken Sie auf **LDAP**, klicken Sie mit der rechten Maustaste auf **Provider**, und wählen Sie **LDAP-Anbieter erstellen aus**.



2. Fügen Sie im Dialogfeld LDAP-Provider erstellen die zuvor erfassten Details hinzu.Hostname oder IP des AnbietersBind-DNBasis-DNFilternAttribut (entweder CiscoAVPair oder ein vordefiniertes Attribut wieKennwort (Kennwort des Benutzers, der in der DN-Buchse verwendet
wird)



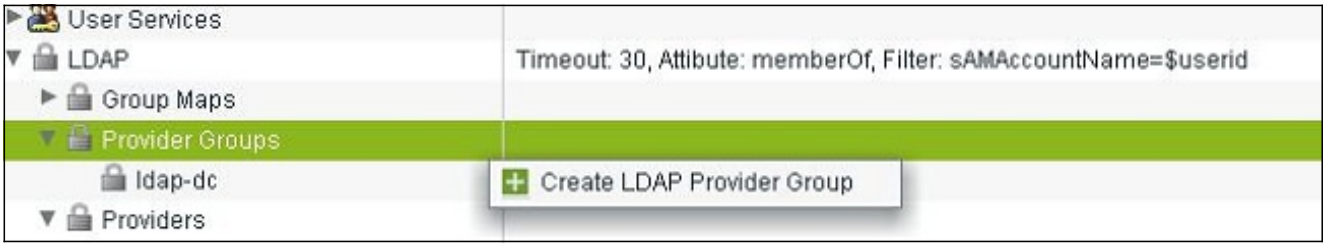
3. Klicken Sie auf **OK**, um die Konfiguration zu speichern und das Dialogfeld zu schließen.

Hinweis: Auf diesem Bildschirm muss kein anderer Wert geändert werden. Die LDAP-Gruppenregeln werden für die UCS Central-Authentifizierung in dieser Version nicht unterstützt.

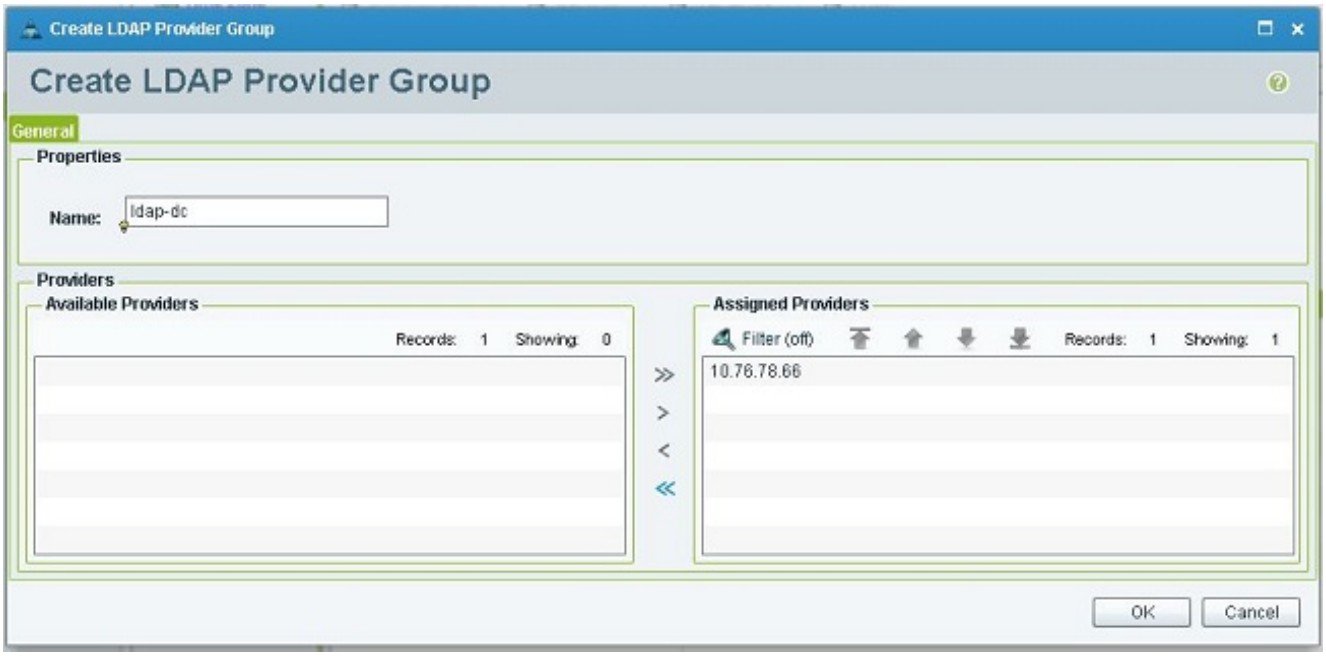
LDAP-Anbietergruppe konfigurieren

Hinweis: In Version 1.0a werden Anbietergruppen nicht unterstützt. In diesem Verfahren wird beschrieben, wie Sie eine Dummy-Anbietergruppe konfigurieren, die später in der Konfiguration verwendet wird.

1. Klicken Sie auf **LDAP**, klicken Sie mit der rechten Maustaste auf **Anbietergruppe**, und wählen Sie **LDAP-Anbietergruppe erstellen aus**.



2. Geben Sie im Dialogfeld Create LDAP Provider Group (LDAP-Anbietergruppe erstellen) im Feld Name den Namen für die Gruppe ein.
3. Wählen Sie in der Liste der verfügbaren Anbieter links den Anbieter aus, und klicken Sie auf das Größer-als-Symbol (**>**), um diesen Anbieter auf der rechten Seite in Zugewiesene Provider zu verschieben.



4. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Bildschirm zu schließen.

Native Authentifizierungsregel ändern

Version 1.0a unterstützt nicht mehrere Authentifizierungsdomänen wie in UCS Manager. Um dies zu umgehen, müssen Sie die systemeigene Authentifizierungsregel ändern.

Bei der nativen Authentifizierung kann die Authentifizierung für Standardanmeldungen oder Konsolenanmeldungen geändert werden. Da mehrere Domänen nicht unterstützt werden, können Sie entweder das lokale Konto oder ein LDAP-Konto verwenden, aber nicht beide. Ändern Sie den Wert von Realm, um entweder lokal oder LDAP als Authentifizierungsquelle zu verwenden.

1. Klicken Sie auf **Authentifizierung**, klicken Sie mit der rechten Maustaste auf **Native Authentication**, und wählen Sie **Eigenschaften aus**.
2. Bestimmen Sie, ob die Standardauthentifizierung, die Konsolenauthentifizierung oder beides gewünscht werden. Verwenden Sie die Standardauthentifizierung für die GUI und die Befehlszeilenschnittstelle (CLI). Verwenden Sie die Konsolenauthentifizierung für die KVM-Ansicht (Virtual Machine, virtuelles System), die auf einem Kernel basiert.
3. Wählen Sie **ldap** aus der Dropdown-Liste Bereich aus. Der Wert von Realm bestimmt, ob lokal oder LDAP die Authentifizierungsquelle
   ist.

4. Klicken Sie auf **OK**, um die Seite zu schließen.
5. Klicken Sie auf der Seite Policies (Richtlinien) auf **Save (Speichern)**, wenn erforderlich, um die Änderungen zu speichern.

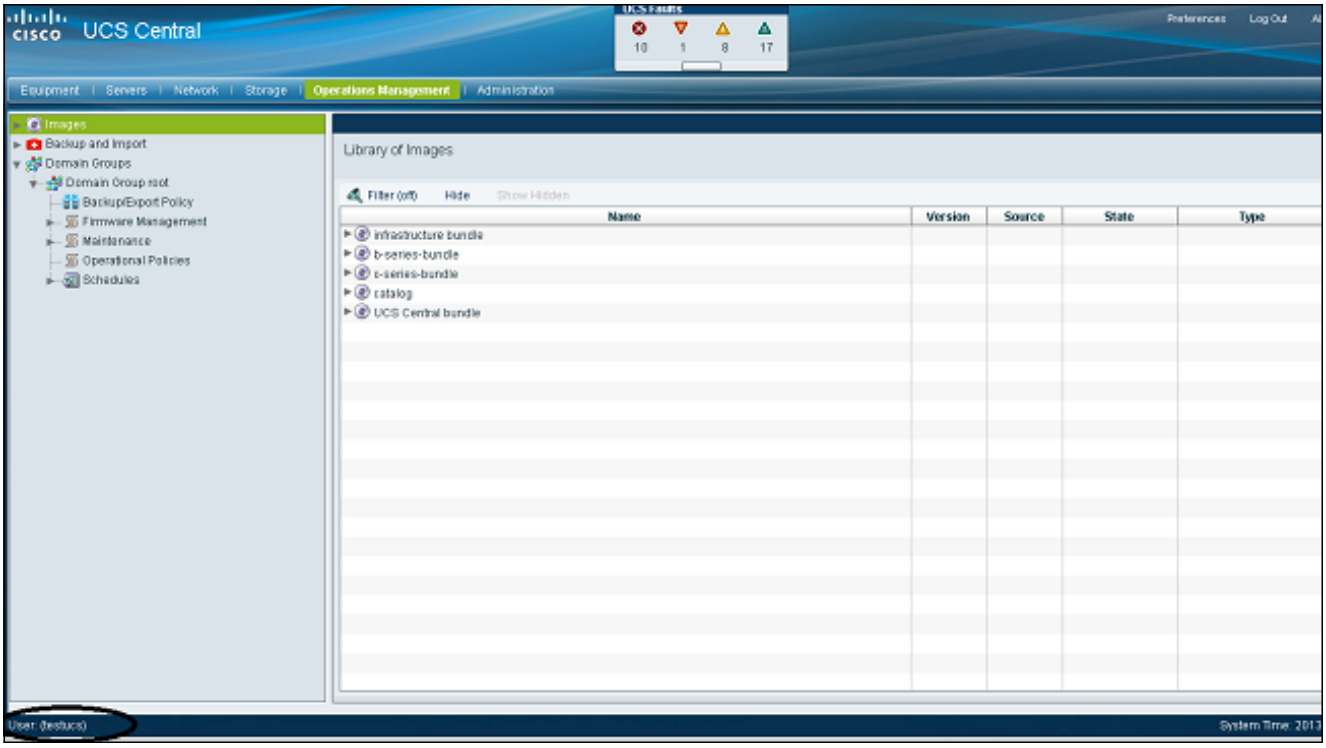
Hinweis: Melden Sie sich erst dann von Ihrer aktuellen Sitzung ab, oder ändern Sie die Konsolenauthentifizierung, wenn Sie überprüfen, ob die LDAP-Authentifizierung ordnungsgemäß funktioniert. Die Konsolenauthentifizierung bietet die Möglichkeit, zur vorherigen Konfiguration zurückzukehren. Weitere Informationen finden Sie im Abschnitt "Überprüfen".

Überprüfen

Dieses Verfahren beschreibt, wie die LDAP-Authentifizierung getestet wird.

1. Öffnen Sie in UCS Central eine neue Sitzung, und geben Sie Benutzername und Kennwort ein. Sie müssen keine Domäne oder kein Zeichen vor dem Benutzernamen einfügen. In diesem Beispiel werden Testgeräte als Benutzer aus der Domäne verwendet.

2. Die LDAP-Authentifizierung ist erfolgreich, wenn Sie das UCS Central-Dashboard sehen. Der Benutzer wird unten auf der Seite
angezeigt.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems