LDAP-verificatievoorbeeld voor UCS Central

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de Lichtgewicht Directory Access Protocol (LDAP)-verificatie voor Cisco Unified Computing System (UCS) Central. De procedures gebruiken de UCS Central grafische gebruikersinterface (GUI), een voorbeelddomein van bglucs.com en een voorbeeldgebruikersnaam voor de testgebruiker.

In versie 1.0 van de UCS Central-software is LDAP het enige op afstand gebaseerde echtheidsprotocol dat wordt ondersteund. Versie 1.0 biedt zeer beperkte ondersteuning voor externe verificatie en LBP-configuratie voor de UCS Central zelf. U kunt echter wel UCS Central gebruiken om alle opties voor de UCS Manager-domeinen te configureren die door UCS Central worden beheerd.

Beperkingen van UCS Central-verificatie op afstand omvatten:

- RADIUS en TACACS worden niet ondersteund.
- De LBP-groepstoewijzing voor roltoewijzing en LBP-groepen voor meerdere

domeincontrollers worden niet ondersteund.
- LDAP gebruikt alleen de Cisco AVPair-eigenschap of elke ongebruikte eigenschap om de rol te vervullen. De doorgegeven rol is één van de vooraf gedefinieerde taken in de lokale UCS Central-databank.
- Meervoudige authenticatiedomeinen/protocollen worden niet ondersteund.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- UCS Central wordt ingezet.
- Microsoft Active Directory wordt geïmplementeerd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- UCS Central versie 1.0
- Microsoft Active Directory

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Verzamelinformatie

Deze sectie vat de informatie samen die u moet verzamelen voordat u de configuratie start.

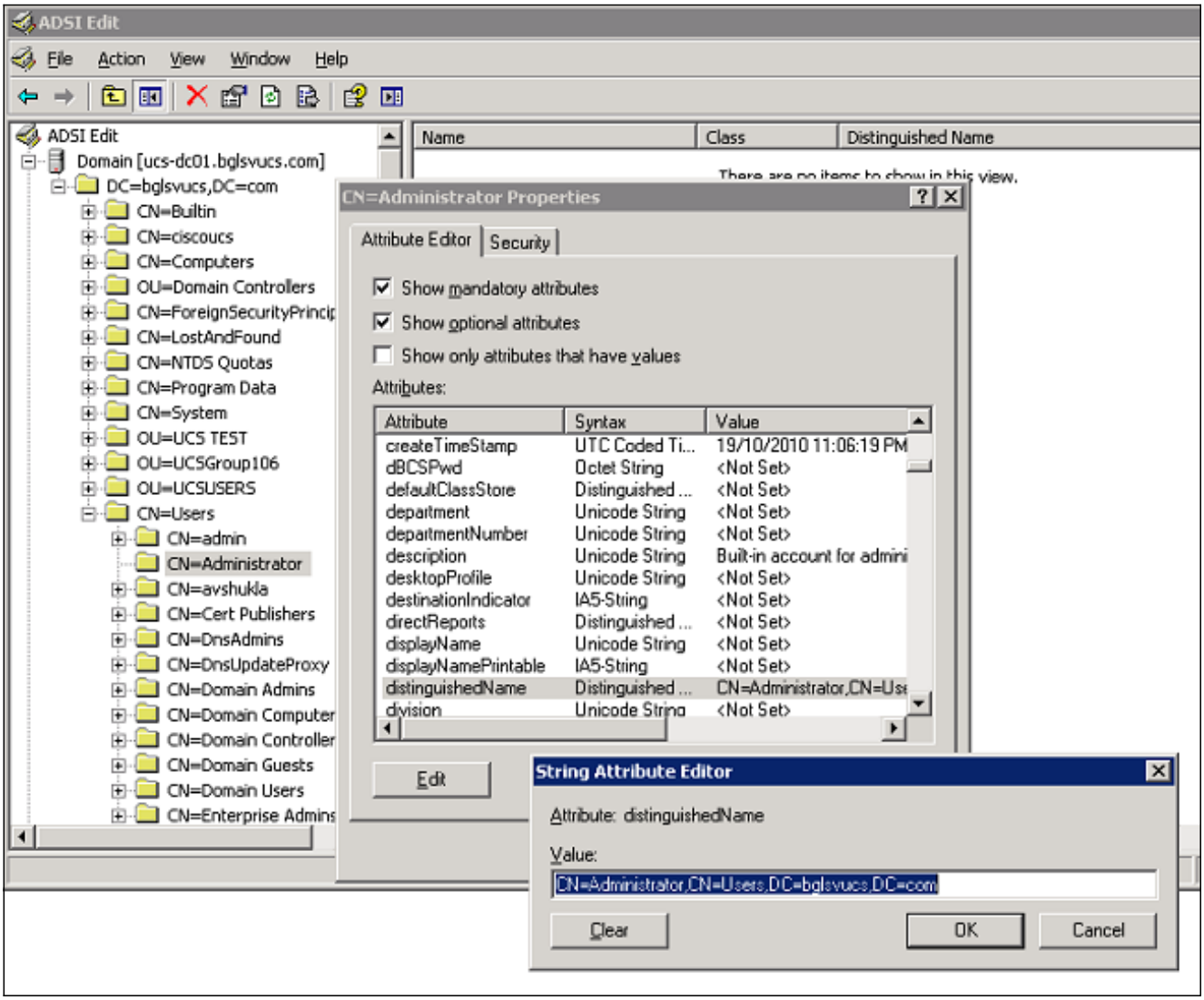
Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Bind gebruikersgegevens

Bindgebruiker kan elke gebruiker van de LDAP in het domein zijn die toegang tot het domein heeft gelezen; voor de configuratie van de LDAP is een gebruiker vereist. UCS Central gebruikt de gebruikersnaam en het wachtwoord van de gebruiker om de actieve map (AD) aan te sluiten en te vragen voor gebruikersverificatie enzovoort. Dit voorbeeld gebruikt de Administrator-account als gebruiker.

In deze procedure wordt beschreven hoe een LDAP-beheerder de ADSI-editor (Active Directory Service Interfaces) kan gebruiken om de DNS te vinden.

1. Open de ADSI-editor.
2. Vind de bind gebruiker. De gebruiker bevindt zich op hetzelfde pad als in de AD.
3. Klik met de rechtermuisknop op de gebruiker en kies **Eigenschappen**.
4. Dubbelklik in het dialoogvenster Eigenschappen op **voornaam**.
5. Kopieer de DNA uit het veld
   Waarde.



6. Klik op **Annuleren** om alle vensters te sluiten.

Om het wachtwoord voor de gebruiker te verkrijgen, neemt u contact op met de AD-beheerder.

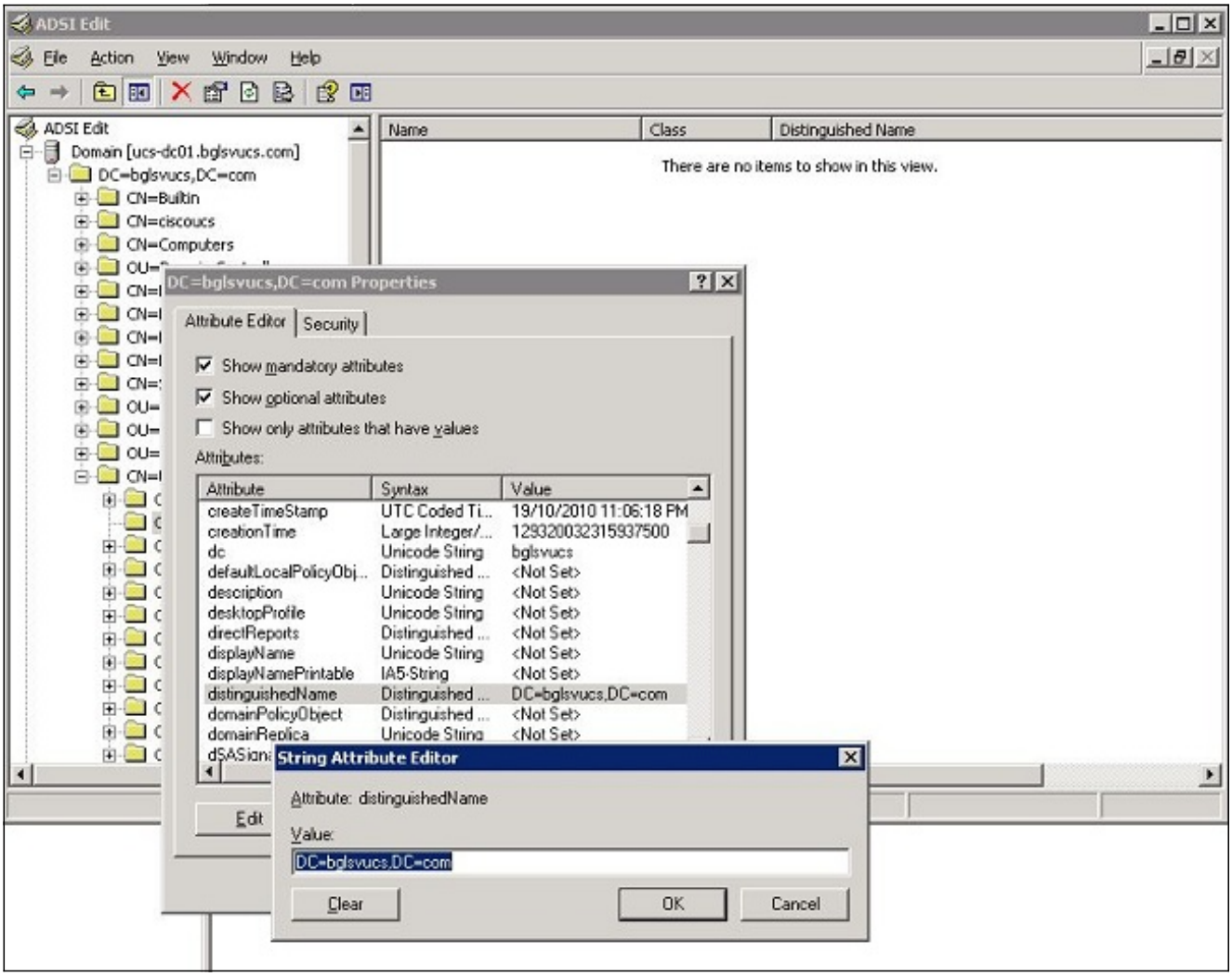
Base-D-details

Base DN is de DN van de organisatorische eenheid (OU) of de container waar de zoektocht naar de gebruiker en gebruikersdetails begint. U kunt de DNA van een OU gebruiken die in de AD is gemaakt voor UCS of UCS Central. U kunt het echter eenvoudiger vinden om de DN te gebruiken voor de domeinwortel zelf.

In deze procedure wordt beschreven hoe een LDAP-beheerder de ADSI-editor kan gebruiken om de Base DN-basis te vinden.

1. Open de ADSI-editor.
2. Zoek de OU of de container die gebruikt wordt als de basis DNA.
3. Klik met de rechtermuisknop op de OU of de container en kies **Eigenschappen**.

4. Dubbelklik in het dialoogvenster Eigenschappen op **voornaam**.
5. Kopieert de DNA-toets uit het waardenveld en noteer alle andere details die u nodig hebt.



6. Klik op **Annuleren** om alle vensters te sluiten.

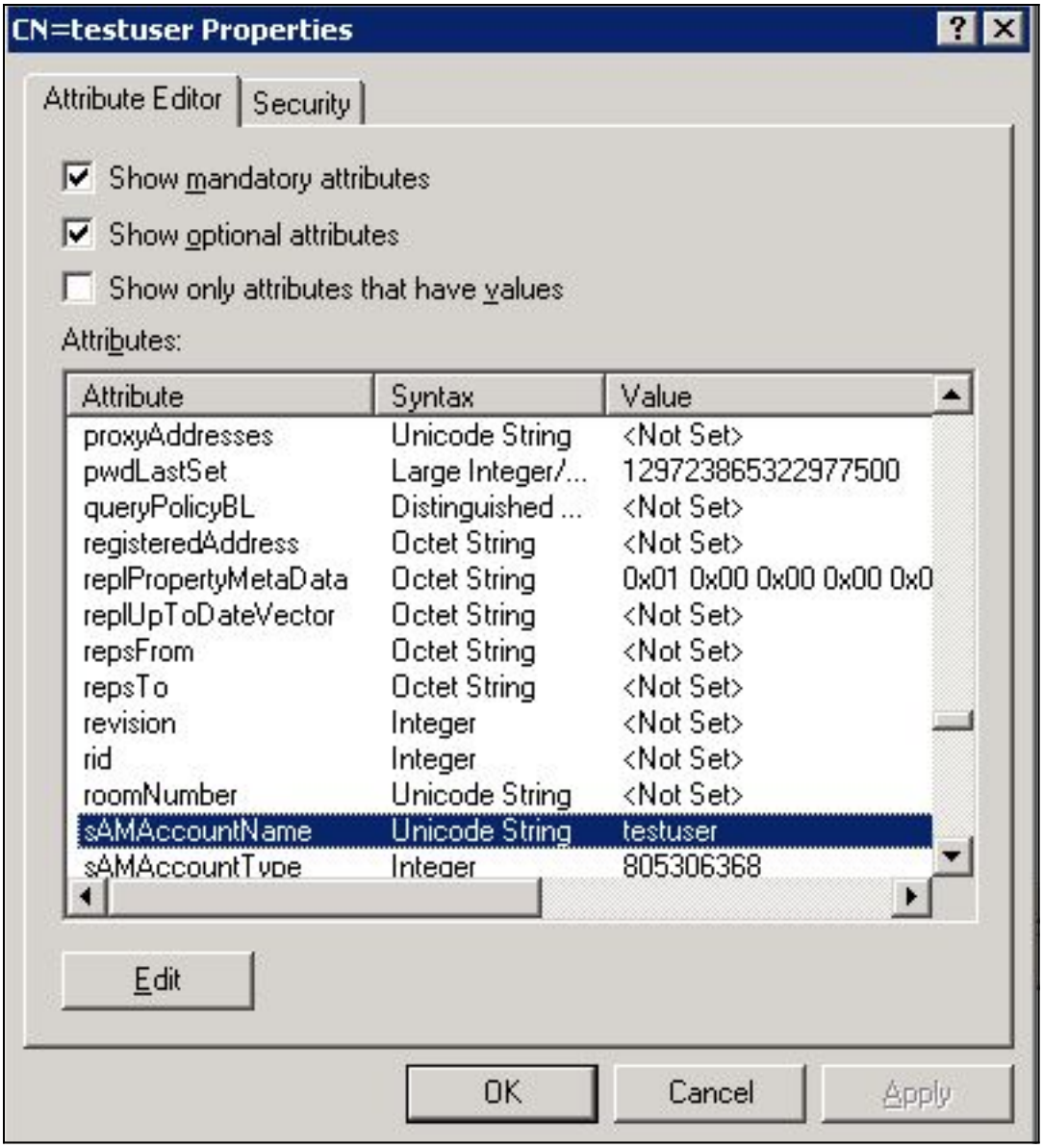
Gegevens van providers

De aanbieder speelt een sleutelrol bij de authenticatie en autorisatie van de LGO in UCS Central. De leverancier is één van de AD servers die UCS Central vragen om de gebruiker te zoeken en te authentiseren en om gebruikersdetails zoals rolinformatie te krijgen. Verzeker u ervan dat u de hostnaam of IP-adres van de AD-server van de leverancier verzamelt.

Filtereigenschap

Het filterveld of de eigenschap wordt gebruikt om de AD-database te doorzoeken. De gebruiker-ID die bij de inlognaam is ingevoerd, wordt teruggegeven naar de AD en vergeleken met het filter.

U kunt sAMAaccountName=$userid gebruiken als de filterwaarde. NetAMAaccountName is een eigenschap in het AD en heeft dezelfde waarde als de AD-gebruiker-ID, die wordt gebruikt om in te loggen op de UCS Central GUI.



Eigenschappen toevoegen en instellen

Deze sectie vat de informatie samen die u nodig hebt om de Cisco AVPair eigenschap (indien nodig) toe te voegen en de Cisco AVPair eigenschap of andere, vooraf gedefinieerde eigenschap bij te werken voordat u de LAN configuratie start.

Het attributieveld specificeert de AD eigenschap (onder de gebruikerseigenschap), die de rol teruggeeft die aan de gebruiker moet worden toegewezen. In release 1.0a van de UCS Central-software kan ofwel de aangepaste eigenschap Cisco AVPair of een andere ongebruikte eigenschap in de AD worden geüpload om deze rol te vervullen.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

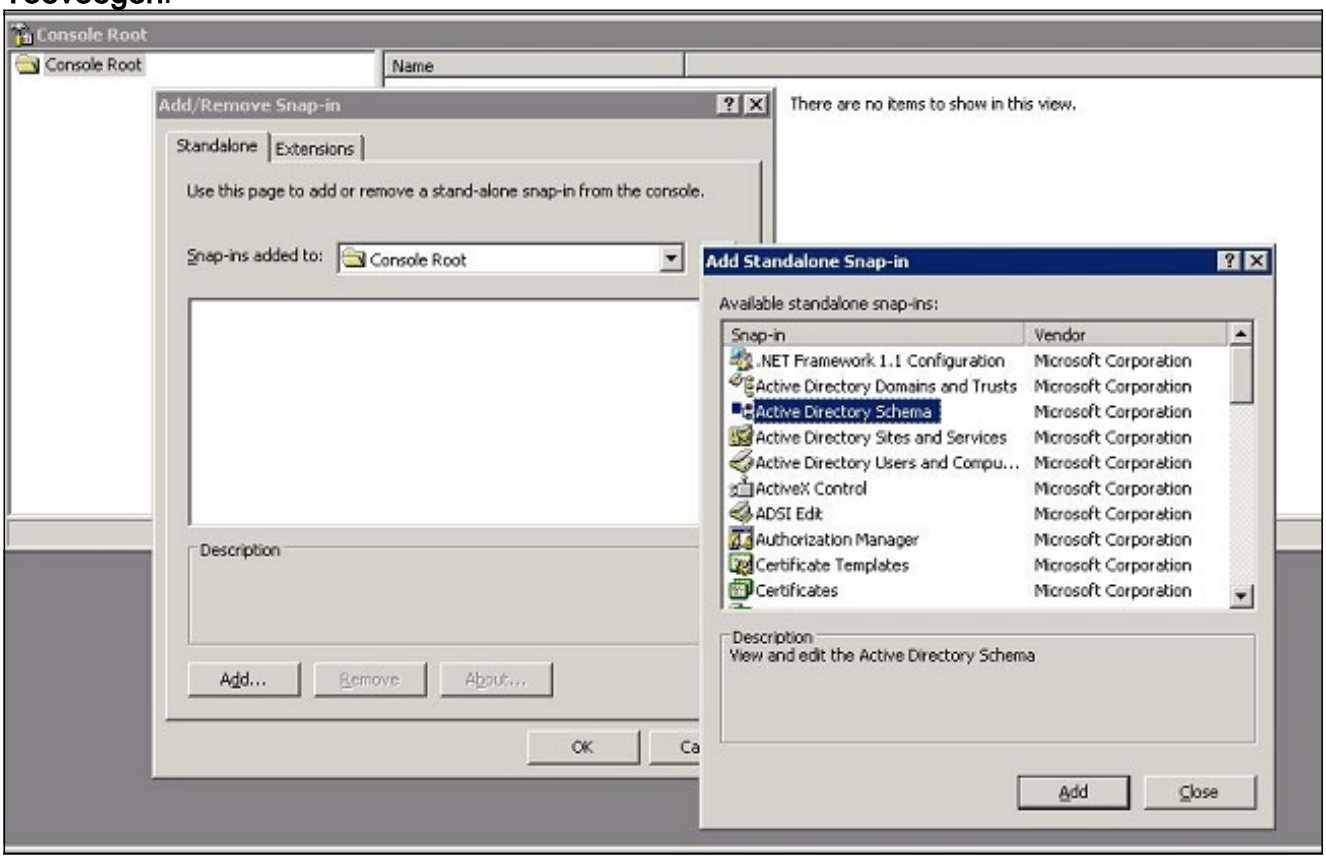
Cisco AVP-kenmerken toevoegen

Om een nieuwe eigenschap aan het domein toe te voegen, breidt het schema van het domein uit, en voegt de eigenschap toe aan de klasse (die, in dit voorbeeld, gebruiker is).

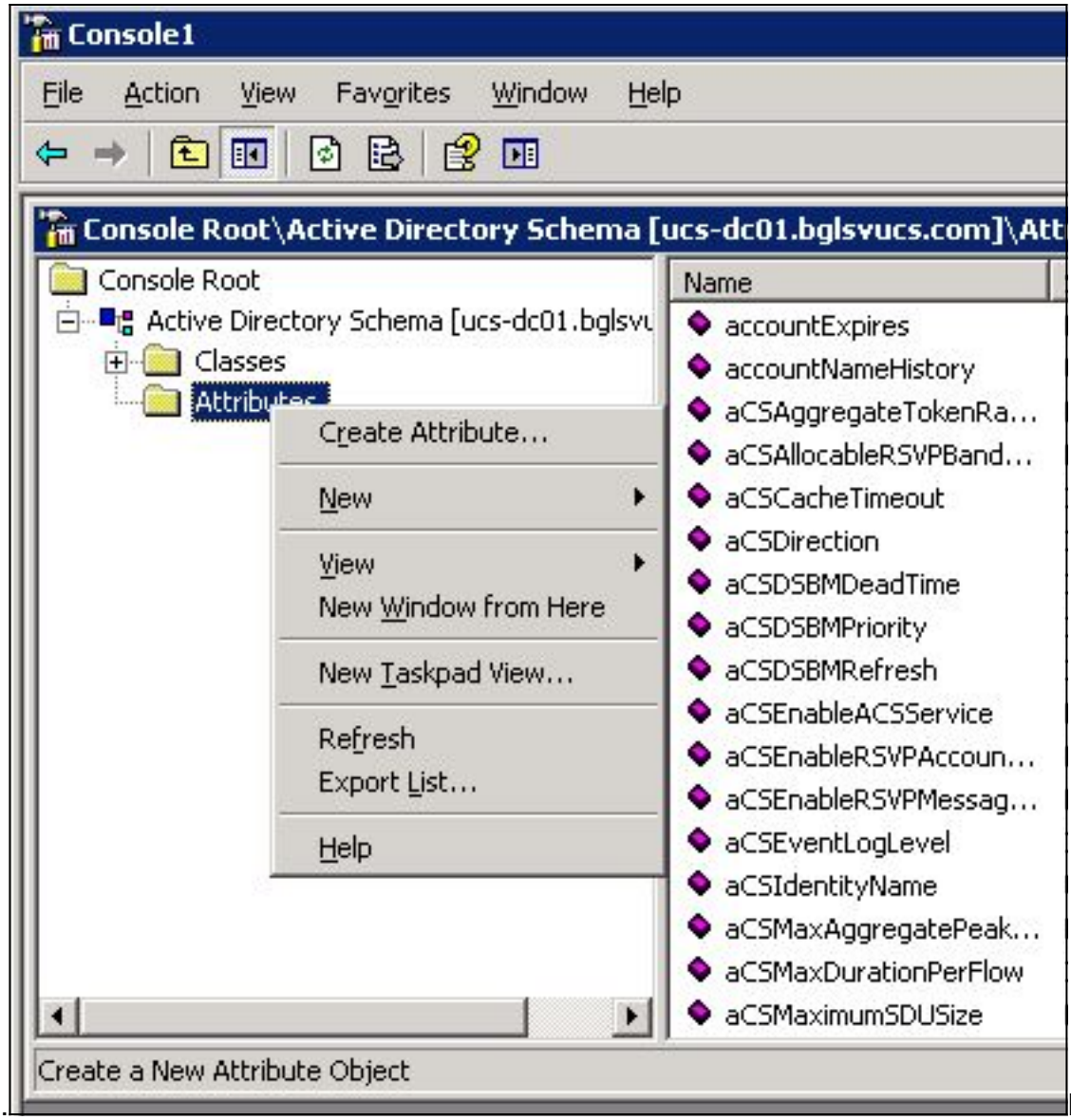
Deze procedure beschrijft hoe u het schema op een Windows AD-server kunt uitvouwen en de

eigenschap Cisco AVPair kunt toevoegen.

1. Meld u aan bij een AD-server.
2. Klik op **Start > Start**, type **mmc** en druk **op** ENTER om een lege Microsoft Management Console (MMC)-console te openen.
3. Klik in de MMC op **Bestand > Toevoegen/Verwijderen Magnetisch-in > Toevoegen**.
4. In het dialoogvenster Magnetisch in toevoegen selecteert u het **programma** voor **actieve map** en vervolgens klikt u op **Toevoegen**.

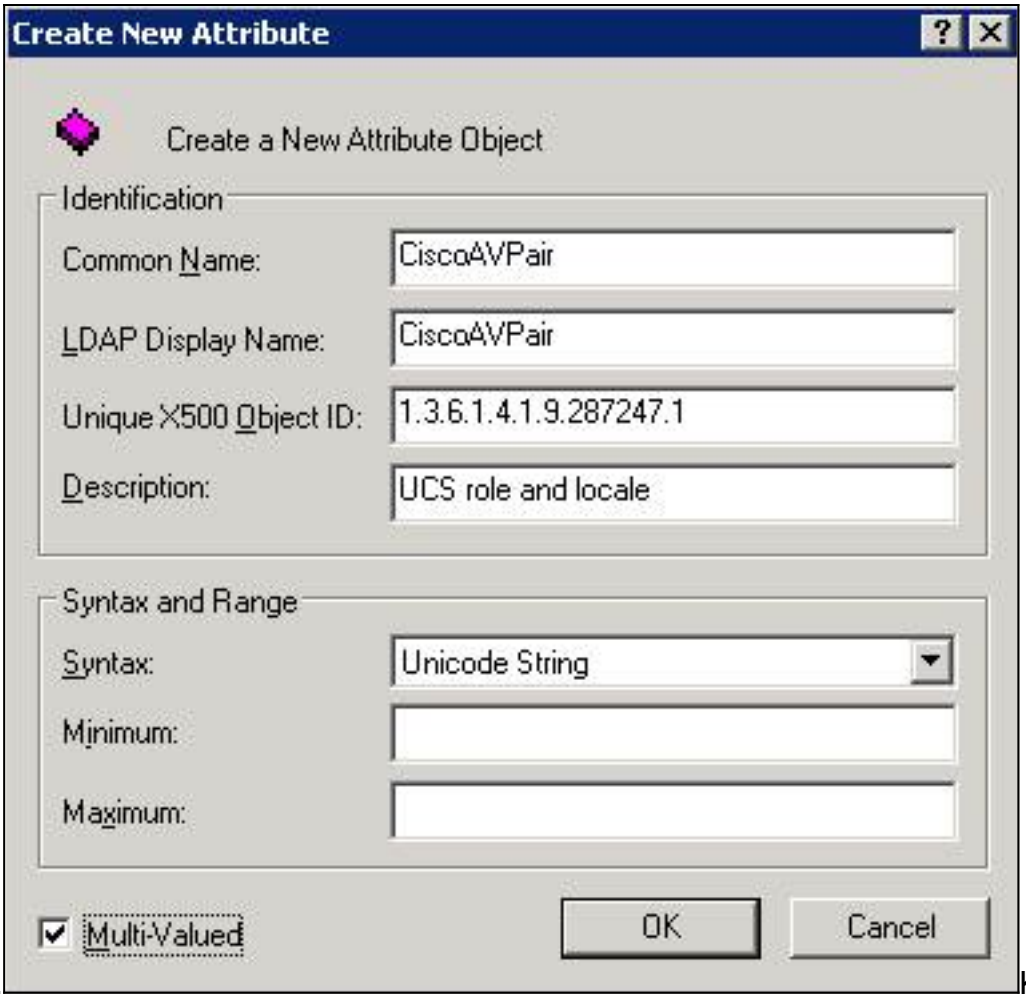


5. In MMC, breid **Active Directory Schema** uit, klik met de rechtermuisknop op **Eigenschappen** en kies **Eigenschappen**



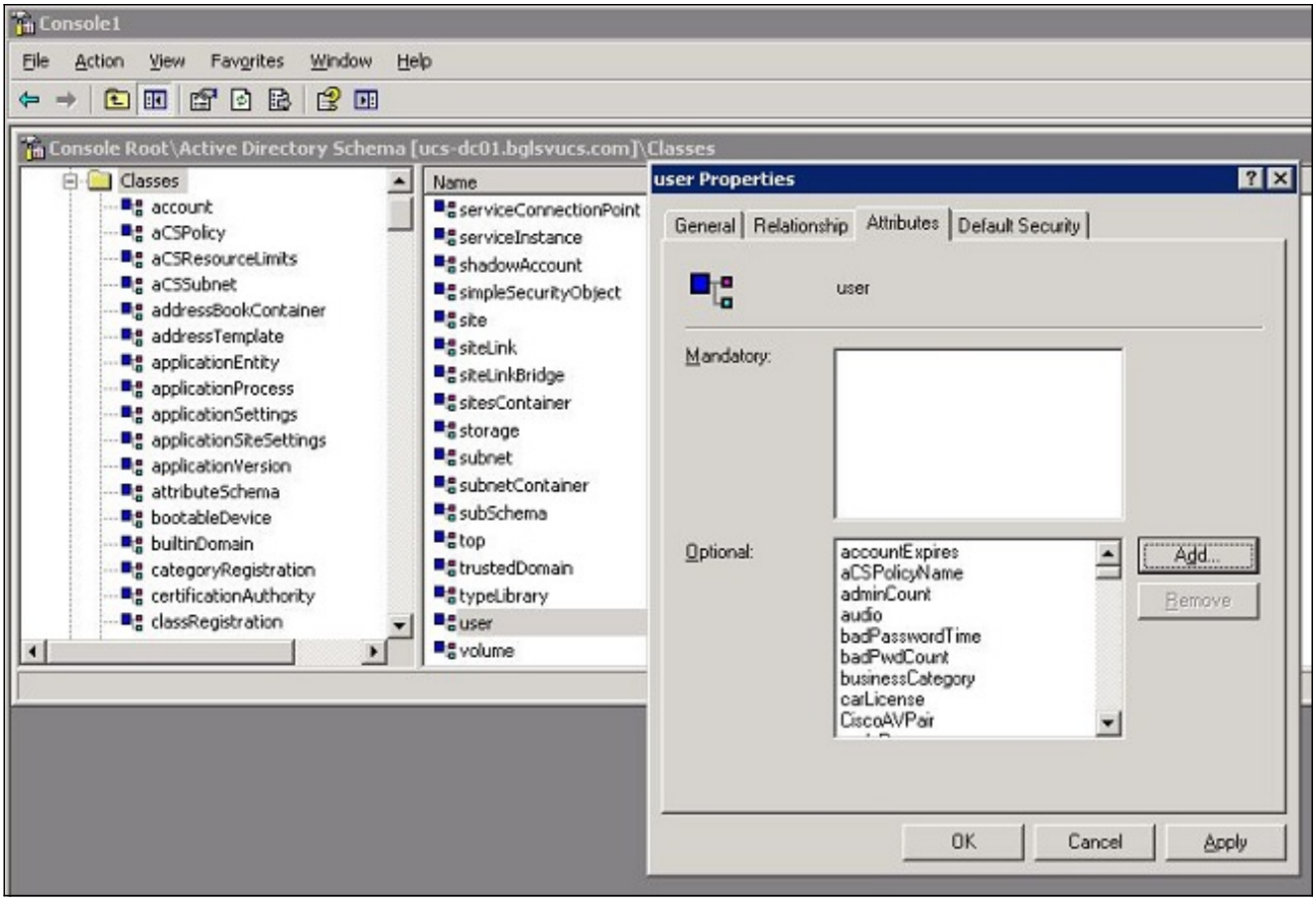
maken.Het dialoogvenster Nieuwe kenmerk maken verschijnt

6. Maak een eigenschap die Cisco AVPair heet in de verre authenticatieservice.Typ in de velden Naam en Naam van de ABBYY genoemde naam **CiscoAVPair**.Voer in het veld unieke 500 object-ID **1.3.6.1.4.1.9.287247.1 in**.Voer in het veld Description de **UCS-rol en het lokale toetsenbord in**.Selecteer in het veld Syntax de optie **Unicode**-string uit de

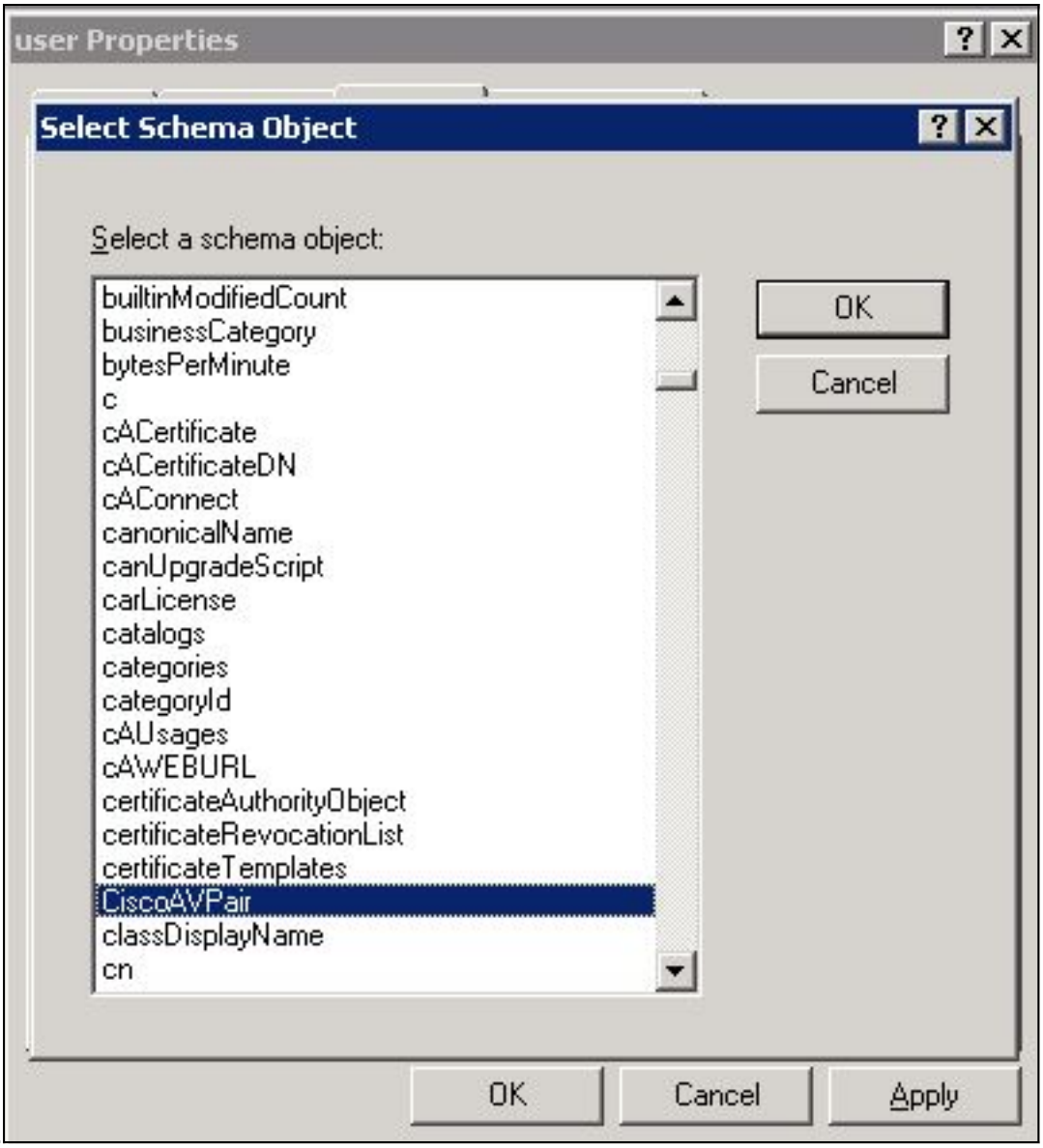


vervolgkeuzelijst.Klik op **OK** om de eigenschap op te slaan en het dialoogvenster te sluiten.Zodra de eigenschap aan het schema wordt toegevoegd, moet het in kaart worden gebracht of in de gebruikersklasse worden opgenomen. Hiermee kunt u de gebruikerseigenschap bewerken en de waarde specificeren die moet worden doorgegeven.

7. In de zelfde MMC die voor de uitbreiding van het schema van de AD wordt gebruikt, **Klasse** uitvouwen, **gebruiker met de** rechtermuisknop klikken, en **Eigenschappen** kiezen.
8. Klik in het dialoogvenster Gebruikerseigenschappen op het tabblad **Eigenschappen** en klik op
Toevoegen.

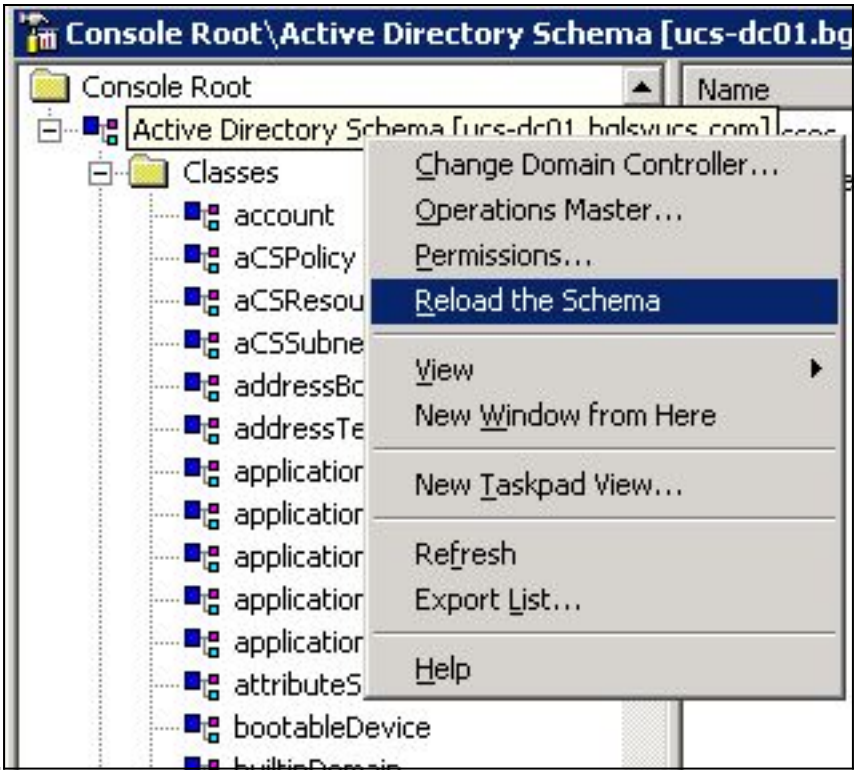


9. In het dialoogvenster Schema object selecteren klikt u op **Cisco AVPair** en vervolgens klikt u



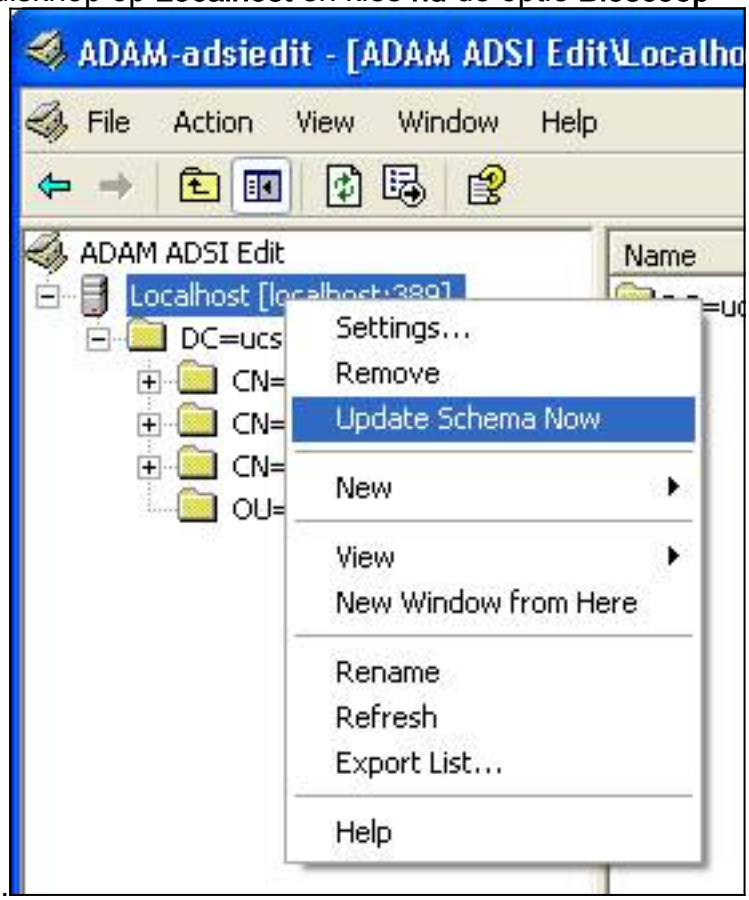
op **OK**.

10. Klik in het dialoogvenster Gebruikerseigenschappen op **Toepassen**.
11. Klik met de rechtermuisknop op **Actief Map-schema** en kies **Herladen van de Schema** om de nieuwe wijzigingen op te



nemen.

12. Gebruik indien nodig de ADSI-editor om het schema bij te werken. Klik met de rechtermuisknop op **Localhost** en kies **nu** de optie **Bioscoop**



bijwerken.

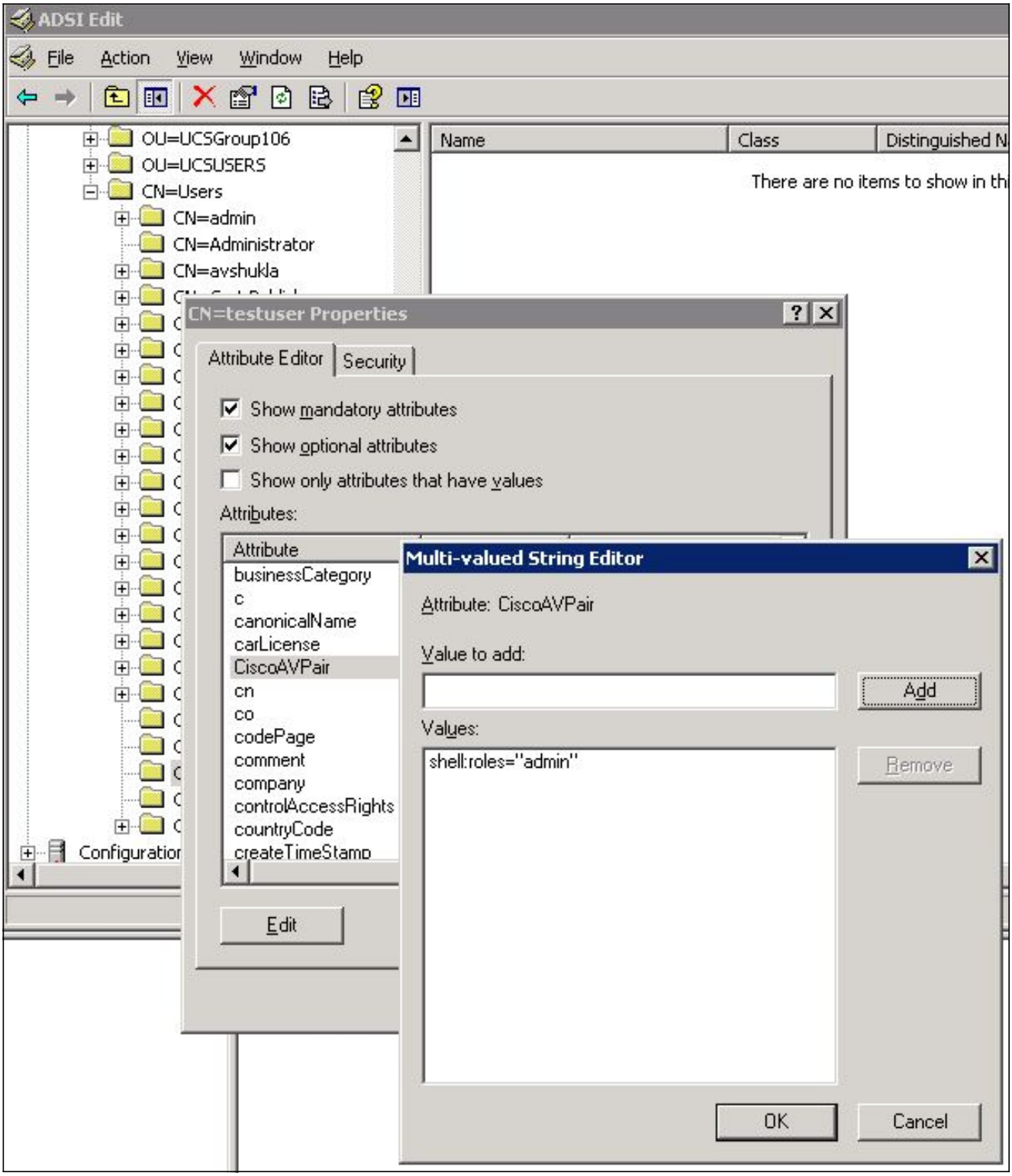
Cisco AVPair-kenmerk bijwerken

Deze procedure beschrijft hoe de eigenschap Cisco AVPair moet worden bijgewerkt. De syntaxis is is `shell:rollen="<rol>"`.

1. In het dialoogvenster ADSI Bewerken kunt u de gebruiker vinden die toegang tot UCS

Central nodig heeft.

2. Klik met de rechtermuisknop op de gebruiker en kies **Eigenschappen**.
3. Klik in het dialoogvenster Eigenschappen op het tabblad **Lijst met kenmerken** en klik op **Cisco AVPair** en klik op **Bewerken**.
4. Typ in het dialoogvenster Taleneditor met meerdere waarden de waarde **shell:rollen="admin"** in het veld Waarden en klik op **OK**.



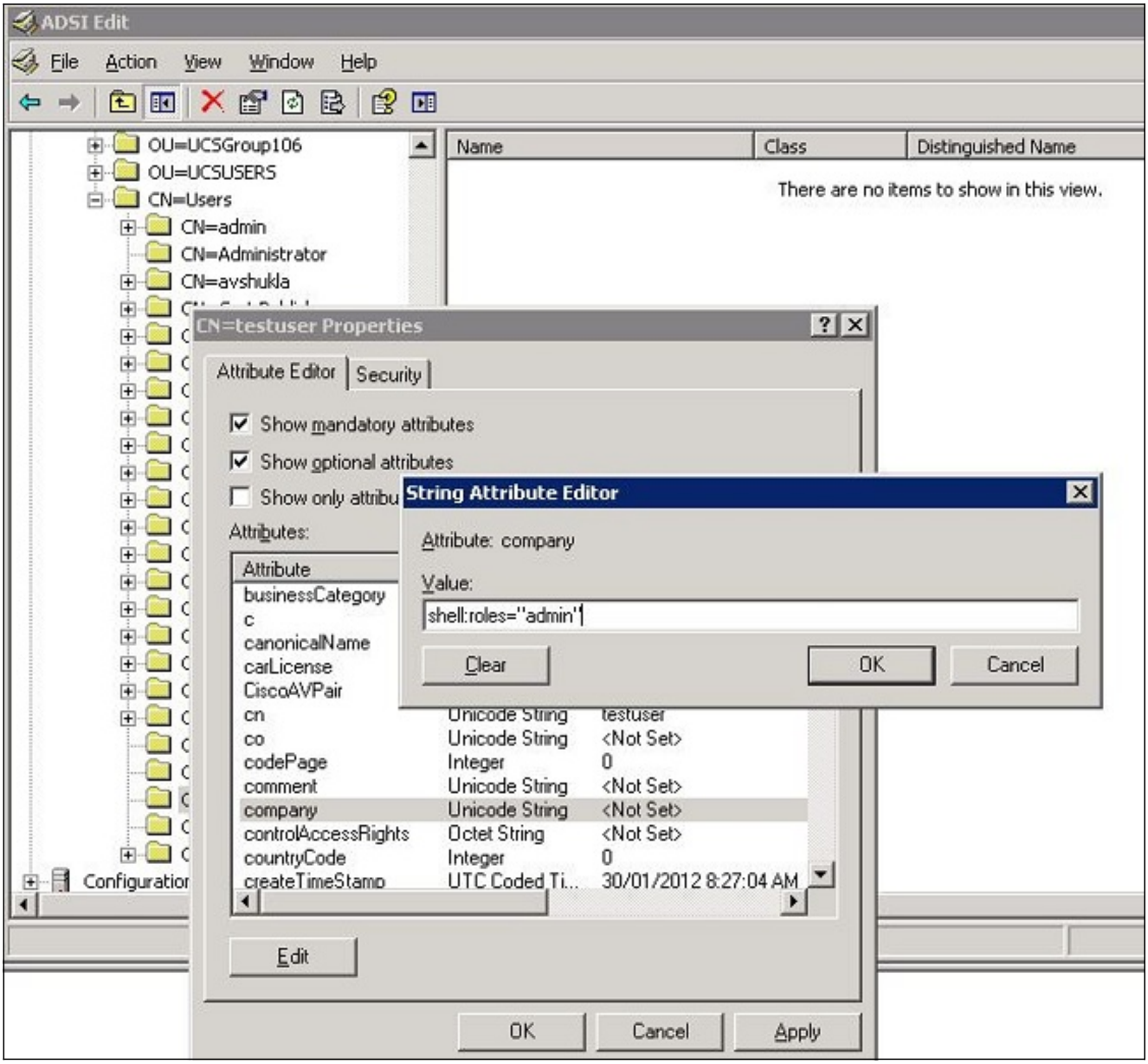
5. Klik op **OK** om de wijzigingen op te slaan en het dialoogvenster Eigenschappen te sluiten.

Vooraf gedefinieerde eigenschap bijwerken

In deze procedure wordt beschreven hoe een vooraf gedefinieerd kenmerk moet worden

bijgewerkt, waarbij de rol een van de vooraf gedefinieerde gebruikersrollen in UCS Central is. Dit voorbeeld gebruikt de *vennootschap* van de eigenschap om de rol te vervullen. De syntaxis is is `shell:rollen="<rol>"`.

1. In het dialoogvenster ADSI Bewerken, dient u de gebruiker te vinden die toegang tot de UCS Central-unit nodig heeft.
2. Klik met de rechtermuisknop op de gebruiker en kies **Eigenschappen**.
3. Klik in het dialoogvenster Eigenschappen op het tabblad **Lijst** van **kenmerken**, klik op **bedrijf** en klik op **Bewerken**.
4. In het dialoogvenster Lijst met string-kenmerken voert u het **waardepagina:rollen="admin"** in het veld Waarde in en klikt u op **OK**.



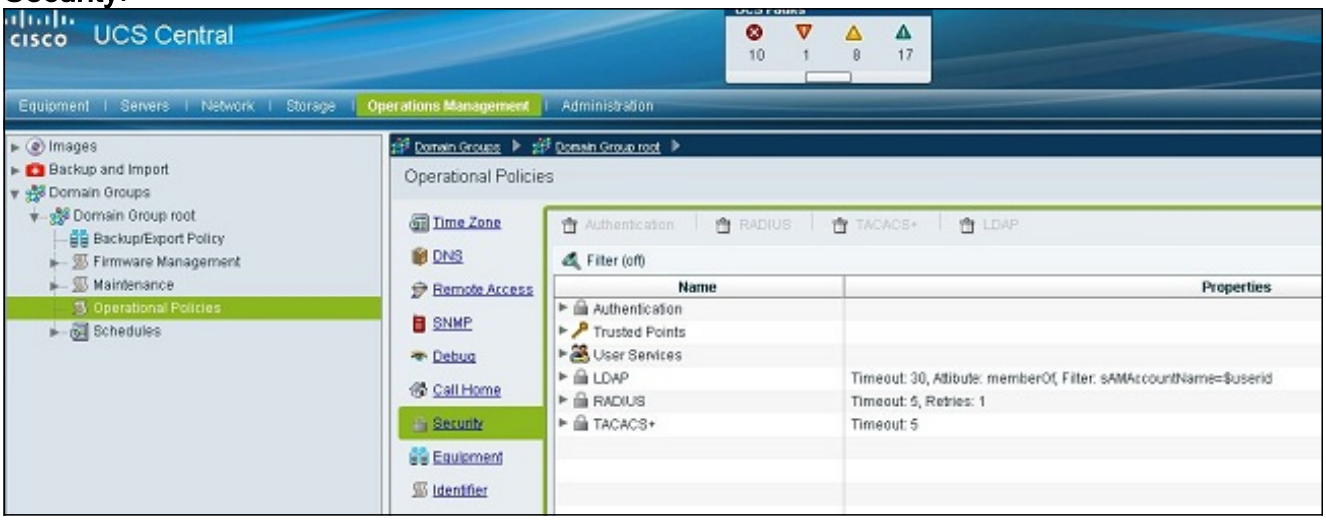
5. Klik op **OK** om de wijzigingen op te slaan en het dialoogvenster Eigenschappen te sluiten.

LDAP-verificatie op UCS Central configureren

De LDAP-configuratie in UCS Central wordt voltooid onder Operations Management.

1. Meld u aan bij UCS Central onder een lokale account.

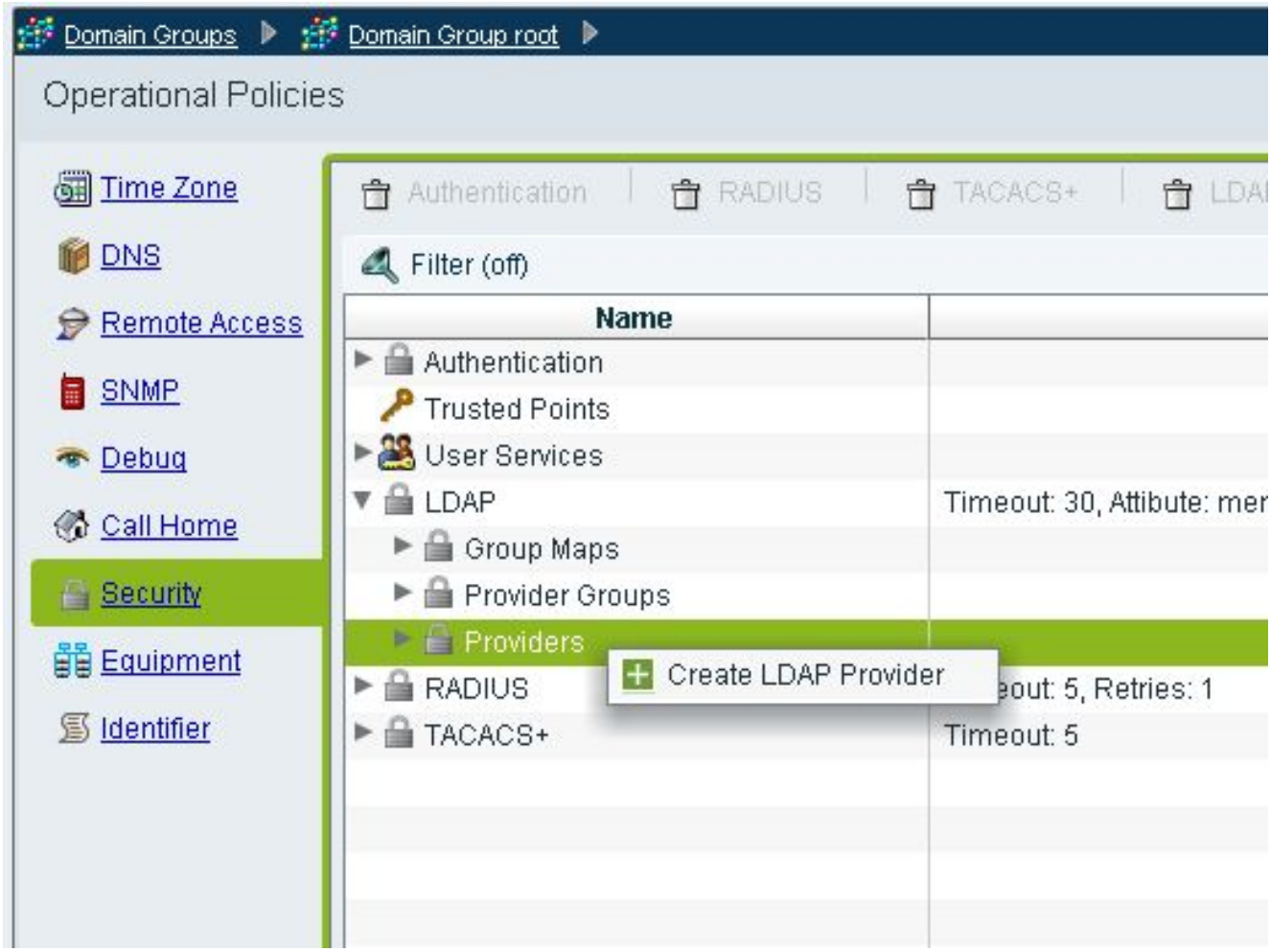
2. Klik op **Operations Management**, breid **domeingroepen uit** en klik op **Operationeel beleid > Security**.



3. Voer de volgende stappen uit om de authenticatie van de LDAP te configureren:Configureer de LDAP provider.Configureer de gebruikersgroep (niet beschikbaar in release 1.0a).Verander de inheemse authentificatieregel.

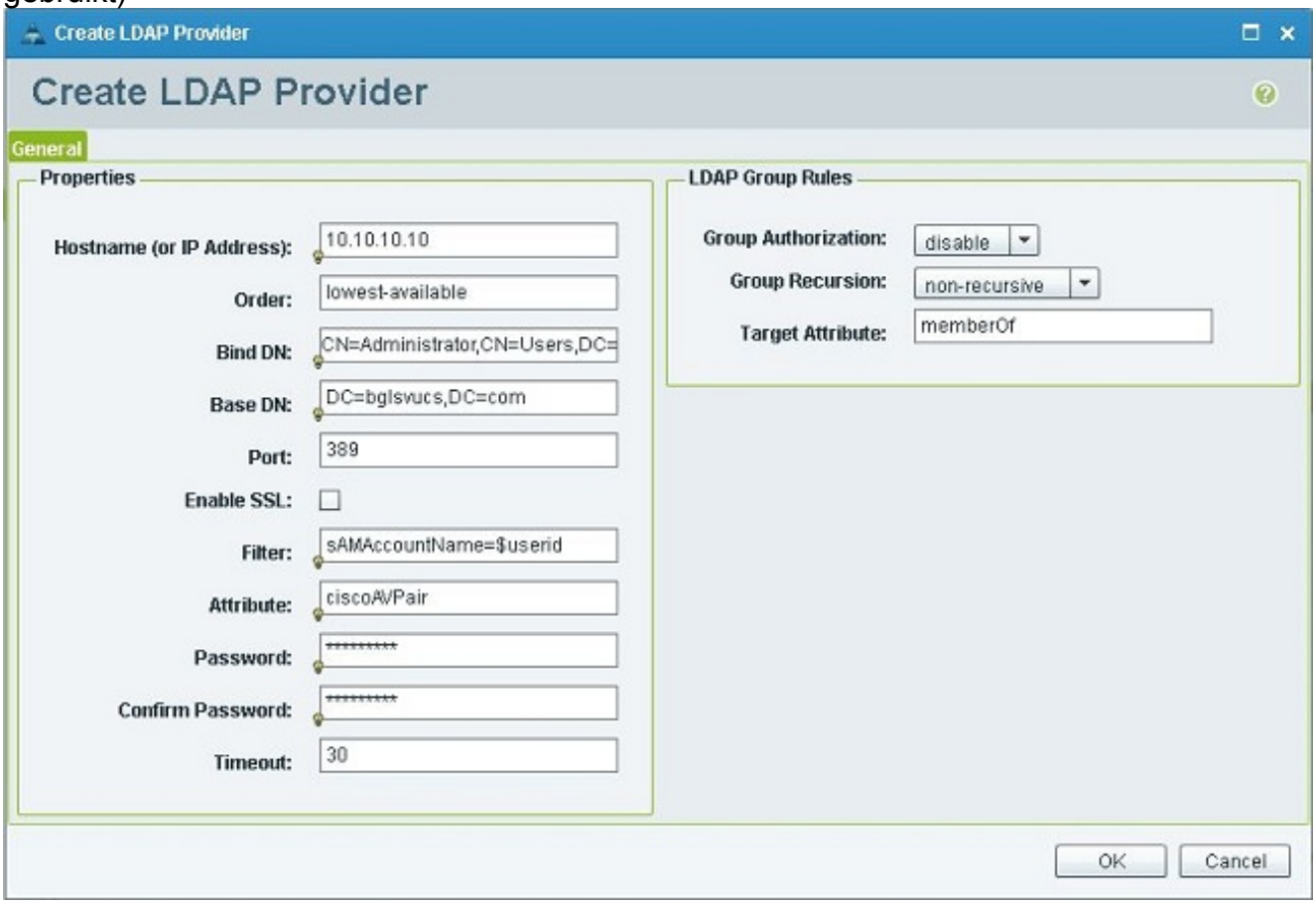
LDAP-provider configureren

1. Klik op **LDAP**, klik met de rechtermuisknop op **Leveranciers** en kies **Maken LDAP Provider**.



2. Voeg in het dialoogvenster Lijst maken toe deze gegevens, die eerder zijn verzameld.Hostnaam of IP van de leverancierBindBase DNfilterenKenmerk (ofwel Cisco

AVPair ofwel een vooraf gedefinieerd kenmerk zoals een bedrijf)Wachtwoord (wachtwoord van de gebruiker dat in bindt DN wordt
gebruikt)



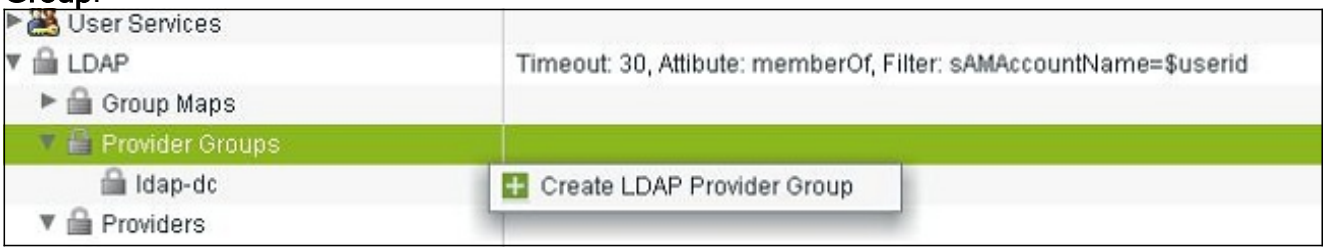
3. Klik op **OK** om de configuratie op te slaan en het dialoogvenster te sluiten.

Opmerking: er hoeft geen andere waarde te worden aangepast op dit scherm. De LDAP - groepsregels worden niet ondersteund voor de UCS Central - authenticatie in deze release.

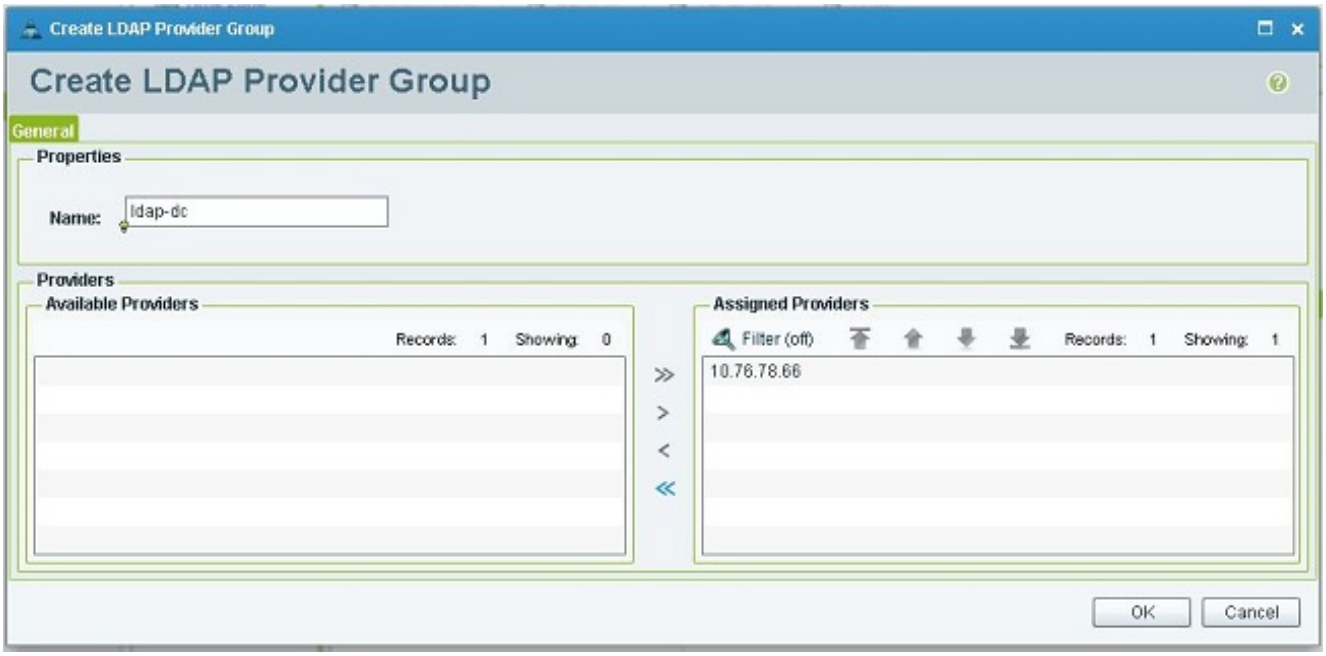
Configureren LDAP Provider Group

Opmerking: in release 1.0a worden provider-groepen niet ondersteund. In deze procedure wordt beschreven hoe u een dummy provider-groep kunt configureren voor gebruik in de configuratie later.

1. Klik op **LDAP**, klik met de rechtermuisknop op **Provider Group** en kies **Maken LDAP Provider Group**.



2. Typ in het dialoogvenster Create LDAP Provider Group de naam voor de groep in het veld Naam.
3. Selecteer de provider in de lijst met beschikbare aanbieders links en klik op het grotere dan het symbool (**>**) om deze aanbieder naar de toegewezen aanbieders aan de rechterzijde te verplaatsen.



4. Klik op **OK** om de wijzigingen op te slaan en het scherm te sluiten.

Native verificatieregel wijzigen

Release 1.0a ondersteunt geen meerdere authenticatiedomeinen zoals in UCS Manager. Om hieraan te werken, moet u de inheemse authenticatieregel wijzigen.

Native authenticatie heeft de optie om de authenticatie voor standaardlogins of console-logins aan te passen. Aangezien meerdere domeinen niet worden ondersteund, kunt u de lokale account of een LDAP account gebruiken, maar niet beide. Wijzig de waarde van Realm om lokale of LDAP te gebruiken als bron van authenticatie.

1. Klik op **Verificatie**, klik met de rechtermuisknop op **Native Authentication** en kies **Eigenschappen**.
2. Bepaal of u een standaardverificatie, een console-verificatie of beide wilt uitvoeren. Gebruik standaardverificatie voor de GUI en de opdrachtregel interface (CLI). Gebruik Console-verificatie voor de KVM-weergave (Virtual Machine) op basis van virtuele machines (KVM).
3. Kies **lappen** uit de vervolgkeuzelijst Opnieuw. De waarde van Realm bepaalt of lokale of LDAP de bron van de authenticatie
   is.

4. Klik op **OK** om de pagina te sluiten.
5. Klik op de pagina Beleid indien nodig op **Opslaan** om de wijzigingen op te slaan.

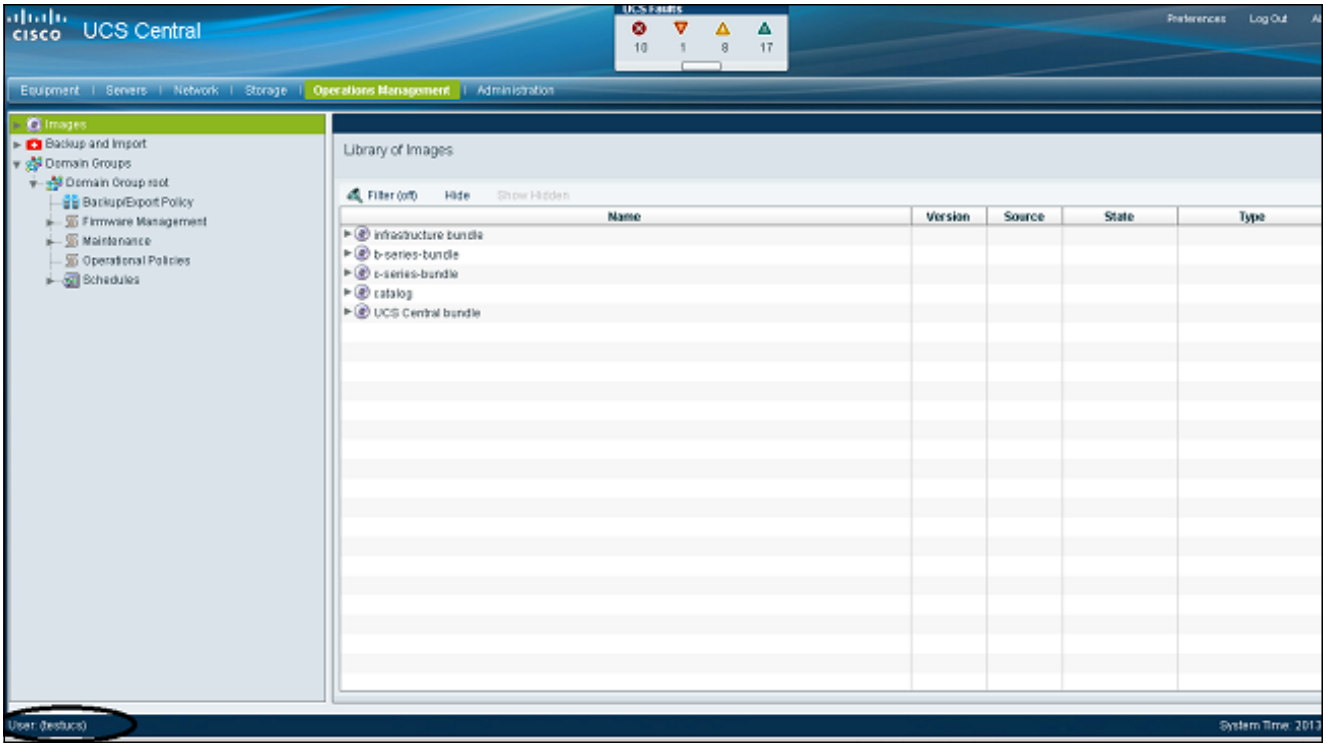
Opmerking: log niet uit uw huidige sessie of wijzig de console-verificatie tot u controleert of de LDAP-verificatie correct werkt. Verificatie van console biedt een manier om terug te keren naar de vorige configuratie. Raadpleeg het gedeelte Verifiëren.

Verifiëren

In deze procedure wordt beschreven hoe de authenticatie van de LDAP moet worden getest.

1. Open een nieuwe sessie in UCS Central en voer het gebruikersnaam en wachtwoord in. U hoeft geen domein of teken vóór de gebruikersnaam op te nemen. Dit voorbeeld gebruikt testucs als de gebruiker uit het domein.

2. LDAP-verificatie is succesvol als u het UCS Central-dashboard ziet. De gebruiker wordt onder op de pagina
weergegeven.



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems