UCS中心的LDAP身份验证配置示例

目录

简介

本文档为思科统一计算系统(UCS)中心的轻量级目录访问协议(LDAP)身份验证提供配置示例。该过程使用UCS中心图形用户界面(GUI)、bglus.com示例域和testuser示例用户名。

在UCS中心软件版本1.0中，LDAP是唯一支持的远程身份验证协议。版本1.0对UCS中心本身的远程身份验证和LDAP配置的支持非常有限。但是，您可以使用UCS中心为UCS中心管理的UCS Manager域配置所有选项。

UCS中心远程身份验证的限制包括：

- 不支持RADIUS和TACACS。
- 不支持角色分配的LDAP组成员身份映射和多个域控制器的LDAP提供程序组。
- LDAP仅使用CiscoAVPair属性或任何未使用的属性来传递角色。传递的角色是UCS中心本地数据库中预定义的角色之一。
- 不支持多个身份验证域/协议。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 部署了UCS中心。
- 部署了Microsoft Active Directory。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCS中心版本1.0
- Microsoft Active Directory

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

收集信息

本节总结在开始配置之前需要收集的信息。

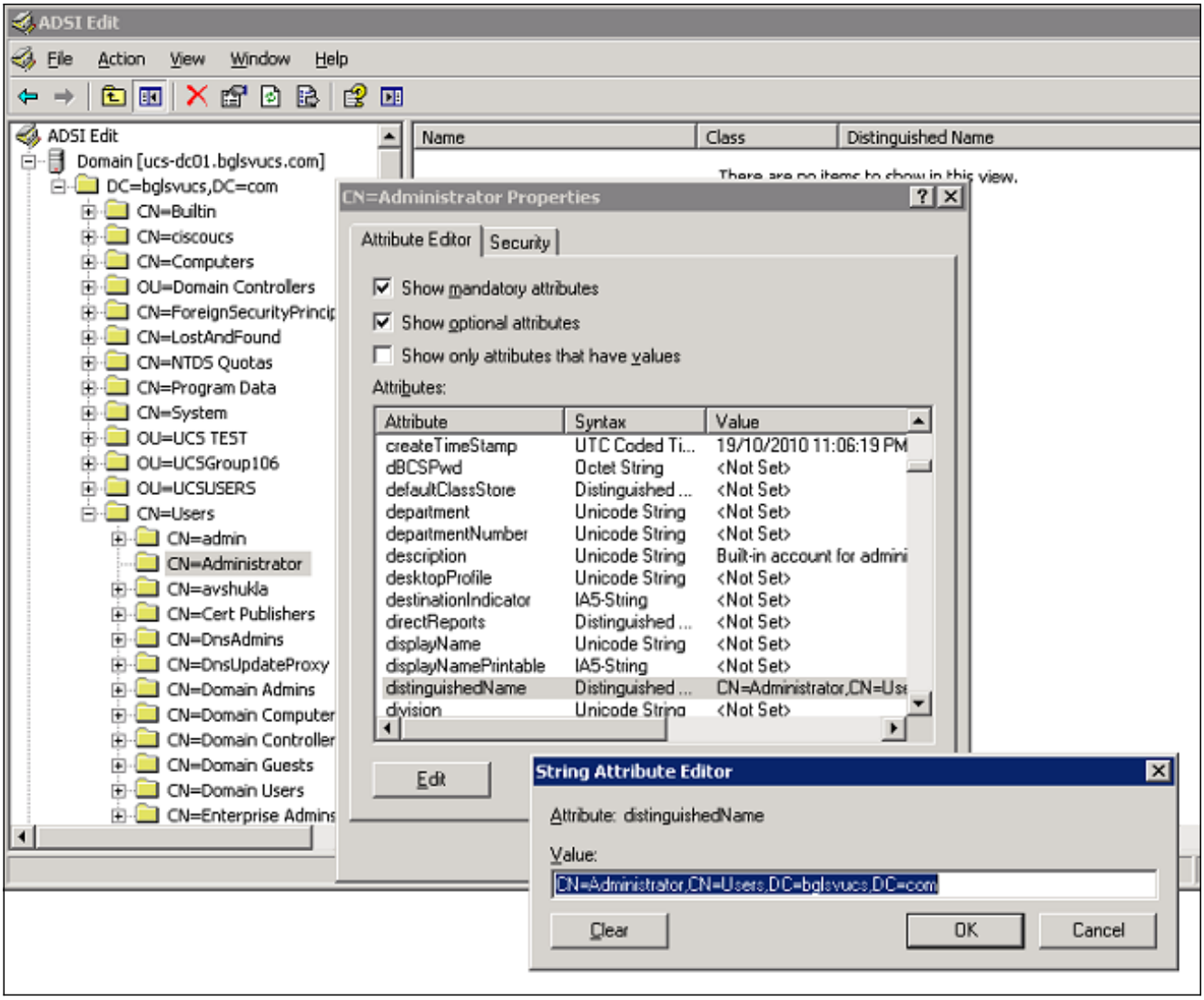
注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

绑定用户详细信息

绑定用户可以是域中对域具有读取访问权限的任何LDAP用户；LDAP配置需要绑定用户。UCS中心使用绑定用户的用户名和密码来连接和查询Active Directory(AD)以进行用户身份验证等。本示例使用管理员帐户作为绑定用户。

此过程介绍LDAP管理员如何使用Active Directory服务接口(ADSI)编辑器来查找DN。

1. 打开ADSI编辑器。
2. 查找绑定用户。用户与AD中的用户处于同一路径。
3. 右键单击用户，然后选择**属性**。
4. 在“属性”对话框中，双击可分辨**名称**。
5. 从Value字段复制DN。



6. 单击**取消**以关闭所有窗口。

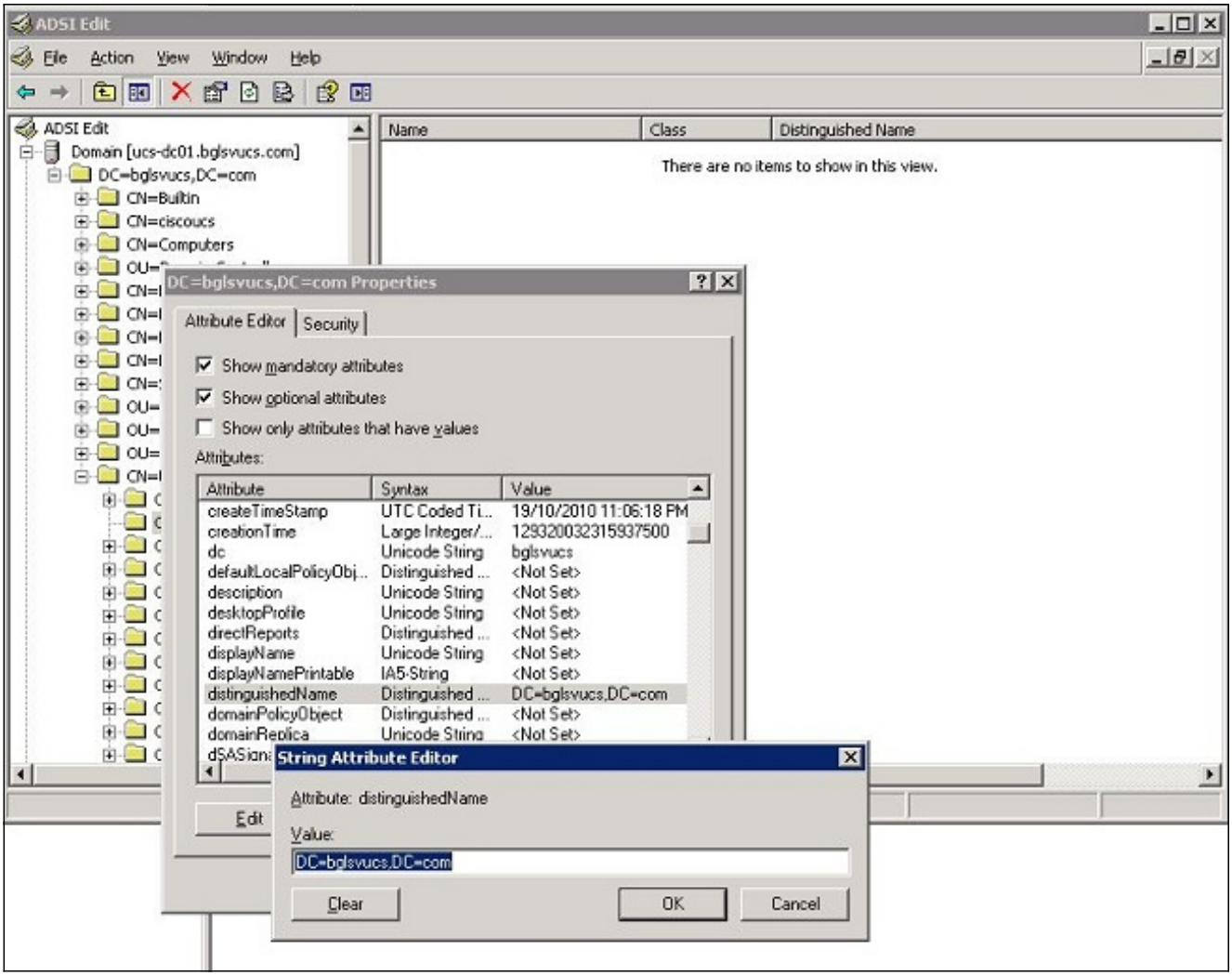
要获取绑定用户的密码，请与AD管理员联系。

基本DN详细信息

基本DN是组织单位(OU)的DN或开始搜索用户和用户详细信息的容器。您可以使用在AD中为UCS或UCS中心创建的OU的DN。但是，您可能会发现为域根本身使用DN更简单。

此过程介绍LDAP管理员如何使用ADSI编辑器查找基本DN。

1. 打开ADSI编辑器。
2. 查找要用作基本DN的OU或容器。
3. 右键单击OU或容器，然后选择“**属性**”。
4. 在“属性”对话框中，双击可分辨**名称**。
5. 从值字段复制DN，并记录您需要的任何其他详细信息。



6. 单击**取消**以关闭所有窗口。

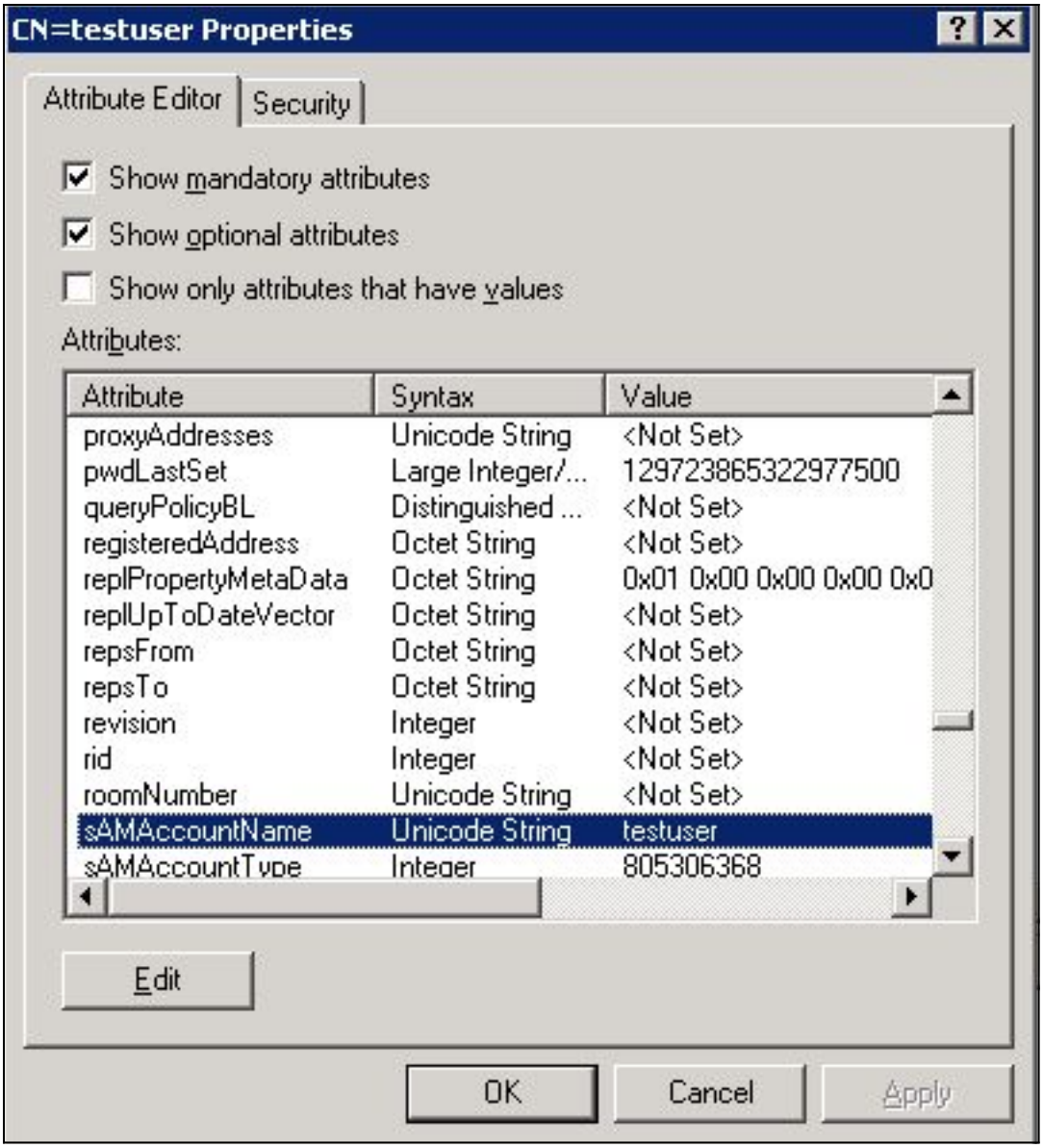
提供商详细信息

提供商在UCS中心的LDAP身份验证和授权中起着关键作用。提供程序是UCS中心查询的AD服务器之一，用于搜索和验证用户以及获取用户详细信息（如角色信息）。请务必收集提供商AD服务器的主机名或IP地址。

过滤器属性

过滤器字段或属性用于搜索AD数据库。登录时输入的用户ID会传回AD，并与过滤器进行比较。

可以使用sAMAccountName=$userid作为筛选值。sAMAccountName是AD中的属性，其值与AD用户ID相同，AD用户ID用于登录UCS中心GUI。



添加和配置属性

本节总结了在开始LDAP配置之前添加CiscoAVPair属性（如果需要）和更新CiscoAVPair属性或其他预定义属性所需的信息。

属性字段指定AD属性（在用户属性下），该属性将传递要分配给用户的角色。在UCS中心软件的版本1.0a中，可以将自定义属性CiscoAVPair或AD中任何其他未使用的属性合并，以传递此角色。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

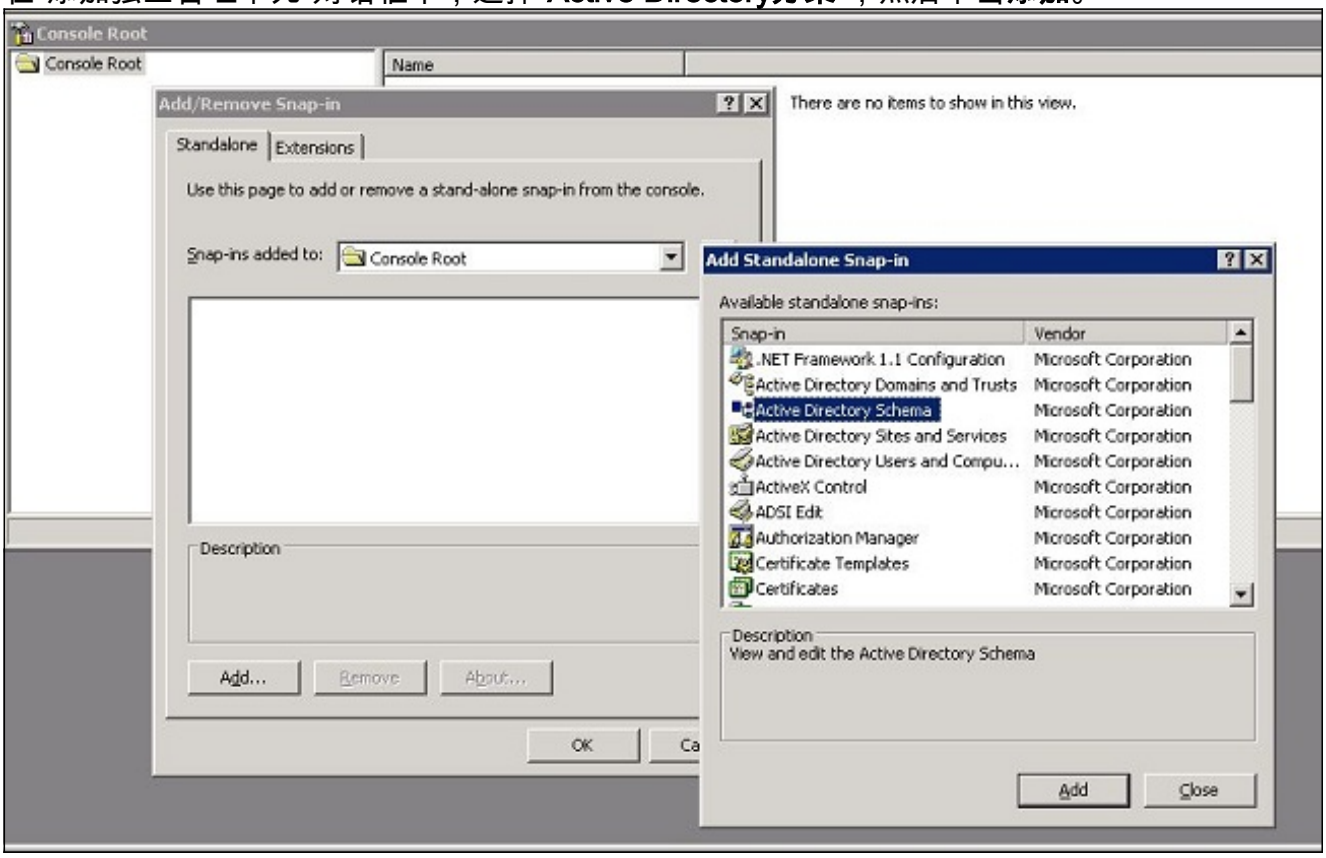
添加CiscoAVPair属性

要向域添加新属性，请展开域的架构，并将属性添加到类（在本例中为用户）。

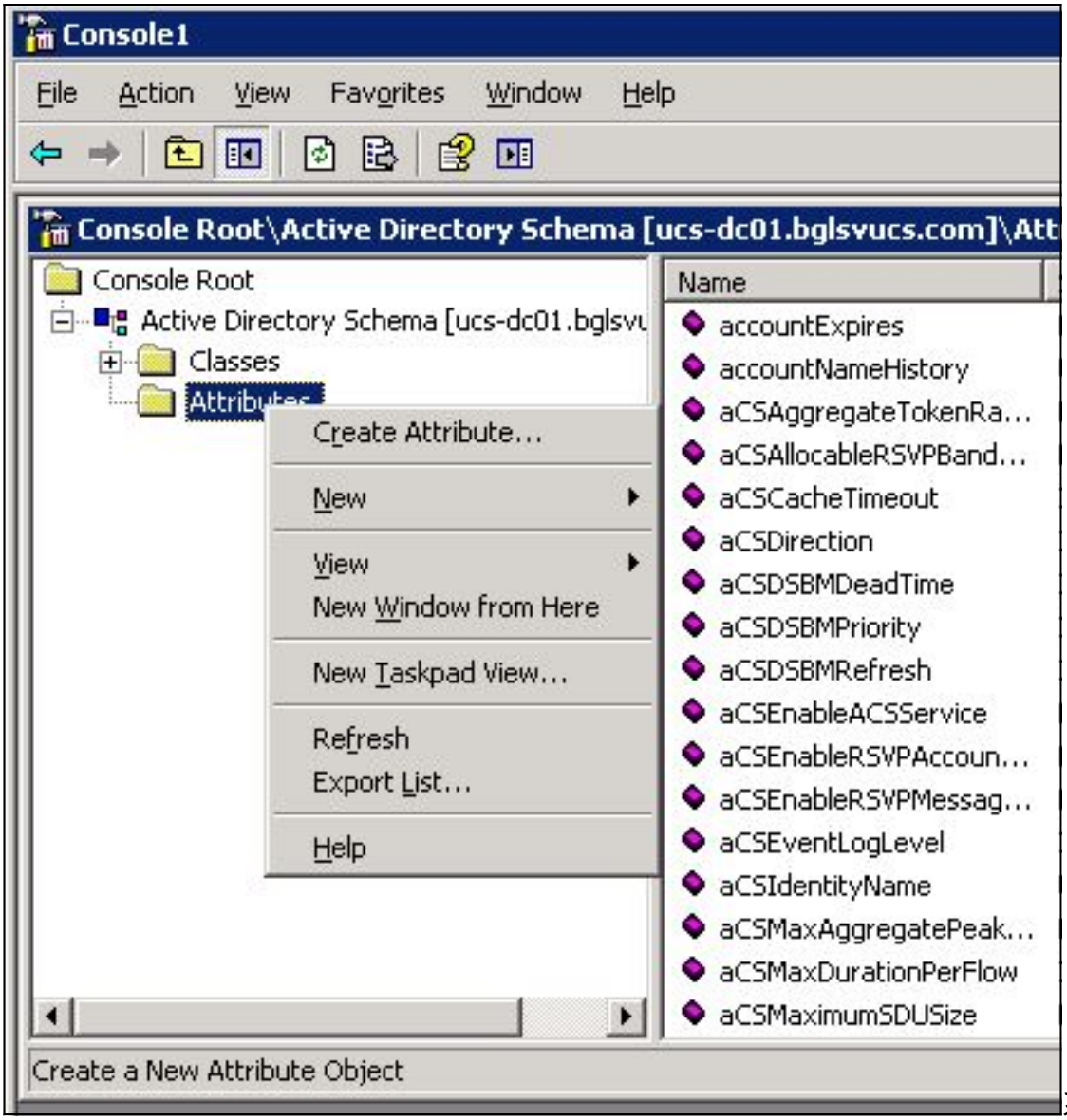
此过程介绍如何在Windows AD服务器上展开架构并添加CiscoAVPair属性。

1. 登录AD服务器。
2. 单击**开始 > 运行**，键入**mmc**，然后按**Enter**以打开空的Microsoft管理控制台(MMC)控制台。
3. 在MMC中，单击**文件 > 添加/删除管理单元> 添加**。

4. 在“添加独立管理单元”对话框中，选择“**Active Directory方案”**，然后单击**添加**。

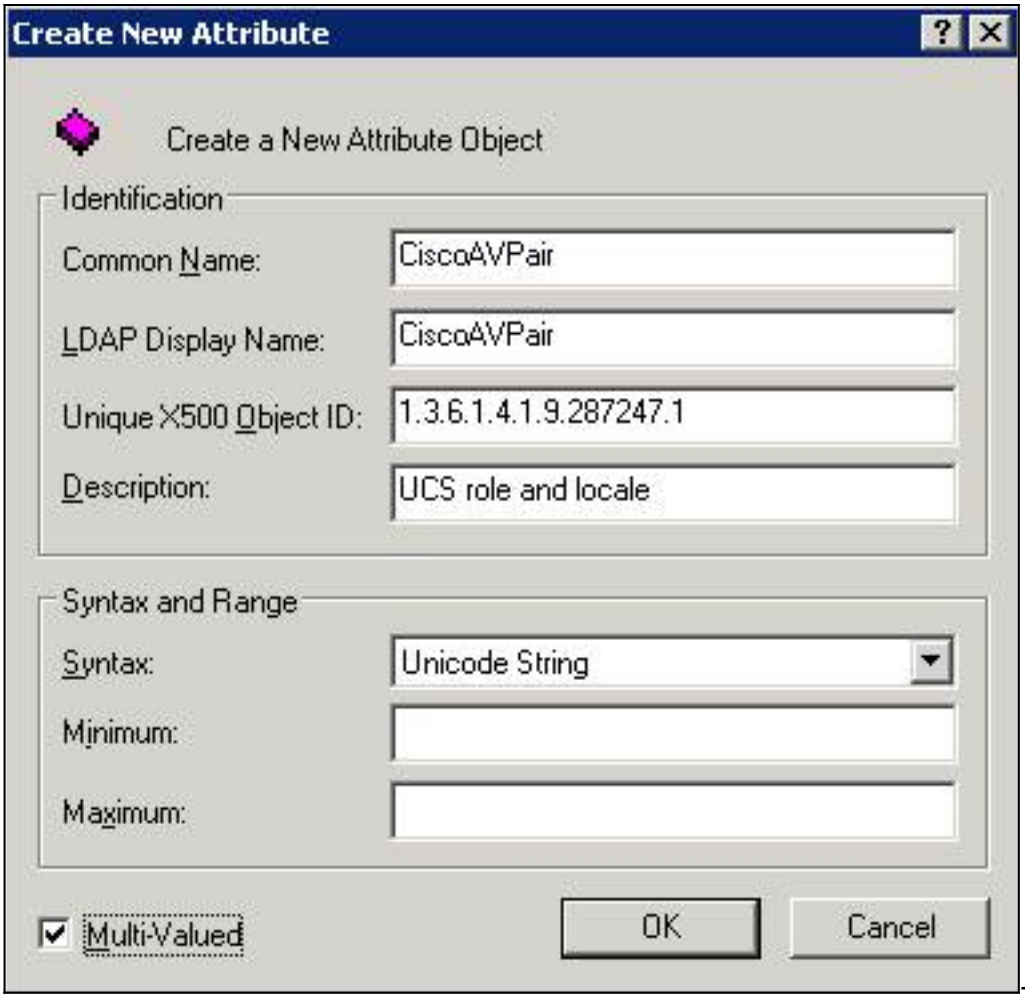


5. 在MMC中，展开**Active Directory架构**，右键单击**属性**，然后选**择创建属性**。



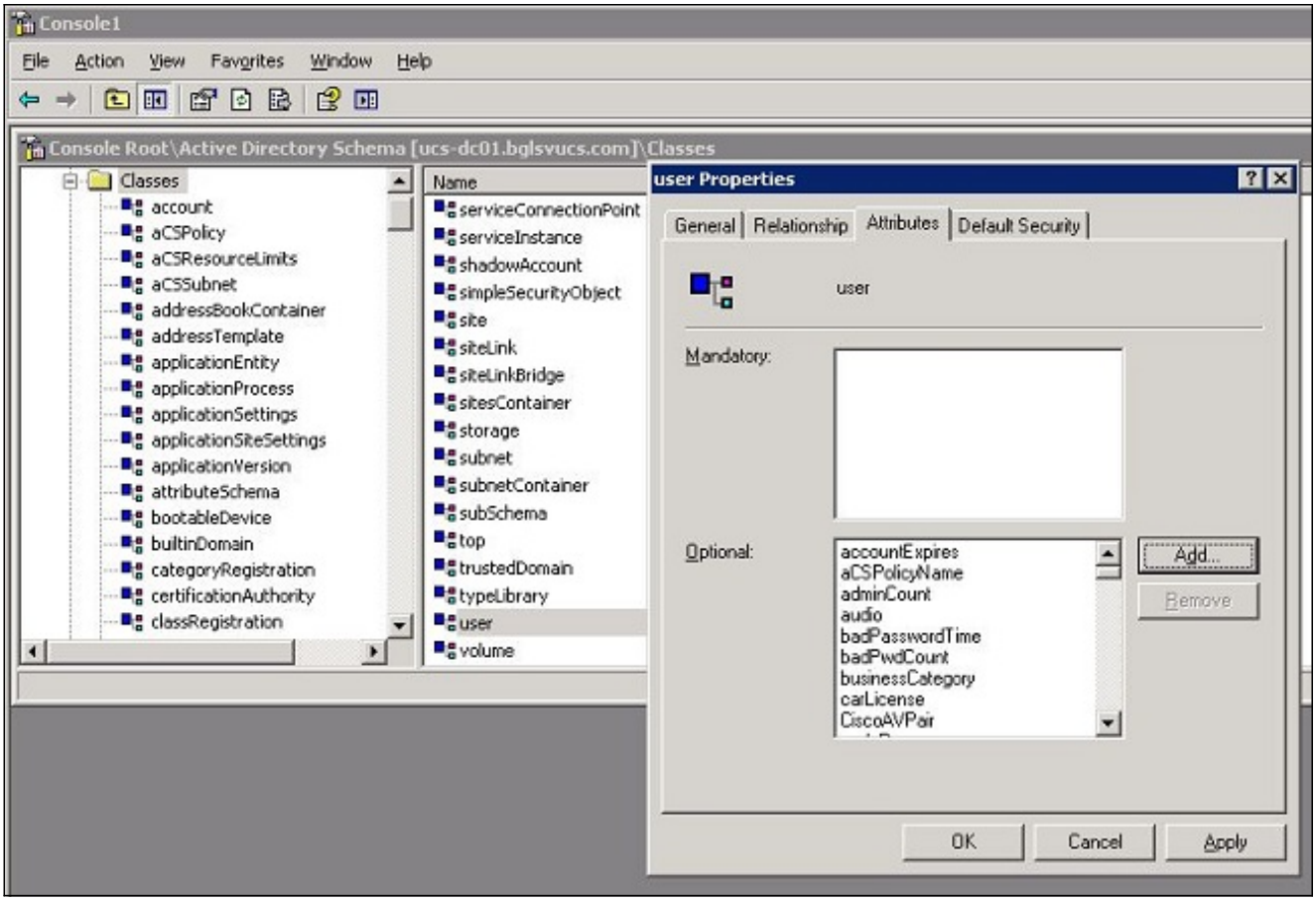
系统将显示“创建新属性”对话框

6. 在远程身份验证服务中创建名为CiscoAVPair的属性。在“公用名”和“LDAP显示名称”字段中，输入**CiscoAVPair**。在唯一500对象ID字段中，**输入1.3.6.1.4.1.9.287247.1**。在“说明”字段中，输入**UCS角色和区域设置**。在“语法”字段中，从下**拉列**表中选择Unicode字符串。

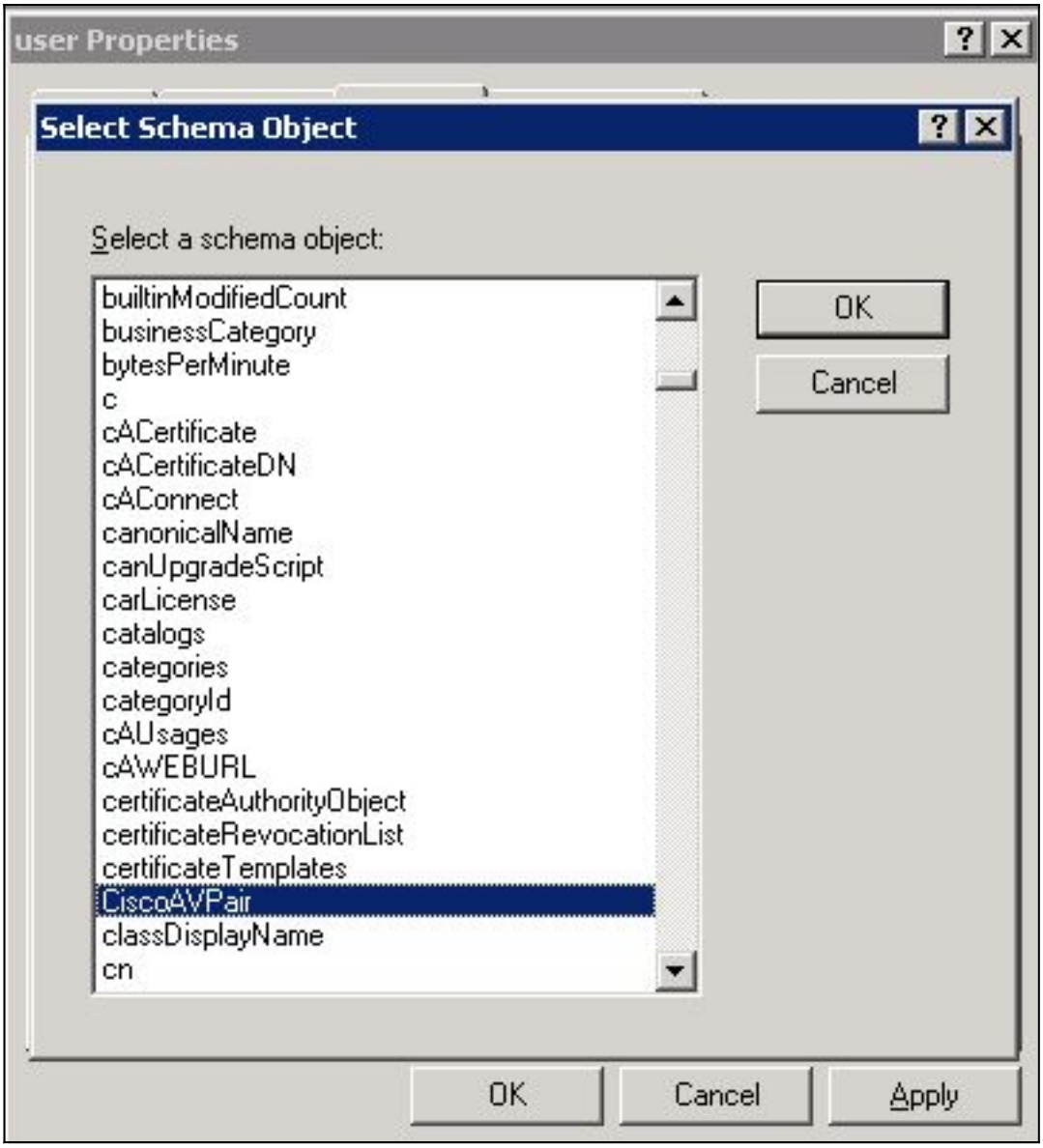


单击**OK**以保存属性并关闭对话框。将属性添加到架构后，必须将其映射或包含在用户类中。这允许您编辑用户属性并指定要传递的角色的值。

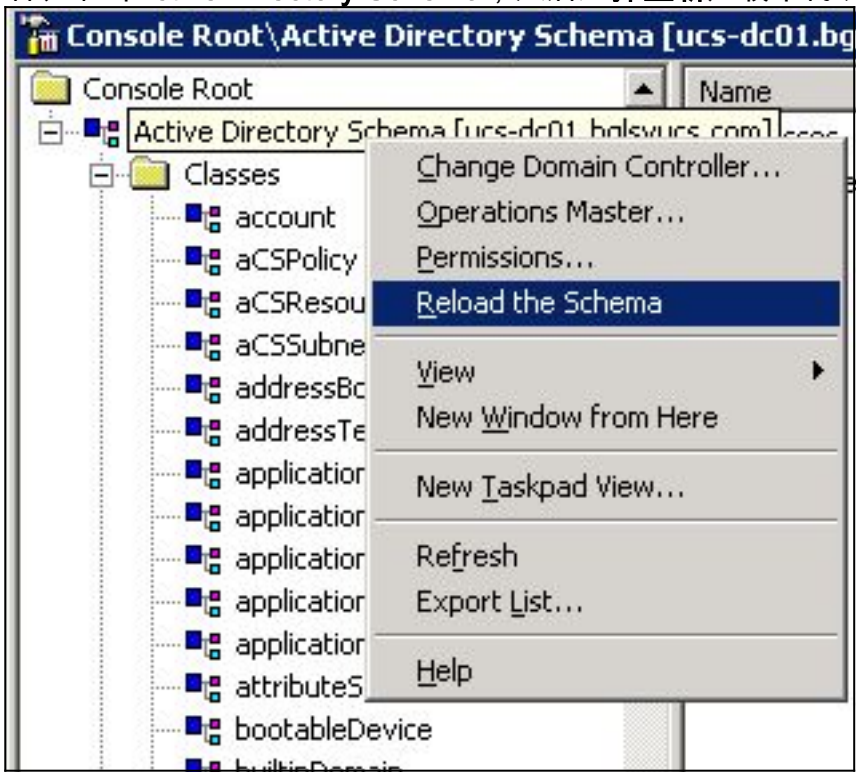
7. 在用于AD架构扩展的同一MMC中，展开**类**，右键单击**用户**，然后选择**属性**。
8. 在用户属性对话框中，单击属**性选**项卡，然后单击**添加**。



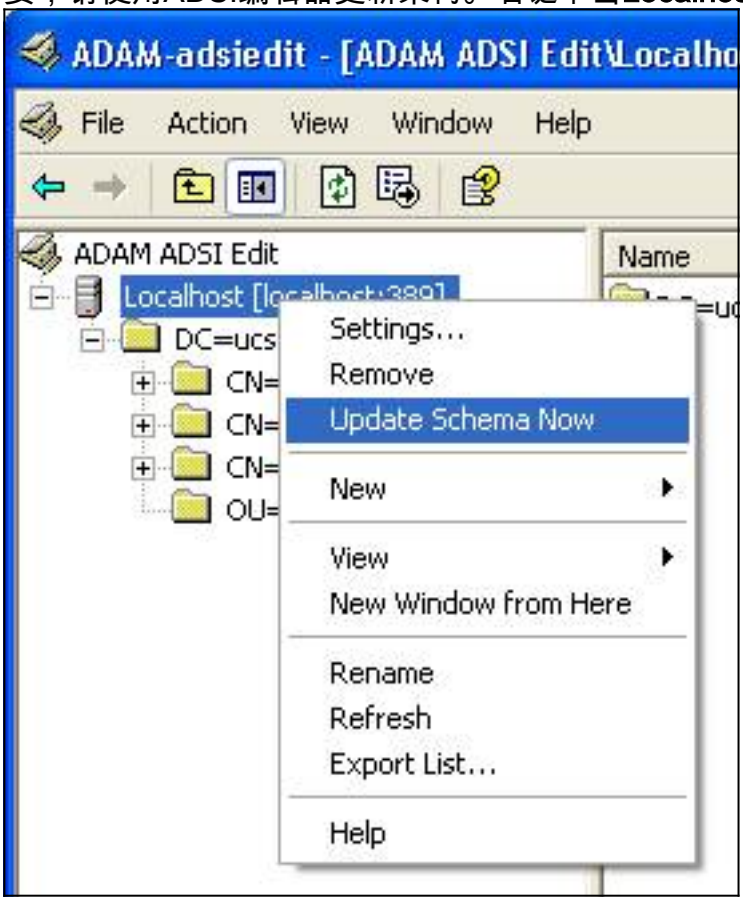
9. 在“选择方案对象”对话框中，单击**CiscoAVPair**，然后单击**确定**。



10. 在用户属性对话框中，单击**应用**。
11. 右键单击**Active Directory Schema**，然后选**择重新**加载架构以包括新更改。



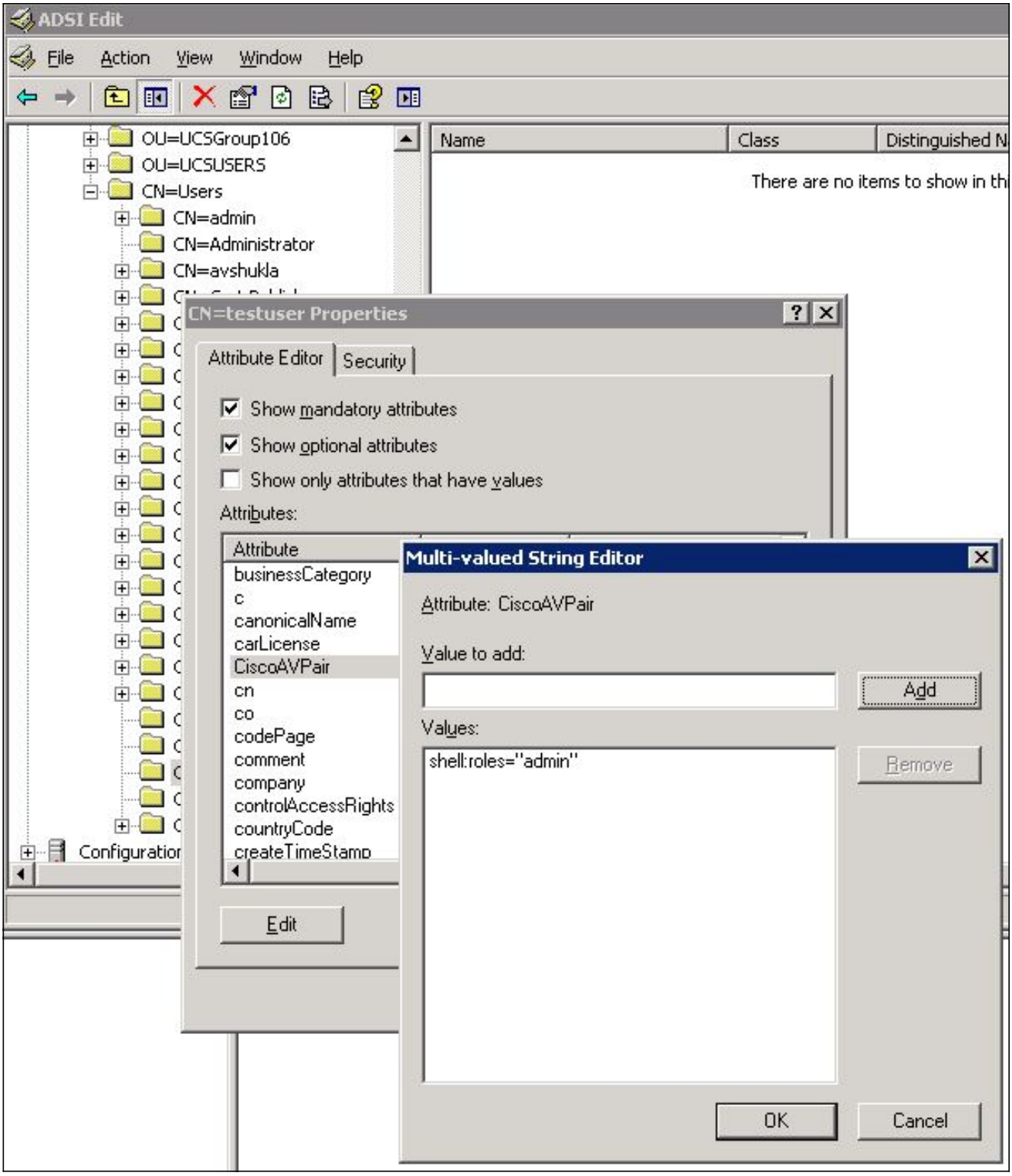
12. 如有必要，请使用ADSI编辑器更新架构。右键单击**Localhost**，然后选择**Update Schema Now**。



更新CiscoAVPair属性

此步骤介绍如何更新CiscoAVPair属性。语法为`shell:roles="<role>"`。

1. 在ADSI Edit对话框中，找到需要访问UCS中心的用户。
2. 右键单击用户，然后选择**属性**。
3. 在“属性”对话框中，单击“属**性编辑器**”选项卡，单**击“CiscoAVPair”**，然后单击**编辑**。
4. 在“多值字符串编辑器”对话框中，在“值”字**段中输入值shell:roles=**"admin"，然后单击“**确定**”。

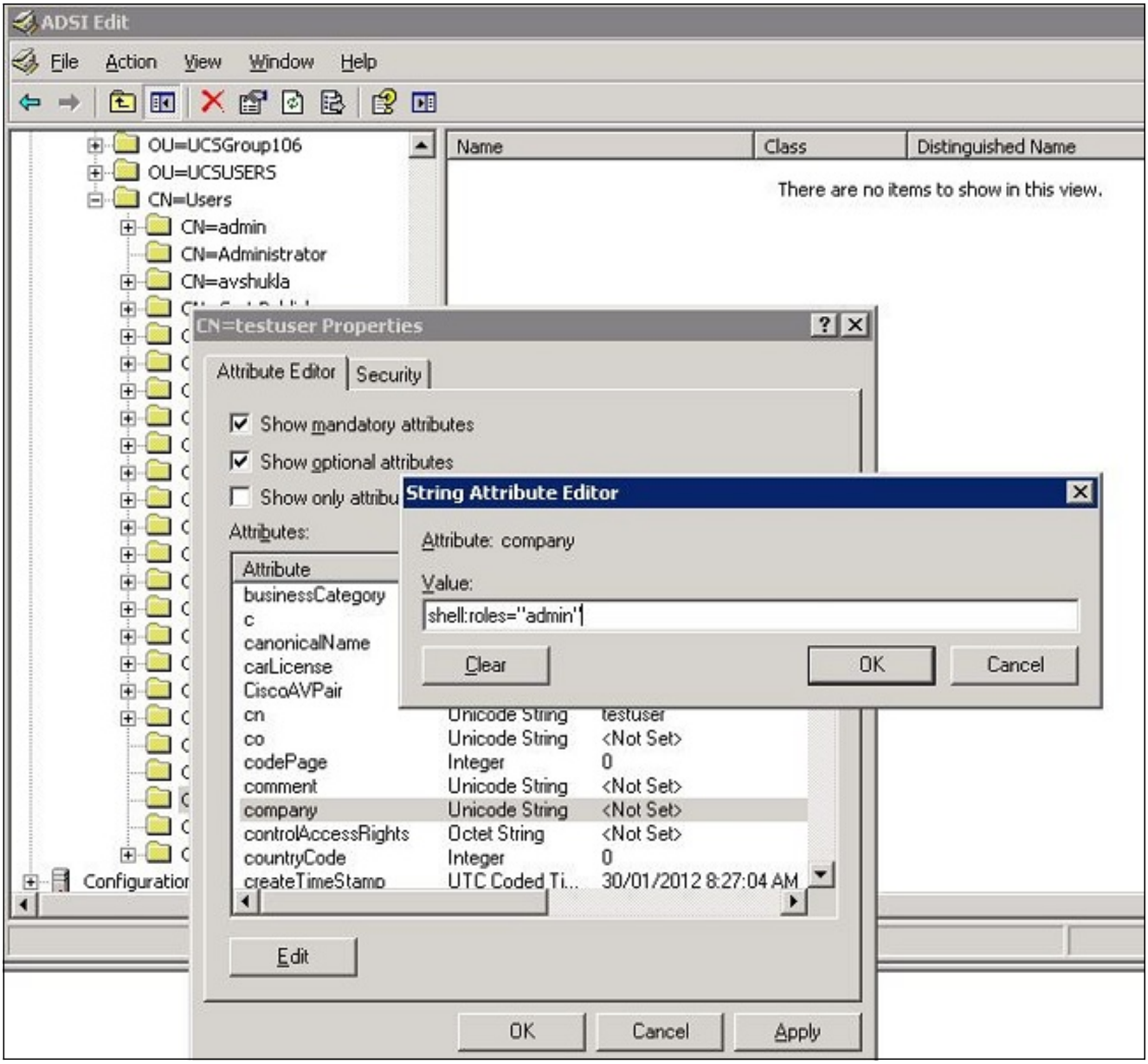


5. 单击**确定**以保存更改并关闭“属性”对话框。

更新预定义属性

此过程介绍如何更新预定义属性，其中角色是UCS中心中预定义的用户角色之一。本示例使用属性*company*传递角色。语法为`shell:roles="<role>"`。

1. 在ADSI Edit对话框中，找到需要访问UCS中心的用户。
2. 右键单击用户，然后选择**属性**。
3. 在“属性”对话框中，单击“属**性编辑器**”选项卡，**单击**“公司”，然**后单击**“编辑”。
4. 在字符串属性编辑器对话框的值字**段中输入shell:roles="admin"**值，然后单击确**定**。

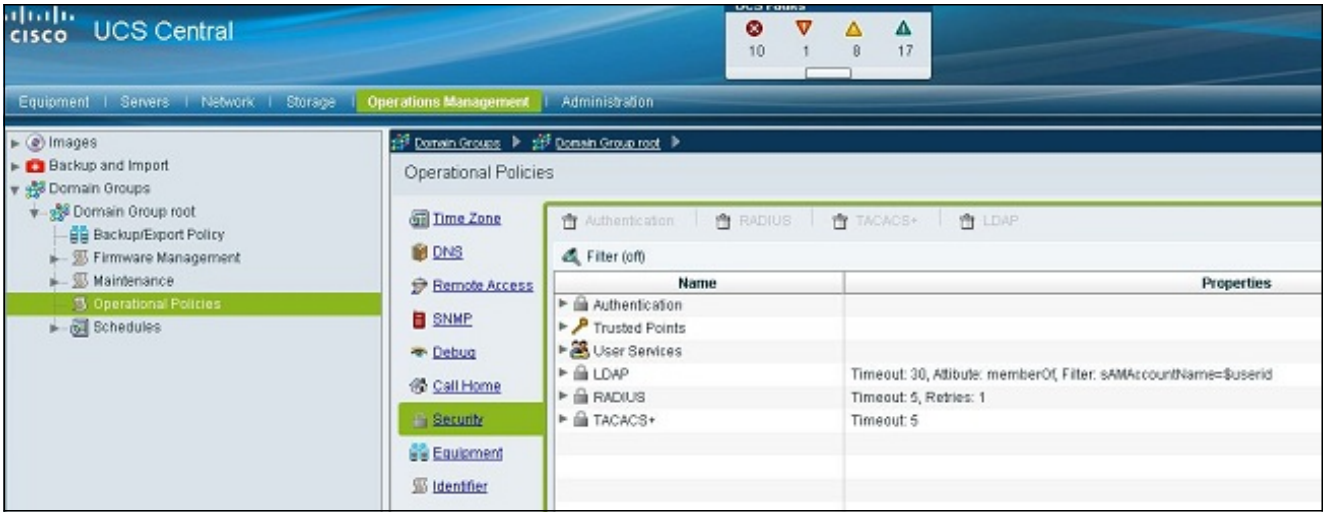


5. 单击**确定**以保存更改并关闭“属性”对话框。

在UCS中心上配置LDAP身份验证

UCS中心中的LDAP配置在Operations Management下完成。

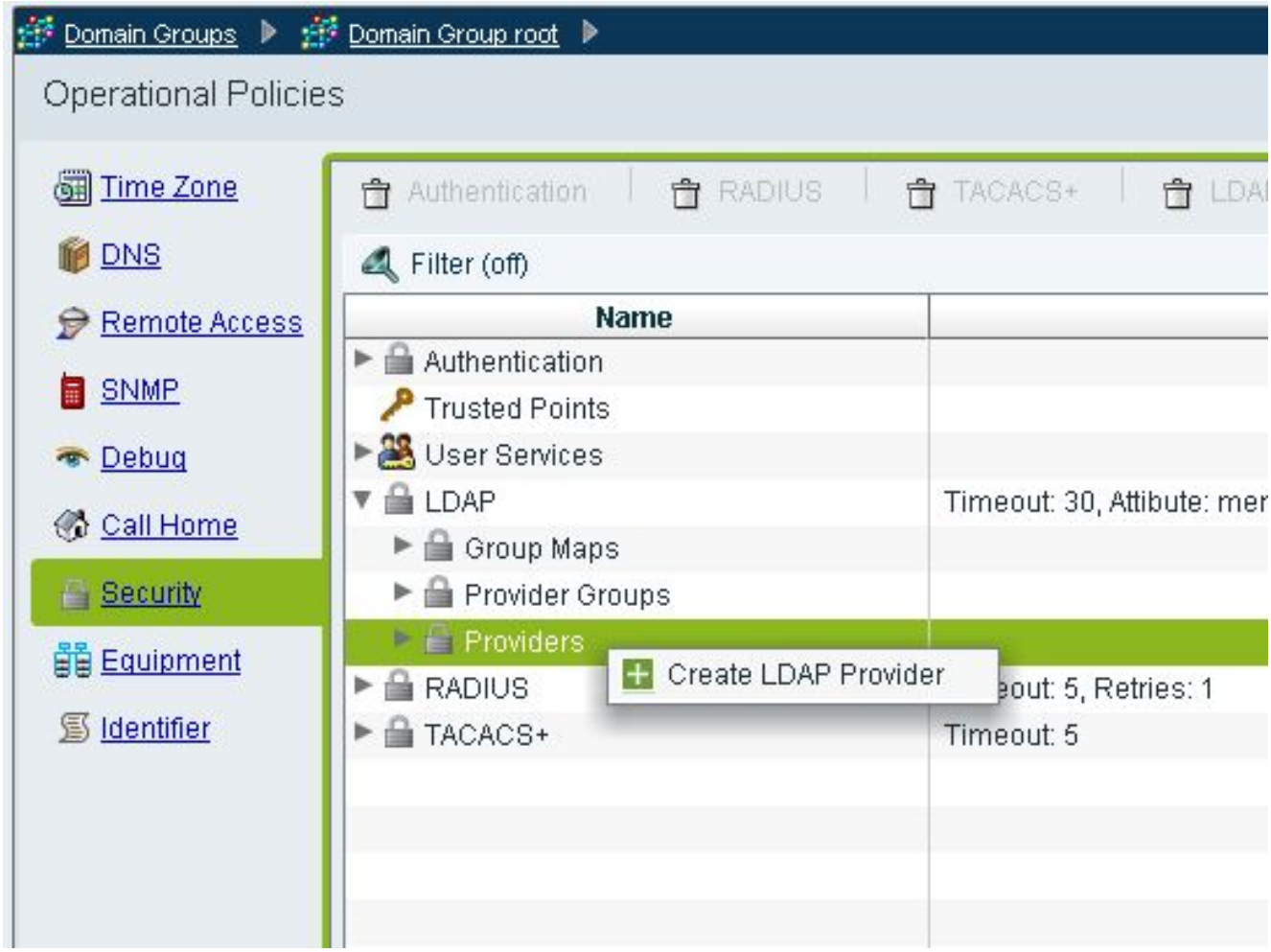
1. 使用本地帐户登录UCS中心。
2. 单击**Operations Management**，展开**Domain Groups**，然后单击**Operational Policies > Security**。



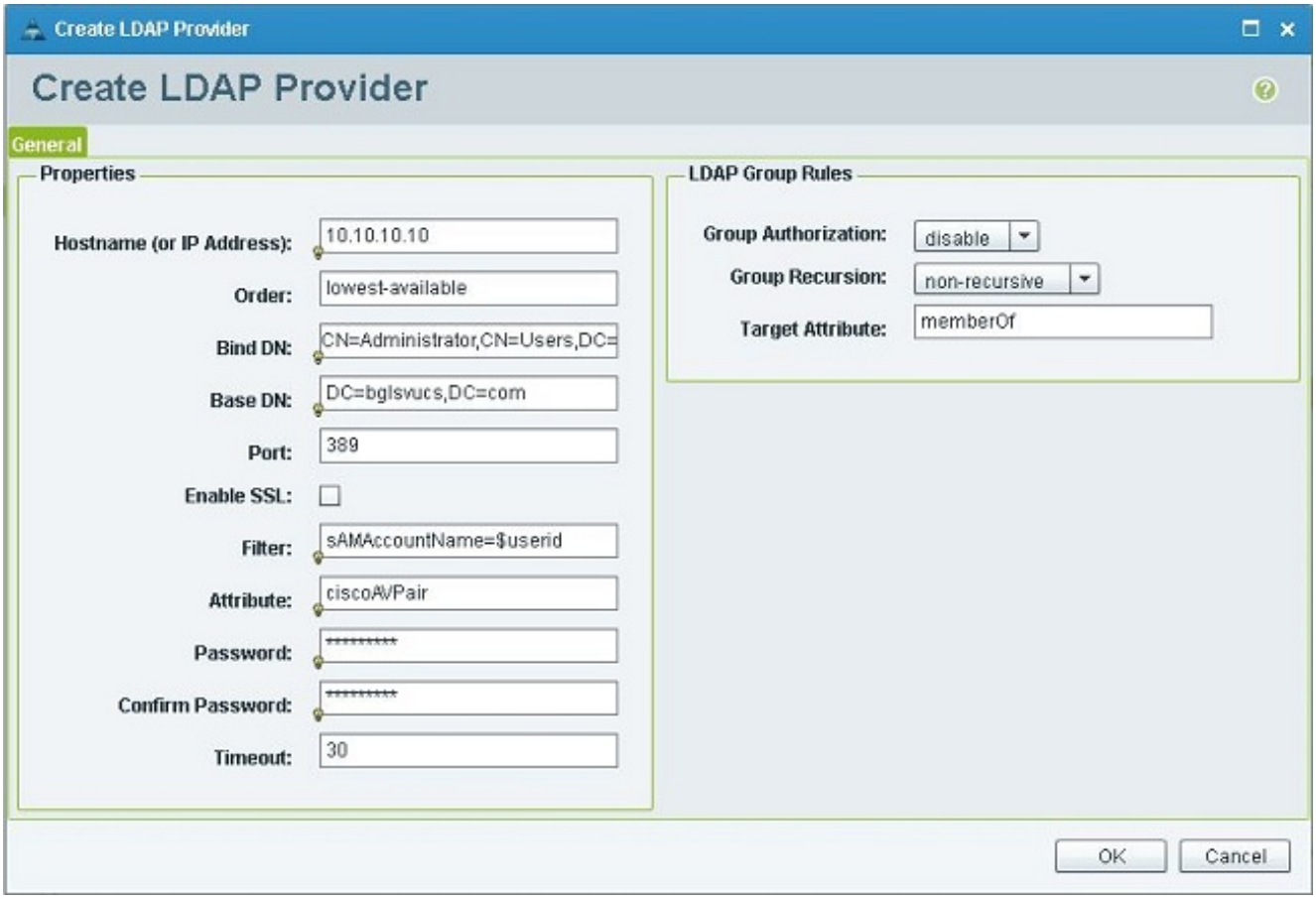
3. 要配置LDAP身份验证，请执行以下步骤：配置LDAP提供程序。配置LDAP提供程序组（在版本1.0a中不可用）。更改本地身份验证规则。

配置LDAP提供程序

1. 单击**LDAP**，右键单击**Providers**，然后选择**Create LDAP Provider**。



2. 在创建LDAP提供程序对话框中，添加之前收集的这些详细信息。提供商的主机名或IP绑定DN基准 DN过滤器属性(CiscoAVPair或预定义属性，如公司密码（绑定DN中使用的用户的密码
）



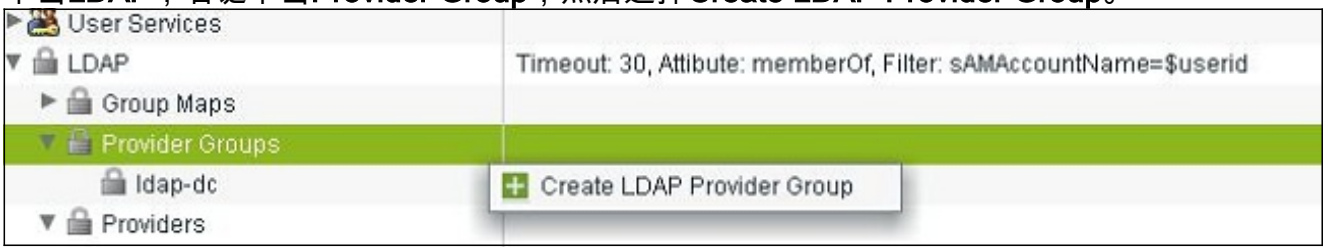
3. 单击**OK**以保存配置并关闭对话框。

注意：此屏幕上无需修改其他值。此版本的UCS中心身份验证不支持LDAP组规则。

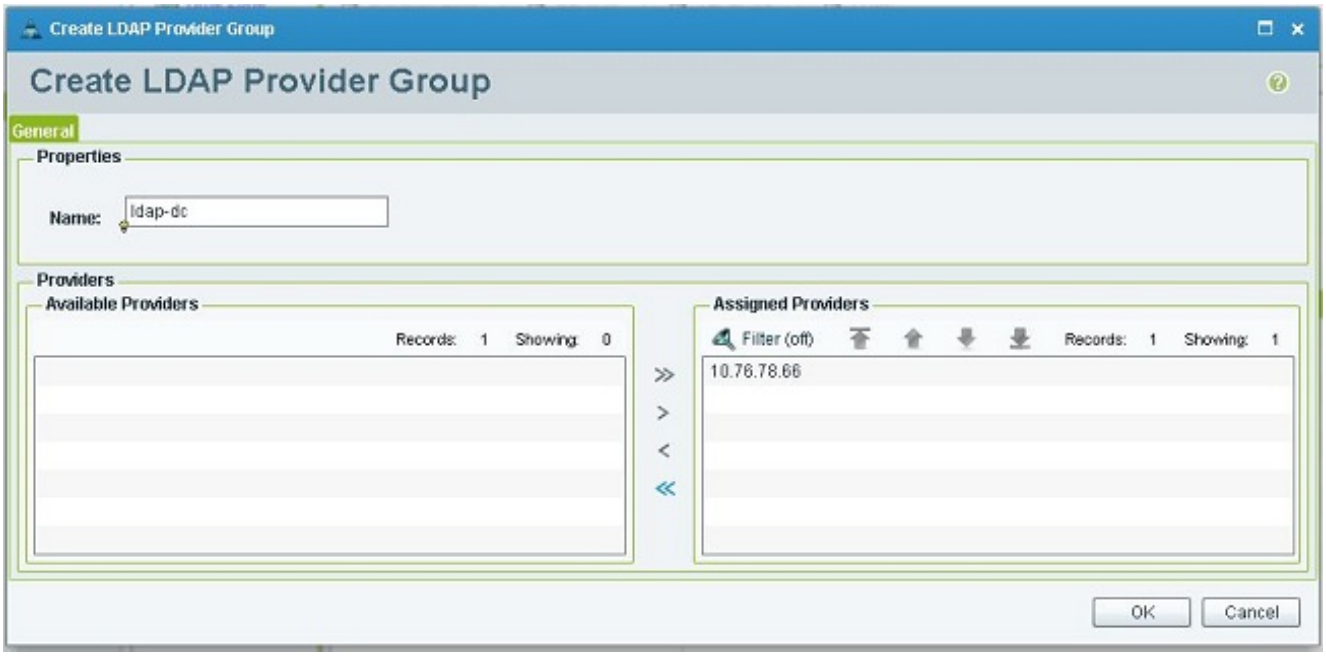
配置LDAP提供程序组

注意：在版本1.0a中，不支持提供程序组。本过程介绍如何配置虚拟提供程序组以在以后的配置中使用。

1. 单击**LDAP**，右键单击**Provider Group**，然后选择**Create LDAP Provider Group**。



2. 在创建LDAP提供程序组对话框的名称字段中输入组的名称。
3. 从左侧的可用提供程序列表中，选择提供程序，然后单击大于号(**>**)，将该提供程序移到右侧的已分配提供程序。



4. 单击**OK**以保存更改并关闭屏幕。

更改本地身份验证规则

版本1.0a不像UCS Manager中那样支持多个身份验证域。要解决此问题，您需要修改本地身份验证规则。

本机身份验证可以修改默认登录或控制台登录的身份验证。由于不支持多个域，因此您可以使用本地帐户或LDAP帐户，但不能同时使用这两个帐户。更改领域值，以使用本地或LDAP作为身份验证源。

1. 单击**Authentication**，右键单击**Native Authentication**，然后选择**Properties**。
2. 确定您是希望使用默认身份验证、控制台身份验证还是两者。对GUI和命令行界面(CLI)使用默认身份验证。 对基于虚拟机(VM)内核的虚拟机(KVM)视图使用控制台身份验证。
3. 从Realm下拉列表中选择**ldap**。Realm的值确定本地还是LDAP是身份验证源。

4. 单击**OK**以关闭页面。
5. 在“策略”(Policies)页面上，如果需要，请**单击**“保存”(Save)以保存更改。

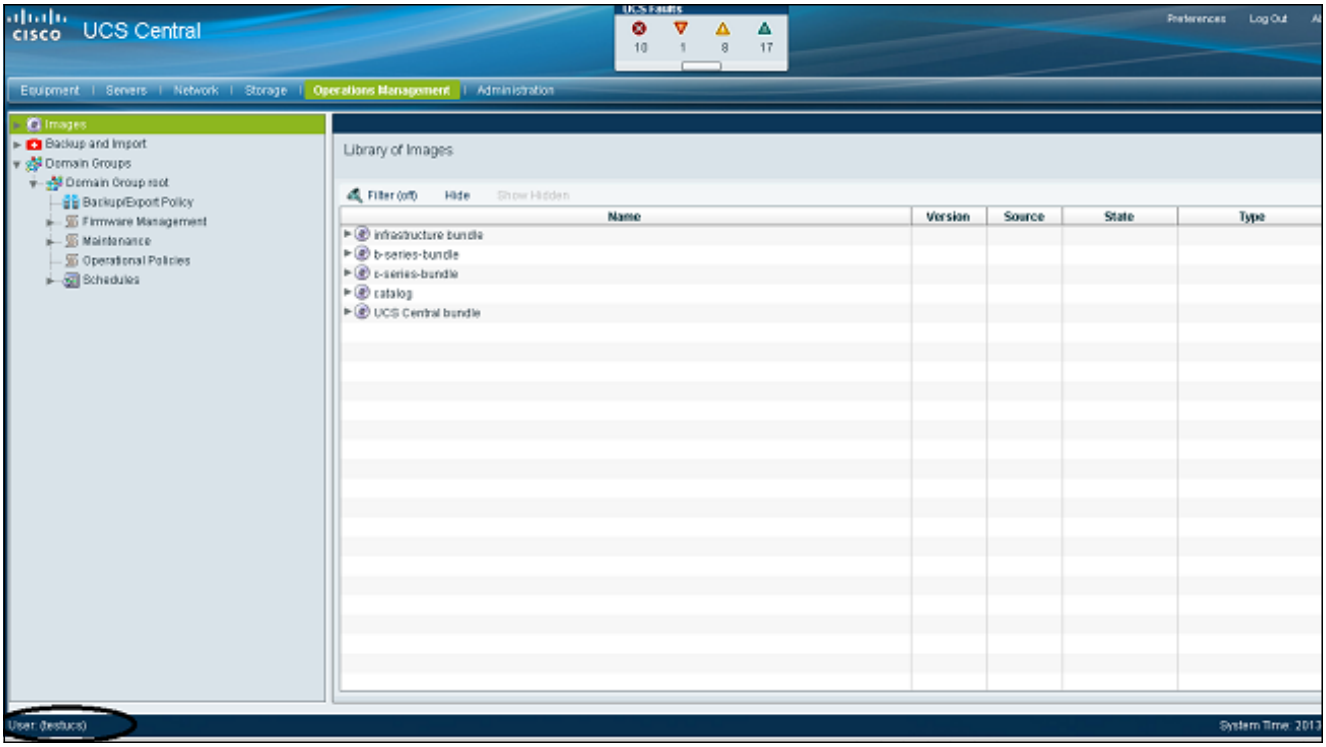
注意：在验证LDAP身份验证是否正常工作之前，请勿注销当前会话或修改控制台身份验证。控制台身份验证提供了一种恢复到先前配置的方法。请参阅“验证”部分。

验证

此过程介绍如何测试LDAP身份验证。

1. 在UCS中心中打开新会话，然后输入用户名和密码。用户名之前无需包含域或字符。本示例使用testucs作为域中的用户。

2. 如果您看到UCS中心控制面板，则LDAP身份验证成功。用户显示在页面底部。



故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems