使用Active Directory和RV34x路由器的远程身份验证和登录指南

目标

本文介绍如何在Cisco RV34x系列路由器上使用Windows Active Directory(AD)配置远程身份验证。此外，还将提供信息以避免潜在的登录错误。

简介

在RV34x路由器上配置服务身份验证设置时，需要选择外部身份验证方法。

默认情况下，RV34x系列路由器上的外部数据库优先级为RADIUS/LDAP/AD/Local。如果在路由器上添加RADIUS服务器，Web登录服务和其他服务将使用RADIUS外部数据库对用户进行身份验证。没有为Web登录服务单独启用外部数据库并为其他服务配置其他数据库的选项。在路由器上创建并启用RADIUS后，路由器将使用RADIUS服务作为外部数据库进行Web登录、站点到站点VPN、EzVPN/第三方VPN、SSL VPN、PPTP/L2TP VPN和802.1x。

如果使用Windows，Microsoft提供内部AD服务。AD存储网络的所有基本信息，包括用户、设备和策略。管理员将AD用作创建和管理网络的单一位置。它便于以统一方式处理互联、复杂和不同的网络资源。

配置后，任何获得授权的人都可以使用外部AD选项（存在于Windows服务器操作系统中）进行身份验证，以在RV34x路由器上使用任何特定服务。授权用户可以使用所提供的功能，只要他们拥有使用此类身份验证所需的硬件和软件。

适用设备 |软件版本
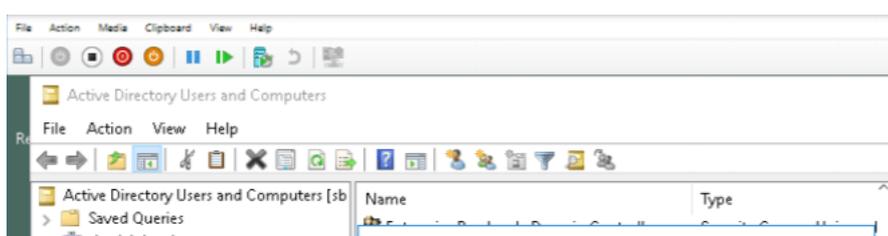
- RV340 |1.0.03.16
- RV340W |1.0.03.16
- RV345 |1.0.03.16
- RV345P |1.0.03.16

目录

确定可分辨名称值

访问Windows *2016服务器*上的Active Directory用户和计算机管理界面。选择"用户"容器文件夹，右键单击鼠标，然后打开"**属性**"。请注意稍后将*在RV34x路*由器用户容器路径字段中*使用的DistinguishedName*值。

为Active Directory创建用户组
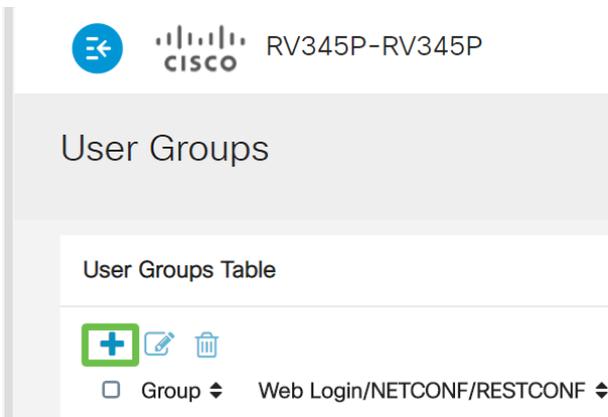
第 1 步

登录RV34x系列路由器。导航至**系统配置>用户组**。
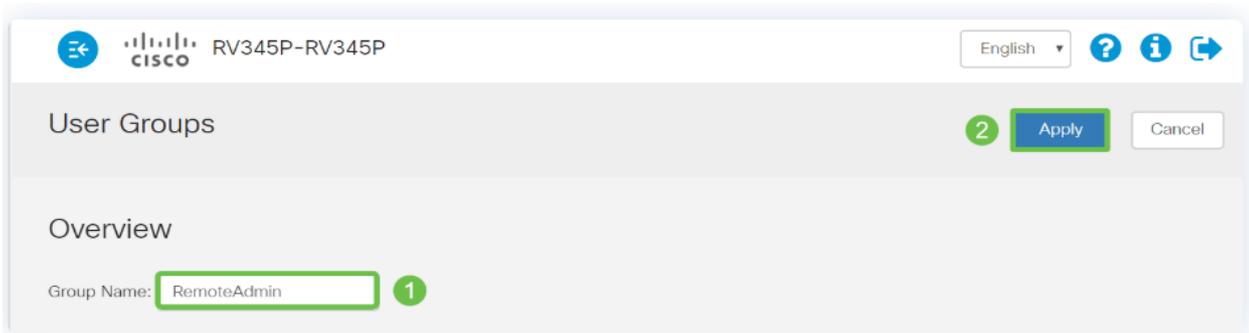
步骤 2

单击加号**图标**。

步骤 3
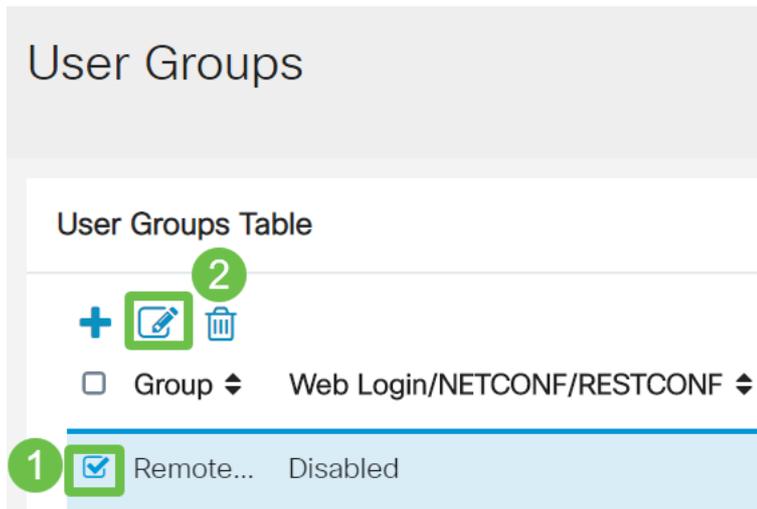
输入组名称。单击 **Apply**。

在本示例中，已*创建*了RemoteAdmin用户组。
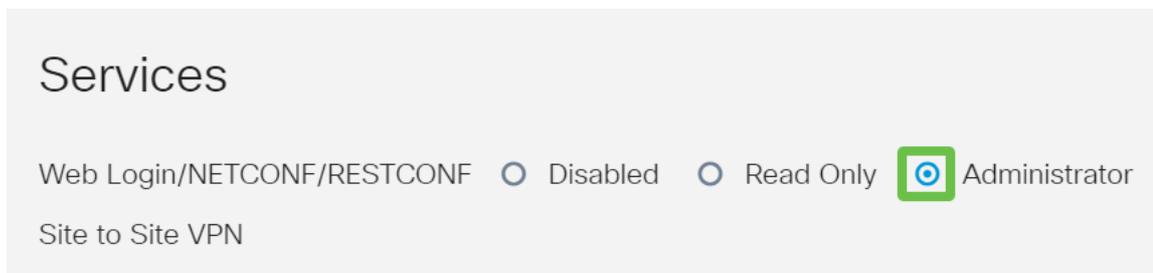
步骤 4

点击新用户组旁边的复选框。单击编**辑图标**。

User Groups

User Groups Table
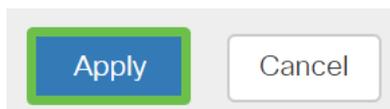
步骤 5

向下滚动页面至"*服务*"。单击"Administrator(**管理员)**"单选按钮。
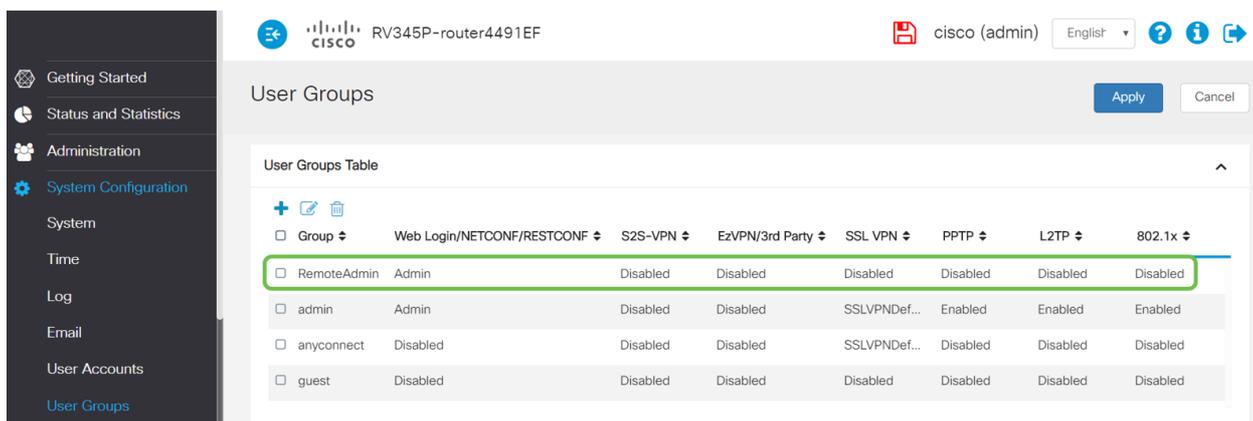
步骤 6

单击 Apply。

步骤 7
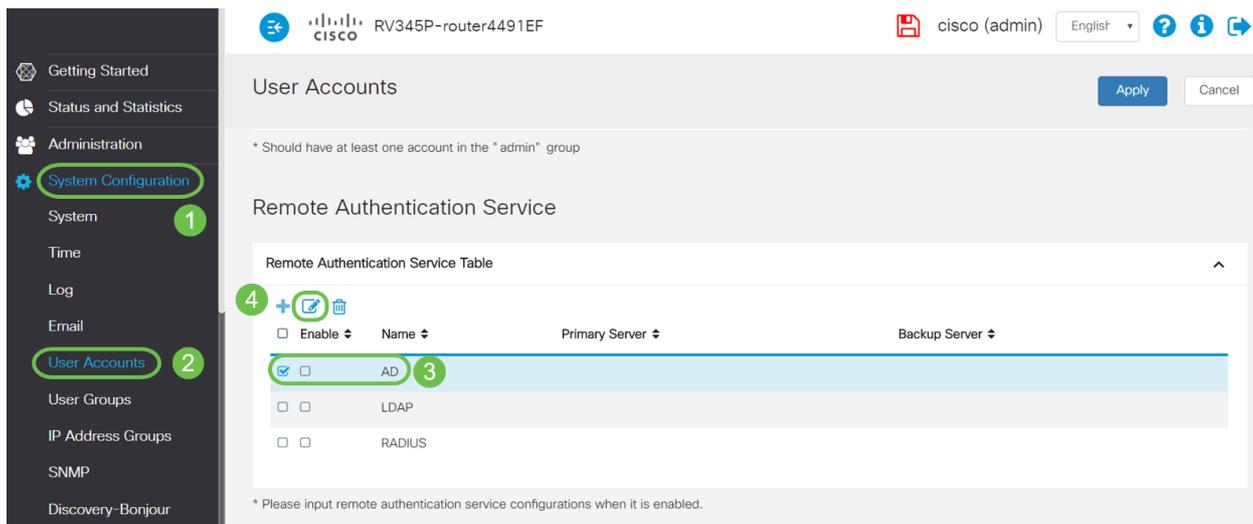
您现在将看到显示具有管理员权限的新用户组。

在RV34x路由器上添加Active Directory详细信息

第 1 步

导航到**系统配置>用户帐户**。选择*AD*选项，然后单击**编**辑图标以添加AD服务器的详细信息。

步骤 2

输入*AD域名、主服务器、端口*和*用户容器路径*详细信息。单击 Apply。
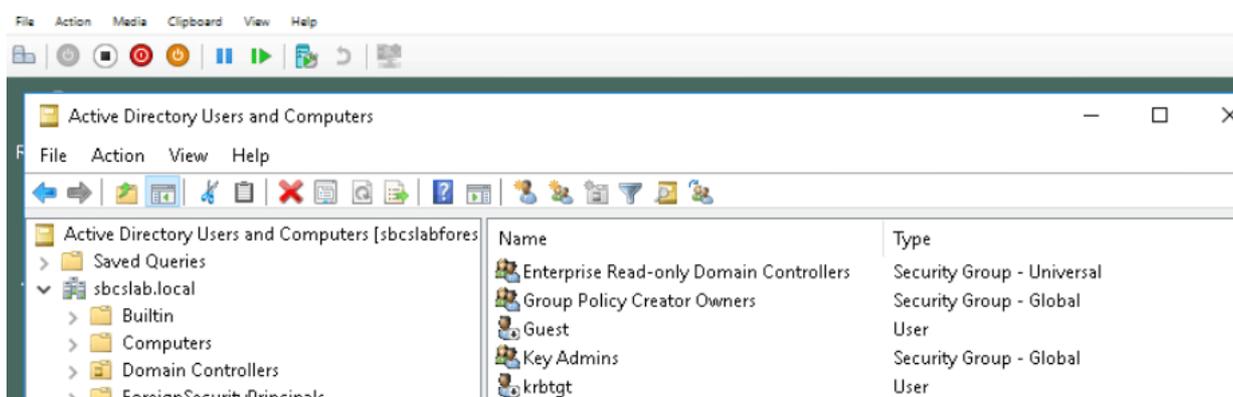
注意：您需要在本文的"识*别可分辨名称值*"部分输入从Windows服**务器捕获的用户容**器路径详细信息。

在本例中，详细信息为*Cn=user，dc=sbcslab，dc=local*。轻量级目录访问协议(LDAP)服务器默认侦听端口为389。

步骤 3

在AD中，验证用户组*是否已*配置，并且它与路由器的用户*组*名称匹配。
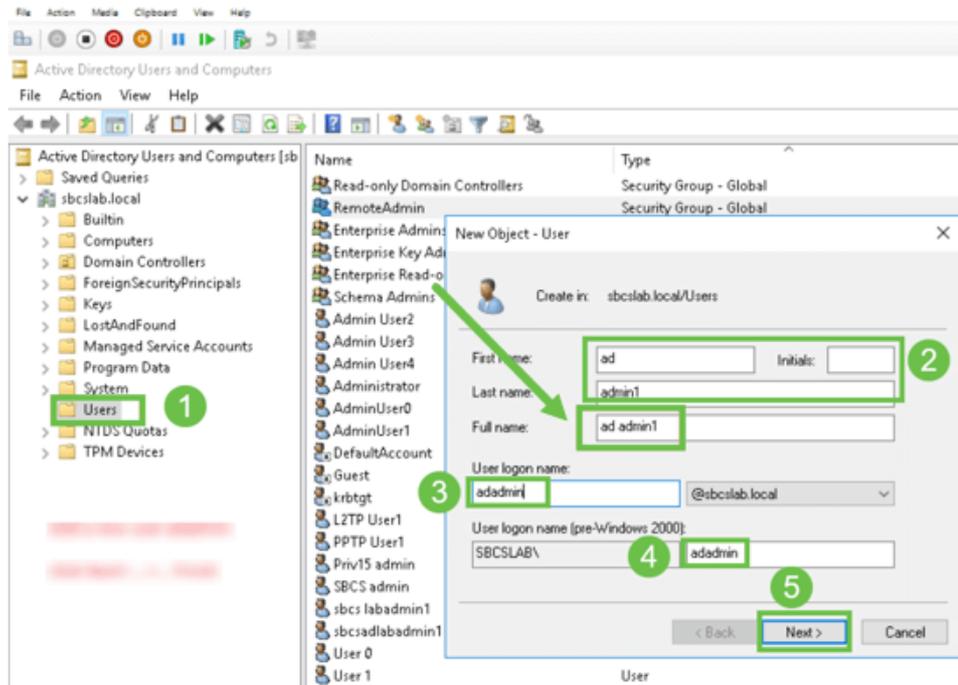
步骤 4

在"新对象 — 用户"下，填写"名"、"名"、"姓"和"姓"，"全名"字段将自动填充，其中显示名和姓之间的空格。

必须删除"全名"框中名字和*姓氏*之间的空格，否则无法正确登录。
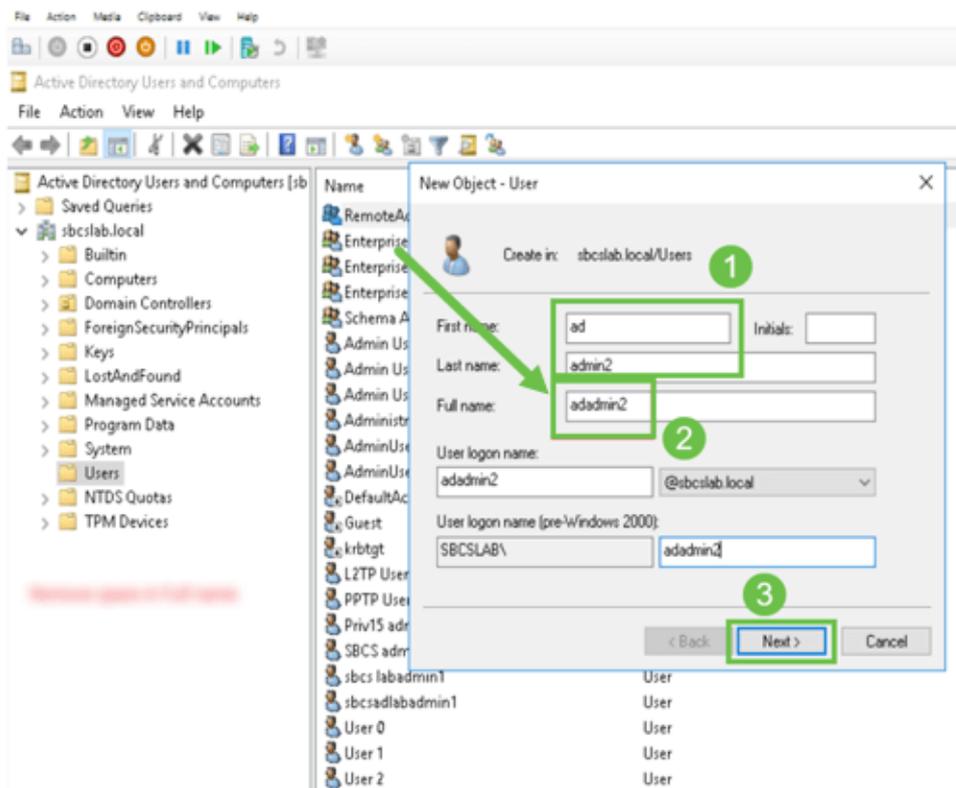
此图显示必须删除的全名中的空间：

步骤 5
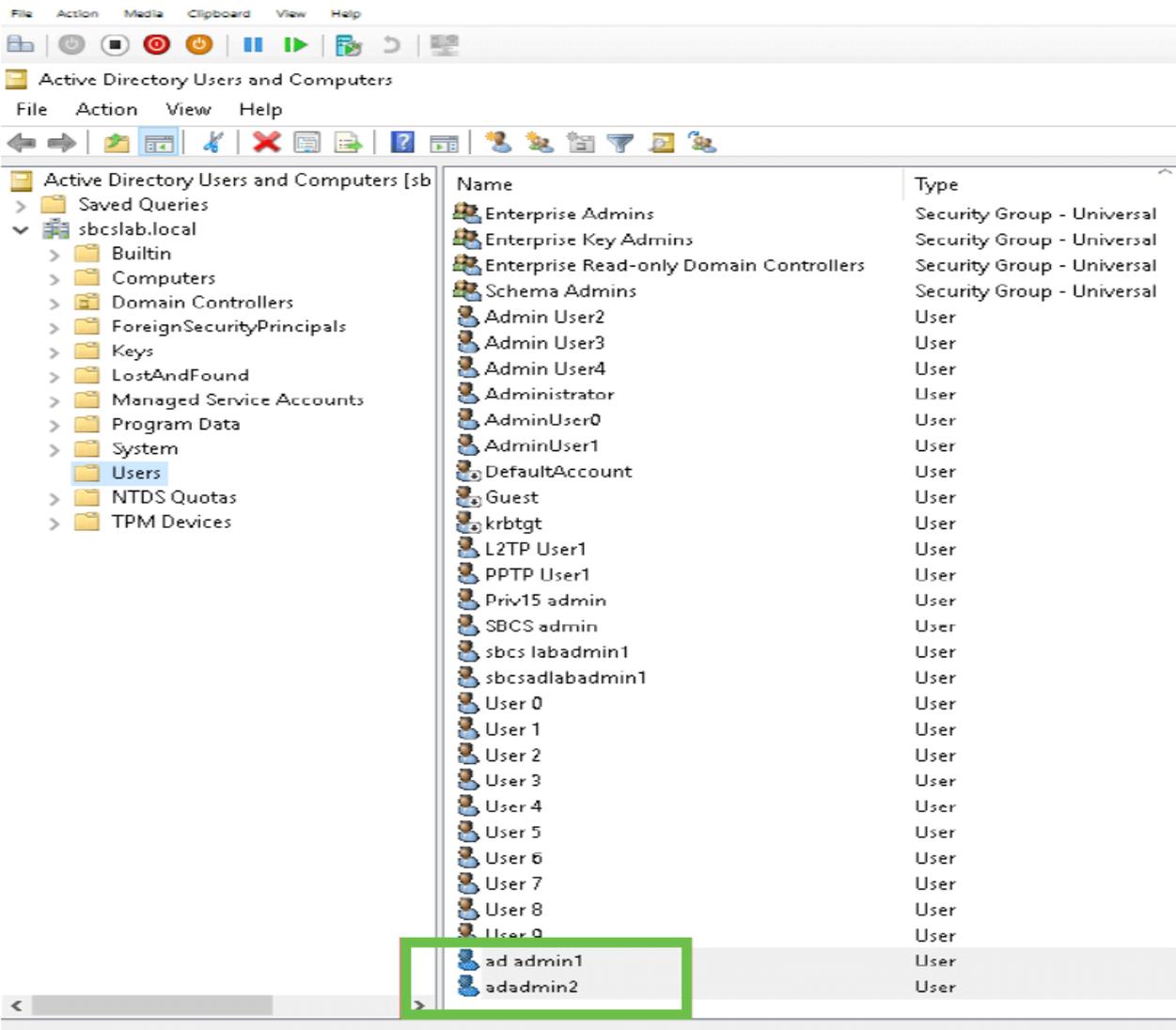
重复上述步骤以创建其他用户。再次，您需要通过删除自动创*建的空格*来修改"全名"字段。单击 Next设置密码并完成用户创建。

此图显示"全名"中的空间已删除。这是添加用户的正确方法：

步骤 6
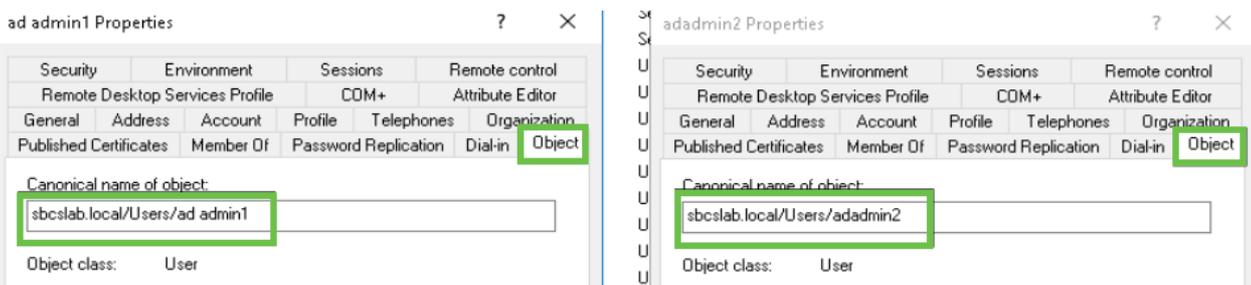
"用户"(Users)列表将显示两个新添加的用户详细信息。
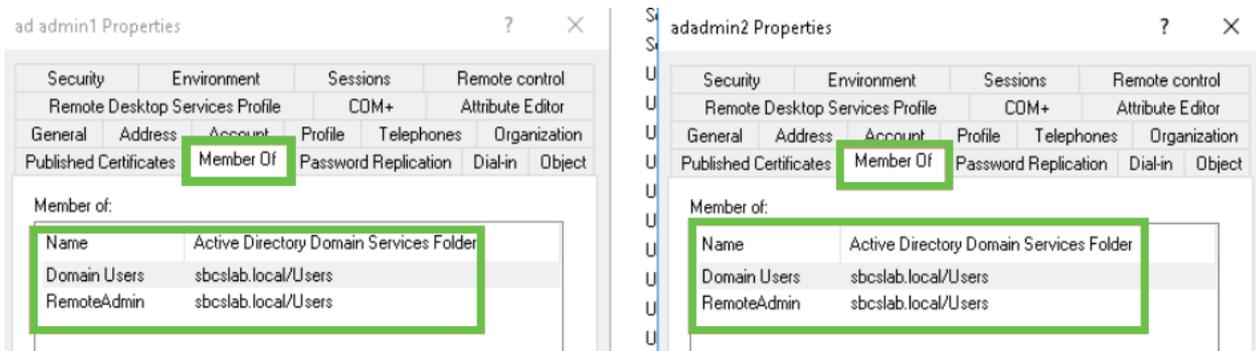
步骤 7

您会注意到，*ad admin1*显示名字和姓氏之间的空格，如果这不是固定的，登录将失败。此错误留在演示中，请勿留空间！*adadmin2*示例正确。
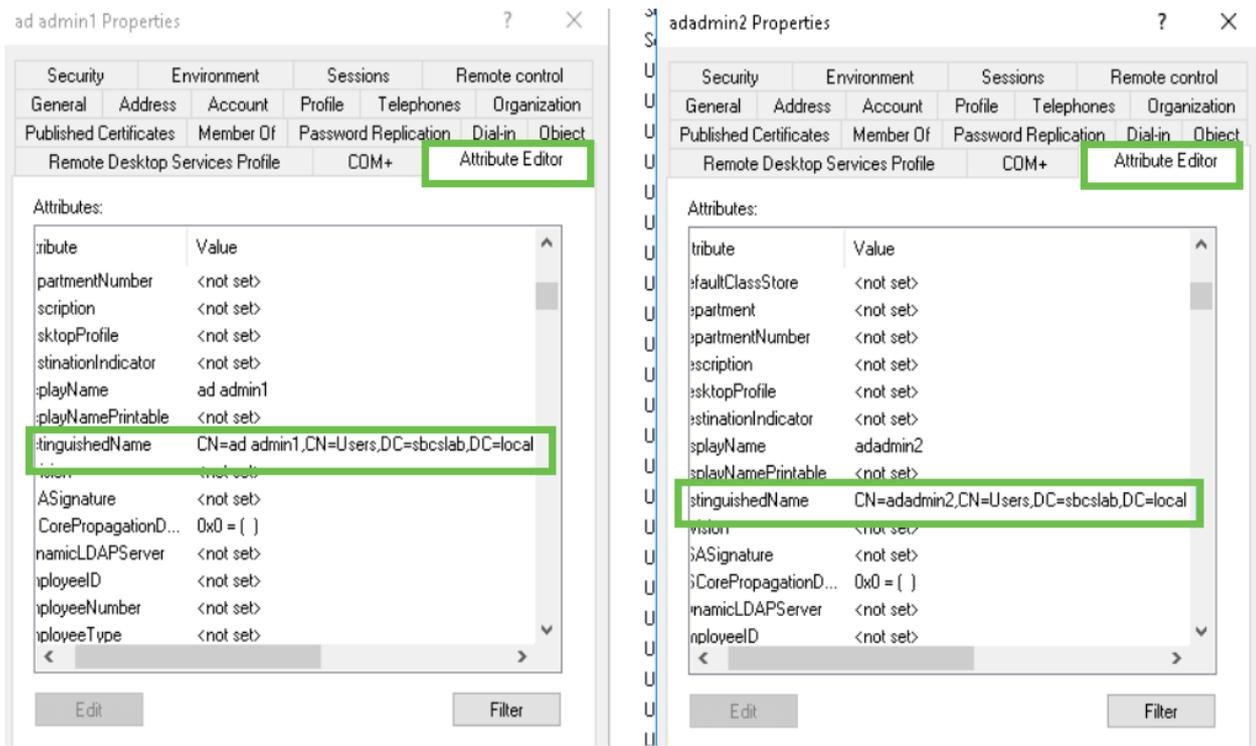
要查看，请右键单击ad admin 1*用户名*，然后选择"**属性**"选项。然后导航至"**对象**"选项卡，查看"**对象**"详细信息的规范名称。

此外，您还可以导航至"*属性*"选项下的"*成员*"选项卡，以验证这些用户名的"*域用户*"和远程管理详细信息。

导航至属性编辑器选项卡，以验证这些用户名的DistinguishedName值。
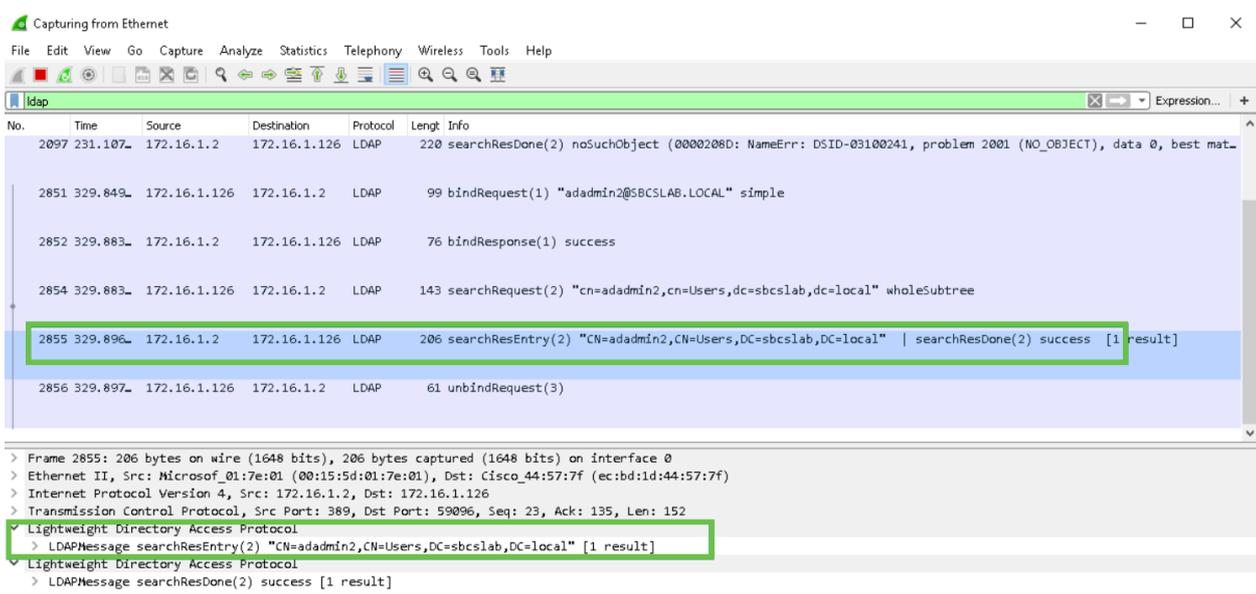
步骤 8

使用用户登录名登录，在本例中为*adadmin2*，您将看到登录成功。

步骤 9

您可以查看数据包捕获的详细信息，如以下屏幕截图所示。

如果不从全名字段中取出空格，会发生什么情况？

如果尝试使用*用户登录名*，在本例中为*adadmin*，则会看到登录失败，因为轻量目录访问协议 (LDAP)服务器无法返回对象，因为全名(在本例中为*adadmin1*,)有空格。您将能够在捕获数据包时看到详细信息，如以下屏幕截图所示。

结论

您现在已成功完成并避免了通过RV34x路由器上的Active Directory进行远程身份验证的失败登录。