

使用Active Directory和RV34x路由器的遠端身份驗證和登入指南

目標

本文說明了如何在Cisco RV34x系列路由器上使用Windows Active Directory(AD)配置遠端身份驗證。此外，還會提供資訊，以避免潛在的登入錯誤。

簡介

在RV34x路由器上配置服務身份驗證設定時，需要選擇外部身份驗證方法。

預設情況下，RV34x系列路由器上的外部資料庫優先順序為RADIUS/LDAP/AD/Local。如果在路由器上新增RADIUS伺服器，Web登入服務和其他服務將使用RADIUS外部資料庫驗證使用者。沒有選項可以單獨為Web登入服務啟用外部資料庫並為其他服務配置另一個資料庫。在路由器上建立並啟用RADIUS後，路由器將使用RADIUS服務作為Web登入、站點到站點VPN、EzVPN/第三方VPN、SSL VPN、PPTP/L2TP VPN和802.1x的外部資料庫。

如果您使用Windows，Microsoft會提供內部AD服務。AD儲存網路的所有基本資訊，包括使用者、裝置和策略。管理員使用AD作為單一位置建立和管理網路。它有助於以統一的方式處理互連、複雜和不同的網路資源。

配置後，任何獲得授權的使用者都可以使用外部AD選項（在Windows伺服器作業系統中）進行身份驗證，以使用RV34x路由器上的任何特定服務。授權使用者可以使用提供的功能，只要他們擁有使用該型別身份驗證所需的硬體和軟體。

適用裝置 | 軟體版本

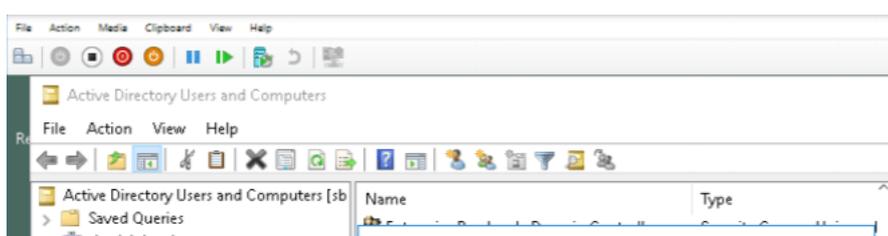
- RV340 | 1.0.03.16
- RV340W | 1.0.03.16
- RV345 | 1.0.03.16
- RV345P | 1.0.03.16

目錄

- [標識可分辨名稱值](#)
- [為Active Directory建立使用者組](#)
- [在RV34x路由器上新增Active Directory詳細資訊](#)
- [如果不從全名欄位中取出空格會發生什麼？](#)

標識可分辨名稱值

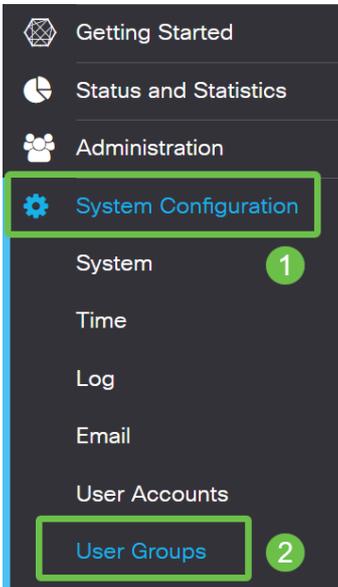
訪問Windows 2016伺服器上的Active Directory使用者和電腦管理介面。選擇Users容器資料夾，按一下右鍵滑鼠，然後開啟Properties。請注意稍後將在RV34x路由器User Container Path欄位中使用的DistinguishedName值。



為Active Directory建立使用者組

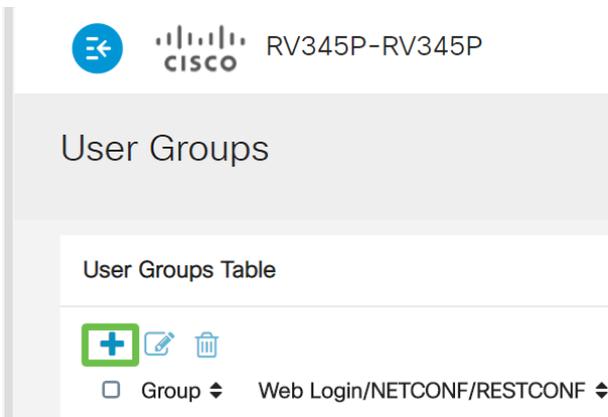
步驟1

登入到RV34x系列路由器。導覽至System Configuration > User Groups。



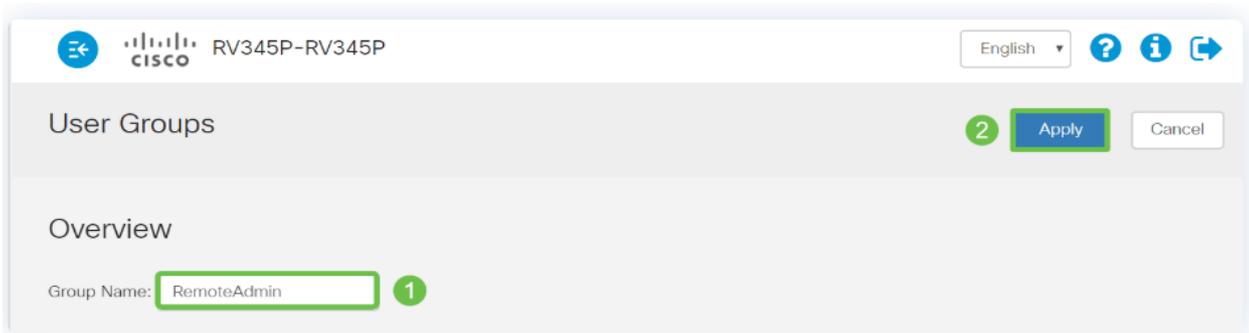
步驟2

點選加號圖示。



步驟3

輸入組名稱。按一下「Apply」。



在此示例中，已創建了一個RemoteAdmin使用者組。

步驟4

按一下新使用者組旁邊的竅取方塊。按一下 **edit** 圖示。

User Groups

User Groups Table

+ [edit] [trash]

Group ▾ Web Login/NETCONF/RESTCONF ▾

1 Remote... Disabled

步驟5

向下滾動頁面至 *Services*。按一下 **Administrator** 單選按鈕。

Services

Web Login/NETCONF/RESTCONF Disabled Read Only Administrator

Site to Site VPN

步驟6

按一下「Apply」。

Apply Cancel

第7步

現在，您將看到顯示具有管理員許可權的新使用者組。

Getting Started
Status and Statistics
Administration
System Configuration
System
Time
Log
Email
User Accounts
User Groups

RV345P-router4491EF cisco (admin) English ? i

User Groups Apply Cancel

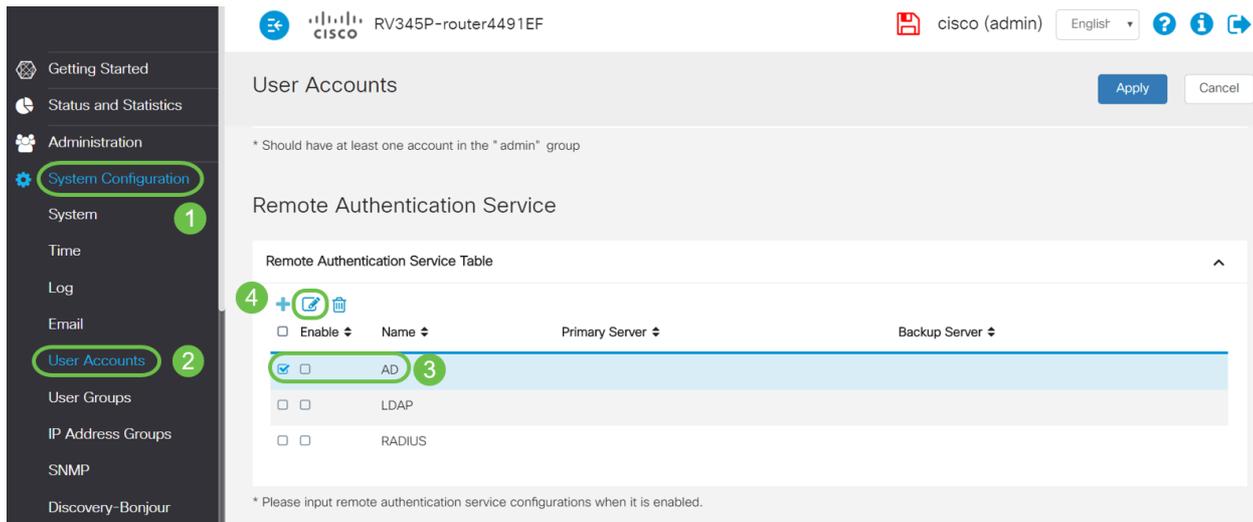
User Groups Table

Group	Web Login/NETCONF/RESTCONF	S2S-VPN	EzVPN/3rd Party	SSL VPN	PPTP	L2TP	802.1x
<input checked="" type="checkbox"/> RemoteAdmin	Admin	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/> admin	Admin	Disabled	Disabled	SSLVPDef...	Enabled	Enabled	Enabled
<input type="checkbox"/> anyconnect	Disabled	Disabled	Disabled	SSLVPDef...	Disabled	Disabled	Disabled
<input type="checkbox"/> guest	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

在RV34x路由器上新增Active Directory詳細資訊

步驟1

導航到系統配置>使用者帳戶。選擇AD選項並按一下edit icon以新增AD伺服器的詳細資訊。



步驟2

輸入AD域名、主伺服器、埠和使用者容器路徑詳細資訊。按一下「Apply」。

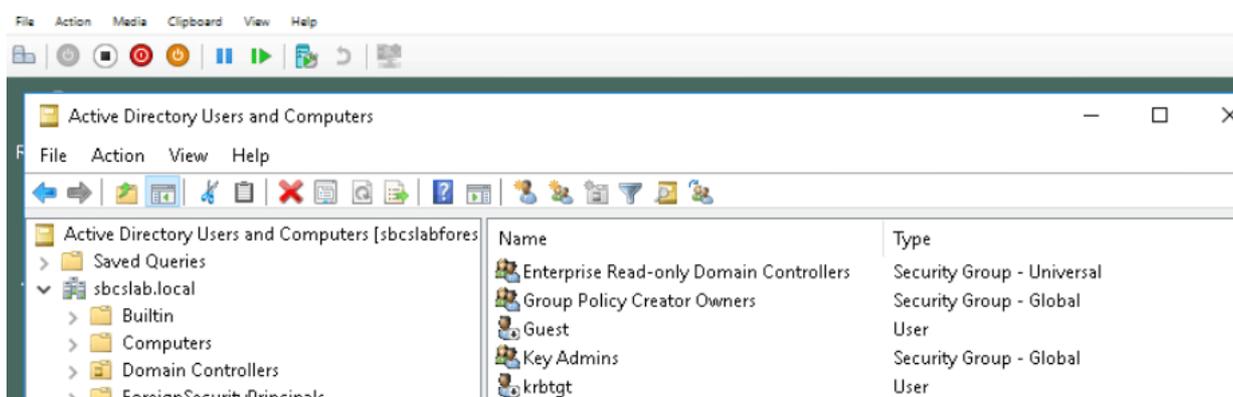


附註：您需要在本文 [識別可分辨名稱值](#) 部分輸入從Windows伺服器捕獲的使用者容器路徑詳細資訊。

在本示例中，詳細資訊是 `Cn=user, dc=sbcslab, dc=local`。輕量型目錄訪問協定(LDAP)伺服器預設偵聽埠為389。

步驟3

在AD中，驗證是否配置了 *User Group*，並且它匹配路由器的 *User Group* 名稱。

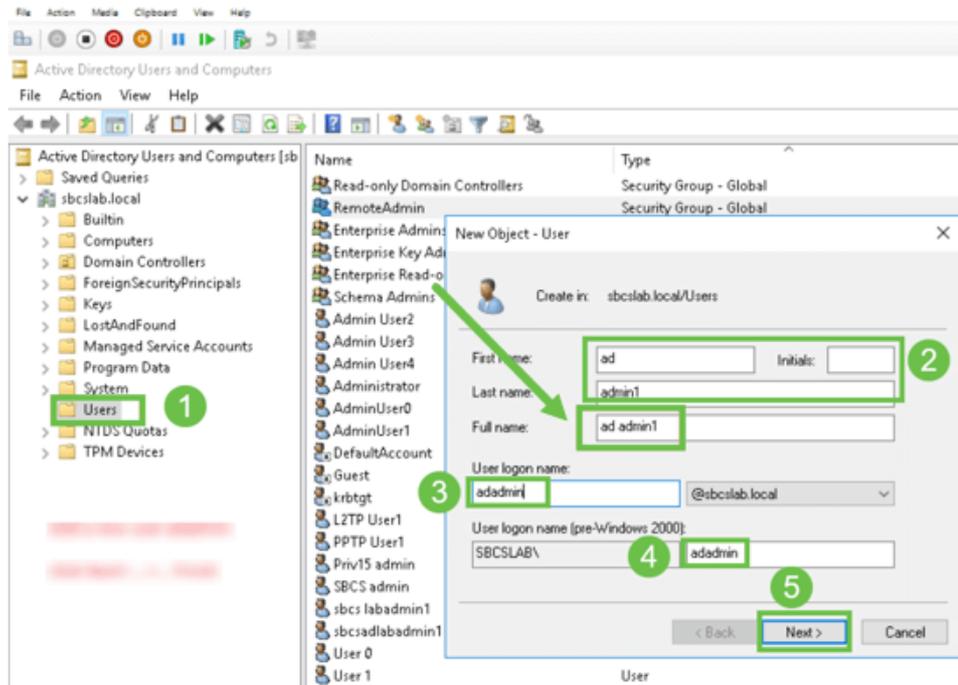


步驟4

在「新對象 — 使用者」(New Object - User)下，填寫名、首字母和姓氏，將自動填充全名欄位，顯示名字和姓氏之間的空格。

全名」框中的名字和姓之間的空格必須刪除，否則將無法正確登入。

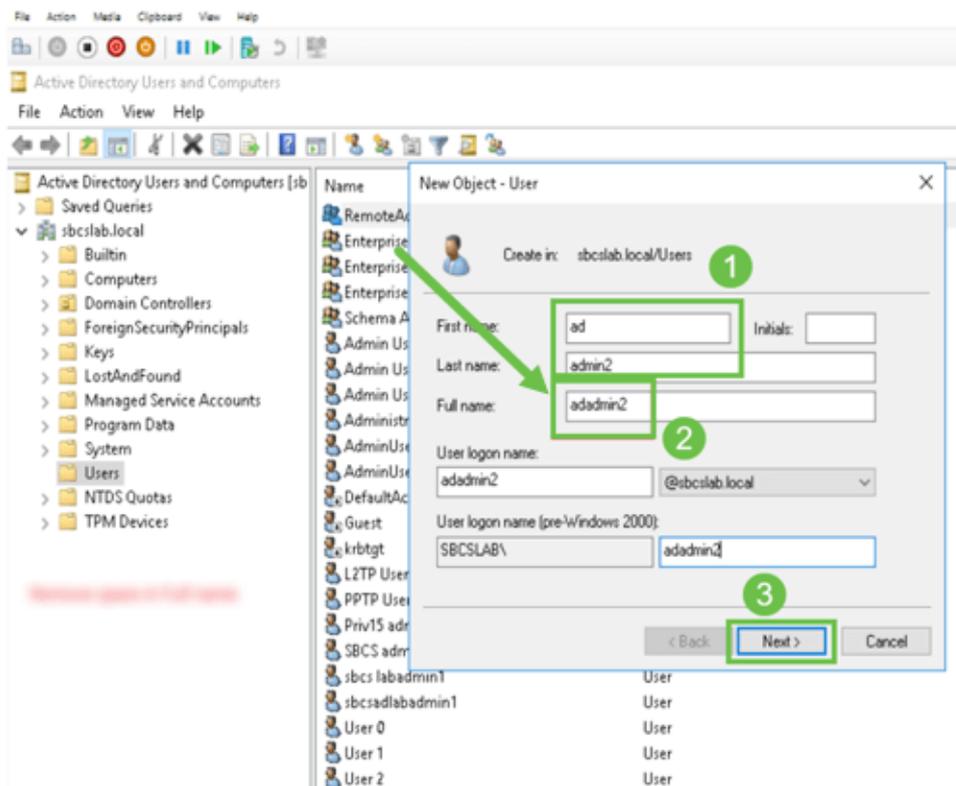
此圖顯示了必須刪除的完整名稱中的空格：



步驟5

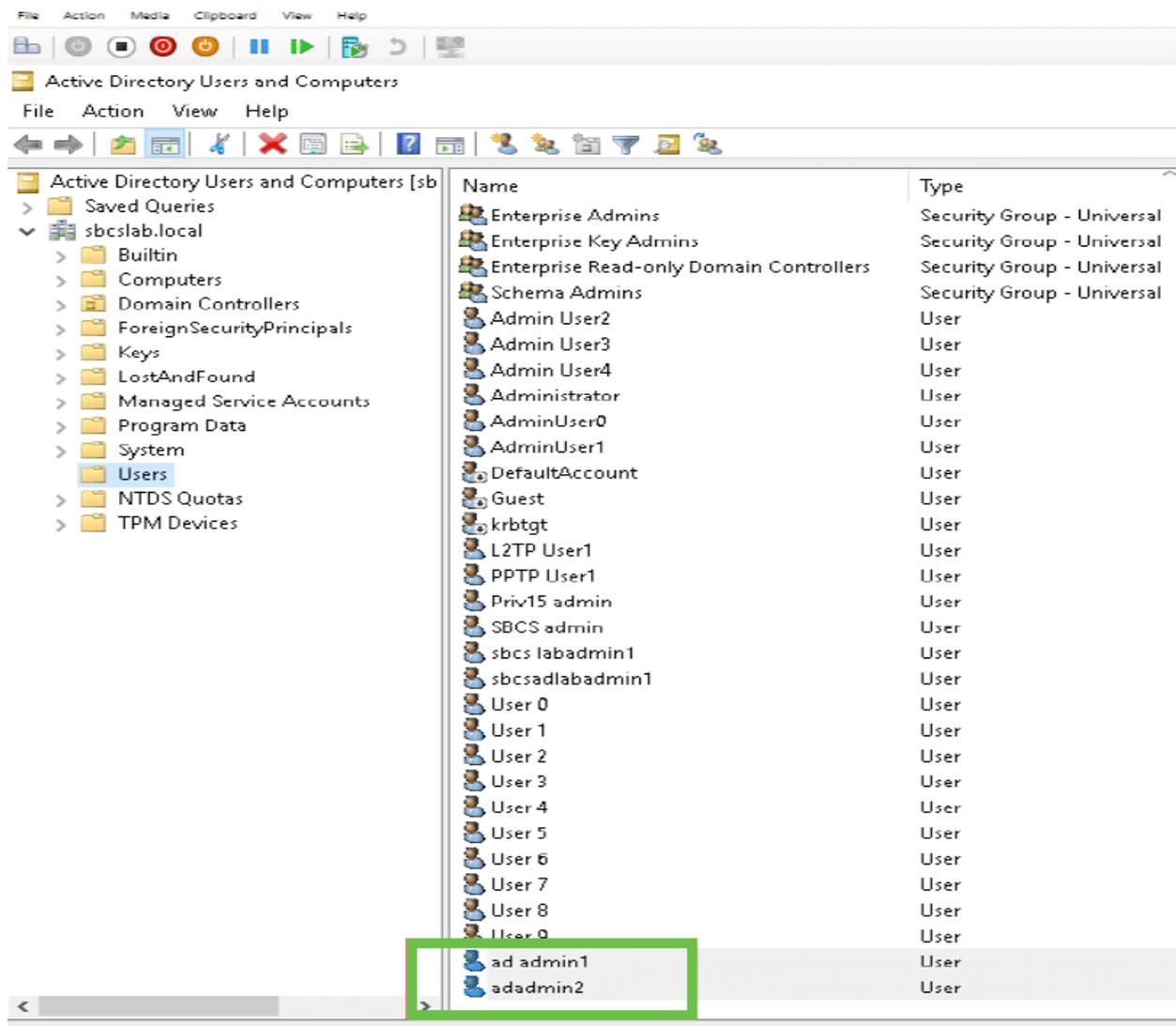
重複這些步驟以建立另一個使用者。同樣，您需要通過刪除自動建立的任何空格來修改全名欄位。按一下下一步設定密碼並完成使用者建立。

此圖顯示「全名」中的空格已被刪除。這是新增使用者的正確方式：



步驟6

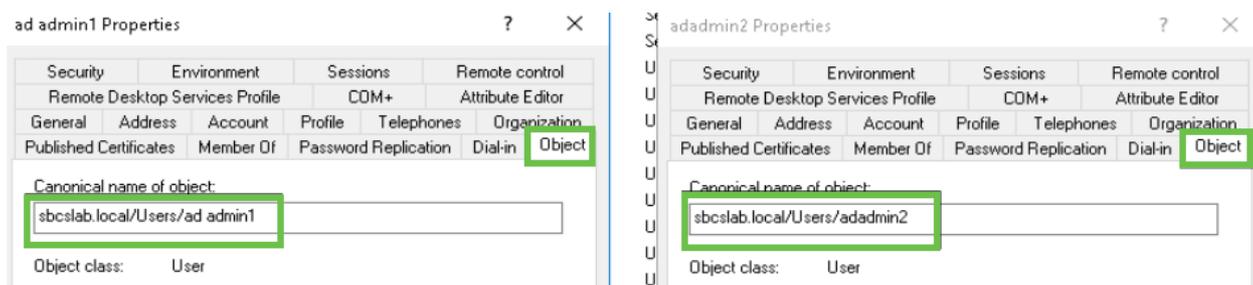
使用者清單將顯示新增的兩個使用者詳細資訊。



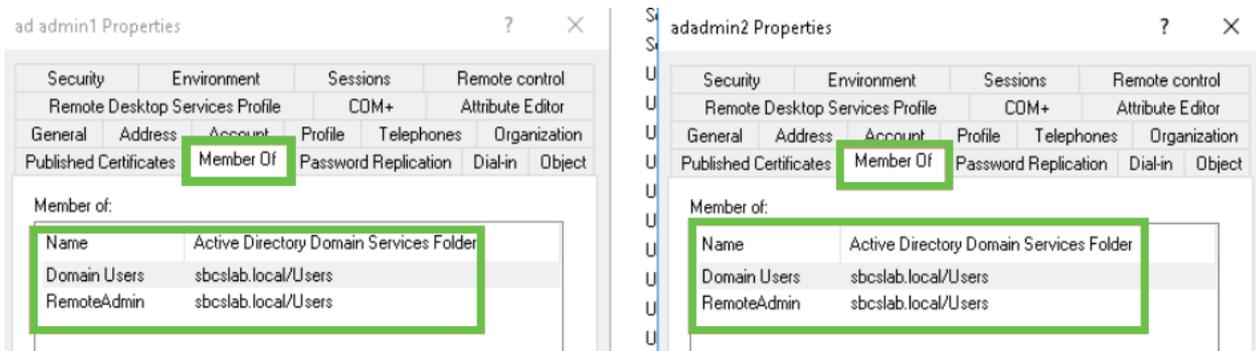
第7步

您會注意到，*ad admin1*顯示名字和姓之間的空格；如果不進行修復，登入將失敗。此錯誤留作演示之用，請勿將空間留在那裡！*adadmin2*示例正確。

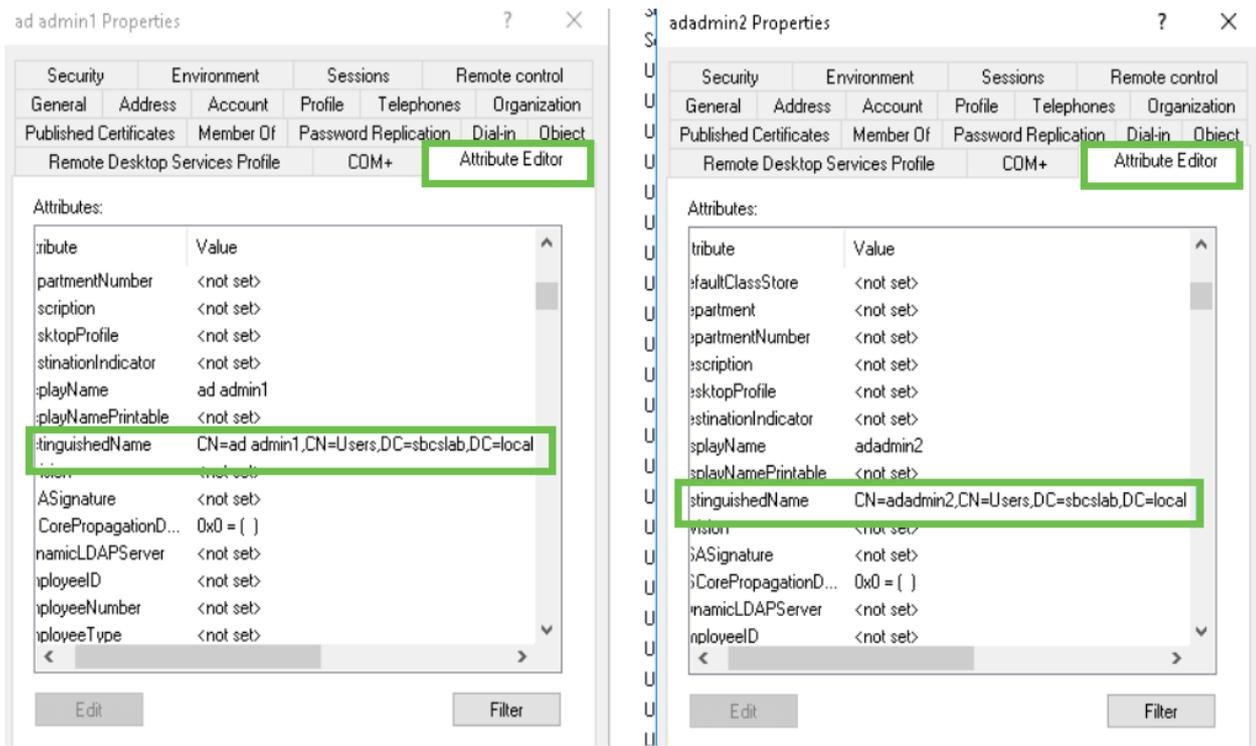
要檢視此檔案，請按一下右鍵*ad admin 1*使用者名並選擇**Properties**選項。然後導航到**Object**頁籤，檢視**Object details**的**規範名稱**資訊。



此外，您還可以導航到**屬性**選項下的**成員**頁籤，驗證這些使用者名稱的域使用者和**RemoteAdmin**詳細資訊。



導航到Attribute Editor選項卡，以驗證這些使用者名稱的DistinguishedName值。

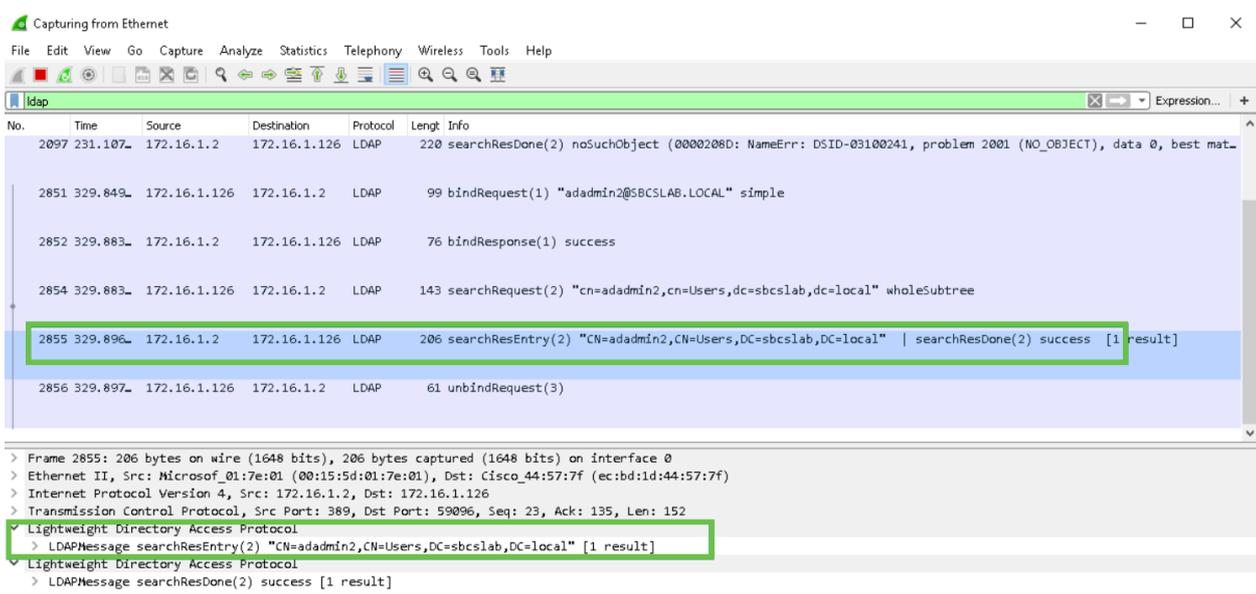


步驟8

使用User logon name(本例中為adadmin2)登入，您將看到登入成功。

步驟9

您可以看到資料包捕獲的詳細資訊，如下面的螢幕截圖所示。



如果不從全名欄位中取出空格會發生什麼？

如果嘗試使用使用者登入名(本例中為`adadmin`)，您將看到登入失敗，因為輕量級目錄訪問協定(LDAP)伺服器無法返回對象，因為全名(本例中為`ad admin1`)有一個空格。捕捉資料包時，您將能夠看到這些詳細資訊，如下面的截圖所示。

結論

現在，您已成功完成並避免了通過RV34x路由器上的Active Directory進行遠端身份驗證的登入失敗。