Active DirectoryおよびRV34xルータを使用したリモート認証およびログインガイダンス

目的

この記事では、Cisco RV34xシリーズルータでWindows Active Directory(AD)を使用してリモート認証を設定する方法について説明します。また、潜在的なログインエラーを回避するための情報も提供されます。

概要

RV34xルータでサービス認証設定を設定する場合は、外部認証方式を選択する必要があります。

デフォルトでは、RV34xシリーズルータの外部データベースプライオリティはRADIUS/LDAP/AD/Localです。ルータにRADIUSサーバを追加すると、Web口グインサービスやその他のサービスは、RADIUS外部データベースを使用してユーザを認証します。Web口グインサービス専用の外部データベースを有効にし、別のサービス用に別のデータベースを設定するオプションはありません。ルータでRADIUSが作成され、有効になると、ルータはRADIUSサービスをWeb口グイン、サイト間VPN、EzVPN/3rd Party VPN、SSL VPN、PPTP/L2TP VPN、および802.1xの外部データベースとして使用します。

Windowsを使用している場合、Microsoftは内部ADサービスを提供します。ADには、ユーザ、デバイス、ポリシーなど、ネットワークに不可欠な情報がすべて保存されます。管理者は、ネットワークを作成および管理するための単一の場所としてADを使用します。相互接続された複雑な異なるネットワークリソースを一元的に扱いやすくします。

設定が完了すると、承認されたユーザは外部ADオプション（Windows Server OSに存在）を使用して認証を行い、RV34xルータ上の特定のサービスを使用できます。権限のあるユーザは、そのタイプの認証を使用するために必要なハードウェアとソフトウェアがある限り、提供された機能を使用できます。

該当するデバイス |ソフトウェアバージョン

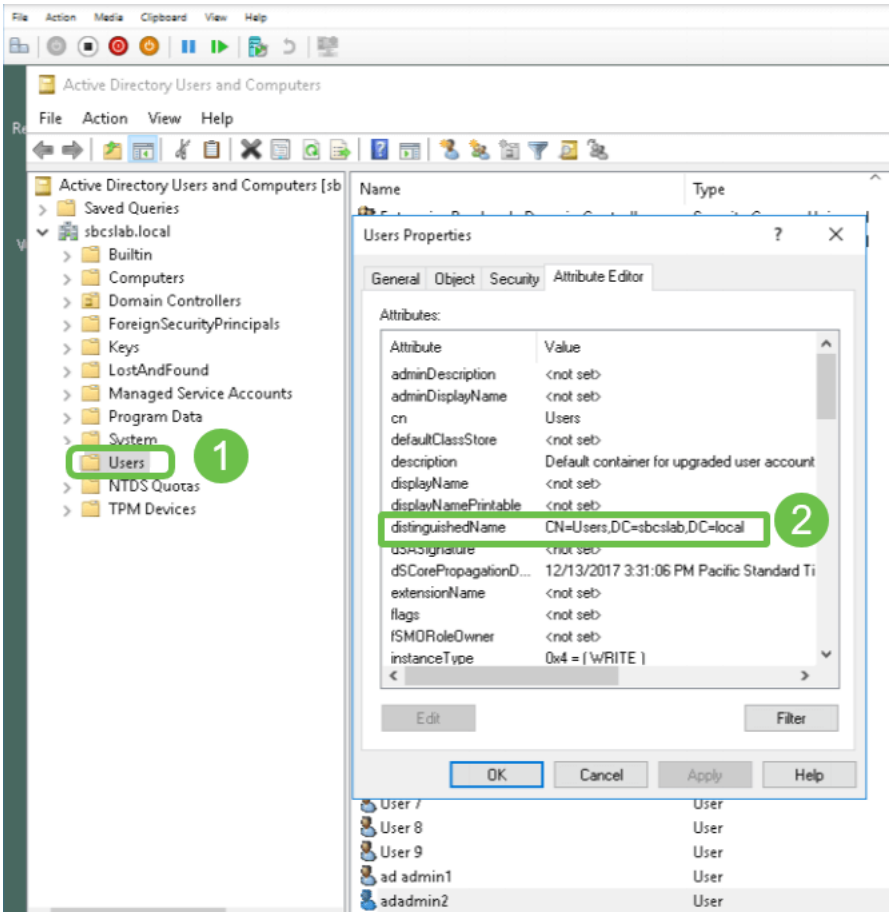
- RV340 |1.0.03.16
- RV340W |1.0.03.16
- RV345 |1.0.03.16
- RV345P |1.0.03.16

目次

識別名の値の特定

Windows 2016サーバ*のActive Directoryユーザーとコンピューター*の管理インターフェイスにアクセスします。Usersコンテナフォ**ルダを選**択し、マウスを右クリックして[プロパティ]を**開きます**

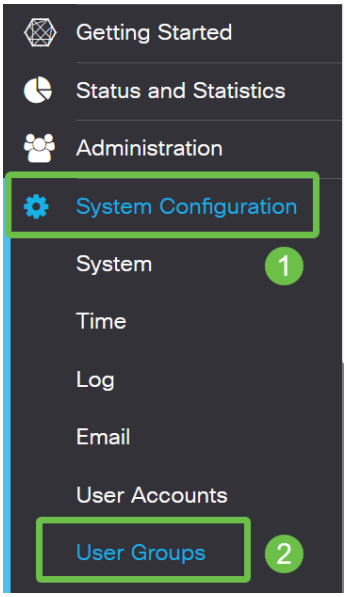
。後でRV34xルータの*User Container Path*フィールドで使用するDistinguishedNameの値を書き留めます。



Active Directoryのユーザグループの作成

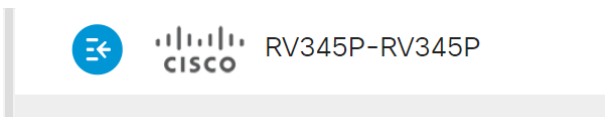
手順 1

RV34xシリーズルータにログインします。[System Configuration] > [User Groups]に移動します。



手順 2

[+]アイコンをクリックします。



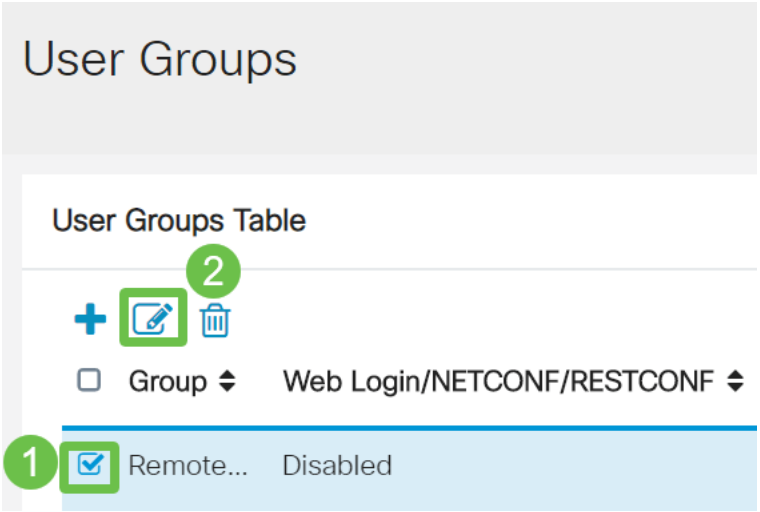
手順 3

グループ名を入力します。[Apply] をクリックします。

この例では、RemoteAdminユーザーグループが作成されています。

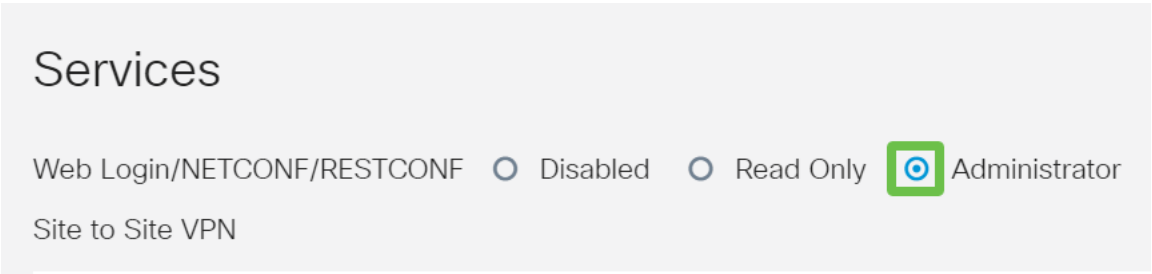
手順 4

新しいユーザグループの横にあるチェックボックスをクリックします。編集アイコンを**クリックします。**



手順 5

ページを下にスクロールして[サービス]に*移動します。*「管理者」ラジオ・**ボタン**をクリックします。

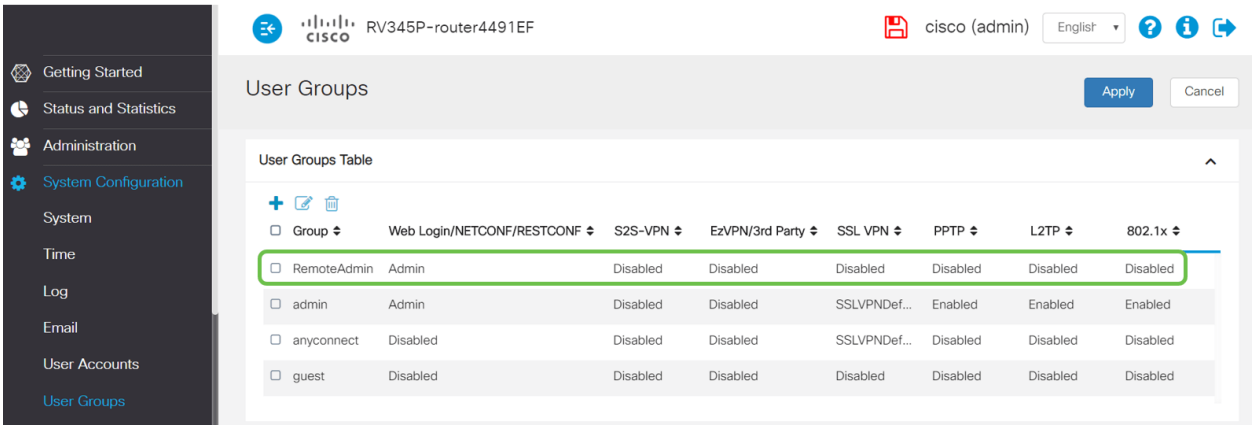


手順 6

[Apply] をクリックします。

ステップ7

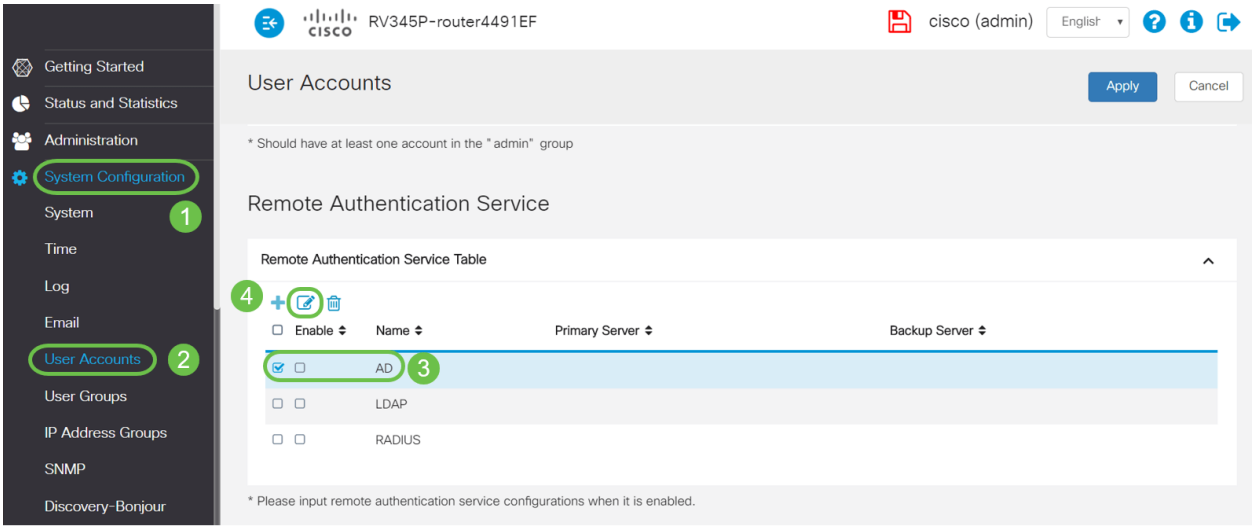
新しいユーザグループが管理者権限で表示されます。



RV34xルータでのActive Directoryの詳細の追加

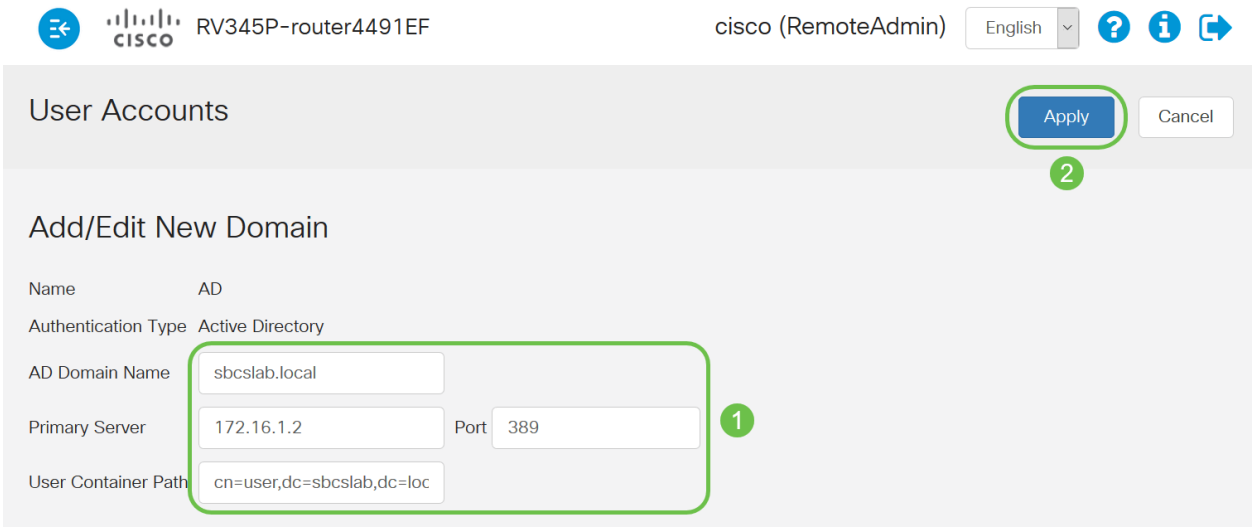
手順 1

[システム構成] > [**ユーザーアカウント]に移動します。**ADオプションを*選択*し、編集アイコンを**クリック**して、ADサーバの詳細を追加します。



手順 2

[*AD Domain Name*]、[*Primary Server*]、[*Port*]、および[*User Container Path*]の*詳細を入力*します。[Apply] をクリックします。

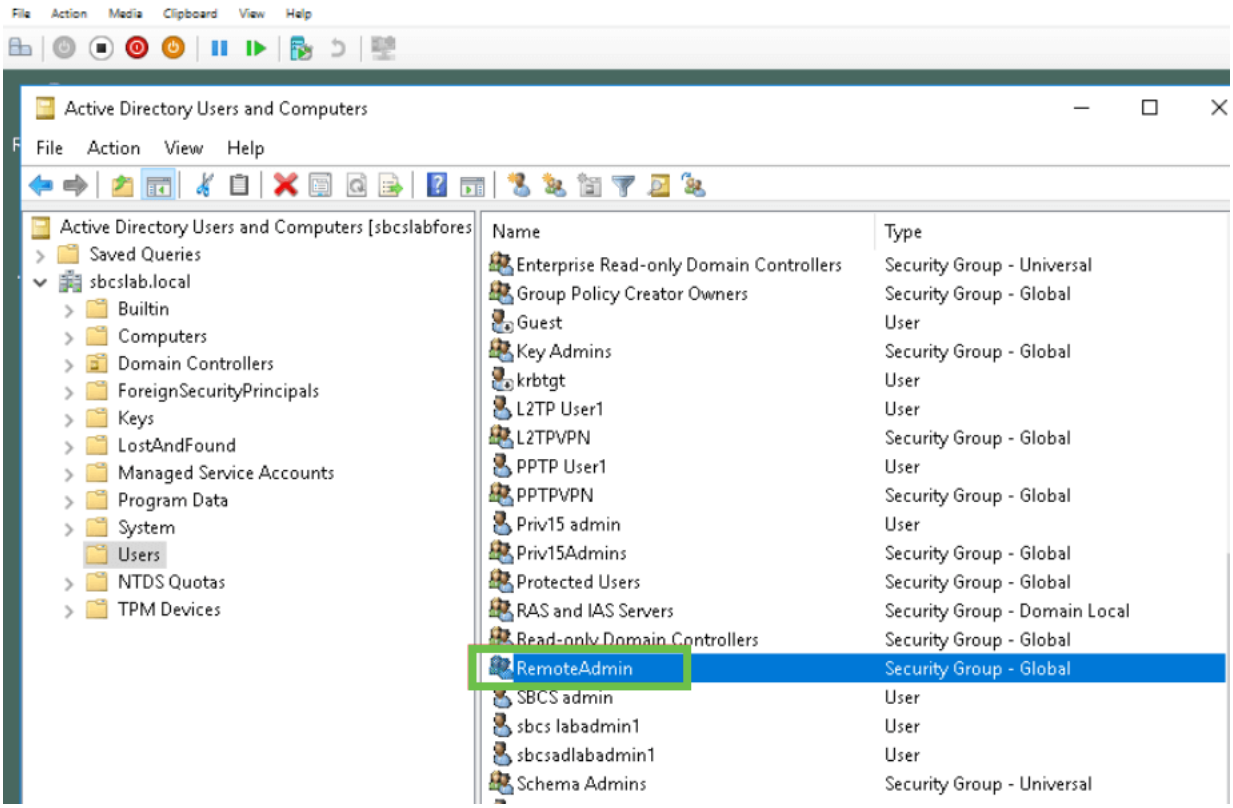


注：この記事の「識別名の識別」*セクション*で、Windowsサーバから取得したユーザコンテナ[パスの詳細を入力する](#)必要があります。

この例では、詳細は*Cn=user,dc=sbcslab,dc=local*です。Lightweight Directory Access Protocol(LDAP)サーバのデフォルトのリスニングポートは389です。

手順 3

ADで、ユーザグループが設定され、*ルータ*のユーザグループ名と一致していることを*確認*します。

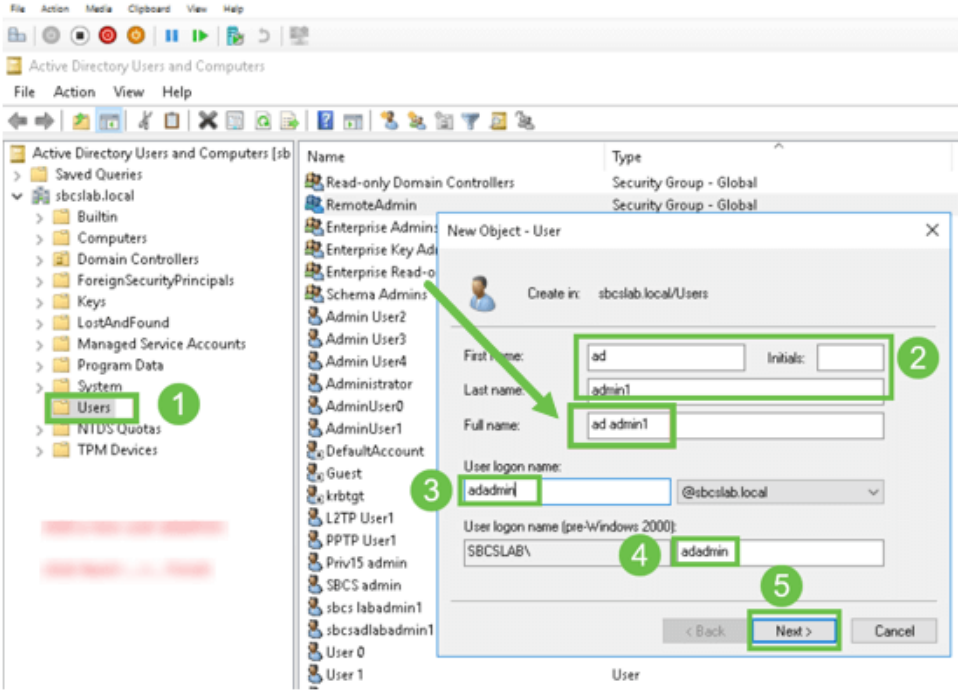


手順 4

[New Object - User]で、[*First name*]、[*Initials*]、[*Last name*]を入力します。[*Full name*]フィールドは自動的に入力され、姓と名の間のスペースが表示されます。

[フルネーム]ボックスの名と姓の間のスペースを*削除*する必要があります。削除しないと、正しくログインできません。

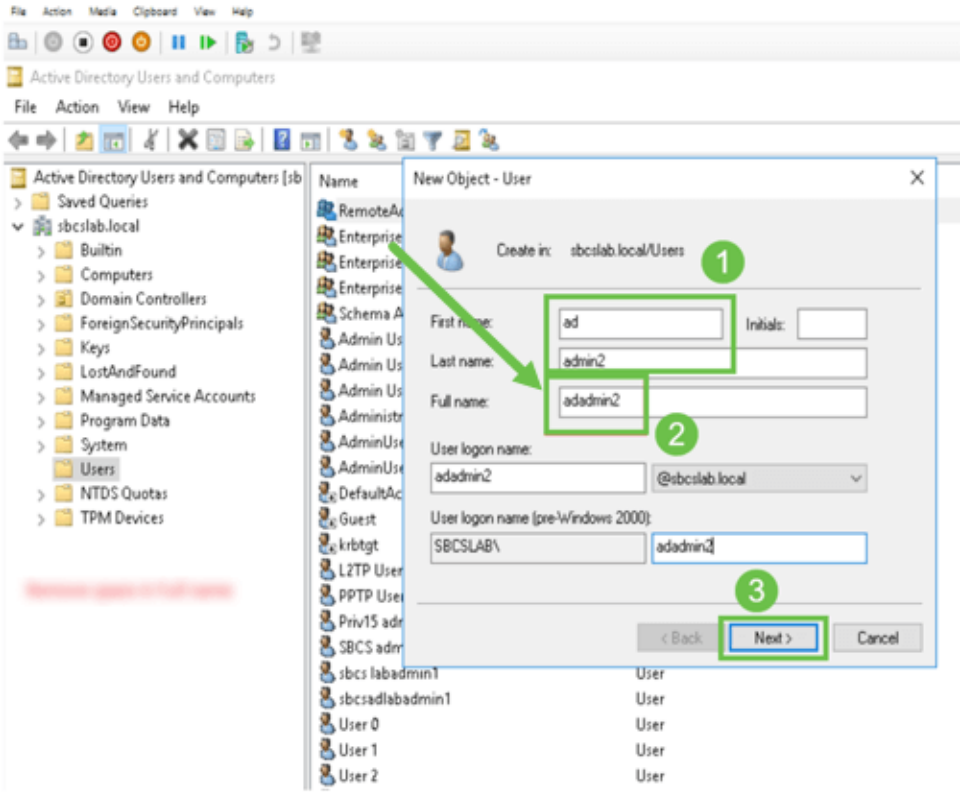
次の図は、削除する必要があるフルネームのスペースを示しています。



手順 5

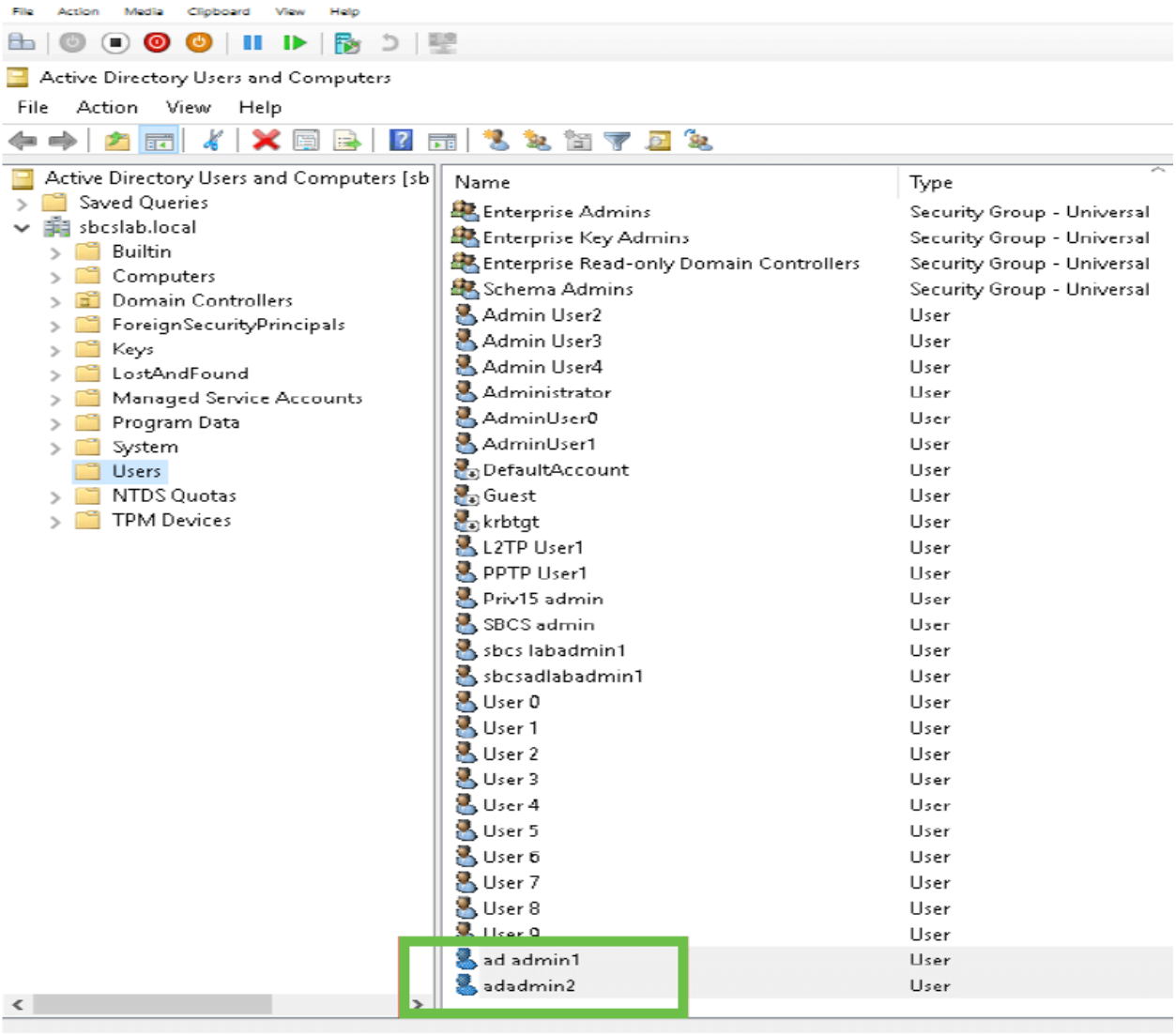
手順を繰り返して、別のユーザを作成します。ここでも、自動的に作成されたスペースを削除して[フルネーム]フィールドを変更する必要があります。[次へ]をクリックして、パスワードを設定し、ユーザの作成を終了します。

次の図は、フルネームのスペースが削除されたことを示しています。ユーザを追加する正しい方法は次のとおりです。



手順 6

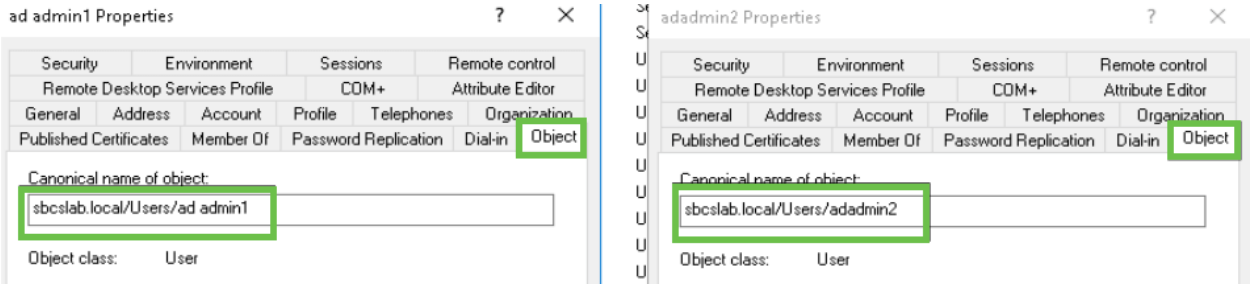
[Users]リストには、新しく追加されたユーザの詳細が両方とも表示されます。



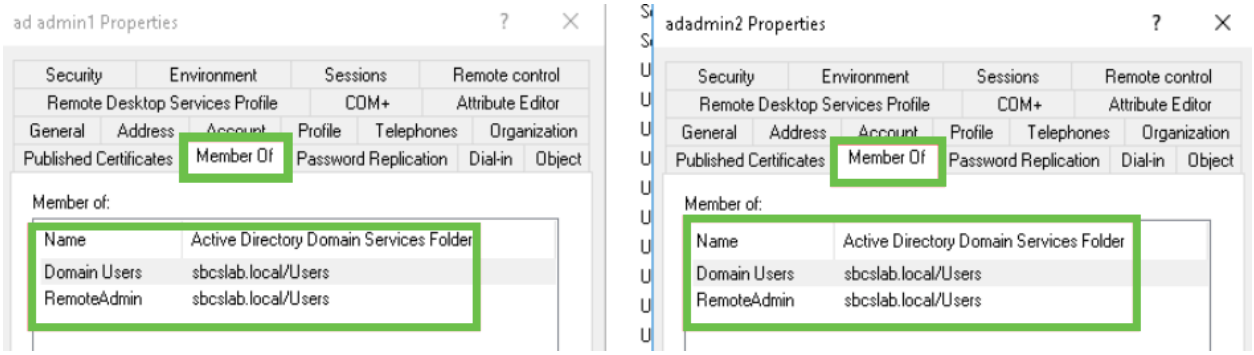
ステップ7

*ad admin1*は姓と名の間にスペースを表示します。このスペースが修正されていない場合、ログインは失敗します。このエラーはデモ用に残されています。スペースを残さないでください。adadmin2*の例*が正しいです。

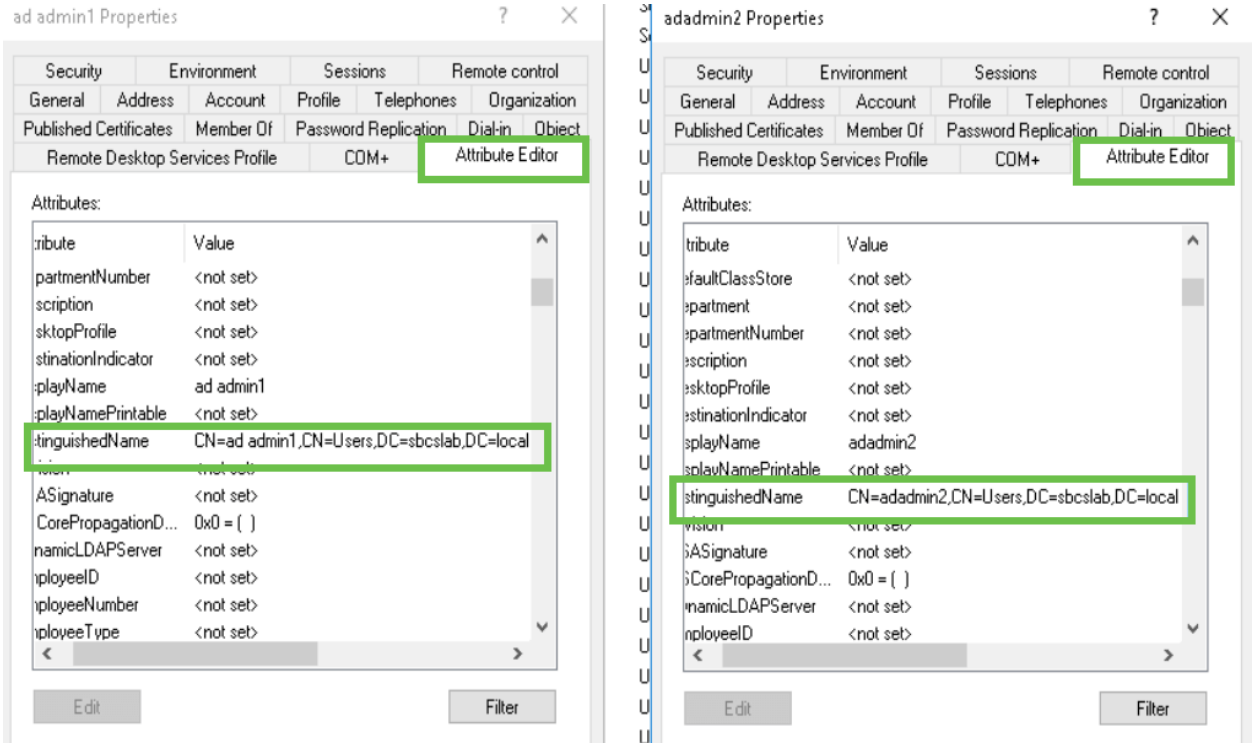
表示するには、ad admin 1ユーザ名を右クリックし、*[プロパティ]*オプションを**選択**します。次に、[オブジェクト**]タブ**に移動し、オブジェクト*の正規名の詳細を確認*します。



また、[Properties]オプションの[*Member Of*]タブに移動することにより、これらのユーザ名の[*Domain Users*]および[*RemoteAdmin*]の詳細を確認でき**ます**。



[Attribute Editor]タブ*に移動し、それらのユーザ名の*DistinguishedName*値を確認します。*

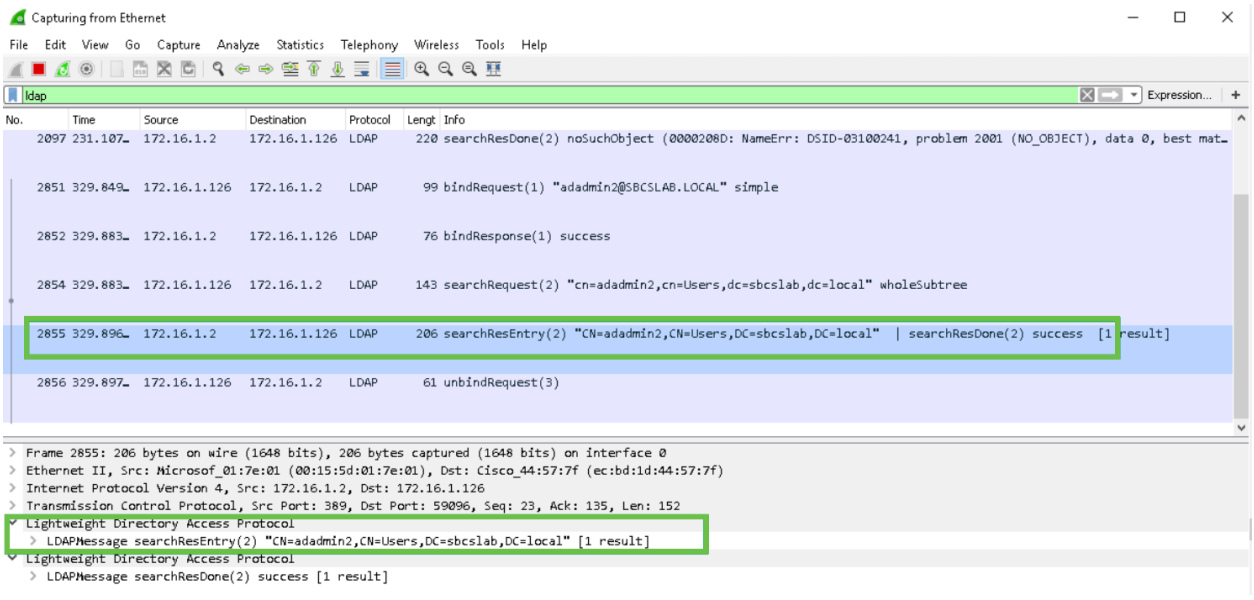


手順 8

User logon name(この場合は*adadmin2*)を使用してログインすると、ログインが正常に行われたことが分かります。

手順 9

次のスクリーンショットに示すように、パケットキャプチャの詳細を確認できます。



完全な名前フィールドからスペースを取らないとどうなりますか。

ユーザーログオン名を使用しようとすると、*adadmin*が表示され、*Lightweight Directory Access Protocol(LDAP)サーバーはオブジェクトを返すことができません*。この場合は*ad admin1*にスペースが入っています。次のスクリーンショットに示すように、パケットをキャプチャすると、その詳細が表示されます。

結論

これで正常に完了し、RV34xルータのActive Directoryを介したリモート認証のログイン失敗を回避できました。