Remote-Authentifizierung und Anmeldeanleitung unter Verwendung von Active Directory und RV34x-Routern

Ziel

In diesem Artikel wird erläutert, wie Sie die Remote-Authentifizierung mithilfe von Windows Active Directory (AD) auf Routern der Cisco Serie RV34x konfigurieren. Darüber hinaus werden Informationen bereitgestellt, um einen möglichen Anmeldefehler zu vermeiden.

Einführung

Wenn Sie die Einstellungen für die Dienstauthentifizierung auf dem RV34x-Router konfigurieren, müssen Sie eine externe Authentifizierungsmethode auswählen.

Die Priorität der externen Datenbank auf dem Router der Serie RV34x lautet standardmäßig RADIUS/LDAP/AD/Local. Wenn Sie den RADIUS-Server auf dem Router hinzufügen, authentifizieren der Weblogin-Dienst und andere Dienste den Benutzer mithilfe der externen RADIUS-Datenbank. Es gibt keine Option, eine externe Datenbank nur für den Weblogin-Dienst zu aktivieren und eine andere Datenbank für einen anderen Dienst zu konfigurieren. Sobald RADIUS erstellt und auf dem Router aktiviert ist, verwendet der Router den RADIUS-Service als externe Datenbank für die Webanmeldung, das Site-to-Site-VPN, das VPN von EzVPN/Drittanbietern, das SSL VPN, das PPTP/L2TP VPN und 802.1x.

Wenn Sie Windows verwenden, stellt Microsoft einen internen AD-Dienst bereit. AD speichert alle wichtigen Informationen für das Netzwerk, einschließlich Benutzer, Geräte und Richtlinien. Administratoren verwenden AD als eine zentrale Stelle für die Erstellung und Verwaltung des Netzwerks. Sie vereinfacht die einheitliche Verwendung von miteinander verbundenen, komplexen und unterschiedlichen Netzwerkressourcen.

Nach der Konfiguration kann sich jede autorisierte Person mithilfe der externen AD-Option (im Windows Server-Betriebssystem vorhanden) authentifizieren, um einen bestimmten Dienst auf dem RV34x-Router zu verwenden. Autorisierte Benutzer können die bereitgestellten Funktionen verwenden, sofern sie über die erforderliche Hardware und Software für die Verwendung dieser Authentifizierungstypen verfügen.

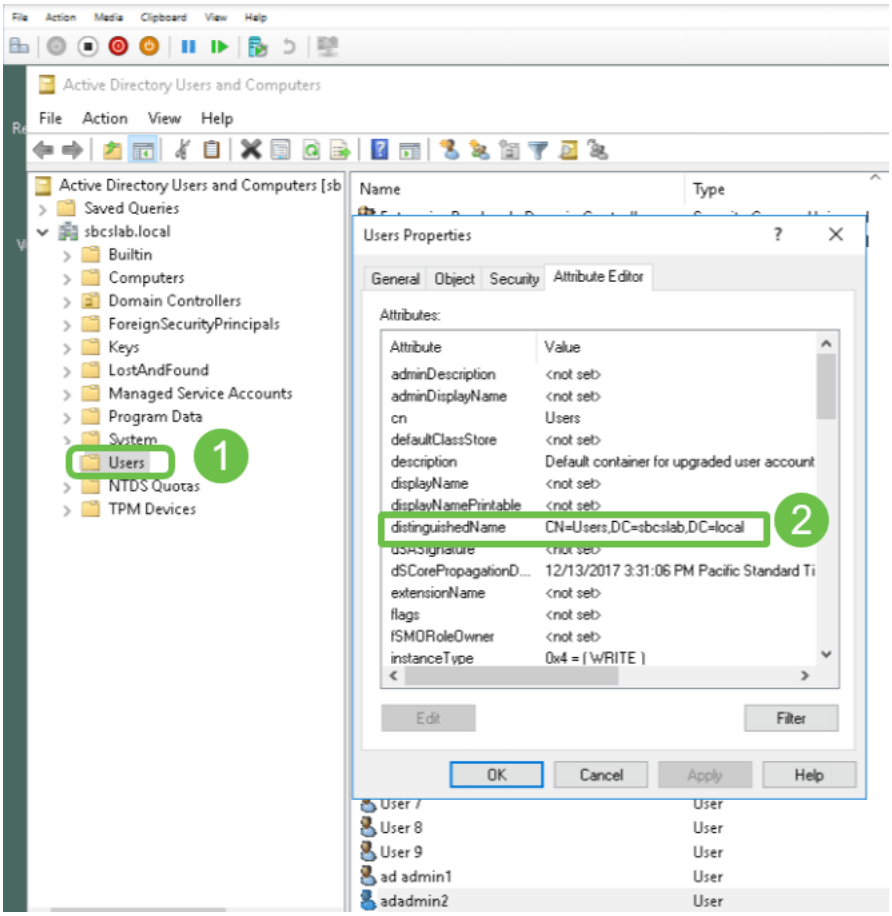
Anwendbare Geräte | Softwareversion

- RV340 | 1.0.03.16
- RV340 W | 1.0.03.16
- RV345 | 1.0.03.16
- RV345P | 1.0.03.16

Inhaltsverzeichnis

Identifizieren des Wertes für den Distinguished Name

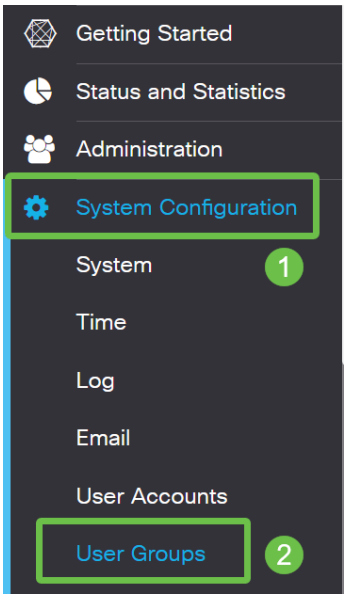
Zugriff auf die Verwaltungsschnittstelle *Active Directory-Benutzer und -Computer* auf dem Windows 2016-Server. Wählen Sie den Ordner **Benutzer**-Container aus, klicken Sie mit der rechten Maustaste, und öffnen Sie **Eigenschaften**. Beachten Sie den Wert *DistinguishedName*, der später im *Feld* RV34x-Router *User Container Path* verwendet wird.



Erstellen einer Benutzergruppe für Active Directory

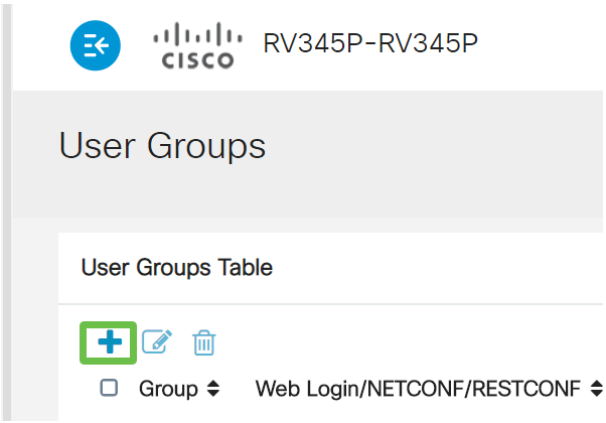
Schritt 1

Melden Sie sich beim Router der Serie RV34x an. Navigieren Sie zu **Systemkonfiguration > Benutzergruppen**.



Schritt 2

Klicken Sie auf das **Pluszeichen**.



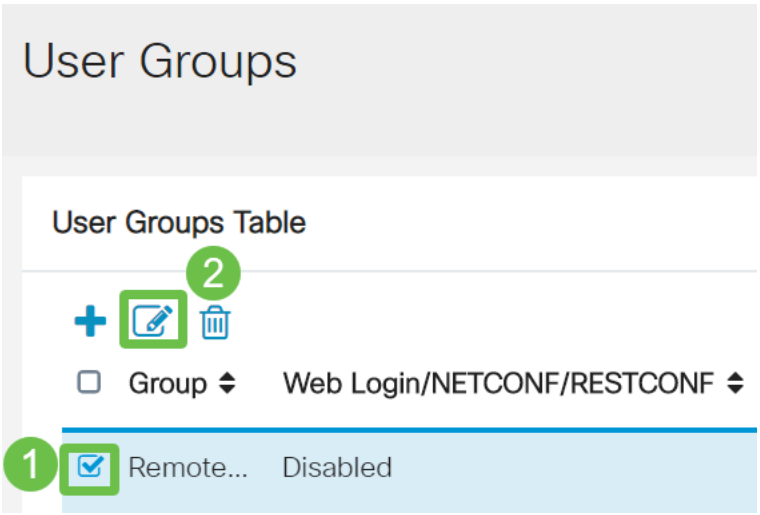
Schritt 3

Geben Sie einen *Gruppennamen ein*. Klicken Sie auf **Übernehmen**.

In diesem Beispiel wurde eine *RemoteAdmin*-Benutzergruppe erstellt.

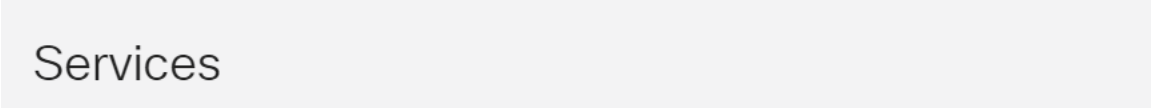
Schritt 4

Klicken Sie auf das Kontrollkästchen neben der neuen Benutzergruppe. Klicken Sie auf das **Bearbeitungssymbol**.



Schritt 5

Blättern Sie auf der Seite nach unten zu *Dienste*. Klicken Sie auf das Optionsfeld **Administrator**.

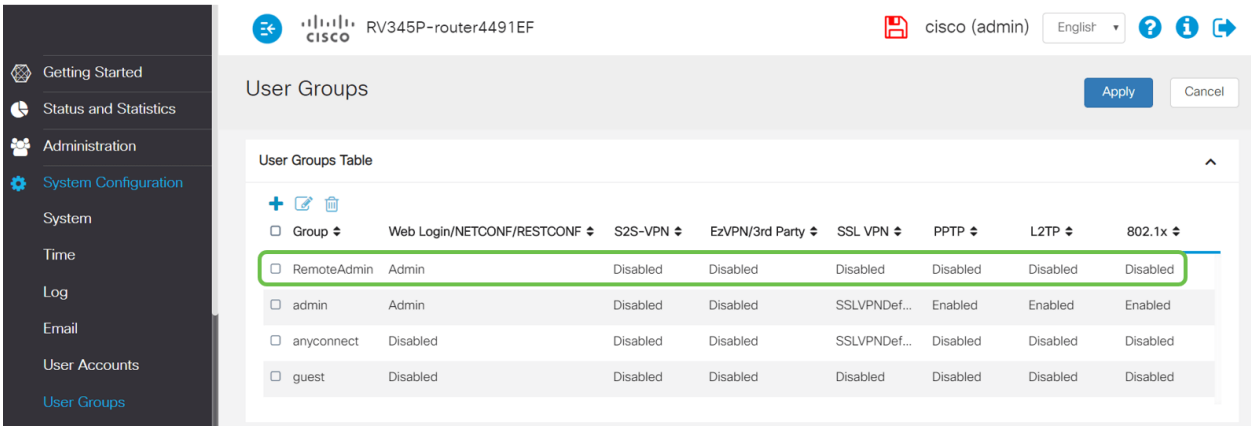


Schritt 6

Klicken Sie auf **Übernehmen**.

Schritt 7

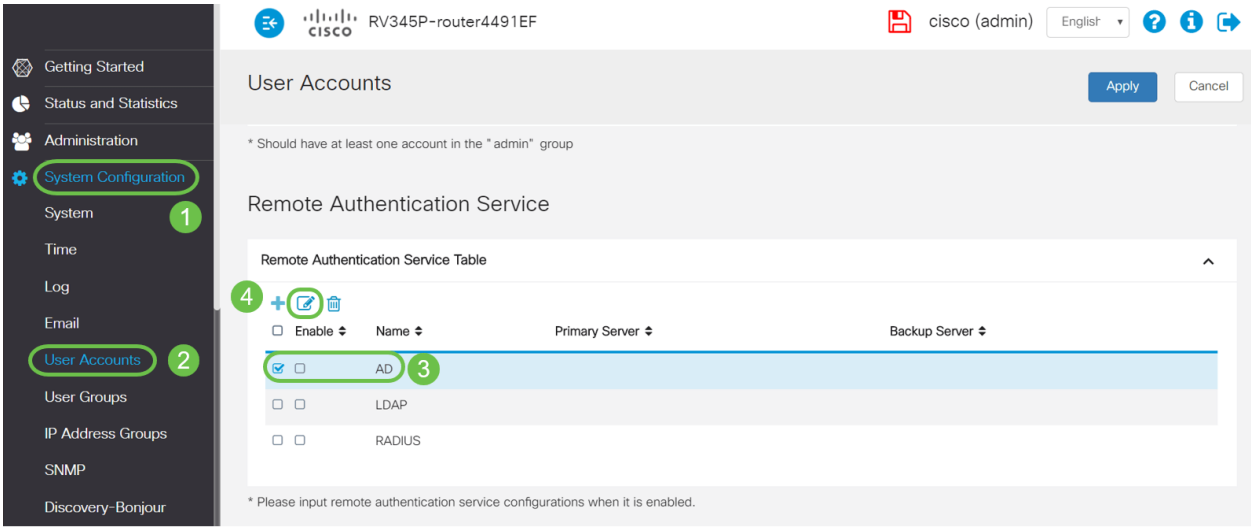
Die neue Benutzergruppe wird nun mit Administratorrechten angezeigt.



Hinzufügen von Active Directory-Details zum RV34x-Router

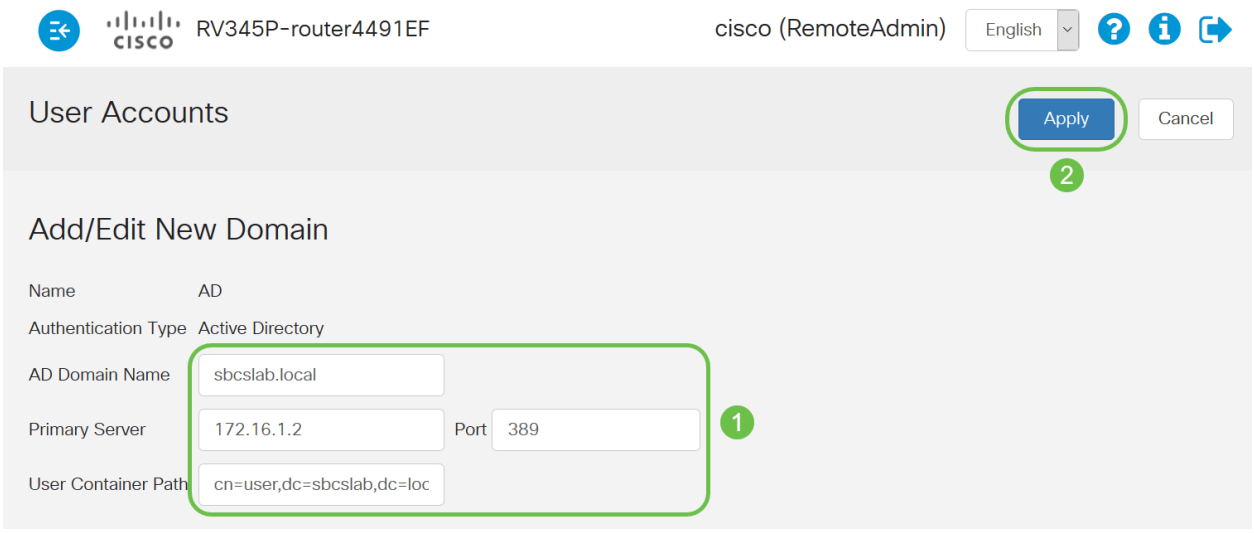
Schritt 1

Navigieren Sie zu **Systemkonfiguration > Benutzerkonten.** Wählen Sie die *AD*-Option aus, und klicken Sie auf das **Bearbeitungssymbol**, um die Details für den AD-Server hinzuzufügen.



Schritt 2

Geben Sie die Details *AD-Domänenname*, *Primärserver*, *Port* und *Benutzercontainerpfad ein*. Klicken Sie auf **Übernehmen**.

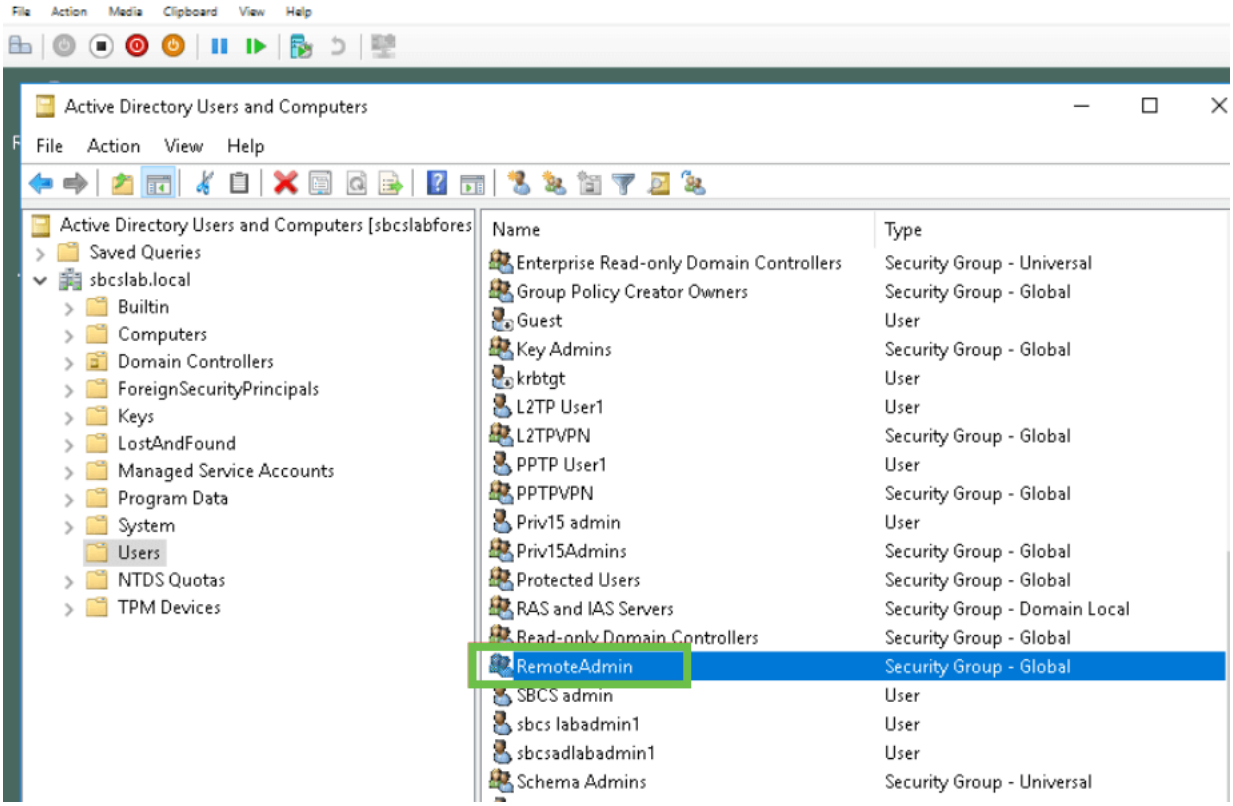


Hinweis: Sie müssen die vom Windows-Server erfassten *User Container Path*-Details im Abschnitt Identify the Distinguished Name Value in diesem Artikel eingeben.

In diesem Beispiel sind die Details *Cn=user,dc=sbcslab,dc=local*. Der Standardüberwachungsport des LDAP-Servers (Lightweight Directory Access Protocol) ist 389.

Schritt 3

Überprüfen Sie im AD, ob die *Benutzergruppe* konfiguriert ist und mit dem *Benutzergruppennamen* des Routers übereinstimmt.



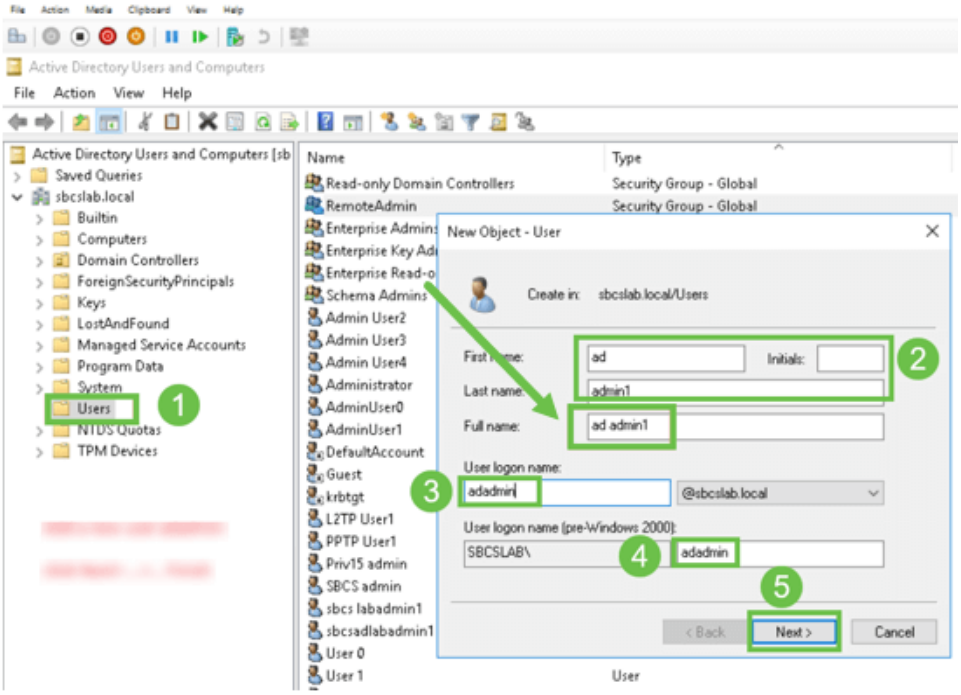
Schritt 4

Unter *Neues Objekt - Benutzer* geben Sie den *Vornamen*, die *Initialen* und den *Nachnamen ein*, das *Feld Vollständiger Name wird automatisch ausgefüllt, sodass ein Leerzeichen zwischen dem Vor- und Nachnamen angezeigt wird.*

Der Abstand zwischen dem Vor- und dem Nachnamen im Feld *Vollständiger Name* muss gelöscht

werden, oder er meldet sich nicht richtig an.

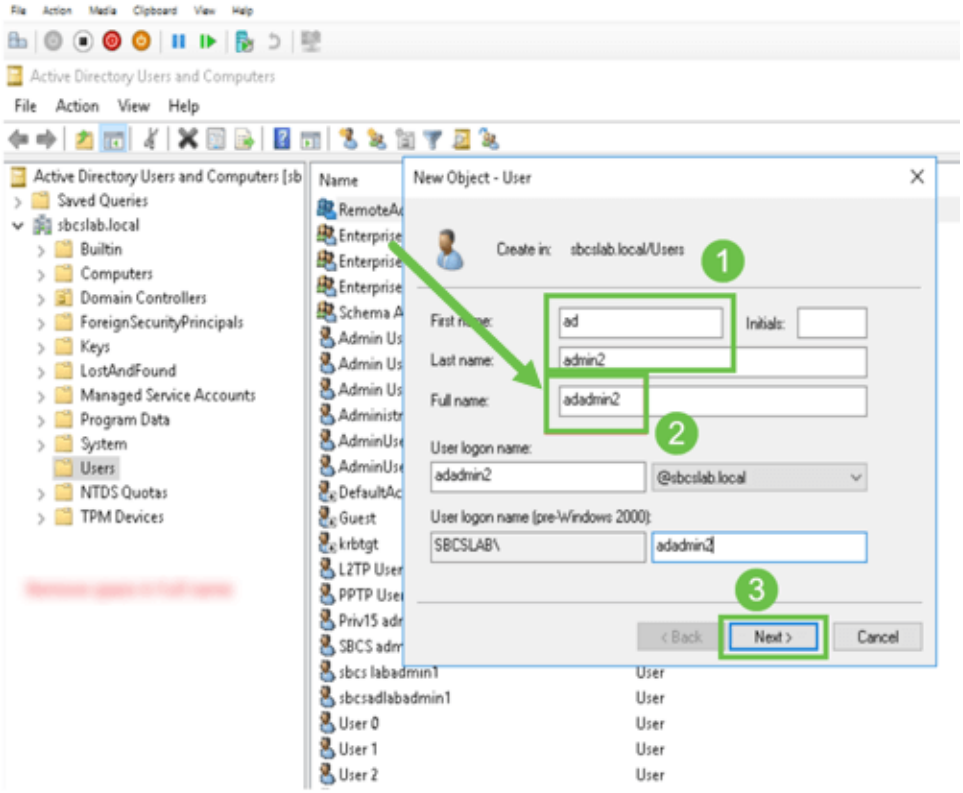
Dieses Bild zeigt das Leerzeichen im vollen Namen, das gelöscht werden muss:



Schritt 5

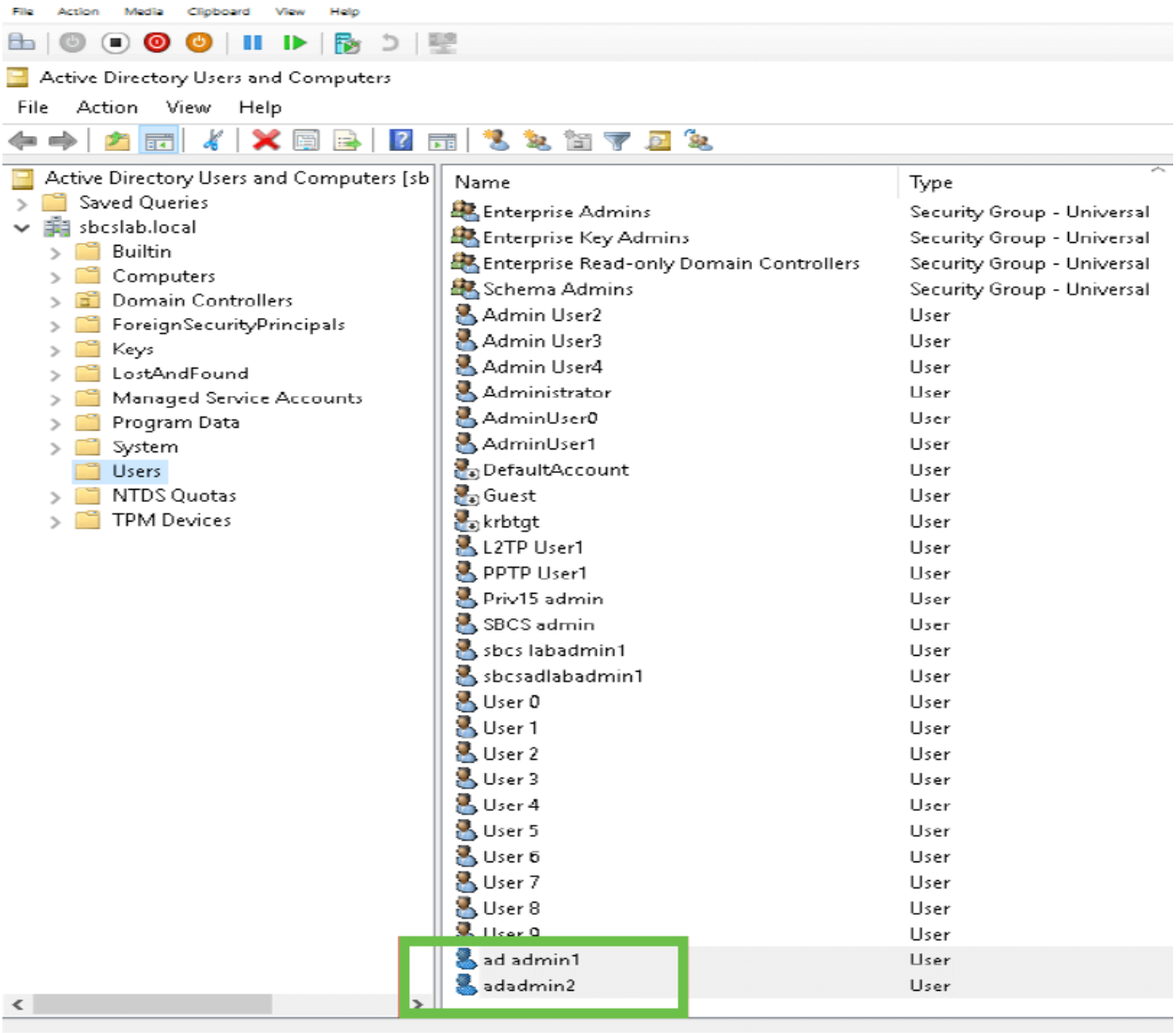
Wiederholen Sie die Schritte, um einen anderen Benutzer zu erstellen. Sie müssen das Feld *Vollständiger Name* erneut ändern, indem Sie automatisch erstellte Leerzeichen entfernen. Klicken Sie auf **Weiter**, um das Kennwort einzurichten und die Erstellung des Benutzers abzuschließen.

Dieses Bild zeigt, dass das Leerzeichen im vollen Namen gelöscht wurde. So können Sie den Benutzer richtig hinzufügen:



Schritt 6

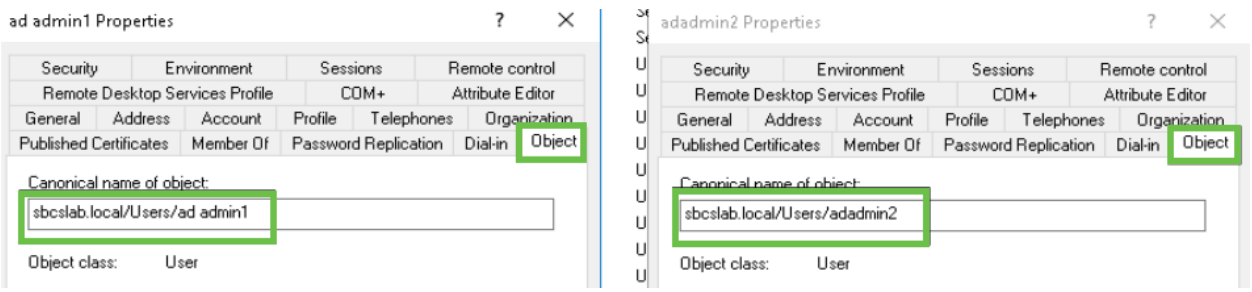
Die Liste Benutzer zeigt beide neu hinzugefügten Benutzerdetails an.



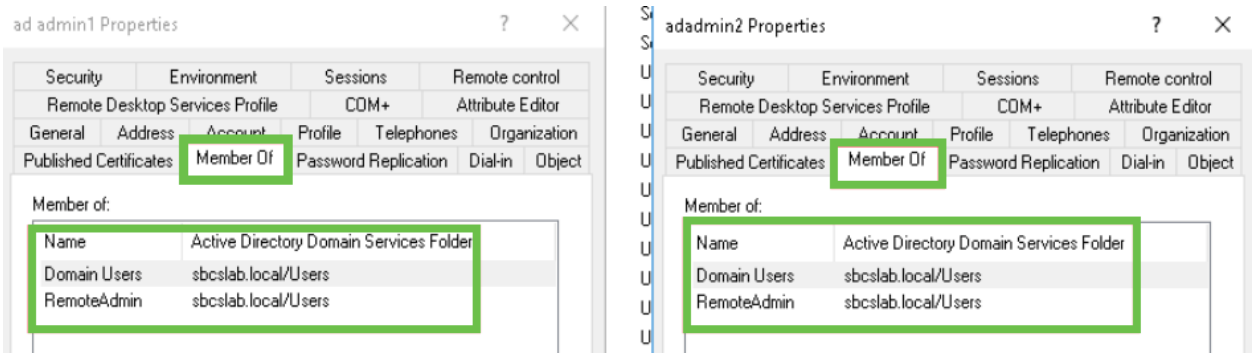
Schritt 7

Sie werden feststellen, dass *admin1* ein Leerzeichen zwischen dem Vor- und Nachnamen anzeigt. Wenn dieser nicht behoben ist, schlägt die Anmeldung fehl. Dieser Fehler wird zu Demonstrationszwecken in gelassen, lassen Sie den Platz nicht dort! Das Beispiel *admin2* ist korrekt.

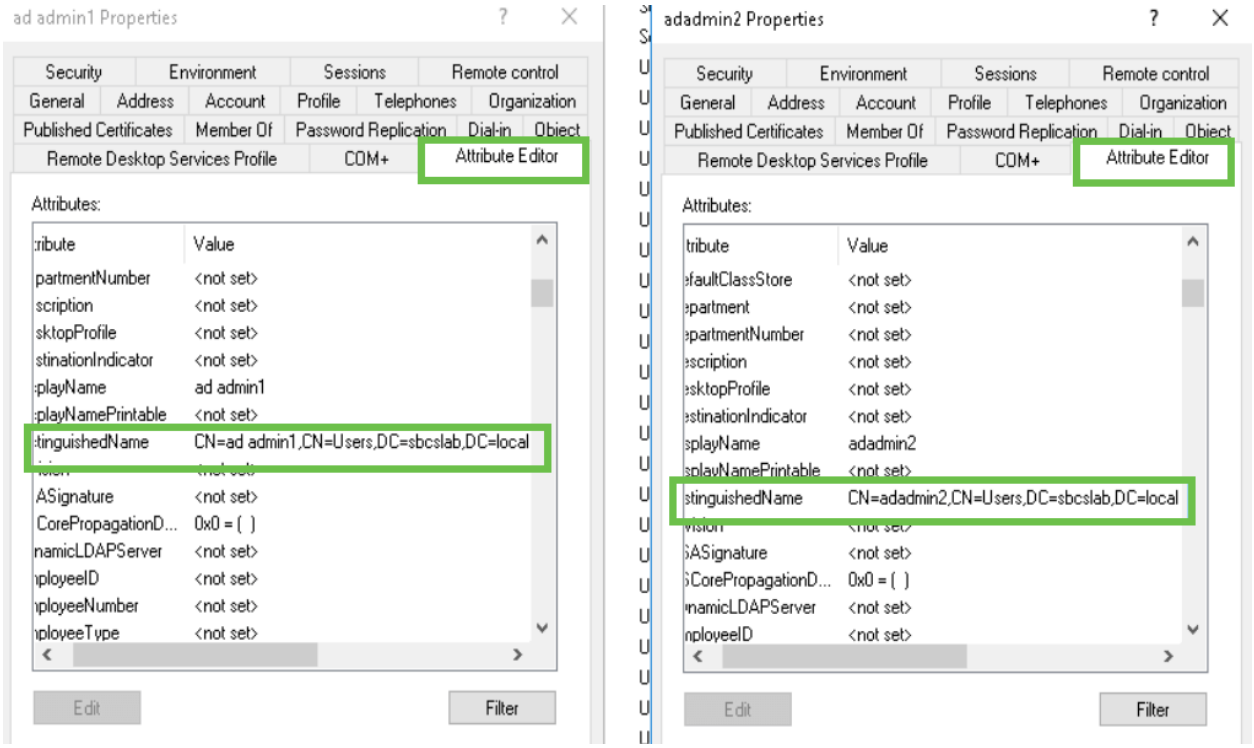
Klicken Sie zum Anzeigen mit der rechten Maustaste auf den Benutzernamen *Admin 1* und wählen Sie die Option **Eigenschaften**. Navigieren Sie dann zur Registerkarte **Objekt**, um den *kanonischen Namen der Object*-Details anzuzeigen.



Sie können auch die *Domänenbenutzer* und die *RemoteAdmin*-Details für diese Benutzernamen überprüfen, indem Sie unter der Option Eigenschaften zur Registerkarte *Member Of navigieren*.



Navigieren Sie zur Registerkarte *Attribute-Editor*, um die *DistinguishedName*-Werte für diese Benutzernamen zu überprüfen.

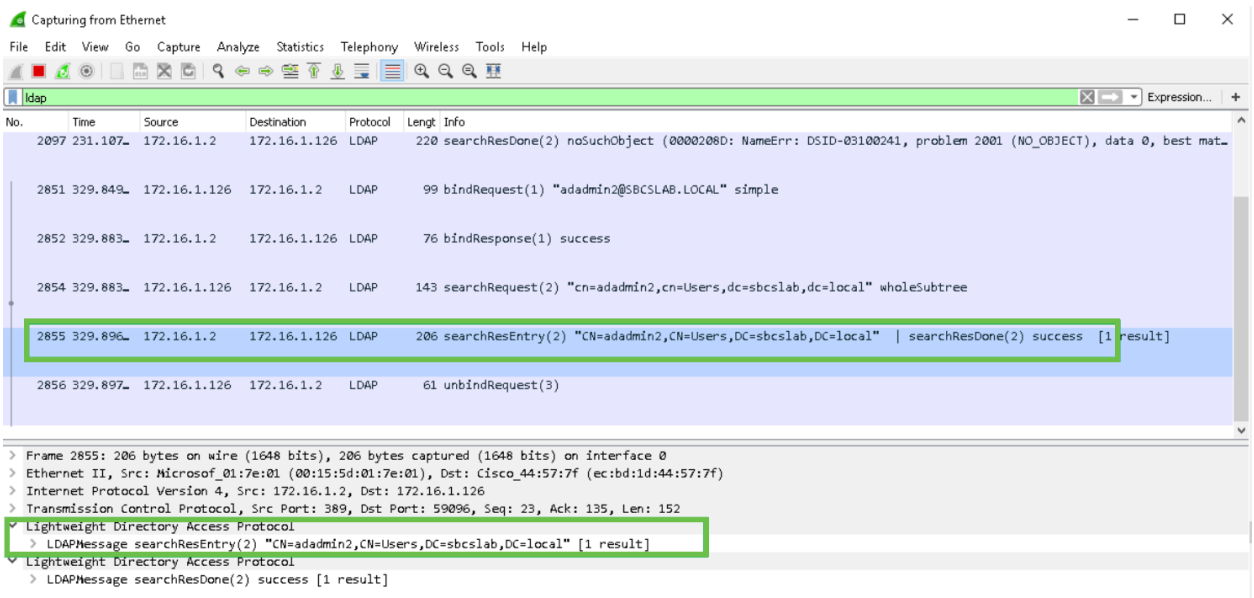


Schritt 8

Melden Sie sich mit dem *Benutzernamen für die Anmeldung an*, in diesem Fall *admin2*, wird angezeigt, dass die Anmeldung erfolgreich war.

Schritt 9

Die Details zur Paketerfassung werden im folgenden Screenshot dargestellt.



Was passiert, wenn Sie den Leerzeichen nicht aus dem Feld "Vollständiger Name" entfernen?

Wenn Sie den *Benutzernamen* verwenden, in diesem Fall *admin*, wird die Anmeldung fehlschlagen, da der LDAP-Server (Lightweight Directory Access Protocol) das Objekt nicht zurückgeben kann, da *Vollname* in diesem Fall *ad admin1* einen Leerzeichen hat. Sie können diese Details beim Erfassen der Pakete sehen, wie im folgenden Screenshot gezeigt.

Schlussfolgerung

Sie haben jetzt eine fehlgeschlagene Anmeldung für die Remote-Authentifizierung über Active Directory auf dem RV34x-Router erfolgreich abgeschlossen und vermieden.