Guide d'authentification et de connexion à distance à l'aide des routeurs Active Directory et RV34x

Objectif

Cet article explique comment configurer l'authentification à distance à l'aide de Windows Active Directory (AD) sur les routeurs de la gamme Cisco RV34x. En outre, des informations seront fournies pour éviter une erreur de connexion potentielle.

Introduction

Lorsque vous configurez les paramètres d'authentification de service sur le routeur RV34x, vous devez sélectionner une méthode d'authentification externe.

Par défaut, la priorité de base de données externe sur le routeur de la gamme RV34x est RADIUS/LDAP/AD/Local. Si vous ajoutez le serveur RADIUS sur le routeur, le service de connexion Web et d'autres services utiliseront la base de données externe RADIUS pour authentifier l'utilisateur. Il n'existe aucune option permettant d'activer une base de données externe pour le service de connexion Web seul et de configurer une autre base de données pour un autre service. Une fois RADIUS créé et activé sur le routeur, le routeur utilise le service RADIUS comme base de données externe pour la connexion Web, le VPN site à site, le VPN EzVPN/tiers, le VPN SSL, le VPN PPTP/L2TP et 802.1x.

Si vous utilisez Windows, Microsoft fournit un service AD interne. AD stocke toutes les informations essentielles pour le réseau, y compris les utilisateurs, les périphériques et les politiques. Les administrateurs utilisent AD en tant qu'emplacement unique pour créer et gérer le réseau. Il facilite l'utilisation de ressources réseau interconnectées, complexes et différentes de manière unifiée.

Une fois configuré, toute personne autorisée peut s'authentifier à l'aide de l'option AD externe (présente dans le système d'exploitation Windows Server) pour utiliser n'importe quel service spécifique sur le routeur RV34x. Les utilisateurs autorisés peuvent utiliser les fonctionnalités fournies, à condition qu'ils disposent du matériel et du logiciel nécessaires pour utiliser ce type d'authentification.

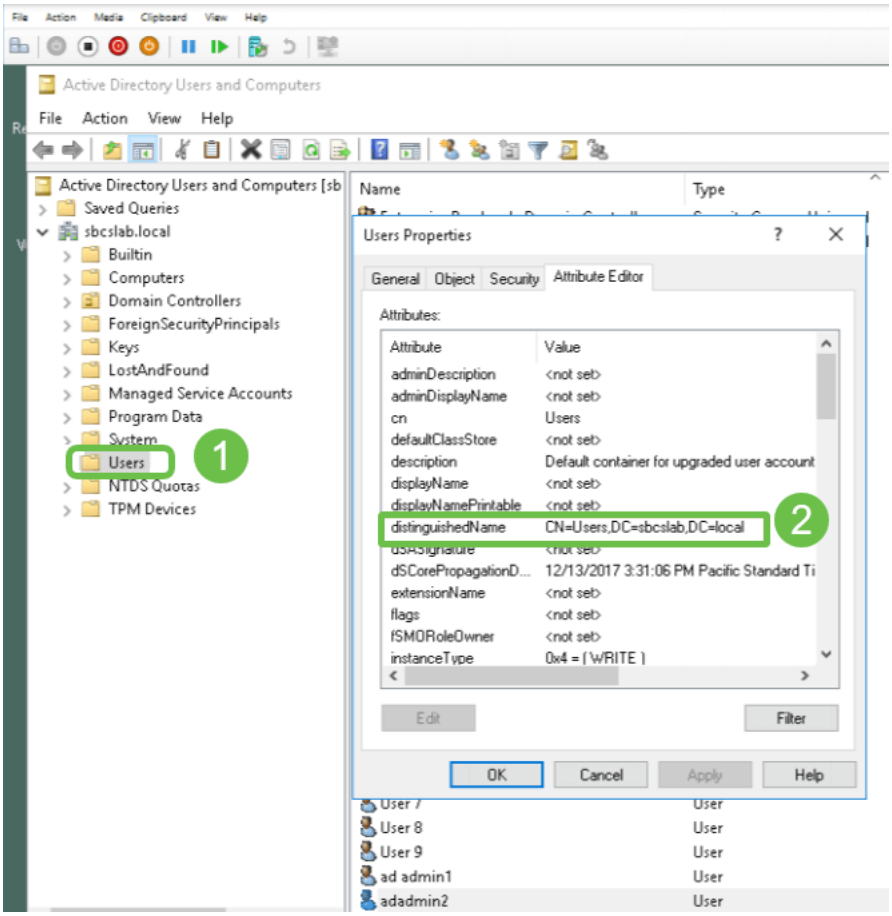
Périphériques pertinents | Version du logiciel

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

Table des matières

Identifier la valeur du nom distinctif

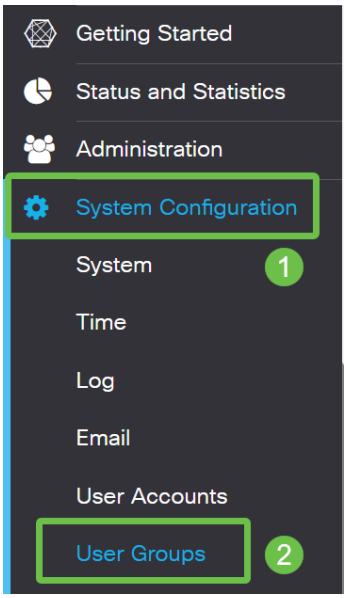
Accédez à l'interface de gestion *Utilisateurs et ordinateurs Active Directory* sur le serveur Windows 2016. Sélectionnez le dossier du conteneur **Utilisateurs**, cliquez avec le bouton droit de la souris et ouvrez **Propriétés**. Prenez note de la valeur *DistinguishedName* qui sera utilisée ultérieurement dans le champ *User Container Path* du routeur RV34x.



Créer un groupe d'utilisateurs pour Active Directory

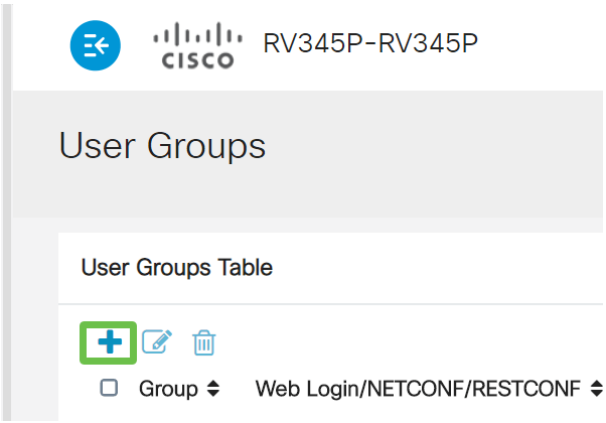
Étape 1

Connectez-vous au routeur de la gamme RV34x. Accédez à **Configuration système > Groupes d'utilisateurs**.



Étape 2

Cliquez sur l'**icône plus**.



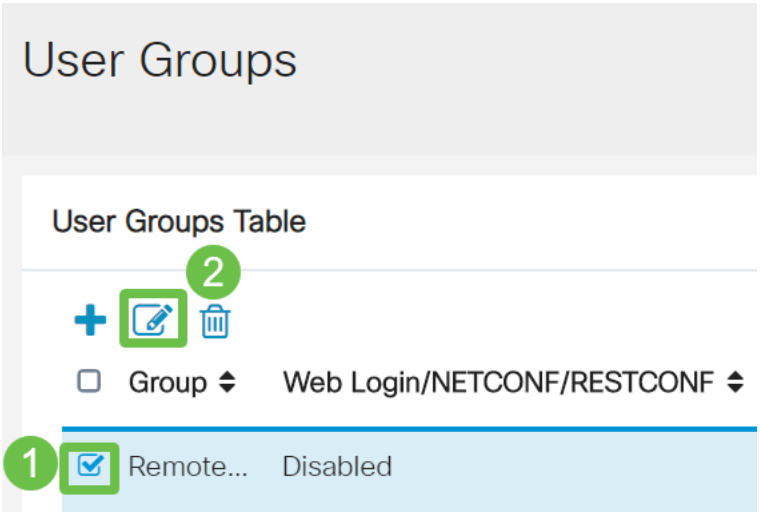
Étape 3

Entrez un *nom de groupe*. Cliquez sur Apply.

Dans cet exemple, un groupe d'utilisateurs *RemoteAdmin* a été créé.

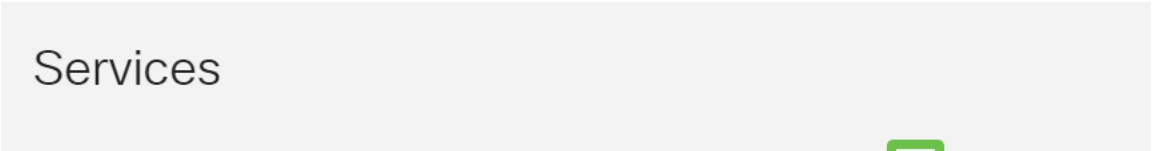
Étape 4

Cochez la case en regard du nouveau groupe d'utilisateurs. Cliquez sur l'**icône de modification**.



Étape 5

Faites défiler la page vers le bas jusqu'à *Services*. Cliquez sur la case d'option **Administrateur**.

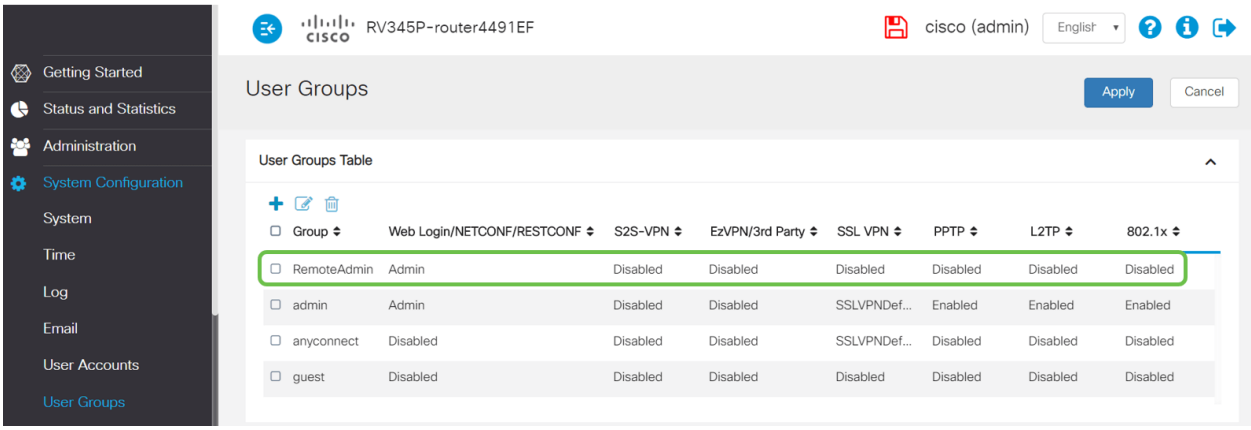


Étape 6

Cliquez sur Apply.

Étape 7

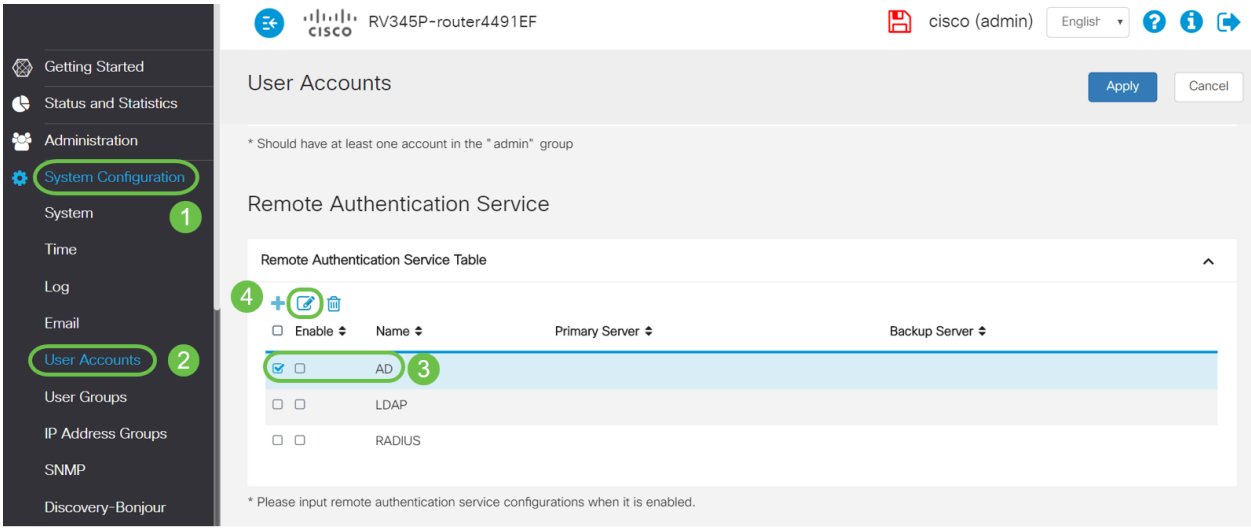
Le nouveau groupe d'utilisateurs s'affiche avec les privilèges d'administrateur.



Ajouter des détails Active Directory sur le routeur RV34x

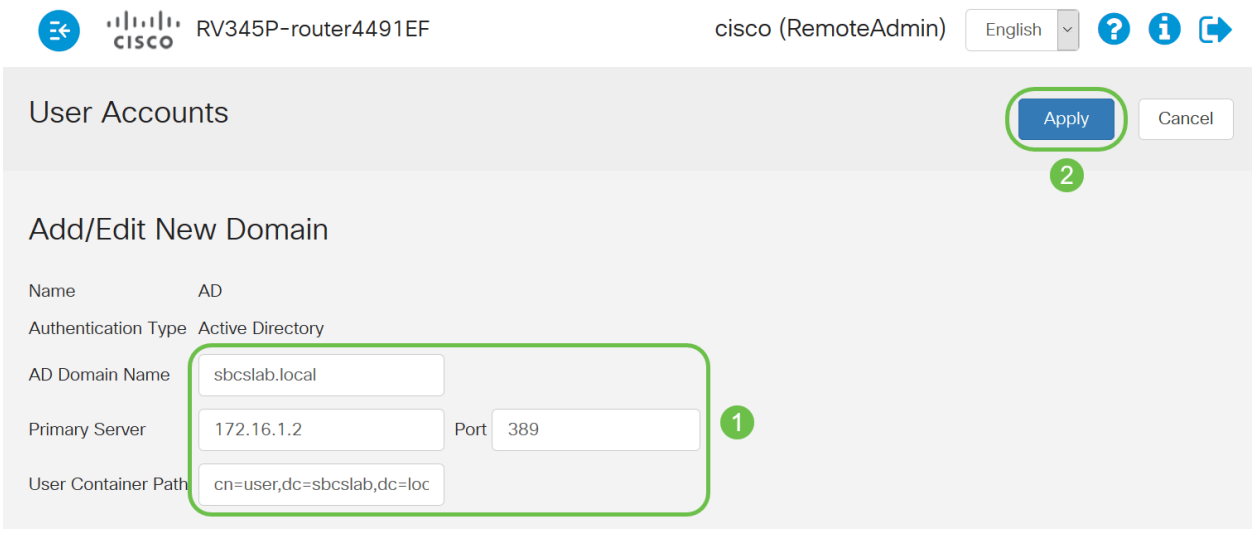
Étape 1

Accédez à **Configuration système > Comptes d'utilisateurs.** Sélectionnez l'option *AD* et cliquez sur l'**icône de modification** pour ajouter les détails du serveur AD.



Étape 2

Entrez les détails *AD Domain Name*, *Primary Server*, *Port* et *User Container Path*. Cliquez sur Apply.

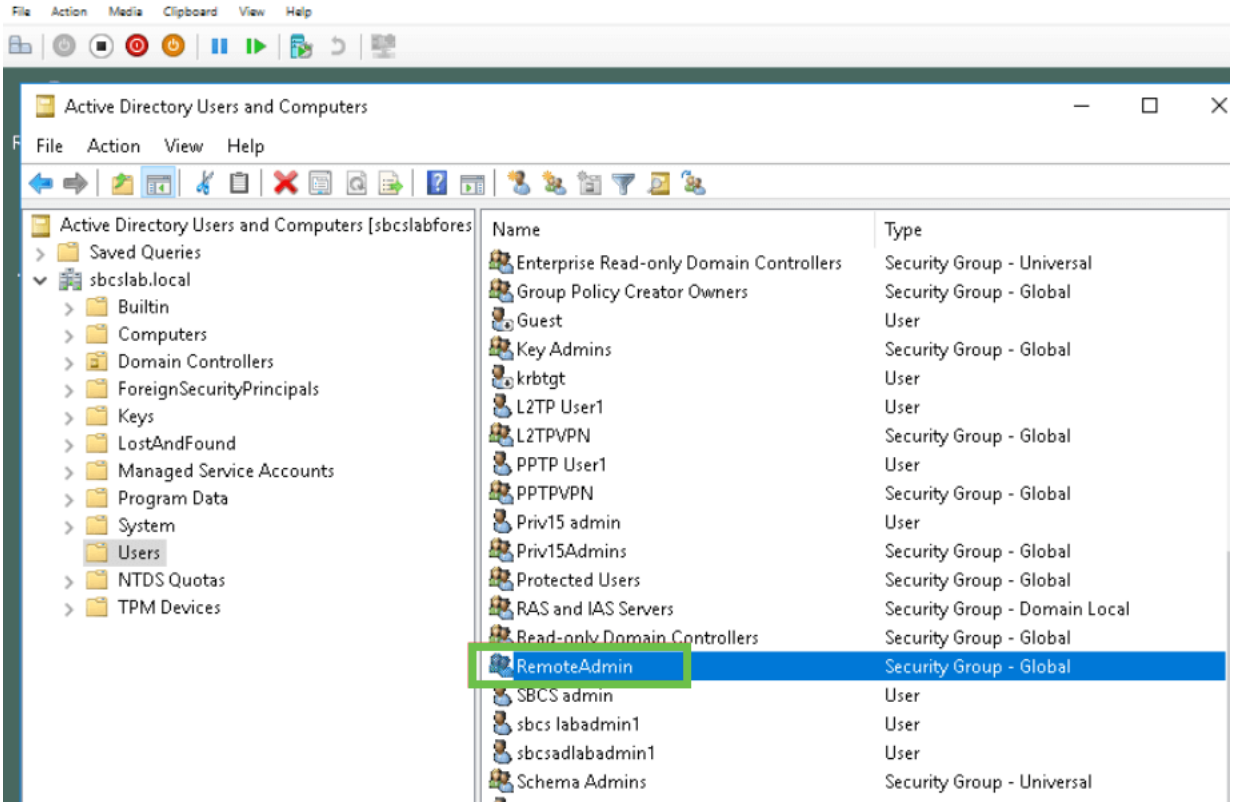


Note: Vous devez entrer les détails du *chemin du conteneur utilisateur* capturés à partir du serveur Windows dans la section [Identifier la valeur du nom distinctif] de cet article.

Dans cet exemple, les détails sont *Cn=user, dc=sbcslab, dc=local*. Le port d'écoute par défaut du serveur LDAP (Lightweight Directory Access Protocol) est 389.

Étape 3

Dans l'AD, vérifiez que le *groupe d'utilisateurs* est configuré et qu'il correspond au nom *du groupe d'utilisateurs* du routeur.

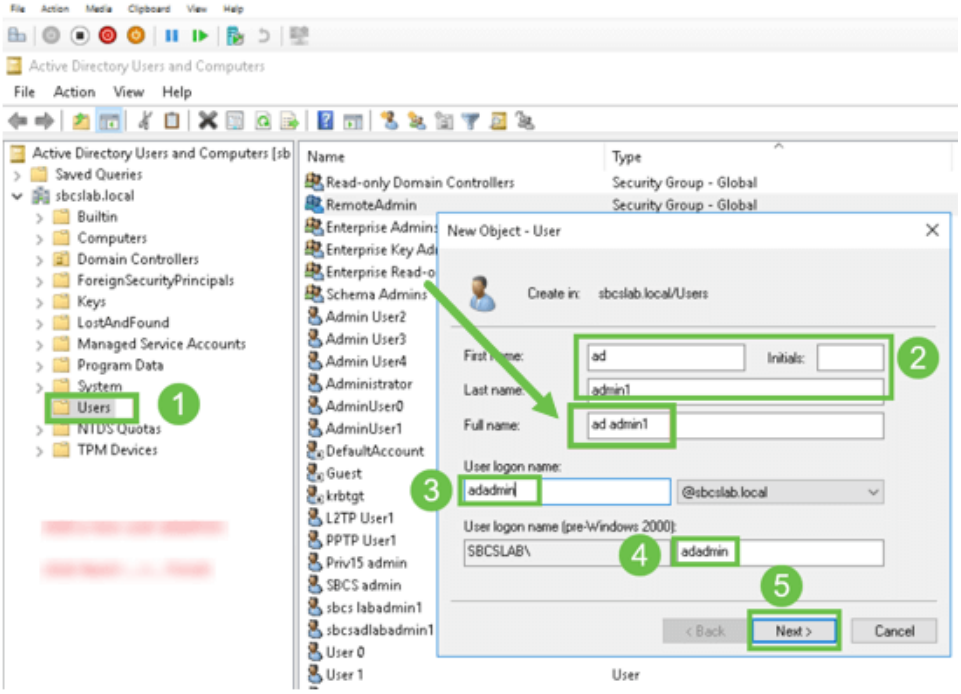


Étape 4

Sous New Object - User, entrez *First name*, *Initials* and *Last name*, le *Full name* sera automatiquement renseigné, indiquant un espace entre le prénom et le nom.

L'espace entre le prénom et le nom dans la zone *Nom complet* doit être supprimé ou il ne se connectera pas correctement.

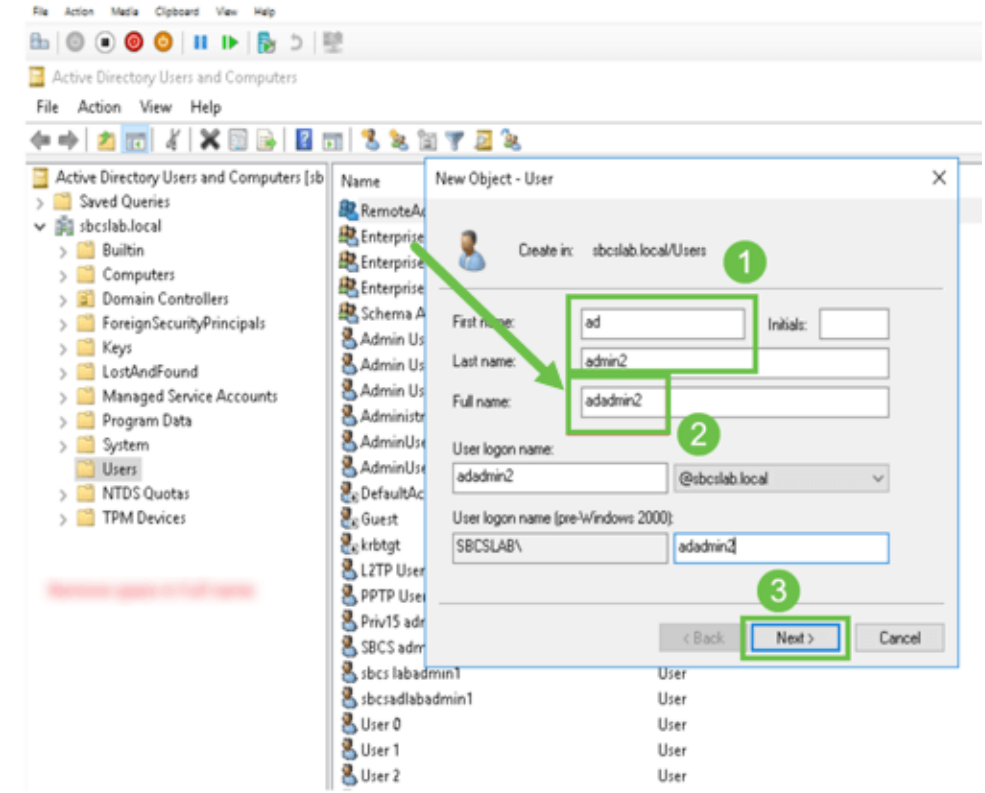
Cette image montre l'espace dans le nom complet qui doit être supprimé :



Étape 5

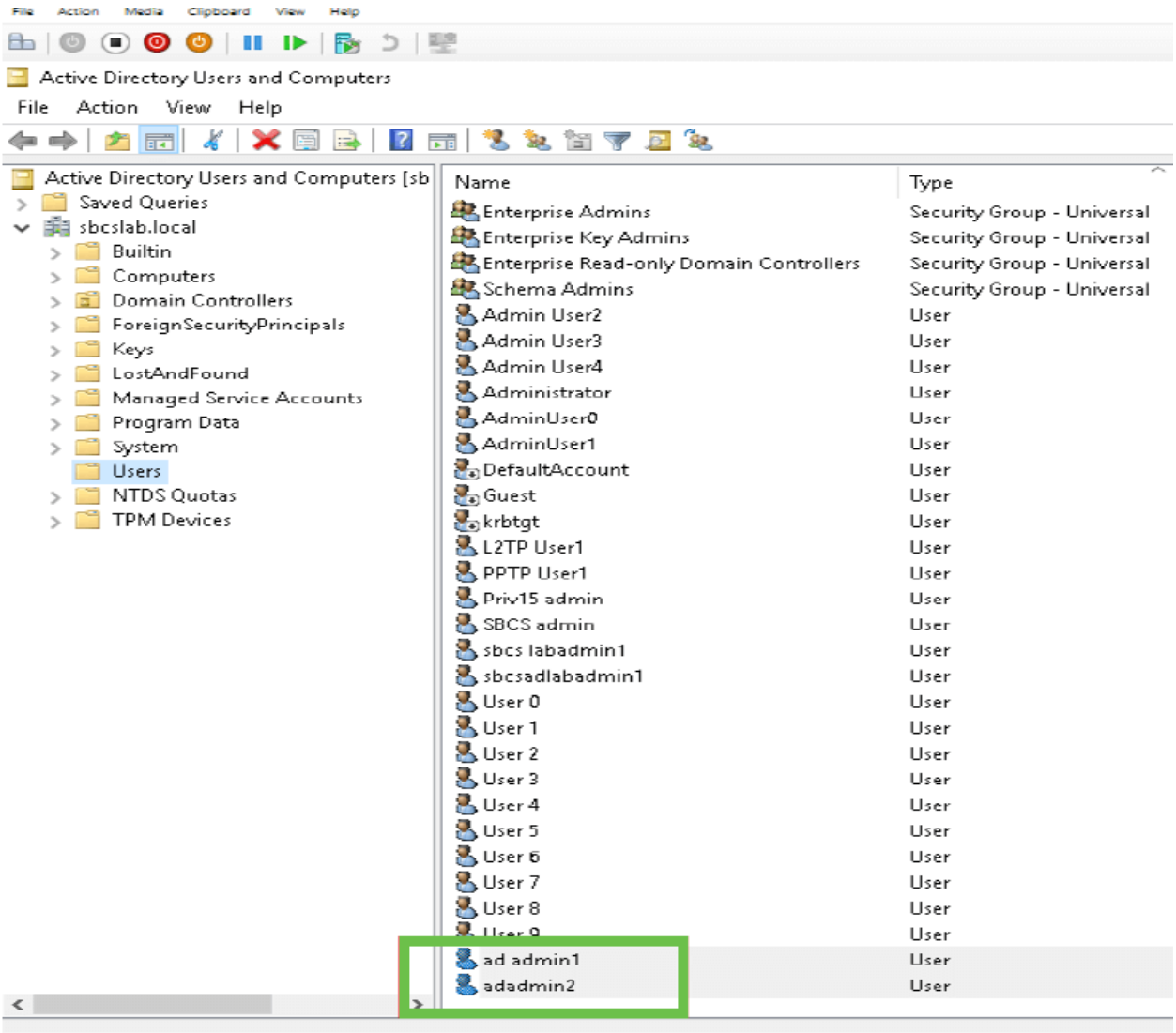
Répétez les étapes pour créer un autre utilisateur. Une fois de plus, vous devez modifier le champ *Nom complet* en supprimant les espaces créés automatiquement. Cliquez sur **Suivant** pour configurer le mot de passe et terminer la création de l'utilisateur.

Cette image montre que l'espace du nom complet a été supprimé. Voici la bonne façon d'ajouter l'utilisateur :



Étape 6

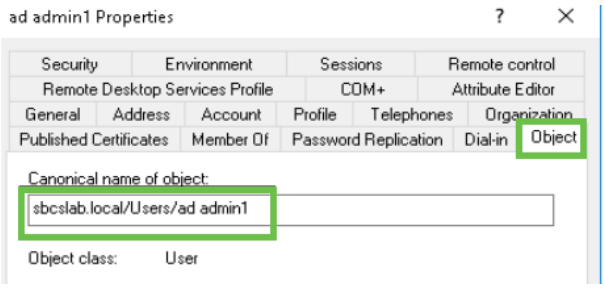
La liste Utilisateurs affiche les deux détails des utilisateurs nouvellement ajoutés.

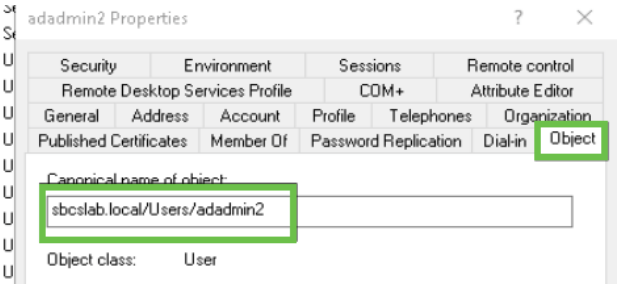


Étape 7

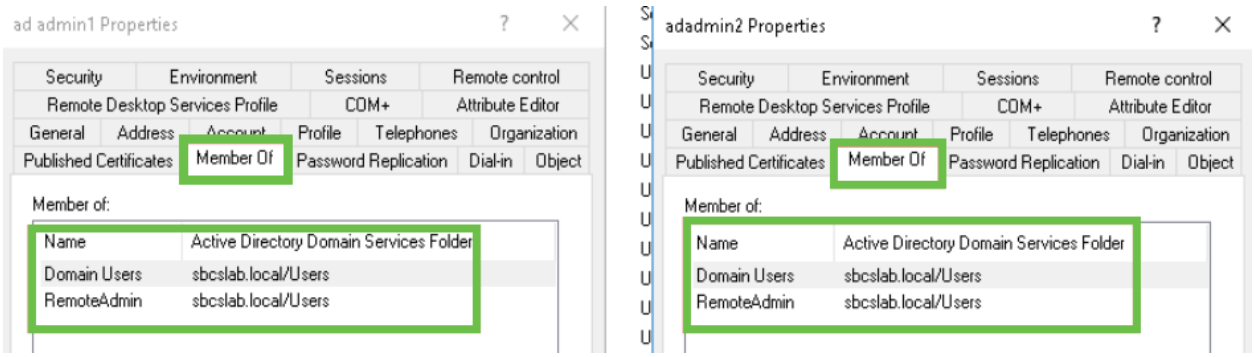
Vous remarquerez que l'*ad admin1* affiche un espace entre le prénom et le nom de famille, si ce n'est pas corrigé, la connexion échouera. Cette erreur est laissée à des fins de démonstration, ne laissez pas l'espace là! L'exemple *admin2* est correct.

Pour afficher, cliquez avec le bouton droit de la souris sur le nom d'utilisateur *admin 1 de l'annonce* et sélectionnez l'option **Propriétés**. Ensuite, accédez à l'onglet **Objet** pour afficher le *nom canonique des* détails *de l'objet*.

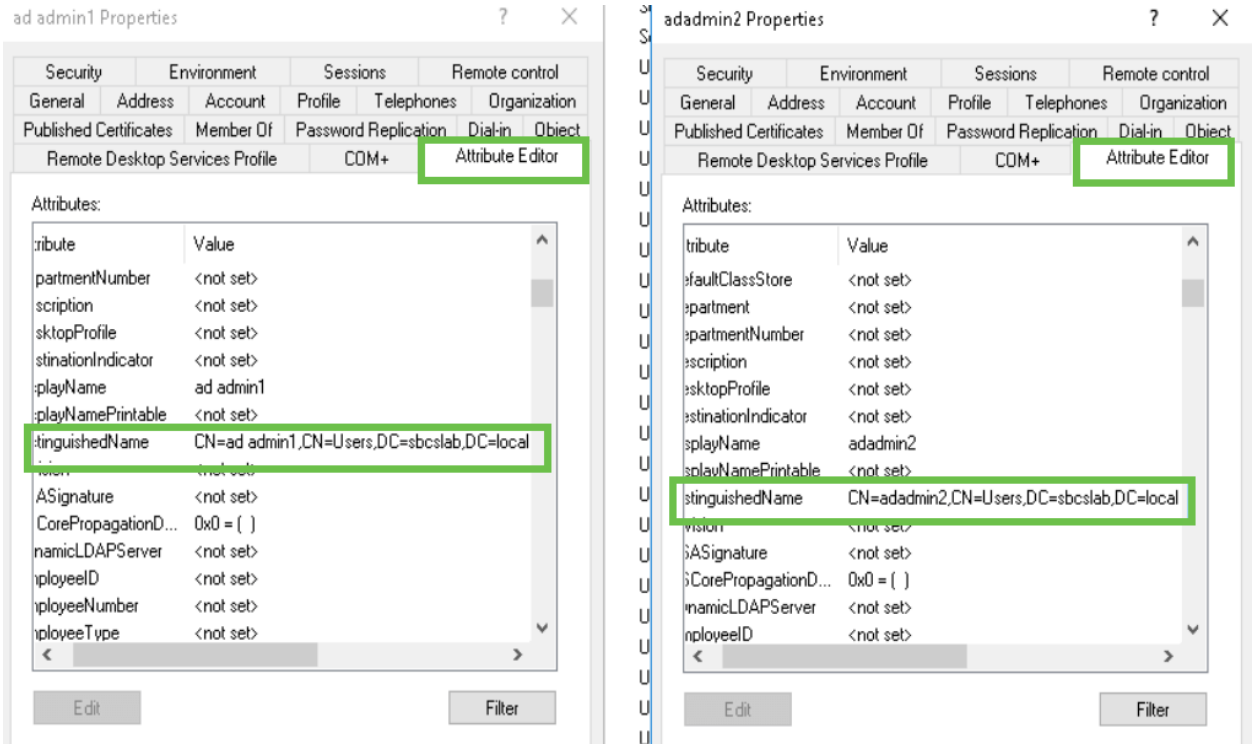




Vous pouvez également vérifier les détails *Domain Users* et *RemoteAdmin* pour ces noms d'utilisateur en accédant à l'onglet *Member Of* sous l'option **Properties**.



Accédez à *l'*onglet *Éditeur d'attributs* pour vérifier les valeurs *DistinguishedName* pour ces noms d'utilisateur.

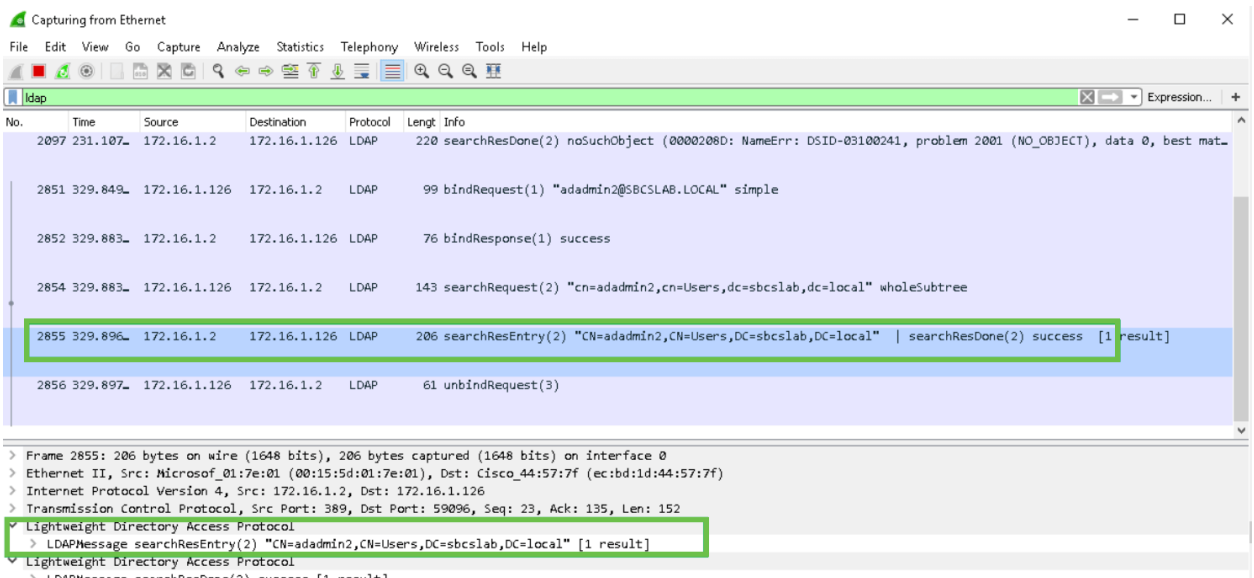


Étape 8

Connectez-vous avec le *nom de connexion de l'utilisateur*, dans ce cas, *admin2*, vous verrez que la connexion a réussi.

Étape 9

Vous pouvez voir les détails de la capture de paquets comme indiqué dans la capture d'écran suivante.



Que se passe-t-il si vous ne retirez pas l'espace du champ de nom complet ?

Si vous essayez d'utiliser le *nom de connexion utilisateur,* dans ce cas *admin*, vous verrez que la connexion échoue car le serveur LDAP (Lightweight Directory Access Protocol) ne peut pas renvoyer d'objet car *Full name,* dans ce cas, *ad admin1,* a un espace. Vous pourrez voir ces détails lors de la capture des paquets, comme indiqué sur la capture d'écran suivante.

Conclusion

Vous avez maintenant réussi et évité une connexion échouée pour l'authentification à distance via Active Directory sur le routeur RV34x.