Autenticación remota y guía de inicio de sesión mediante routers Active Directory y RV34x

Objetivo

En este artículo se explica cómo configurar la autenticación remota mediante Windows Active Directory (AD) en los Cisco RV34x Series Routers. Además, se proporcionará información para evitar un posible error de inicio de sesión.

Introducción

Cuando configura los parámetros de autenticación de servicio en el router RV34x, debe seleccionar un método de autenticación externo.

De forma predeterminada, la prioridad de la base de datos externa en el router serie RV34x es RADIUS/LDAP/AD/Local. Si agrega el servidor RADIUS en el router, el servicio de inicio de sesión web y otros servicios utilizarán la base de datos externa RADIUS para autenticar al usuario. No hay ninguna opción para habilitar una base de datos externa para el servicio de inicio de sesión web solo y configurar otra base de datos para otro servicio. Una vez que se crea RADIUS y se habilita en el router, el router utilizará el servicio RADIUS como base de datos externa para el inicio de sesión web, VPN de sitio a sitio, VPN EzVPN/de terceros, VPN SSL, VPN PPTP/L2TP y 802.1x.

Si utiliza Windows, Microsoft proporciona un servicio AD interno. AD almacena toda la información esencial para la red, incluidos los usuarios, los dispositivos y las políticas. Los administradores utilizan AD como un único lugar para crear y administrar la red. Facilita el trabajo con recursos de red diferentes, complejos e interconectados de forma unificada.

Una vez configurada, cualquier persona autorizada puede autenticarse usando la opción AD externa (presente en el sistema operativo del servidor Windows) para utilizar cualquier servicio específico en el router RV34x. Los usuarios autorizados pueden utilizar las funciones proporcionadas, siempre que dispongan del hardware y el software necesarios para utilizar ese tipo de autenticación.

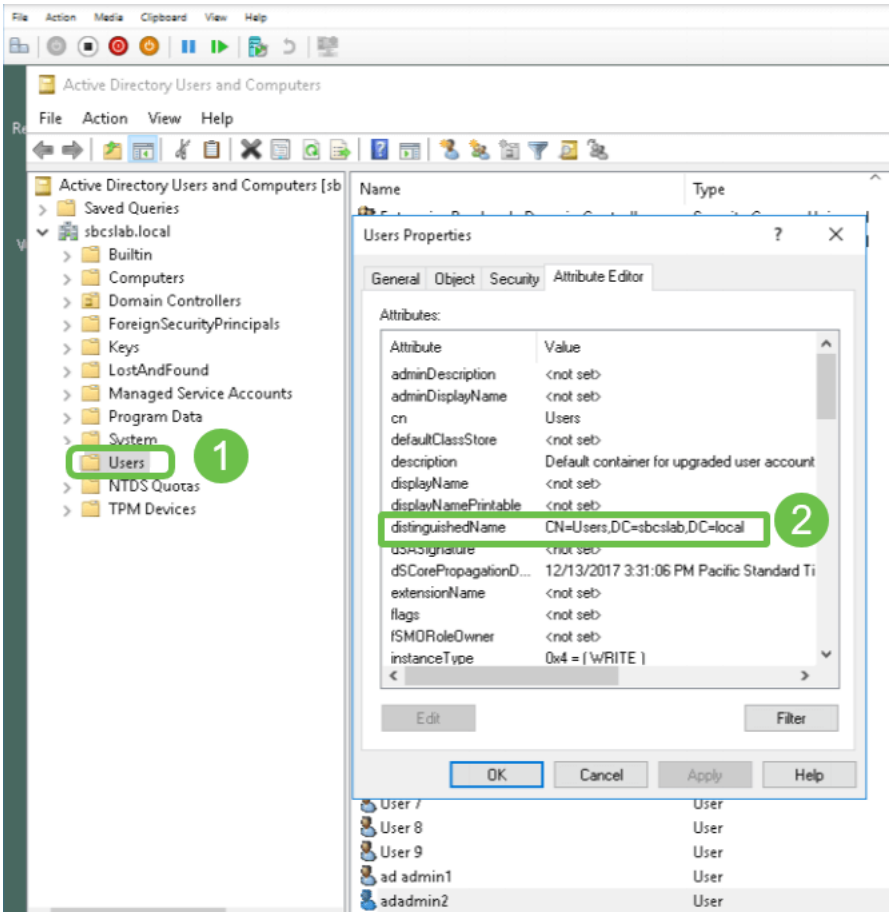
Dispositivos aplicables | Versión de software

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

Table Of Contents

Identificar el valor de nombre distinguido

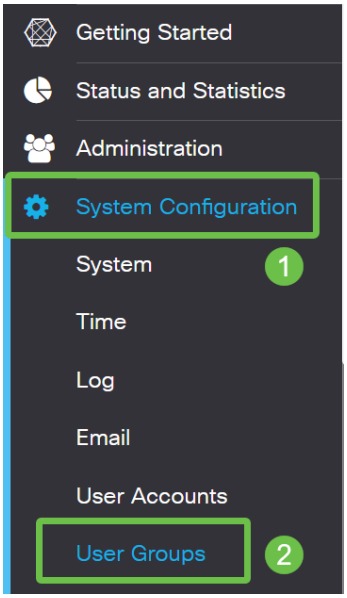
Acceda a la interfaz de administración *Usuarios y equipos de Active Directory* en el servidor Windows 2016. Seleccione la carpeta del contenedor **Users**, haga clic con el botón derecho del ratón y abra **Properties**. Tenga en cuenta el valor *DistinguishedName* que se utilizará más adelante en el campo *User Container Path* del router RV34x.



Crear un grupo de usuarios para Active Directory

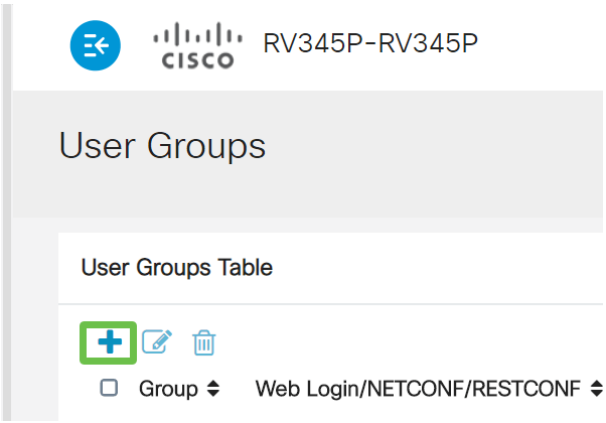
Paso 1

Inicie sesión en el router de la serie RV34x. Vaya a **Configuración del sistema > Grupos de usuarios**.



Paso 2

Haga clic en el **icono más**.



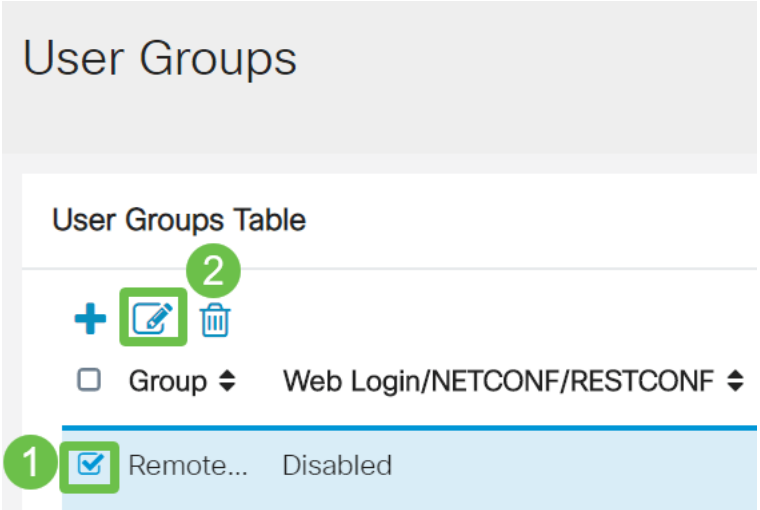
Paso 3

Introduzca un *nombre de grupo*. Haga clic en Apply (Aplicar).

En este ejemplo, se ha creado un grupo de usuarios *RemoteAdmin*.

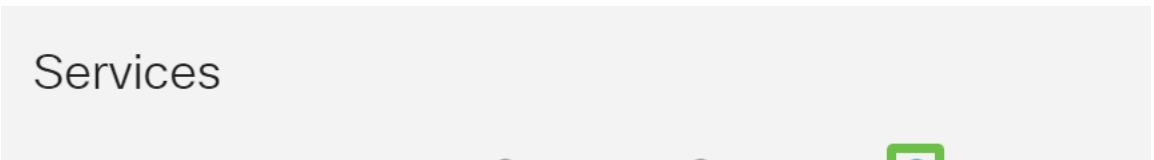
Paso 4

Haga clic en la casilla de verificación junto al nuevo grupo de usuarios. Haga clic en el **icono de edición**.



Paso 5

Desplácese hacia abajo por la página hasta *Services*. Haga clic en el botón de opción **Administrator**.

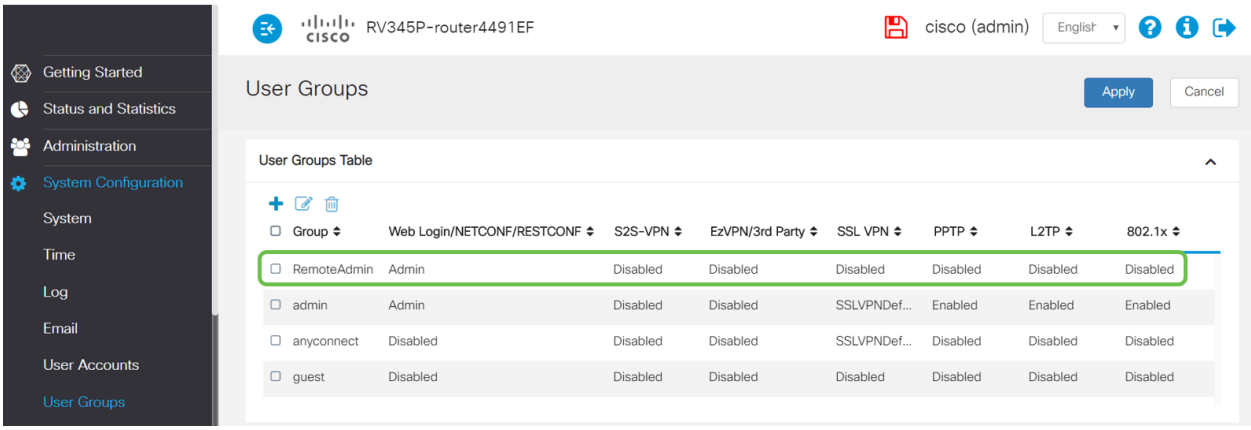


Paso 6

Haga clic en Apply (Aplicar).

Paso 7

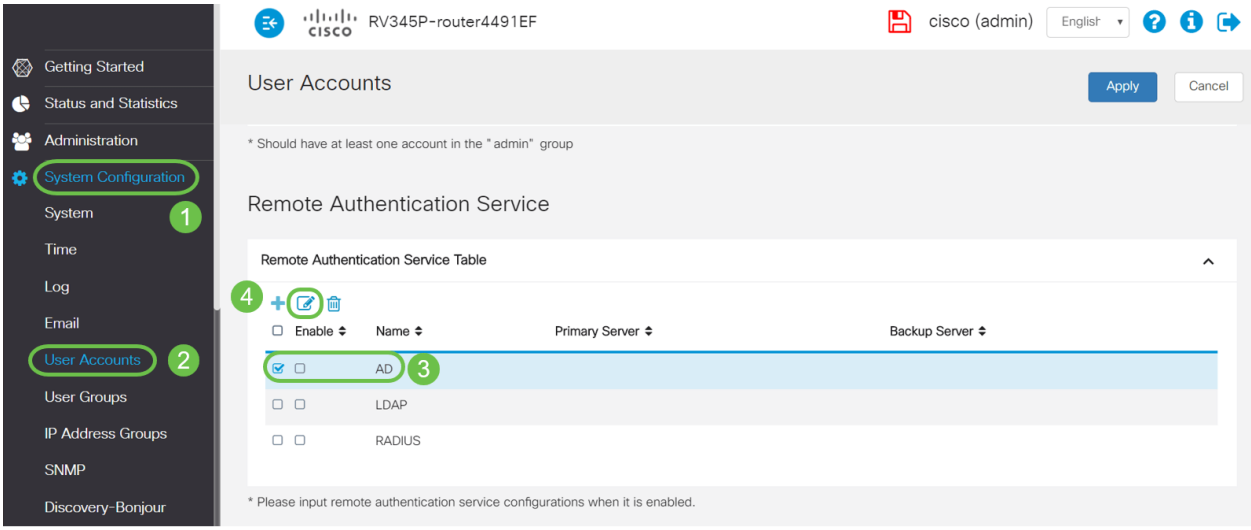
Ahora verá el nuevo grupo de usuarios mostrándose con privilegios de administrador.



Agregar detalles de Active Directory en el router RV34x

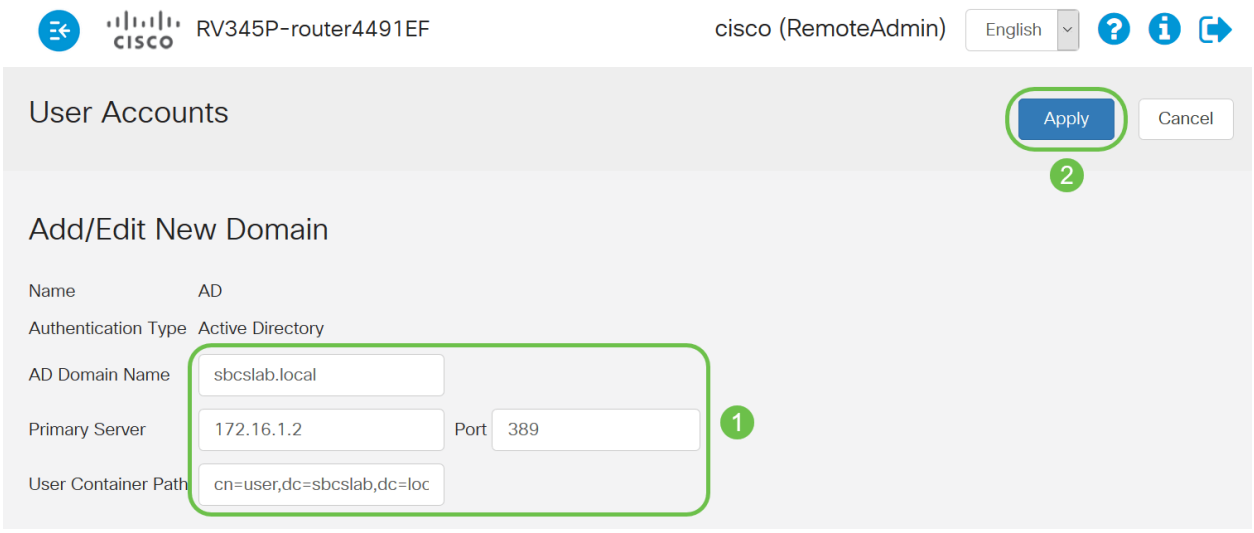
Paso 1

Vaya a **Configuración del sistema > Cuentas de usuario.** Seleccione la opción *AD* y haga clic en el **icono de edición** para agregar los detalles para el servidor AD.



Paso 2

Ingrese los detalles *AD Domain Name*, *Primary Server*, *Port* y *User Container Path*. Haga clic en Apply (Aplicar).

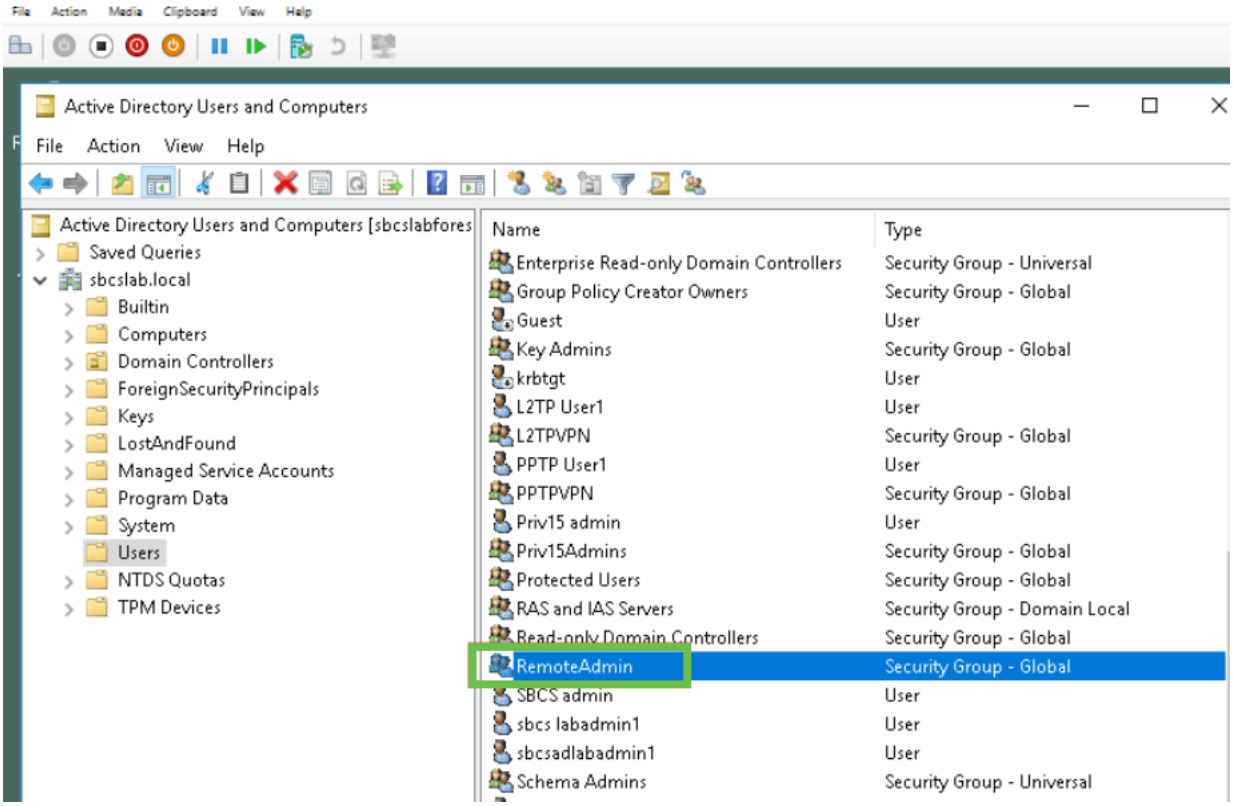


Nota: Debe ingresar los detalles de *la ruta de contención de usuario* capturados del servidor de Windows en la sección [Identificar el valor de nombre distinguido] de este artículo.

En este ejemplo, los detalles son *Cn=user,dc=sbcslab,dc=local*. El puerto de escucha predeterminado del servidor LDAP es 389.

Paso 3

En AD, verifique que el *grupo de usuarios* esté configurado y coincida con el *nombre de grupo de usuarios* del router.

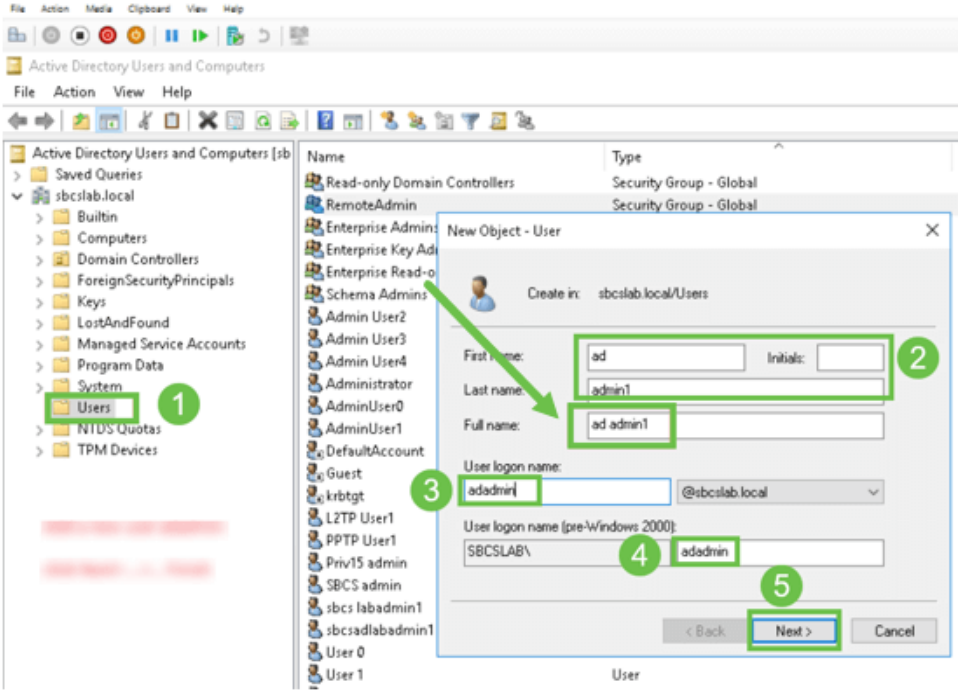


Paso 4

En New Object - User, rellene *First name*, *Initials* y *Last name*, el campo *Full name* se rellenará automáticamente, mostrando un espacio entre el nombre y los apellidos.

El espacio entre el nombre y los apellidos en el cuadro *Nombre completo* debe eliminarse o no se iniciará sesión correctamente.

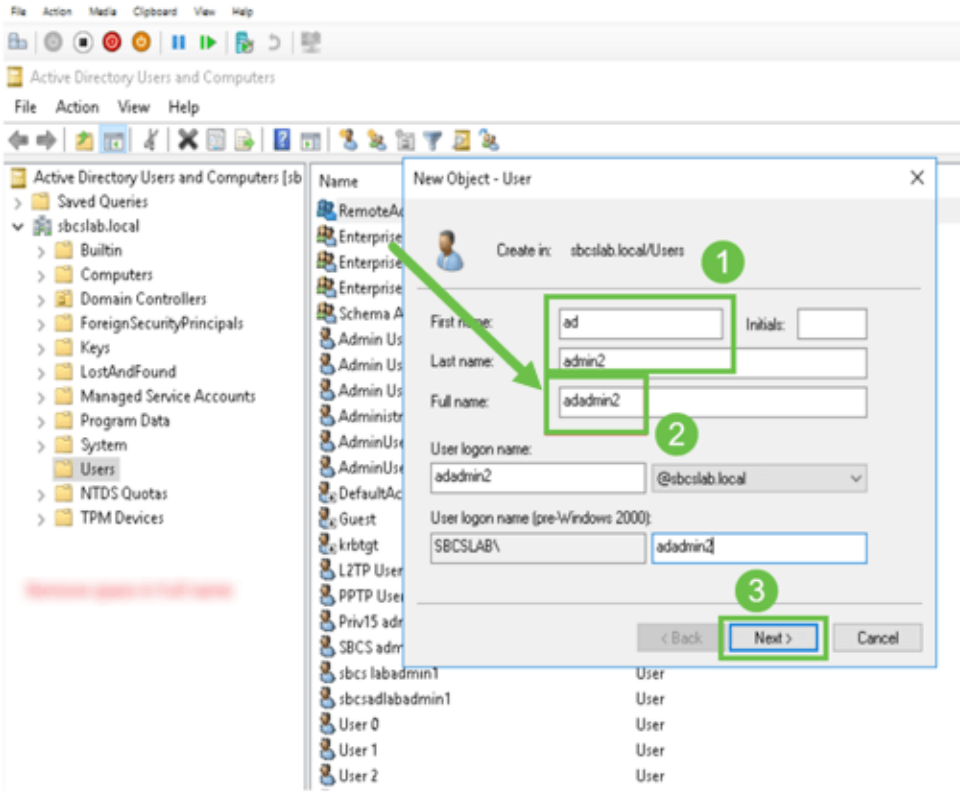
Esta imagen muestra el espacio en el nombre completo que se debe eliminar:



Paso 5

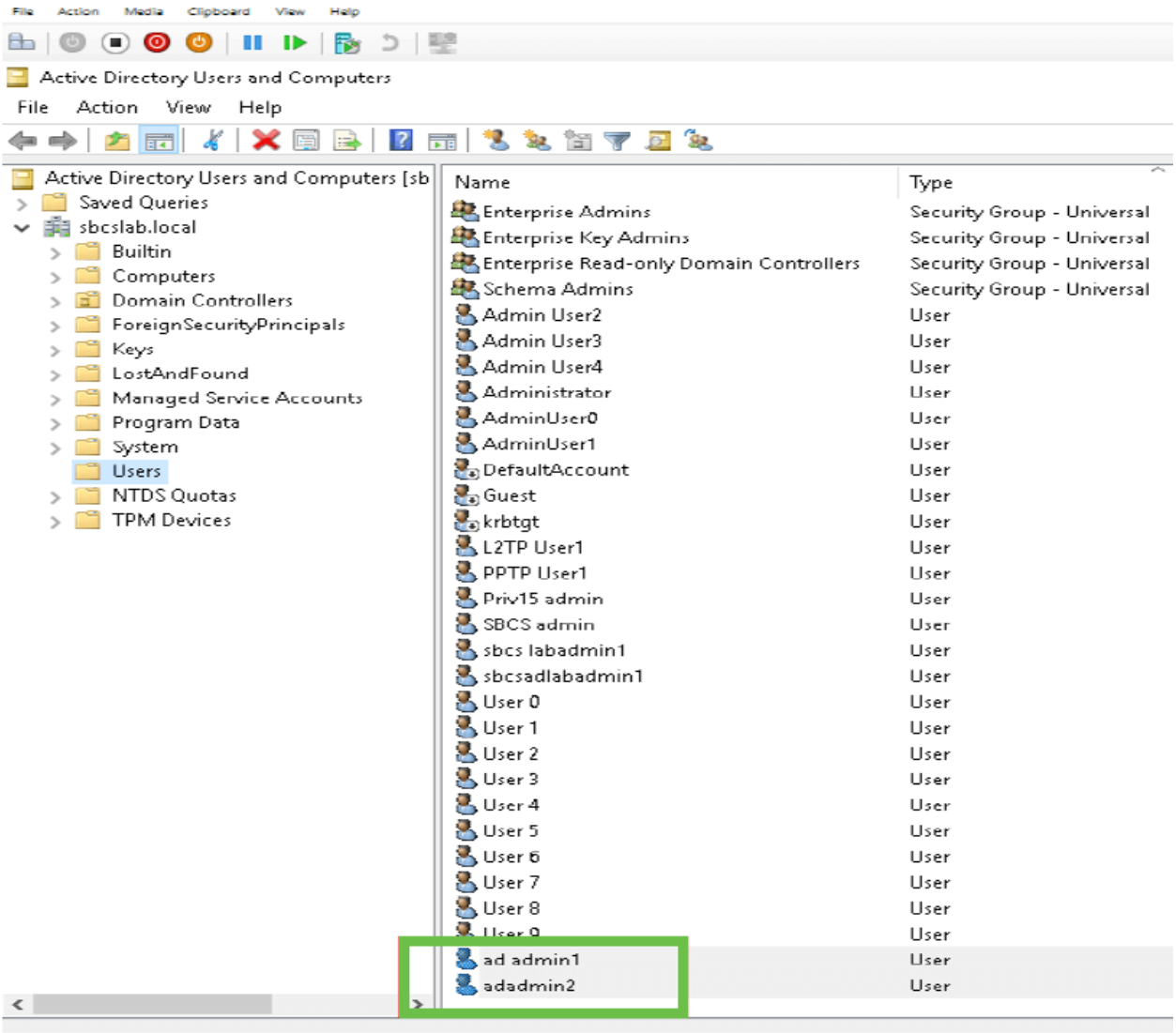
Repita los pasos para crear otro usuario. Una vez más, debe modificar el campo *Full Name* quitando los espacios creados automáticamente. Haga clic en **Next** para configurar la contraseña y finalizar la creación del usuario.

Esta imagen muestra que se eliminó el espacio en el nombre completo. Esta es la forma correcta de agregar el usuario:



Paso 6

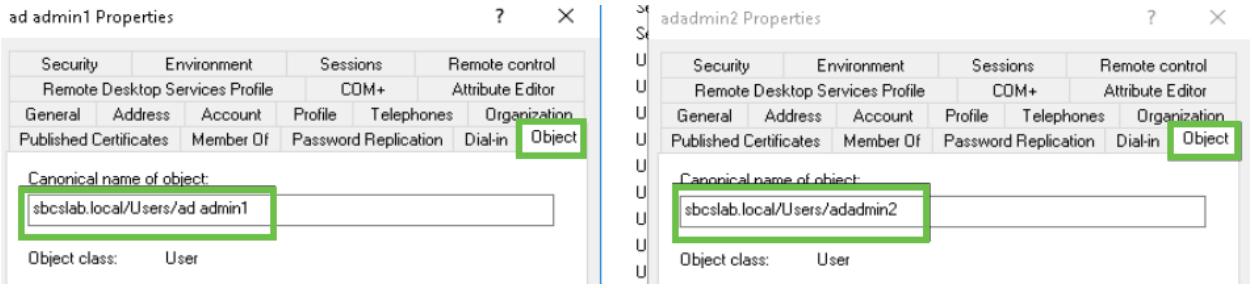
La lista Usuarios mostrará los dos detalles de usuario recién agregados.



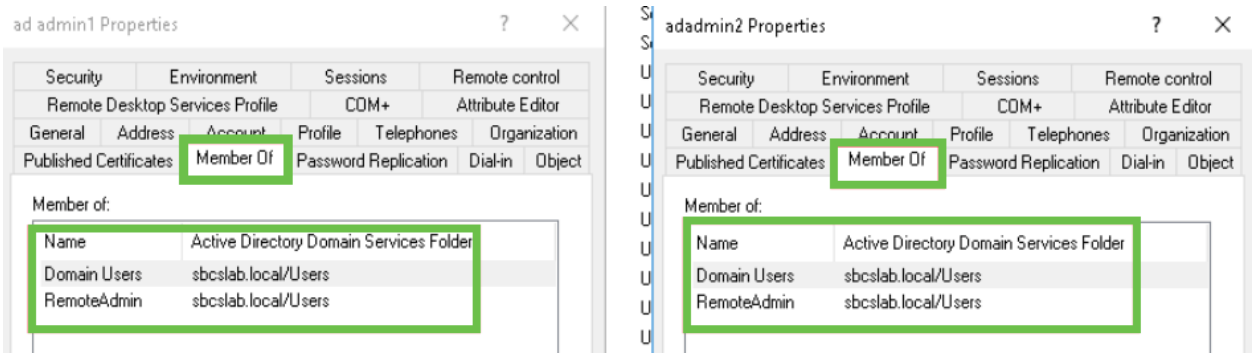
Paso 7

Observará que el *anuncio admin1* muestra un espacio entre el nombre y los apellidos, si esto no se corrige, el login fallará. Este error se está dejando para fines de demostración, no deje el espacio ahí! El ejemplo *adadmin2* es correcto.

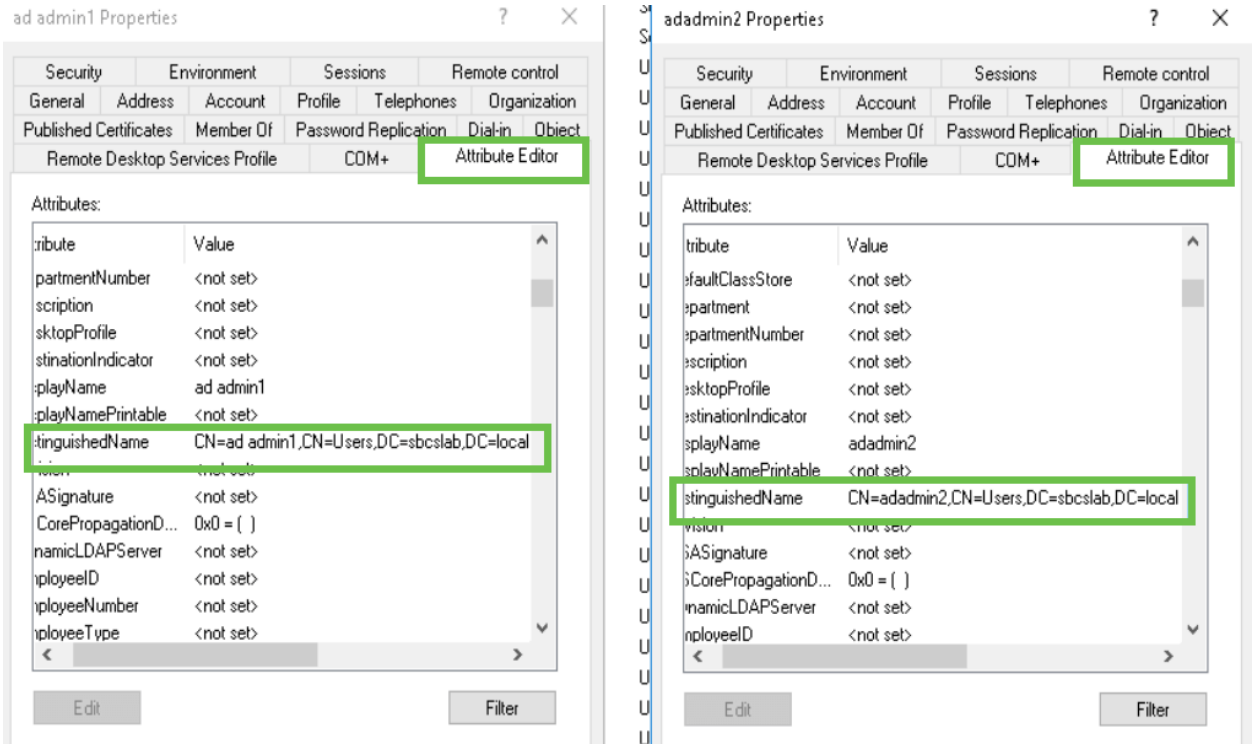
Para ver, haga clic con el botón derecho en el nombre de usuario *ad admin 1* y seleccione la opción **Properties**. A continuación, vaya a la ficha **Object** para ver los detalles *Canónicos de Object*.



Además, puede verificar los detalles *Domain Users* y *RemoteAdmin* para esos nombres de usuario navegando a la pestaña *Member Of* bajo la opción *Properties*.



Navegue hasta *la* ficha *Editor de atributos* para verificar los valores *DistinguishedName* para esos nombres de usuario.

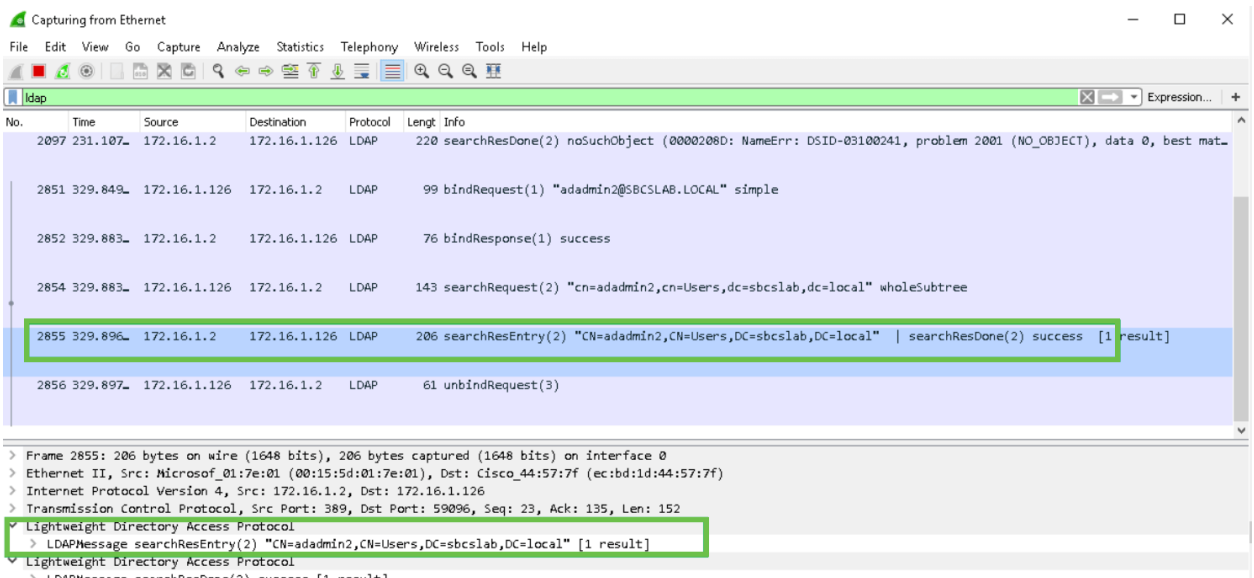


Paso 8

Inicie sesión con el *nombre de inicio de sesión del usuario*, en este caso, *adadmin2*, verá que el login es exitoso.

Paso 9

Puede ver los detalles de la captura de paquetes como se muestra en la siguiente captura de pantalla.



¿Qué sucede si no quita el espacio del campo de nombre completo?

Si intenta utilizar el *nombre de inicio de sesión de usuario,* en este caso *adadmin*, verá que el inicio de sesión falla porque el servidor LDAP (protocolo ligero de acceso a directorios) no puede devolver el objeto porque *Nombre completo*, en este caso, *ad admin1,* tiene un espacio. Podrá ver esos detalles al capturar los paquetes como se muestra en la siguiente captura de pantalla.

Conclusión

Ya ha completado correctamente y evitado un inicio de sesión fallido para la autenticación remota a través de Active Directory en el router RV34x.