

لوخدلا ليجست تاداشراو دعب نع ةقداصملا RV34x و Active Directory تاهجوم مادختساب

فدهلا

Windows Active Directory (AD) مادختساب دعب نع ةقداصملا نيوكت ةيفيك لاقملا اذه حرشي بنجتل تامولعمل ري فوت متيس ،كلذ ىل ةفاضل اب Cisco RV34x ةلسلس تاهجوم ىل لوخدلا ليجست يف لمتحم أطخ ثودح

ةمدقملا

يجراخ ةقداصم بولسا ديدحت كمزلي ،RV34x هجوملا ىل ةمدخل ةقداصم تاداعل نيوكت دنع

ه RV34x ةلسلسلا نم هجوم ىل ةيجراخ تانايبلا ةدعاق ةيولوا نوكت ،يضارتفا لكشب ةمدخ مدختستس ف ،هجوملا ىل RADIUS مداخ ةفاضل تمق اذا .RADIUS/LDAP/AD/Local ةقداصم ةيجراخ RADIUS تانايب ةدعاق ىرخال تامدخال او بيولا ىل لوخدلا ليجست اهدحو بيولا ىل لوخدلا ليجست ةمدخل ةيجراخ تانايب ةدعاق نيكمتل راخي دجوي ال .مدختسملا ،هجوملا ىل هنيكمتو RADIUS ءاشن درجمبو .ىرخا ةمدخل ىرخا تانايب ةدعاق نيوكتو ،بيولا ىل لوخدلا ليجست ةدعاق RADIUS ةمدخ هجوملا مدختسي ،نم (VPN) ةيرهاطلا ةصاخلا ةكبشلاو ،عقوم ىل عقوم نم (VPN) ةيرهاطلا ةصاخلا ةكبشلاو ، ةكبشلاو ،SSL صارقا كرحم (VPN) ةيرهاطلا ةصاخلا ةكبشلاو ،ثلاثلا فرطل/EzVPN (802.1x) ةيرهاطلا ةصاخلا ةكبشلاو ،PPTP/L2TP لوكوتوربل (VPN) ةيرهاطلا ةصاخلا

عيجم نيختب AD موقى .ةيلخاد AD ةمدخ Microsoft رفوت ،Windows مدختست تنك اذا مدختسي .تاسايسلاو ةزهجال او نيمدختسملا كلذ يف امب ةكبشلا ةيساسالا تامولعمل دراوم مادختساب لمعلا لهسي وهو .اهترادوا ةكبشلا ءاشنال دحاو ناكمك AD نولوؤسملا .ةدحوم ةقيرطب ةعونتملاو ةدقعمل او ةطبارتملا ةكبشلا

دوجوملا) يجراخ AD راخي مادختساب ةقداصملا هل حرصم صخش يأل نكمي ،اهنيوكت درجمبو نكمي .RV34x هجوم ىل ةنيعم ةمدخ ي مادختسالا (Windows Server ليجشت ماظن يف ةزهجال ىل نورفوتي مهنا املاط ،ةرفوتملا تازيملا مادختسالا نيدمتعمل نيمدختسملا ةقداصملا نم عونلا اذه مادختسالا ةبولطملا جماربلاو

جماربال رادصا | قيبطتلل ةلباقلا ةزهجال

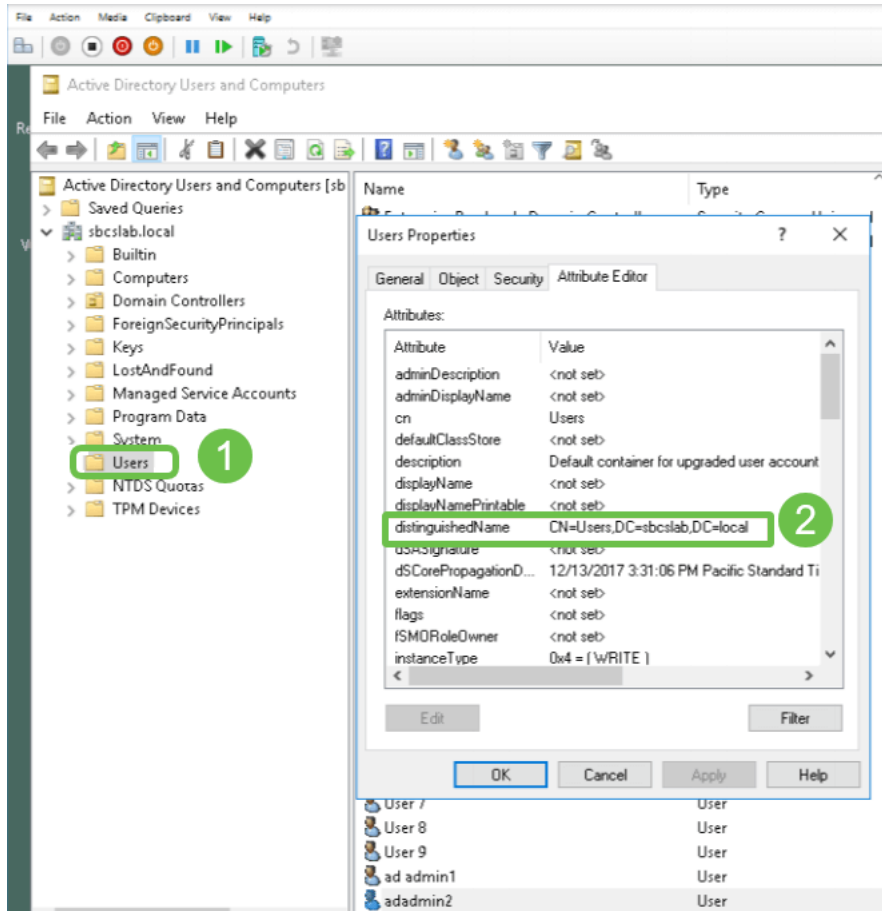
- RV340 | 1.0.03.16
- RV340W | 1.0.03.16
- RV345 | 1.0.03.16
- RV345P | 1.0.03.16 زارطلا

تايوتحمل لودج

- [زيمل مسالا ةميق ىل فرعلا](#)
- [Active Directory ل نيمدختسم ةعومجم ءاشنا](#)
- [RV34x هجوملا ىل Active Directory ليصافت ةفاضل](#)
- [لمالكلا مسالا ل قح نم ةحاسملا ذخأت مل اذا ثدحي اذام](#)

زيمل مسالا ةميق ىل فرعلا

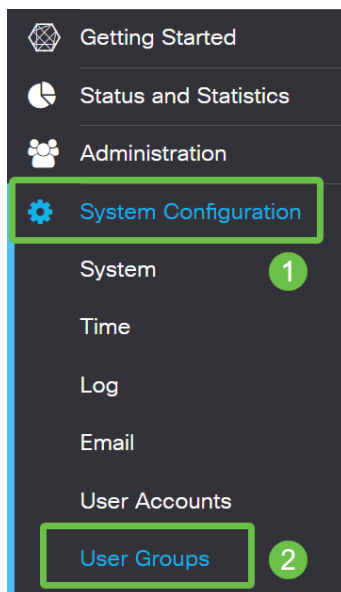
Windows 2016 مداخل رتوي بملء أوجه أو *Active Directory* يمدختم ةرادإ ةهجاو ىلإ لوصول
صائصه لاحتفا م، سوامل قوف نميال سوامل رزب رقنا م، نيمدختم سمل ةيواح دلجم دح
مدختم سمل ةيواح راسم لقح يف اقحال اهمادختم سمل متيس يتل *DistinguishedName* ةمي ق طحال
هجوم RV34x.



ل Active Directory نيمدختم سمل ةعومجم عاشنإ

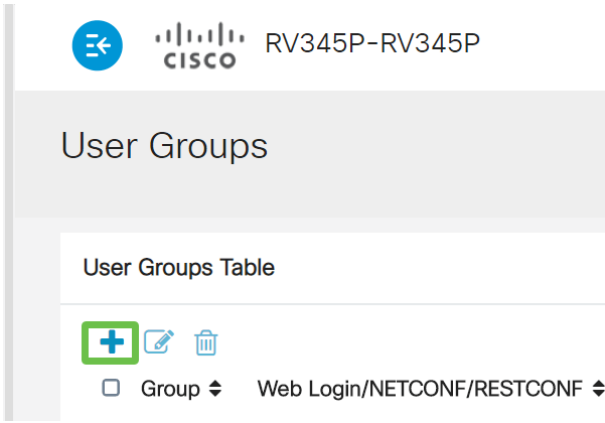
1 ةوطخل

تاعومجم > ماظنل نيوكت ىلإ لقتنا RV34x ةلسلسل نم هجوم ىلإ لخدلا ليجستب مق
نيمدختم سمل.




2 ةوطخل

دئاز ٺنوقڻي آيلع رقنا



3 ؤوطخل

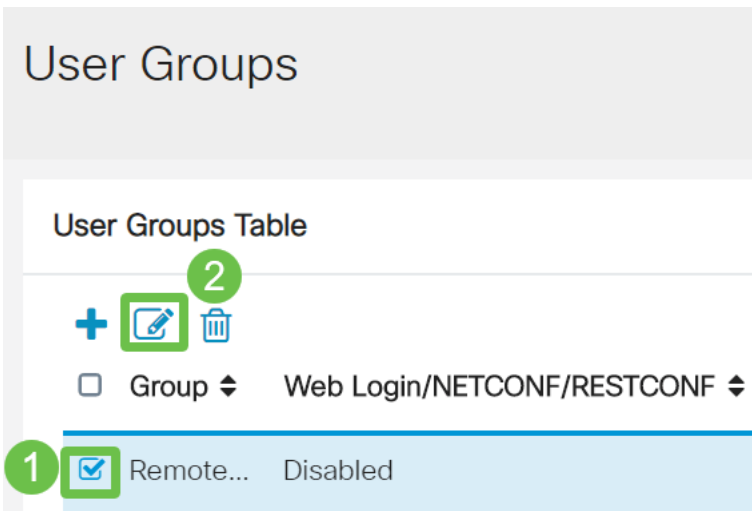
قبطي ؤق طقط. ؤعومجم مسا لخدأ



RemoteAdmin نيمدختسم ؤعومجم عاشنإ مت، لاثملا اذيف

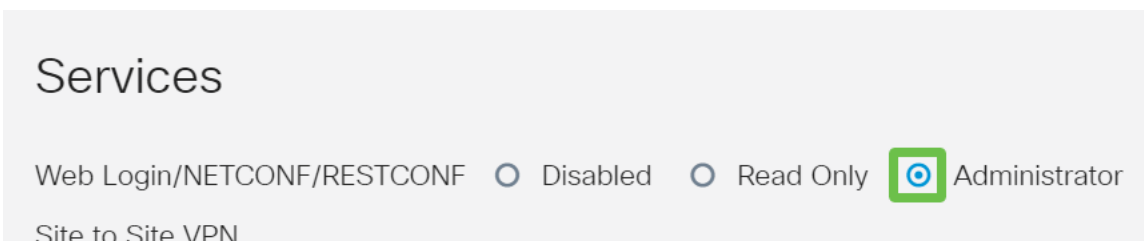
4 ؤوطخل

ريرحتلا ؤنوقڻي رقنا. ؤديجل نيمدختسملا ؤعومجملا ؤرولامل رايثخالا ؤناخ قوف رقنا



5 ؤوطخل

Administrator Radio رز يلع رقنا. تامدخلا يلى لفسأل ريرمتلاب مق



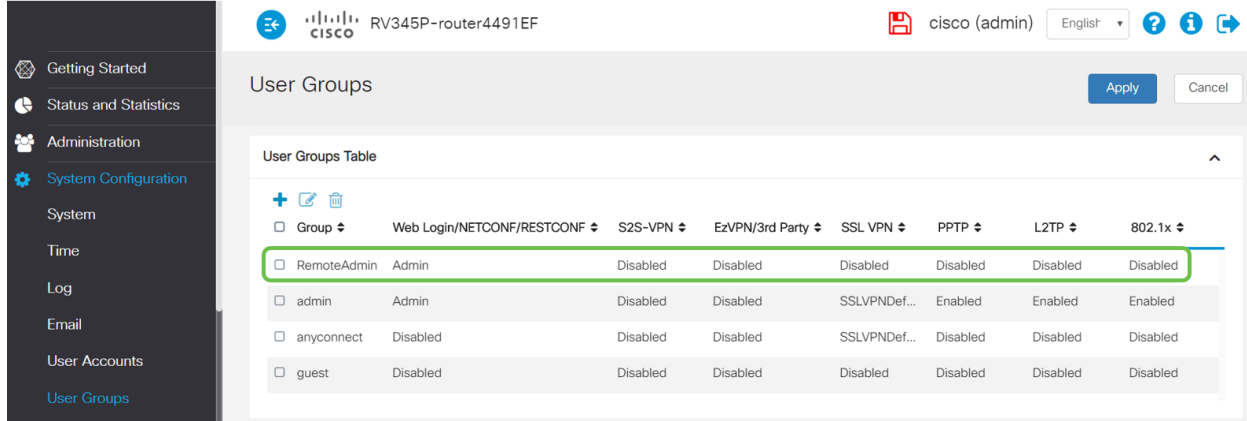
6 ةوطخل

قبطي ةققط.



7 ةوطخل

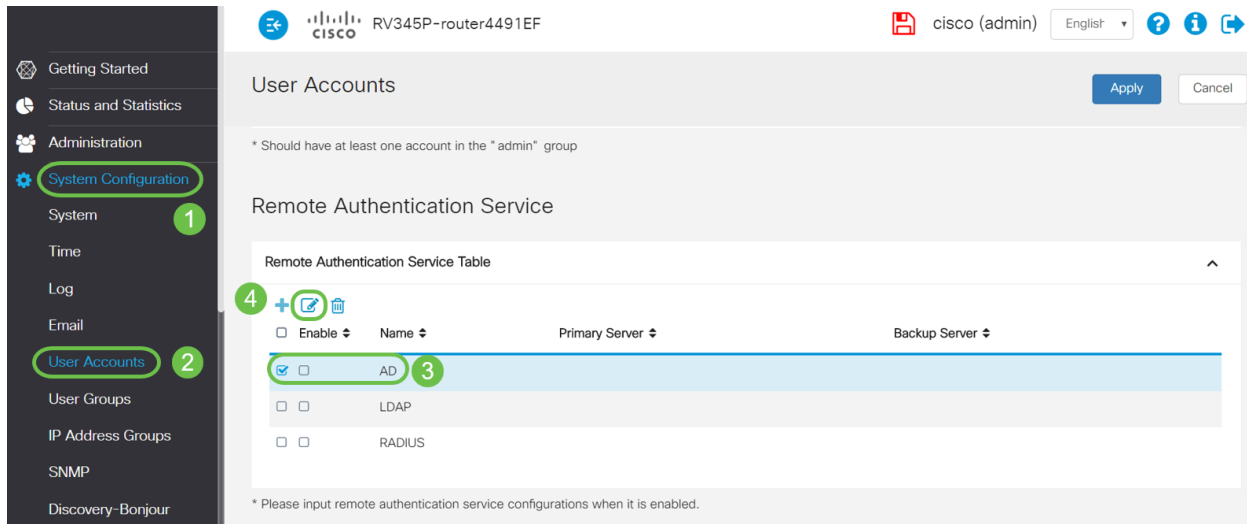
لوؤسمل تازايتماب رهظت يتي الل ةديجل ني مدختسمل ةومجم نآل دهاشتس.



Active Directory لي صافات ةفاضل

1 ةوطخل

ريحتل ةنوقي رقن او AD راخي دح. ني مدختسمل تاباسح > ماظنل نيوكت يتي لقتنل AD. مداخل لي صافات ةفاضل.



2 ةوطخل

ةققط. مدختسمل ةيواح راسم و ذفنم او ياساسل مداخل او نال ةلال لاجم مسل لي صافات لخدأ قبطي.

User Accounts

Apply

Cancel

2

Add/Edit New Domain

Name	AD		
Authentication Type	Active Directory		
AD Domain Name	sbcslab.local		
Primary Server	172.16.1.2	Port	389
User Container Path	cn=user,dc=sbcslab,dc=loc		

1

في Windows مداخل نم ةطقن لمل المدخس مل ةي و ا ح راسم لي صافات لا خد ا ل ا ج ا ح ت : ةظ ا ح مل ة ل ا ق م ل ا ه ذ ه في [ة ز ي م م ل ا م س ا ل ا ة م ي ق ي ل ع ف ر ع ت ل ا](#) م س ق

ي ض ا ر ت ف ا ل ا ع ا م ت س ا ل ا ذ ف ن م . `cn=user, dc=sbcslab, dc=local` ي ه لي ص ا ف ت ل ا ، ل ا ث م ل ا ا ذ ه في 389 و ه (LDAP) لي ل د ل ل و ص و ل ل في ف ا خ ل ل و ك و ت و ر ب ل ا م د ا خ ل

3 ة و ط خ ل ا

ن ي م د خ ت س م ل ا ة و م ج م م س ا ق ب ا ط ا ت ا ه ن ا و ، ن ي م د خ ت س م ل ا ة و م ج م ن ي و ك ت ن م ق ق ح ت ، ن ا ل ع ا ل ا ي ف ه ج و م ل ل .

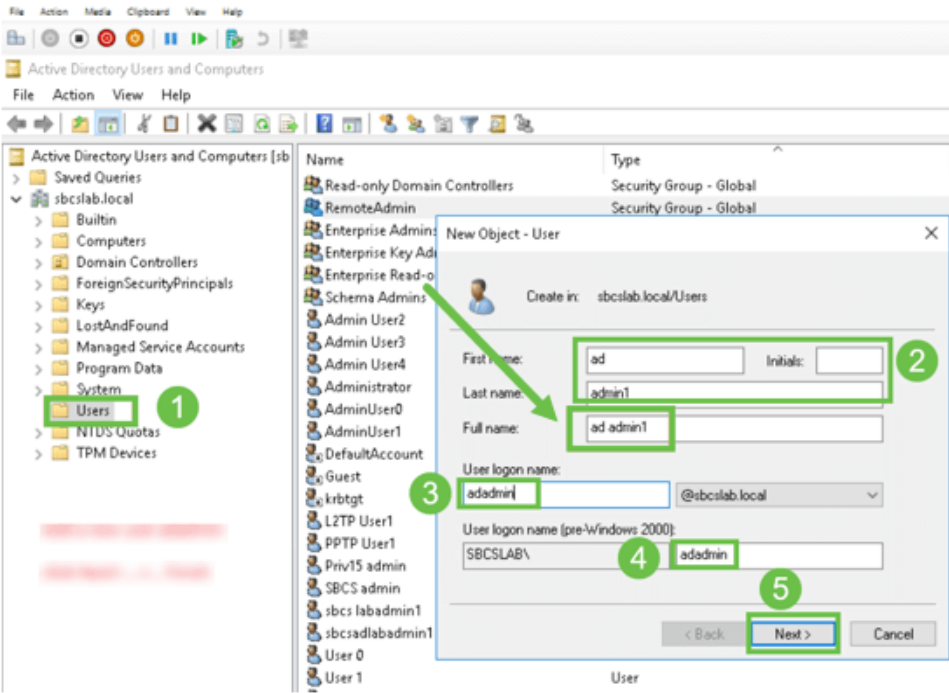
Name	Type
Enterprise Read-only Domain Controllers	Security Group - Universal
Group Policy Creator Owners	Security Group - Global
Guest	User
Key Admins	Security Group - Global
krbtgt	User
L2TP User1	User
L2TPVPN	Security Group - Global
PPTP User1	User
PPTPVPN	Security Group - Global
Priv15 admin	User
Priv15Admins	Security Group - Global
Protected Users	Security Group - Global
RAS and IAS Servers	Security Group - Domain Local
Read-only Domain Controllers	Security Group - Global
RemoteAdmin	Security Group - Global
SBCS admin	User
sbcslabadmin1	User
sbcsladlabadmin1	User
Schema Admins	Security Group - Universal

4 ة و ط خ ل ا

م ت ي س ، ة ل ئ ا ع ا ل ا م س ا و ي ل و ا ل ا ف و ر ح ل ل ، ل و ا ل ا م س ا ل ا ة ئ ب ع ت ب م ق ، م د خ ت س م - د ي ج ن ئ ا ك ت ح ت ة ل ئ ا ع ا ل ا م س ا و ل و ا ل ا م س ا ل ا ن ي ب ة ف ا س م ر ا ه ظ ا ع م ، ا ي ئ ا ق ل ت ل م ا ك ل ل م س ا ل ا ل ق ح ع ل م

م ت ي ن ل و ا ل م ا ك ل ل م س ا ل ا ع ب ر م ي ف ر ي خ ا ل ا م س ا ل ا و ل و ا ل ا م س ا ل ا ن ي ب ة ف ا س م ل ا ف ذ ح ب ج ي ح ي ح ص ل ك ش ب ل و خ د ل ا ل ي ج س ت

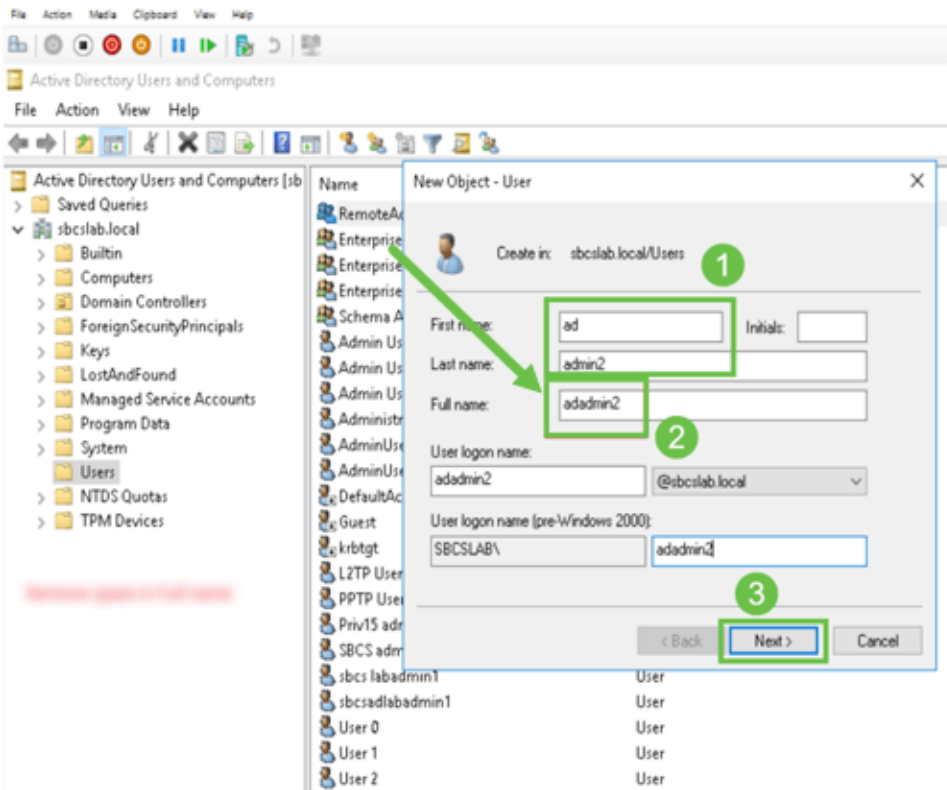
اهفدح بچي يتلا لمالكلا مسالا يف ةحاسملا ةروصلا هذه ضرعت:



5 ةوطخلال

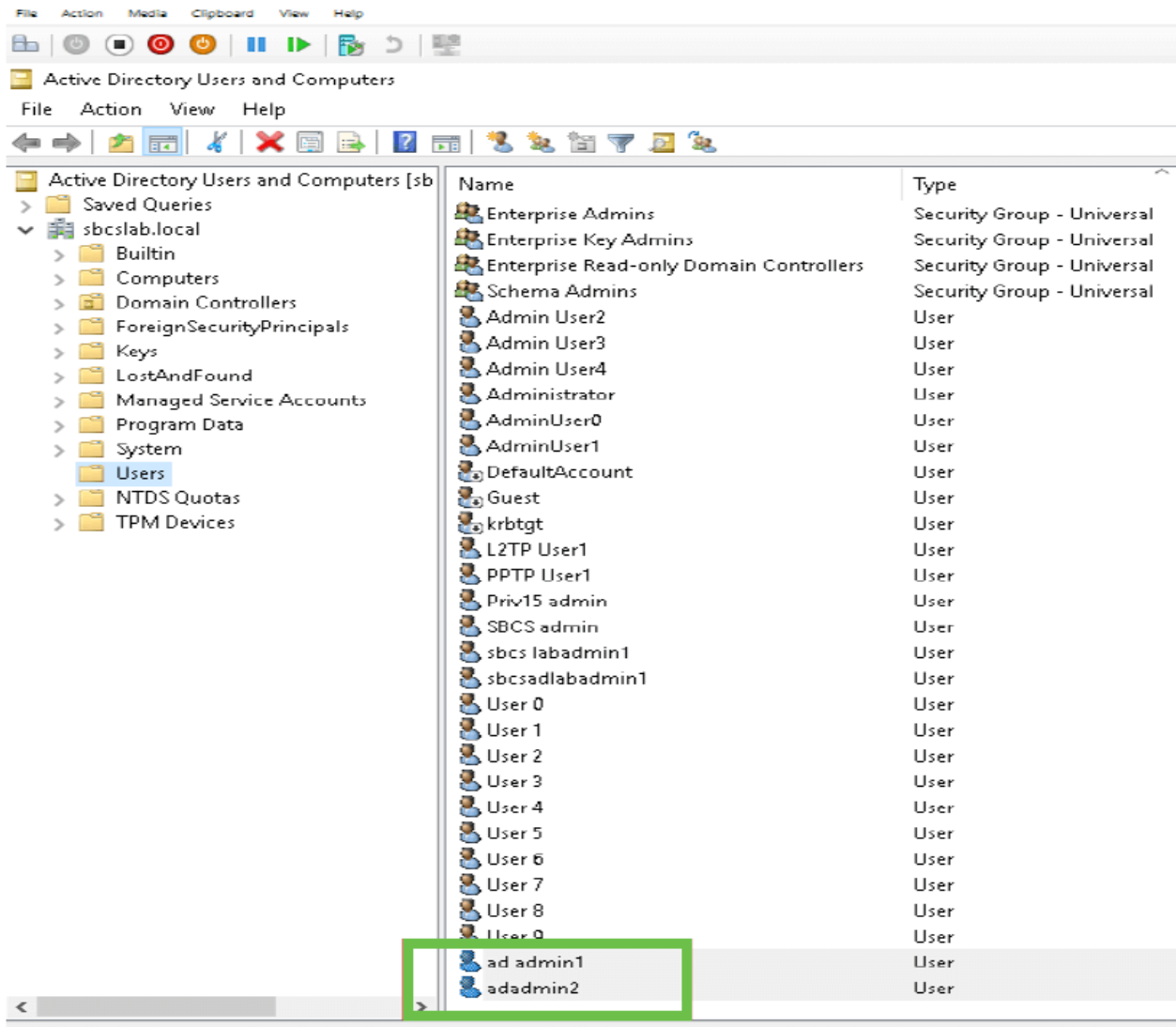
يا ةلازاب لمالكلا مسالا لقح ليدعت لاجاتحت ،يرخأ ةرم .رخأ مدختسم عاشنإل تاوطخلال ررك عاشنإ ءاهنإب مق مث رورملا ةملك دادعال يلاتلا قوف رقنا .ايئاقلت اهؤاشنإ مت تافاسم مدختسملا .

ةحصلا ةقيرطالا يه هذه .لمالكلا مسالا يف ةحاسملا فدح مت هنأ ةروصلا هذه حضوت مدختسملا ةفاضال :



6 ةوطخلال

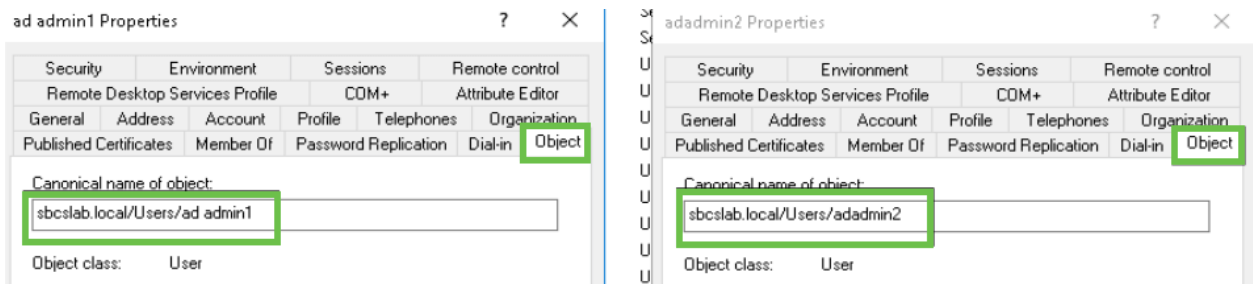
ا.ثي دح اهتفاض | تمت يتي لادختس مل ل ي صافات نم لك ني مدختس مل ا عمئاق رهظت



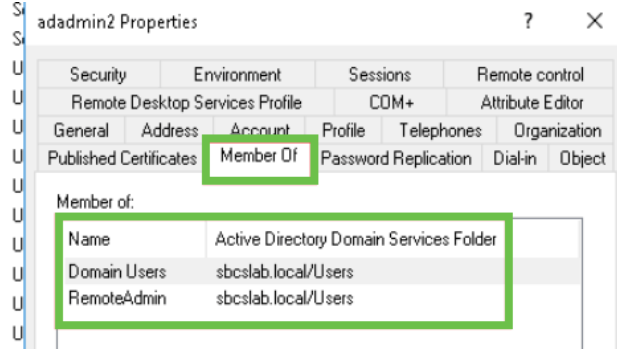
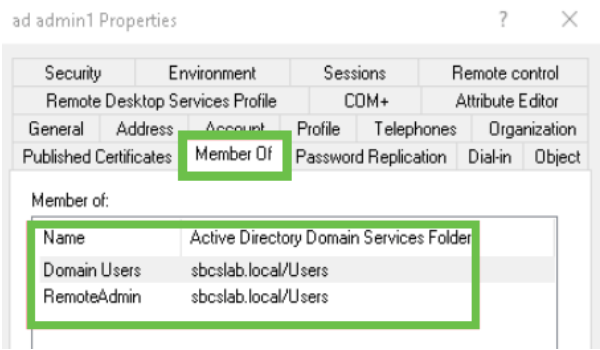
7 ةوطخل

اذه نكي مل اذا، ةلئاعل مساو لوالا مسالا ني ب ة فاسم رهظي نالعالا لوؤسم نا طحالاس كرتت ال، يحيضوتل ضرعل اضارعال اطخال اذه كرت متي. لوخدلا ليحست لش فيس، اتباث يحيص adadmin2 لاثم! اكانه ةحاسملا

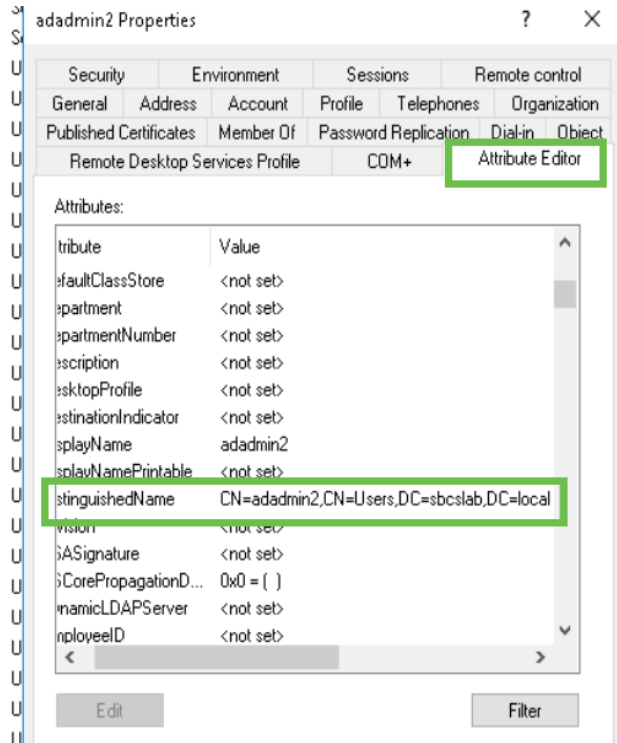
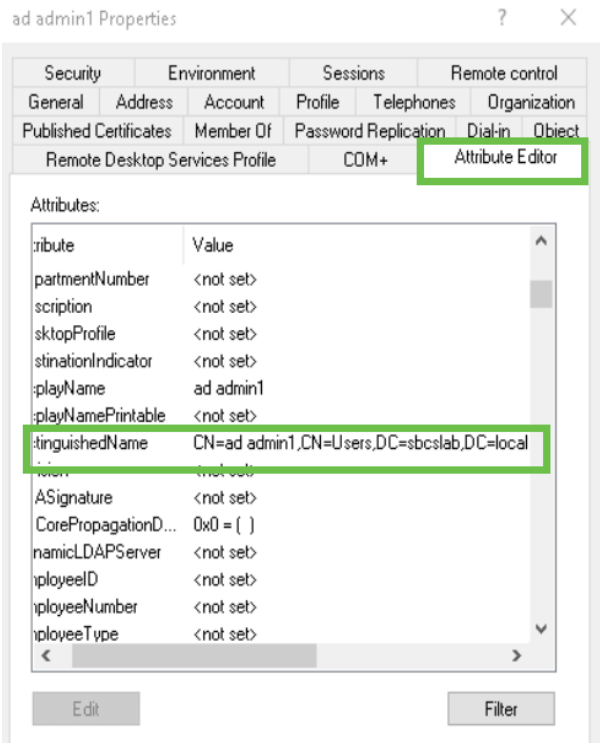
م. صئاصخل راخي ددحو ad admin 1 مدختس م مسا قوف نميالا سواملا رزب رقنا، ضرعلل نئاللا لي صافاتل هيلع فراعتمل مسالا یرتل نئاللا بيوبتلا ةمالع ىلا لقتنا



عامساب ةصاخلا RemoteAdmin و لاجملا ي مدختس م لي صافات نم ققحتلا كنكمي امك Properties راخلا نمض بيوبتلا ةمالع وضع ىلا لالقتنالا لال نم هذه ني مدختس م



صاخال ال *DistinguishedName* ميق نم ققحتلل تامسلا ررحم بيوبتلا عمال ع لى لقتنا هذه ني مدختسملا عامسأب.

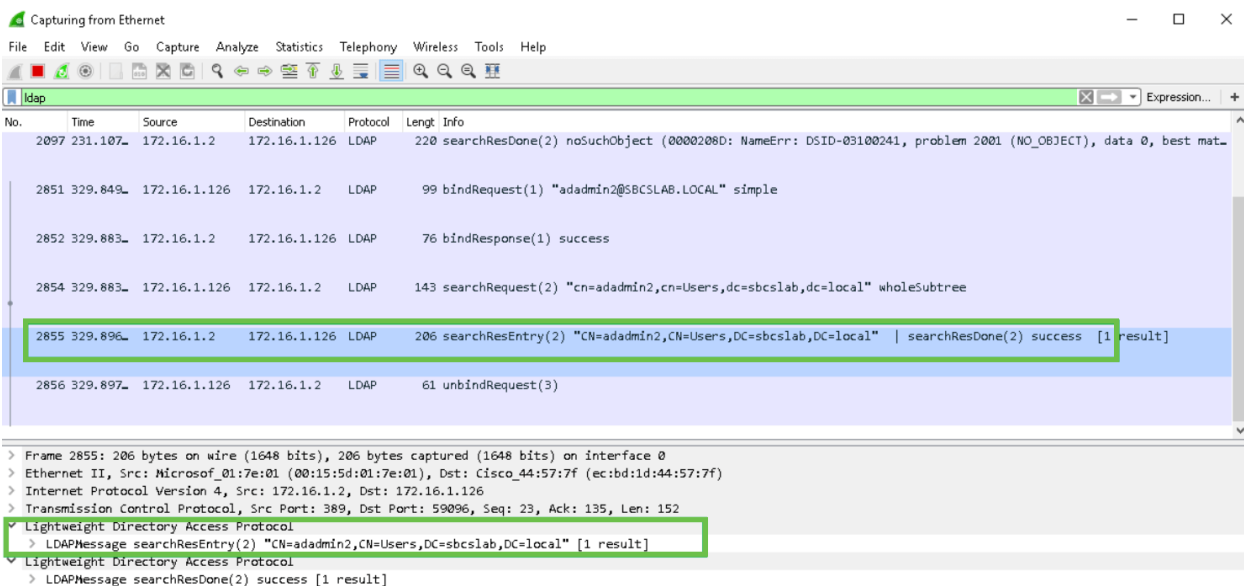


8 ةوطخال

adadmin2، ةالجال هذه يفو، مدختسملا لوخد ليجست مسامادختساب لوخدال ليجستب مق حججان لوخدال ليجست نأ ىرتس.

9 ةوطخال

ةيلاتلا ةشاشلا ةطقل يف حضوم وه امك ةمزحلا طاقتلال لوخ لىصافتلا ةيؤر كنكمي.



لمالك المسال لقح نم ةحاسملا ذخأت مل اذا ثدحي اذام

لجست نأ ىرتس *adadmin*، ةلاجل هذه يف، مدختسملا لوخذ لجست مس ا مدختسا تلواح اذا
عاجرا هنكمي ال (LDAP) نزولا في فخ ليلدلا لىل لوصول لوكوتورب م داخ نأل لش في لوخدلا
ةفورىل ع ارداق نوكتس. ةحاسم هب، *ad admin1*، ةلاجل هذه يف، *لمالك المسال* نأل نئالكلا
ةيلاتلا ةشاشلا ةطقل يف حضوم وه امك مزحلا طاقتلا دن ع لىصافتلا كلت

رارقلا

دعب نع ةقداصملا يف لشف ثودح تب نجت و حاجنب لوخدلا لجست لامك نم نآلا تي هتنا دقل
RV34x هوملا لىل ع Active Directory ربع

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا