

مدخستسملا ةيوهو (LDAP) AD ةقداصم نيوكت ءالمعل FDM ةطساوب ةرادملا FTD لعل AnyConnect

تايوتحمل

[ةمدقمل](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدخستسملا تانوكملا](#)

[نيوكتلا](#)

[ويرانيسلاو ةكبش ليل طيختللا مسرلا](#)

[AD تانوكت](#)

[DN يساسأل LDAP ديخت](#)

[FTD باسح عاشنا](#)

[\(يرايتخا\) تانالعا تاعومجم يلا نيمدخستسم ةفاض او تانالعا تاعومجم عاشنا](#)

[\(STARTTLS أو LDAPs لطقف بولطم\) LDAP ب صاخلا SSL ةداهش رذخ خسن](#)

[FDM تانوكت](#)

[صيخرتلا نم ققحتلا](#)

[تانالعالا ةيوه ردصم دادعا](#)

[AD ةقداصملا AnyConnect نيوكت](#)

[مدخستسملا ةيوهل نامأل تاسايس نيوكتو ةيوهل جهن نيكمت](#)

[ةحصللا نم ققحتلا](#)

[يئاهنلا بيترتلا](#)

[اهنم ققحتلاو AnyConnect نم لوصولا يف مكحتلا ةسايس دعاوقب لاصتالا](#)

[اهخالص او عاخالصا فاشكتسا](#)

[عاخالصا حيحصت](#)

[ةلماعلا LDAP عاخالصا حيحصت](#)

[LDAP مداخب لاصتلا عاشنا رذعت](#)

[ةحيحص ريغ طبرلل رورملا ةملك و/أو DN](#)

[مدخستسملا مسالا لعل روثعلا LDAP مداخ لعل رذعت](#)

[مدخستسملا مسالا ةحيحص ريغ رورملا ةملك](#)

[AAA رابتخا](#)

[مزللا طاقتلا](#)

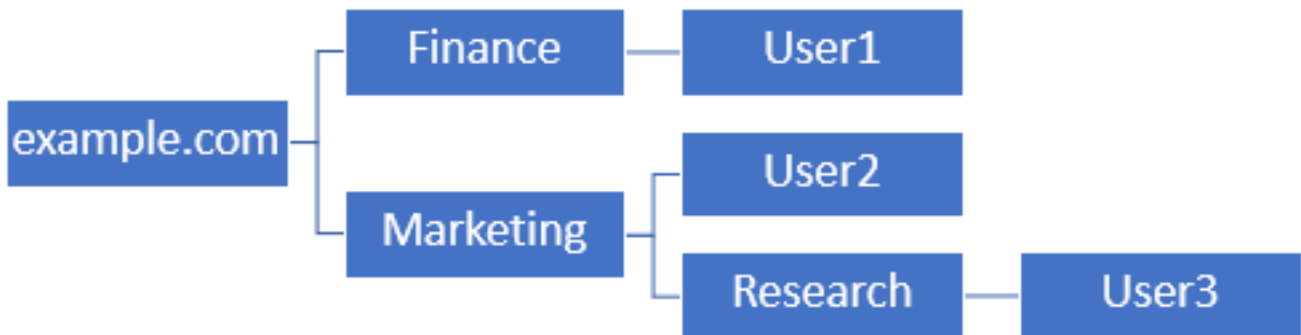
[Windows Server ثادحا ضراع تالجس](#)

ةمدقمل

ءالمعل (AD) Active Directory ةقداصم نيوكت ةيفيك حيضوت وه دننتسملا اذه نم ضرغل
ةطساوب ةرادملا Cisco نم (FTD) FirePOWER ديدهت نع عافدب نولصتي نيذل AnyConnect
لوصولا تاسايس يف مدخستسملا ةيوه مادختسا متيس. (FDM) FirePOWER زاهج ةرادا
ةنيعم ذفانمو IP نيوانعب AnyConnect يمدخستسم ديقتل.

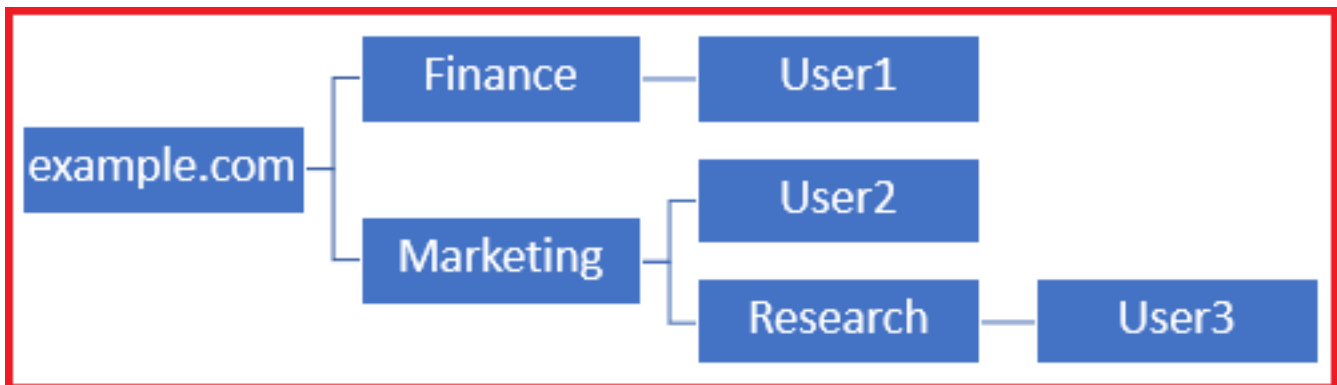
نم ليلق ددع رفوت مزلي، FTD يلع بسانم لكش ب مدختس مالا ةيوهو AD ةقداصم نيوكتل نيوكتل اارج لبق Microsoft مداخل يلع اهعيجت وا ليصافتلا هذه عيج عاشنا بجي .ميقلا يه ةيسيئرلا ميقل (FDM). لوجملا تانايب ةدعاق ةرادا يلع

- مسا وه example.com، اذه نيوكتل ليلدي في .مدخلل لاجملا مسا وه اذه :لاجملا مسا لاجملا.
- مت اذا Microsoft مداخل يلا لوصولل مدختس مالا FQDN وا IP ناووع :مدخلل IP/FQDN ناووع نيوكتل ليلدي في . FQDN لجل FTD و FDM لخاد DNS مداخل نيوكتل بجي في ، FQDN مادختسا 192.168.1.1 يلا لجل متي يذلا win2016.example.com يه ميقل هذه نوكت ، اذه مدختس يسي ، يضا رتفا لكش ب . LDAP ةمدخ ةطساوب مدختس مالا ذفنملا :مدخلل ذفنم LDAP TCP 636 ذفنم SSL (LDAPs) ربع LDAP و LDAP ل TCP 389 ذفنم STARTTLS و LDAP عجرملا مادختسا مزلي ، STARTTLS و LDAP مادختسا ةلاح في : رذجلل قداصملا عجرملا LDAPs. ةطساوب ةمدختس مالا SSL ةداهش عيقوتل رذجلل قداصملا
- FTD و FDM لبق نم مدختس مالا باسحلل وه اذه :رورملا ةمكلو ليلدل مدختس مالا مسا متي .تاعومجمو ني مدختس مالا نع ثحبلل او ني مدختس مالا ةقداصم و LDAP مداخل طبرلل ضرغل اذهل " FTD لوؤسم " مسا باسح عاشنا
- نم FTD بلطيس و FDM ءدبلا ةطقن يسياس الال DN لثمي (DN) يسياس الال زيمملا مسالا متي ، اذه نيوكتل ليلدي في . ني مدختس مالا نع ثحبلل دنع ءدبلا Active Directory دق ، جاتنال ةئيبل ، كلذ عم و ، يسياس الال DN هنا يلع example.com رذجلل لاجملا مادختسا يلع . لضاف LDAP ل يمرهال جردتلل لخاد يفاضل لكش ب يسياس الال DN مادختسا نوكتي اذه LDAP يمرهال جردتلل مدختسا ، لاثملا ليلبس



يلع نيرداق ةيميظنتلا قيوسنتلا ءدحو لخاد نومدختس مالا نوكتي نا دي ري لوؤسملا ناك اذا كلذ نإف ، (example.com) رذجلل يلع هن ييغت نكمي يذلا يسياس الال DN يلع ةقداصملا اضيأ لوخدلا ليحستب ةي لاملا ةيميظنتلا ءدحو لا نمض دوجوملا User1 ل اضيأ حمسي .ثحبلل او قيوسنتلا ءدحو ليلد يلا هجتو رذجلل نم ادب يسي مدختس مالا ثحبل نال ارظن

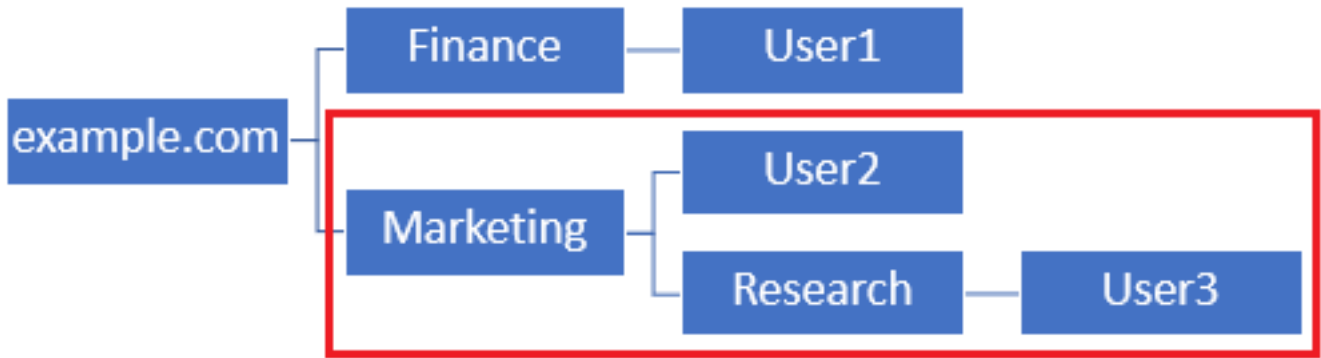
وا قيوسنتلا example.com يلع يسياس الال DN نييغت مت



وا قيوسنتلا ءدحو يلا ءدحو في طقف ني مدختس مالا لوخدلا ليحست تاي لمع دييقت لجا نم ل نال نكمي . "قيوسنتلا" يلع يسياس الال DN نييغت كلذ نم ادب لوؤسملا نكمي ، هاندا

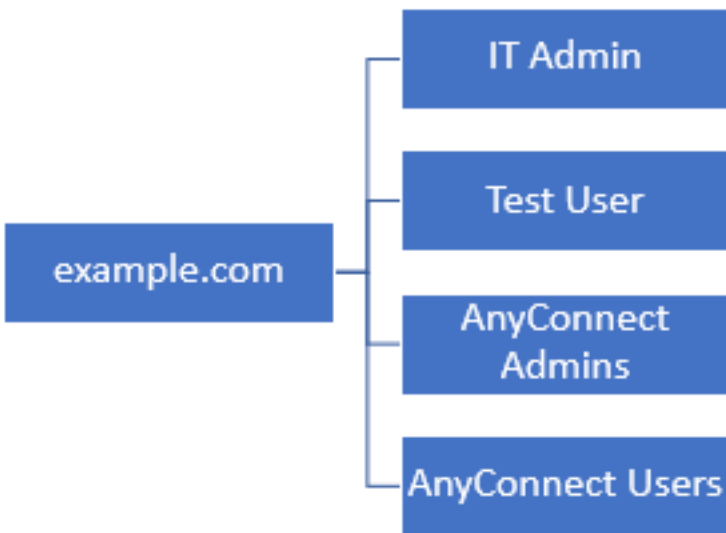
"قيوستلا" ي ف أدبيس شحبال نأل ةقداصلما طقف User2 و User3

قيوستلا لىل عيساسأل DN نييت



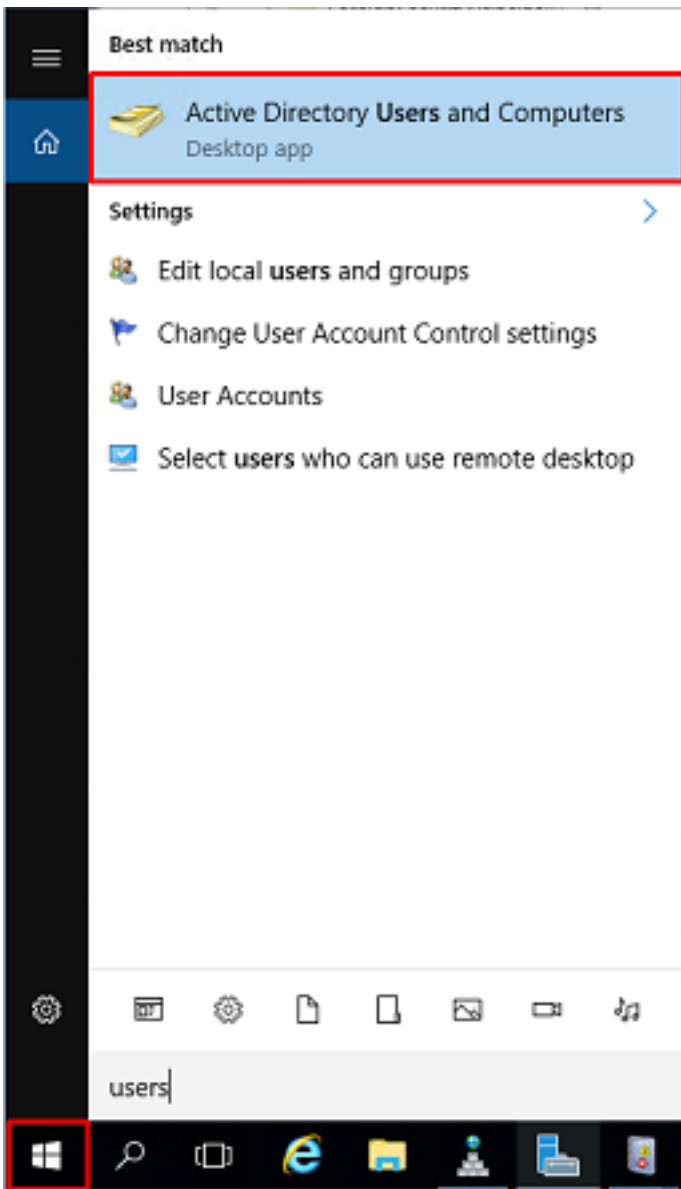
نيمدختسملل حامسلال متيس يذلاو FTD لخاد تايوتسملال ددعت م كحتلا نم ديزمل هنا طحال م، ةصاخلا AD تامس لىل اذانتسا نيمدختسملل فل تخم ضيوقت نييت وا ليصوتب LDAP ضيوقت ةطيرخ نيوكت نييتسي.

مادختسا متيس واذه نيوكتلا لىل د ي ف طسبملا LDAP ل يمرهال جردتلا اذه مادختسا متي DN لىل example.com رذجلل DN.

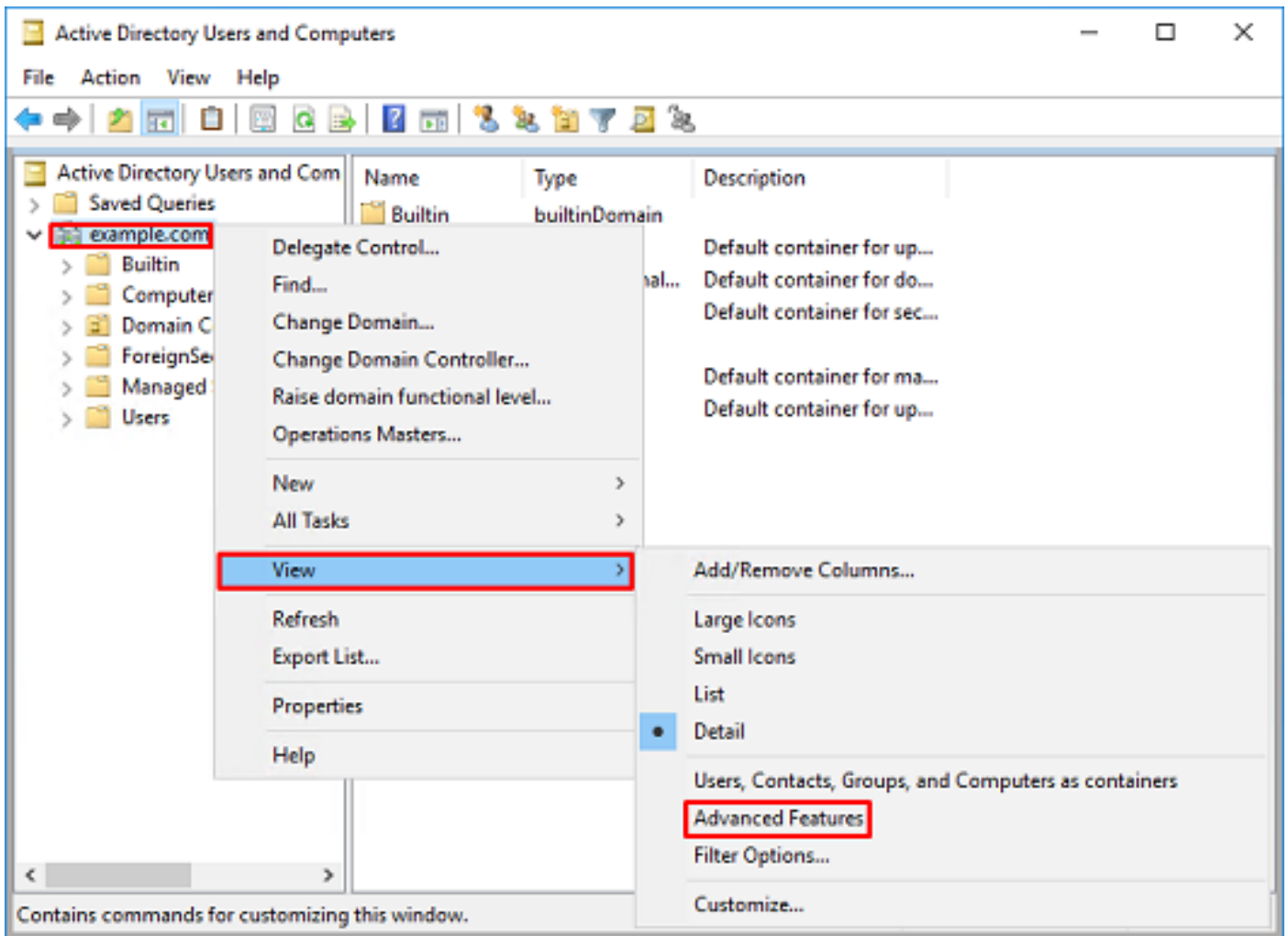


DN يساسأل LDAP ديحت

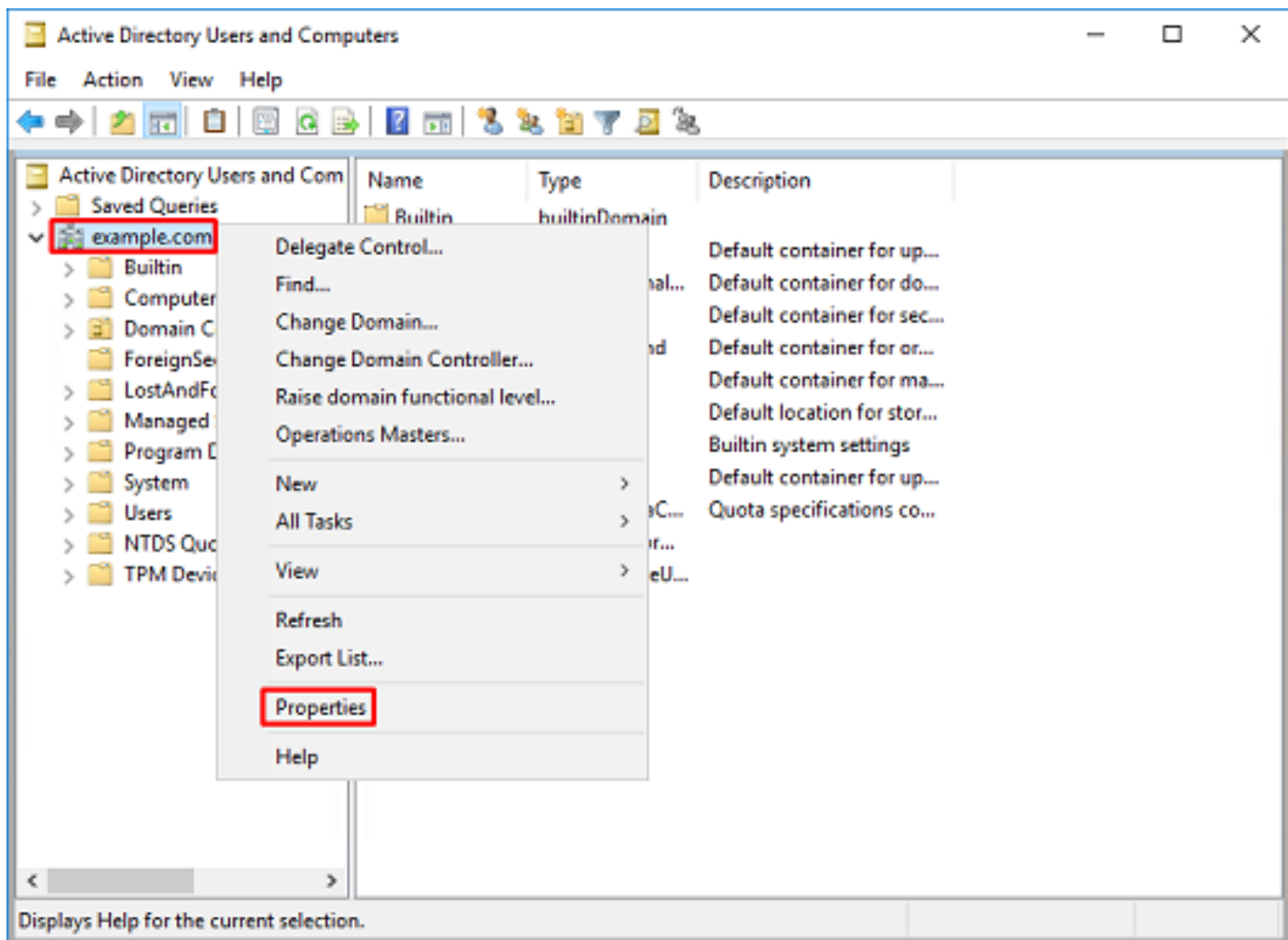
رتويبمكلا ةزهجأو حوتفملا نالعالا ومدختسم 1.



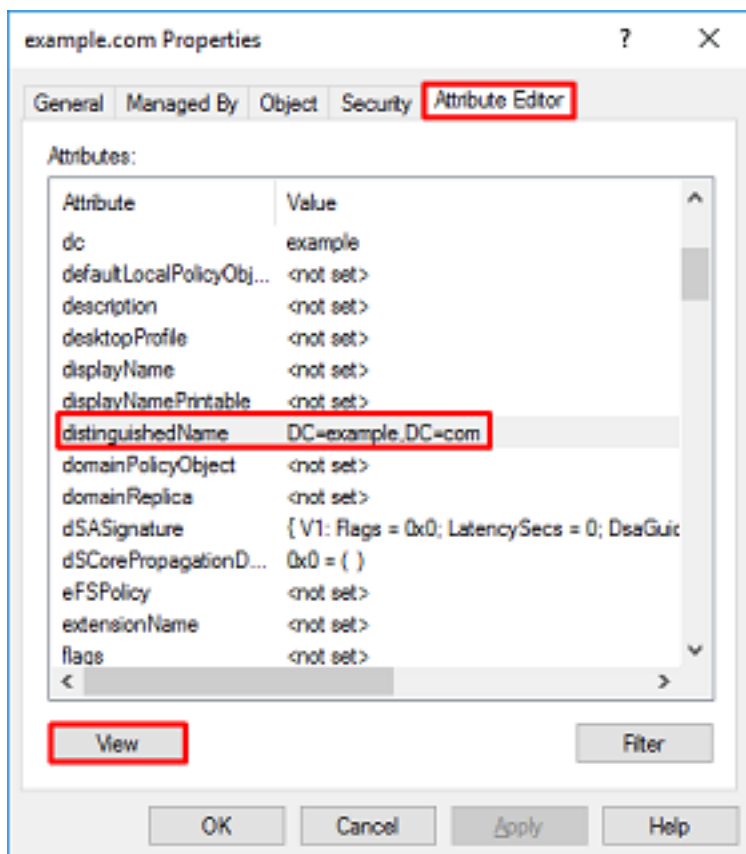
2. نميأل سواملا رزب رقنا م ث، (ةيواحل حتفل) رذجل لاجملا قوف نميأل سواملا رزب رقنا م ث. ةمدقتم تازيم قوف رقناو ضرع ىلإ لقتنا م ث، رذجل لاجملا قوف



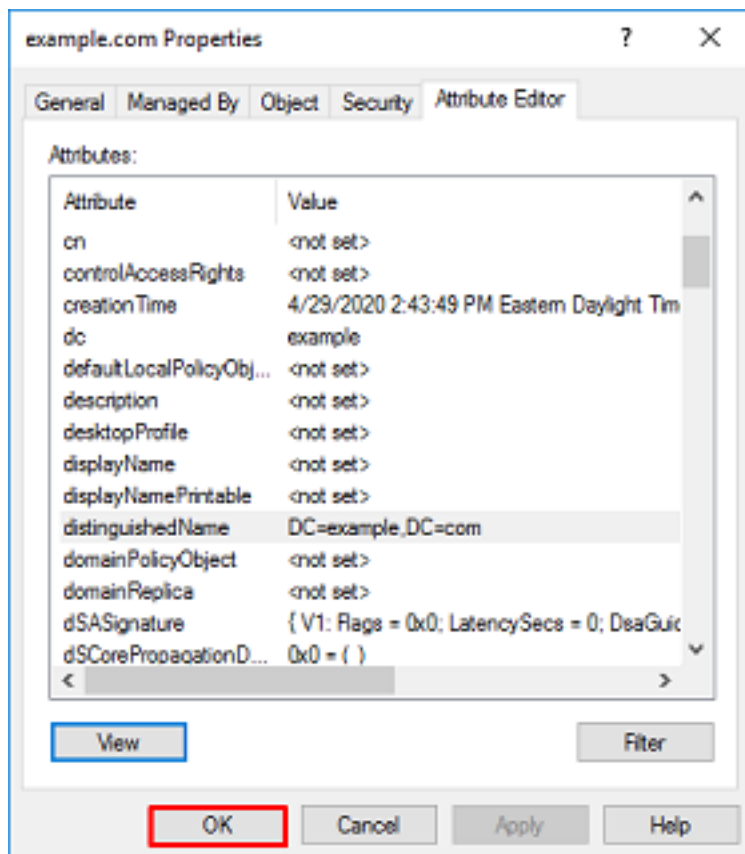
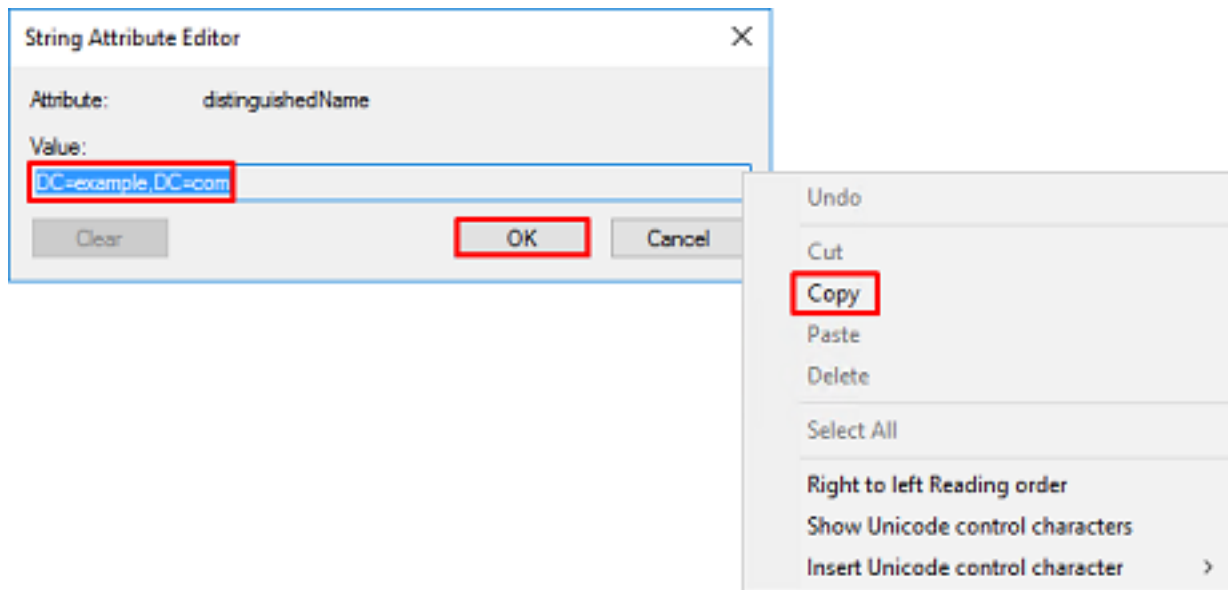
3. روثعلل، لاثم لاي بس ىلع AD تانئاك تحت ةيفاضإلا صئاصخال ضرع لك لذحي تي س. قوف نميال سواملا رزب رقنا، example.com يسيئرلا رزلاب ةصاخال DN ةكبش ىلع صئاصخالا ىلا لقتنا مث example.com.



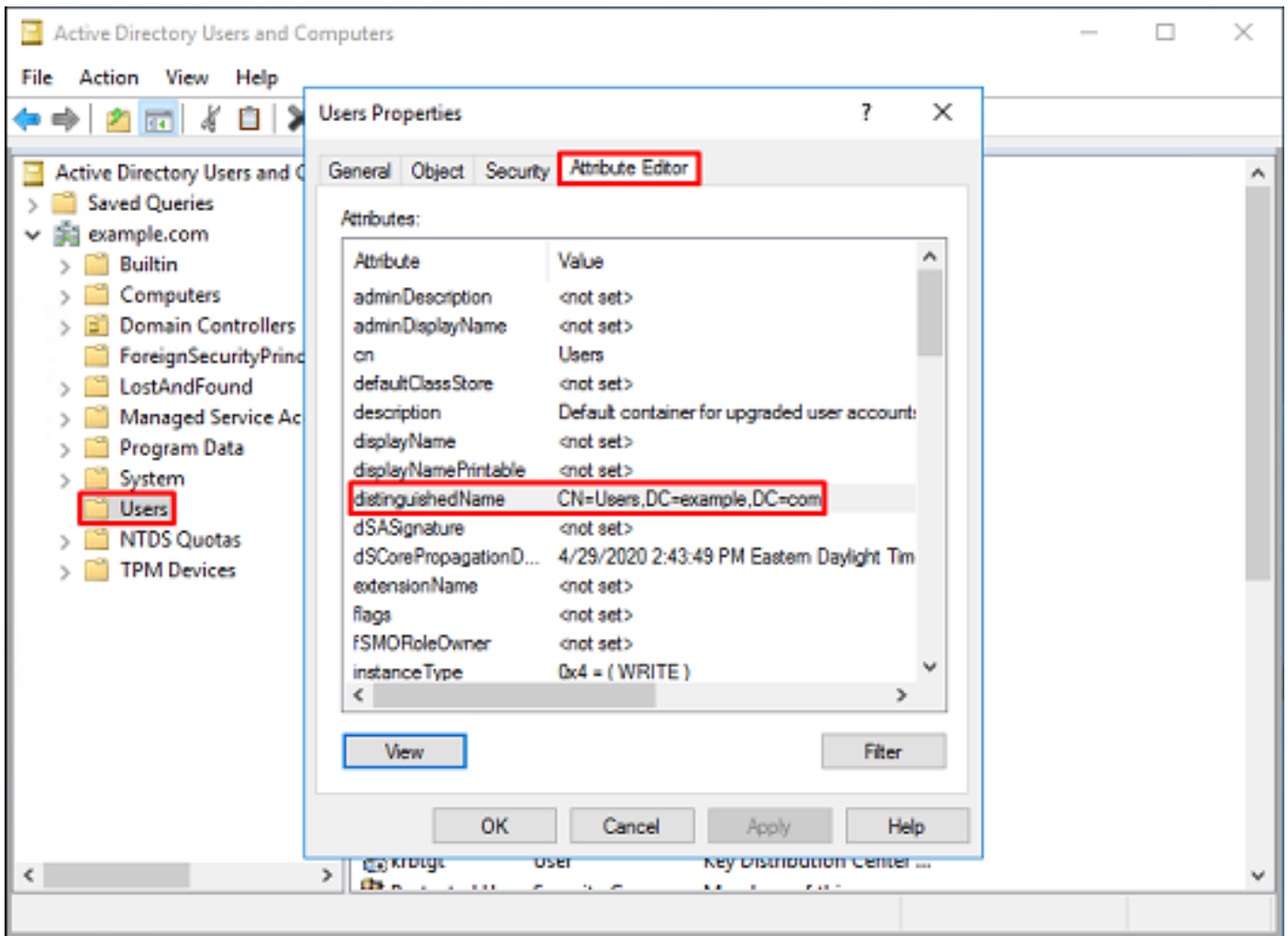
4. تامسلا تحت زيم مسانع شحبا. تامسلا ررحم بيوبتلا عمالع قوف رونا، صئاصخ تحت. ضرع قوف رونا مث.



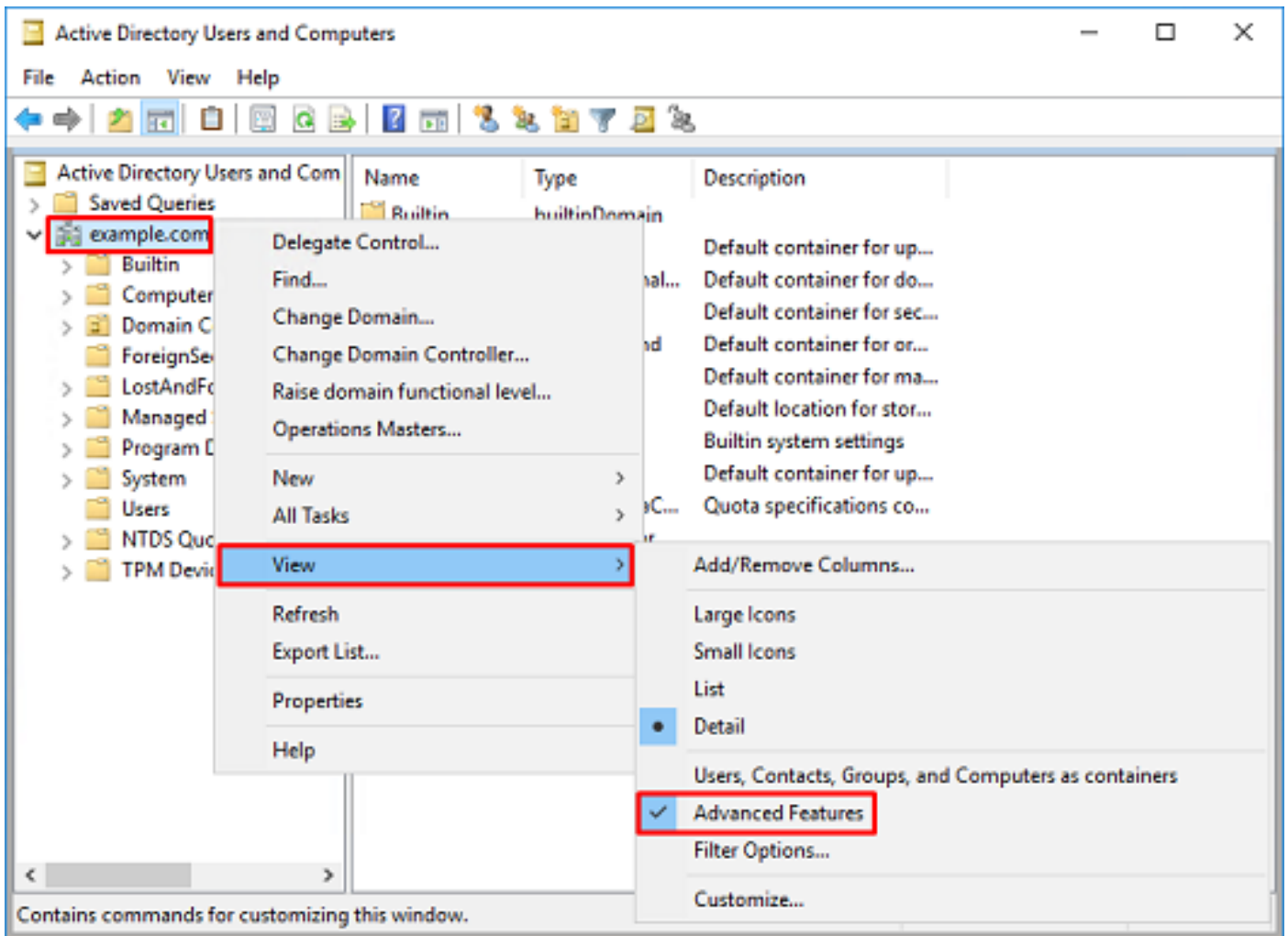
5. اذہ ڀف اقحال FDM ڀف هوقصلو DN خسن نكمي شيح ءديج ءذفان حتف ىل اكلذ ڀدؤي س. نم جورخلل قفاوم قوف رقنا . ءميقلال خسننا . DC=example، dc=com وه روجل DN نوکي ، لالم لاصخلل نم جورخلل ىرخأ ءرم قفاوم قوف رقناو ، ءلسلسلا تامس ررحم ءذفان



مادختسا متي ، لالم لىبس ىل ع . AD لخاد ءدءتم تانئاك ءبسنلاب اكلذب مايقلا نكمي مدختسما ءيواحب صاخلا DN ىل ع روئعلل تاوطلخل هءه



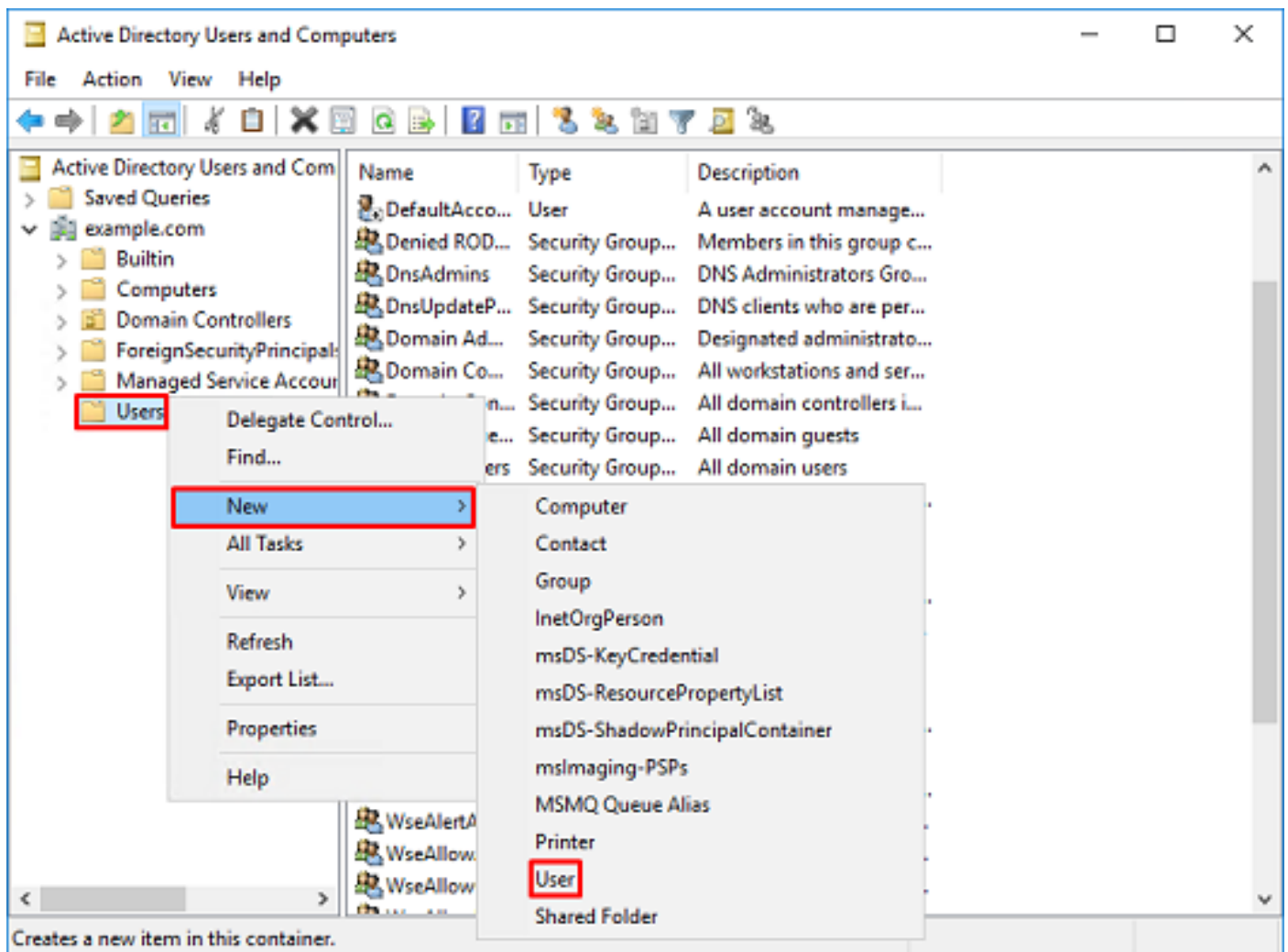
6. رذجل DN ةكبش ىلع نميال سوامل رزب رقنا . ةمدقتملا تازيملا ضرع ةقيرط ةلازا نكمي .
 ىرخا ةرم ةمدقتملا تازيملا قوف رقناو ، ضرعلل حفصتو .



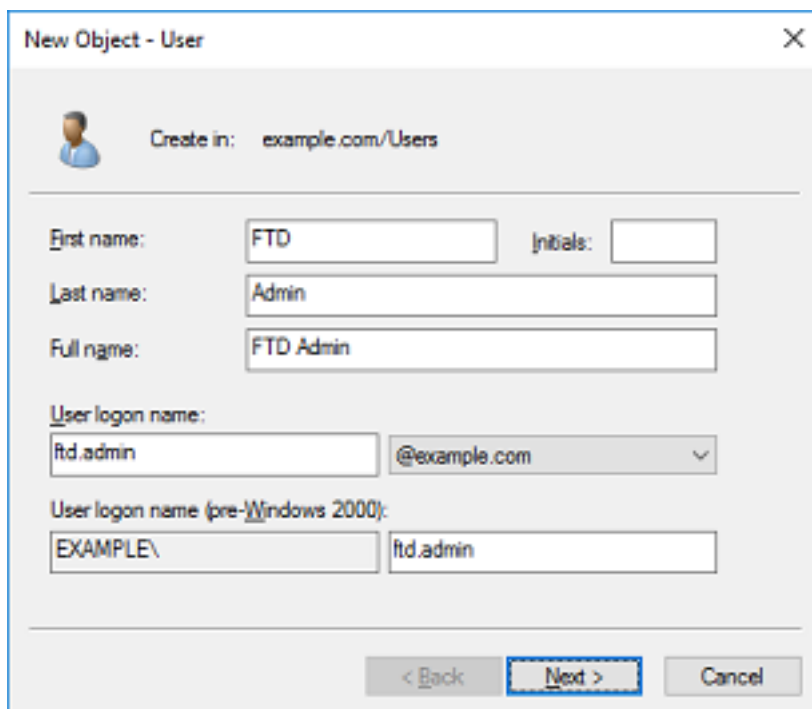
FTD باسح عاشن

نېم دختس مالا نغ تح بلل AD عم طبارت لاب FTD و FDM ل اذه مدختس مالا باسح حمسي سحرص مالا ريغ لوصولا عنم وه لصفنم FTD باسح عاشن نم ضرغلا. مهتقد اصم و تاومج مالا و نأ مزلي ال. طبرلل عم دختس مالا دامتعالا تانايب قارتخأ مت اذا ةكبشلا لخاد رخأ ناكم يلا هب يساسالا DN قاطن نمض باسحالا اذه نوكي.

1. عم ظنم لالا/ةيواحلا قوف نم يالا سواملا رزب رقنا. **Active Directory Users and Computers** نمض FTD باسح ةفاضلا متيس يتلا نمض FTD باسح ةفاضلا متتس، نيوكتلا اذه ي. اهلا FTD باسح ةفاضلا متيس يتلا نمض "نوم دختس مالا" ةيواح نم يالا سواملا رزب رقنا. **ftd.admin@example.com** مدختس مالا مسانمض "نوم دختس مالا" ةيواح مدختسم > ديچ قوف رقنا مت، نېم دختسم قوف



2. مدخستسم - ديدج نئاك جالعام ربع لقننتال.



New Object - User

Create in: example.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

New Object - User

Create in: example.com/Users

When you click Finish, the following object will be created:

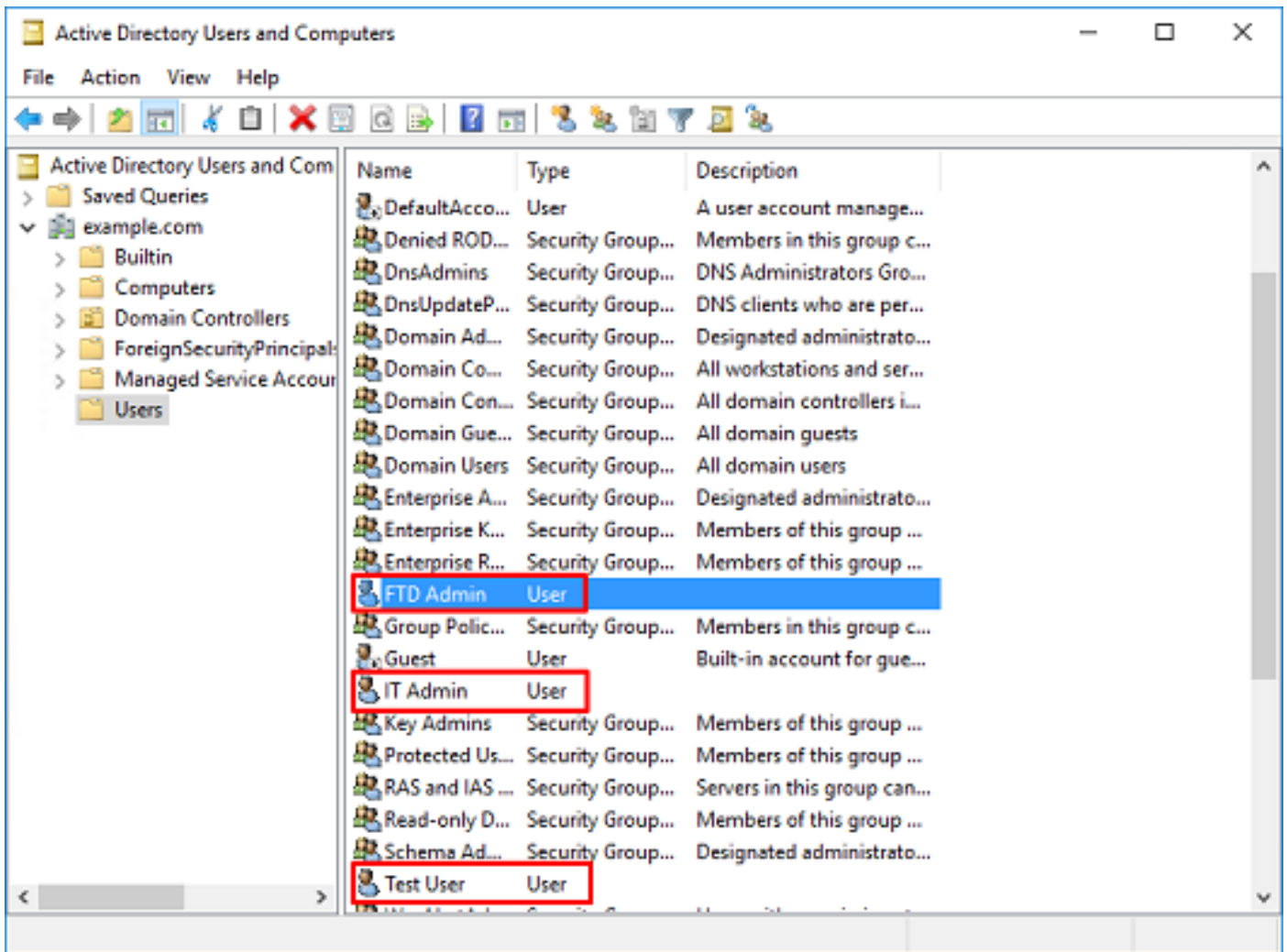
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

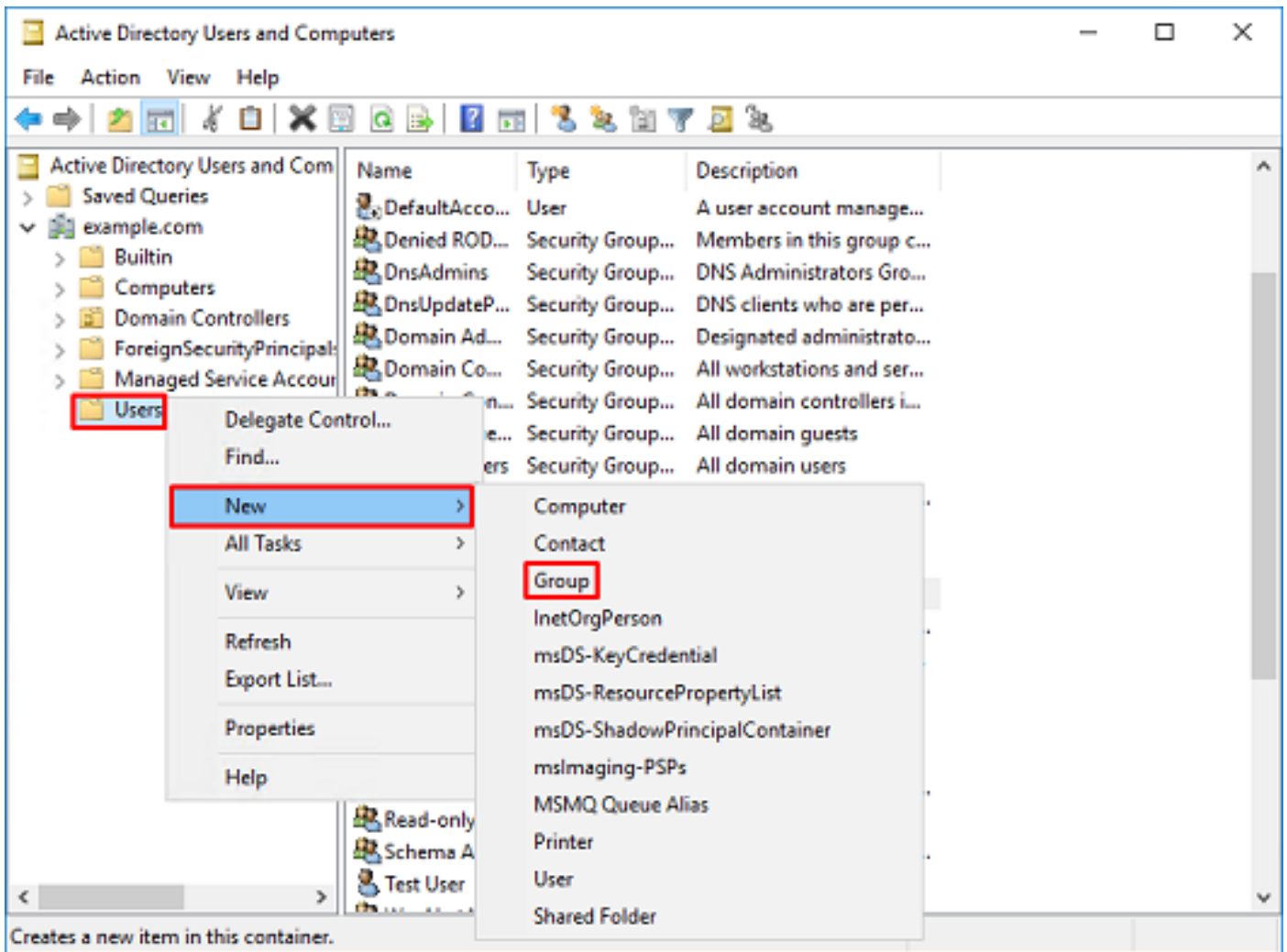
امهو، نبي فاضا نبي باسح عاشنا مت، كلذى لى افاضا لى ابو. FTD باسح عاشنا نم ققحت. 3.
رابخال المدختسمو تامول عمل اة نقت لوؤسم.



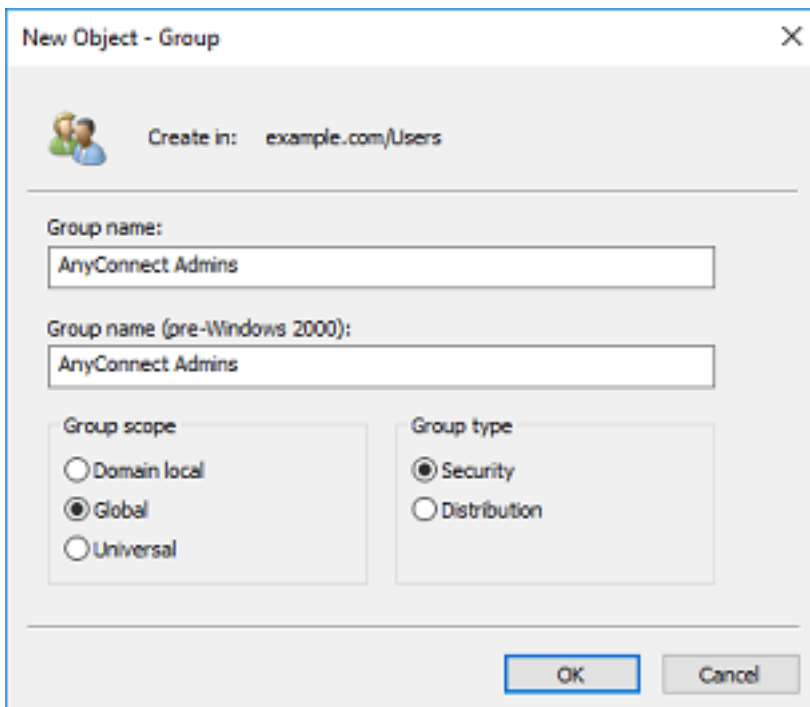
(يراي تخ) تانال ع تاعومجم ىلا ني مدختسم ةفاض او تانال ع تاعومجم عاشنا

قېب طت ليه ستل تاعومجم ل امدختس ا نكمي ، ةقداصلما ىل ا عجال مدع نم مغرلا ىلع و نيوكتلا ليلد ي ف LDAP ضيوفت ىل ا ةفاض ا ل ني مدختسم ةدع ىل لوصولا تاسايس ةيوه لال خ نم اقحال لوصولاب مكحتلا جهن تادادع ا قېب طتل تاعومجم ل امدختس ا متيس ، اذه ةفدم ل خاد مدختس ل ا.

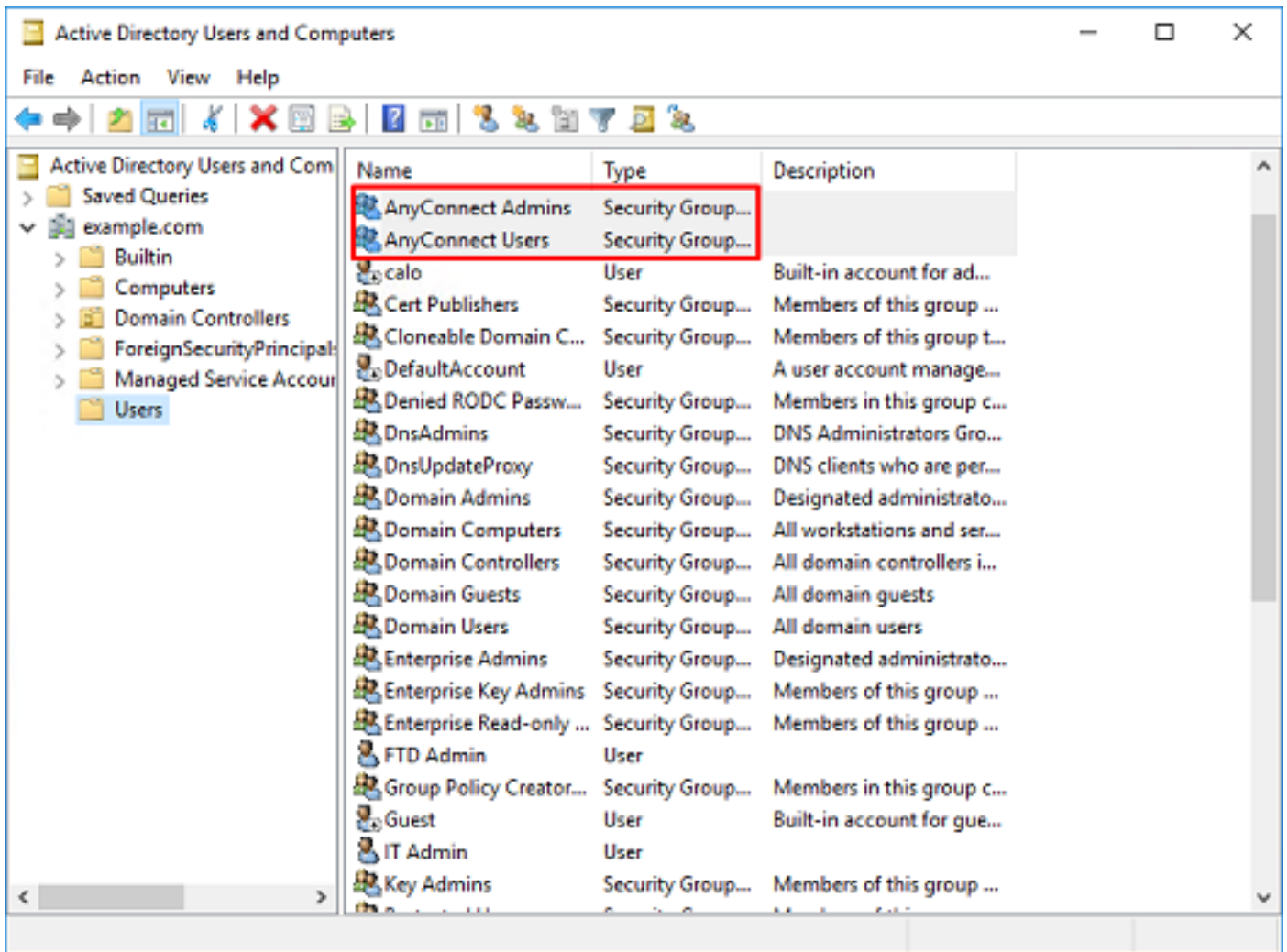
1. ةسسؤلما/ ةيواجال قوف نم ا ل سوام ل رزب رقنا ، **Active Directory Users and Computers** ي ف ا ل وؤسم ةفاض ا متتس ، ل ا ثم ا اذه ي ف . ا ه ل ا ةديجال ا عومجم ل ا ةفاض ا متتس ي ت ل ا قوف نم ا ل سوام ل رزب رقنا . ني مدختسم ةيواجال نم ض ا عومجم ل ا ي ف **AnyConnect** ةومجم > ديدج قوف رقنا م ت ، ني مدختس ل ا .



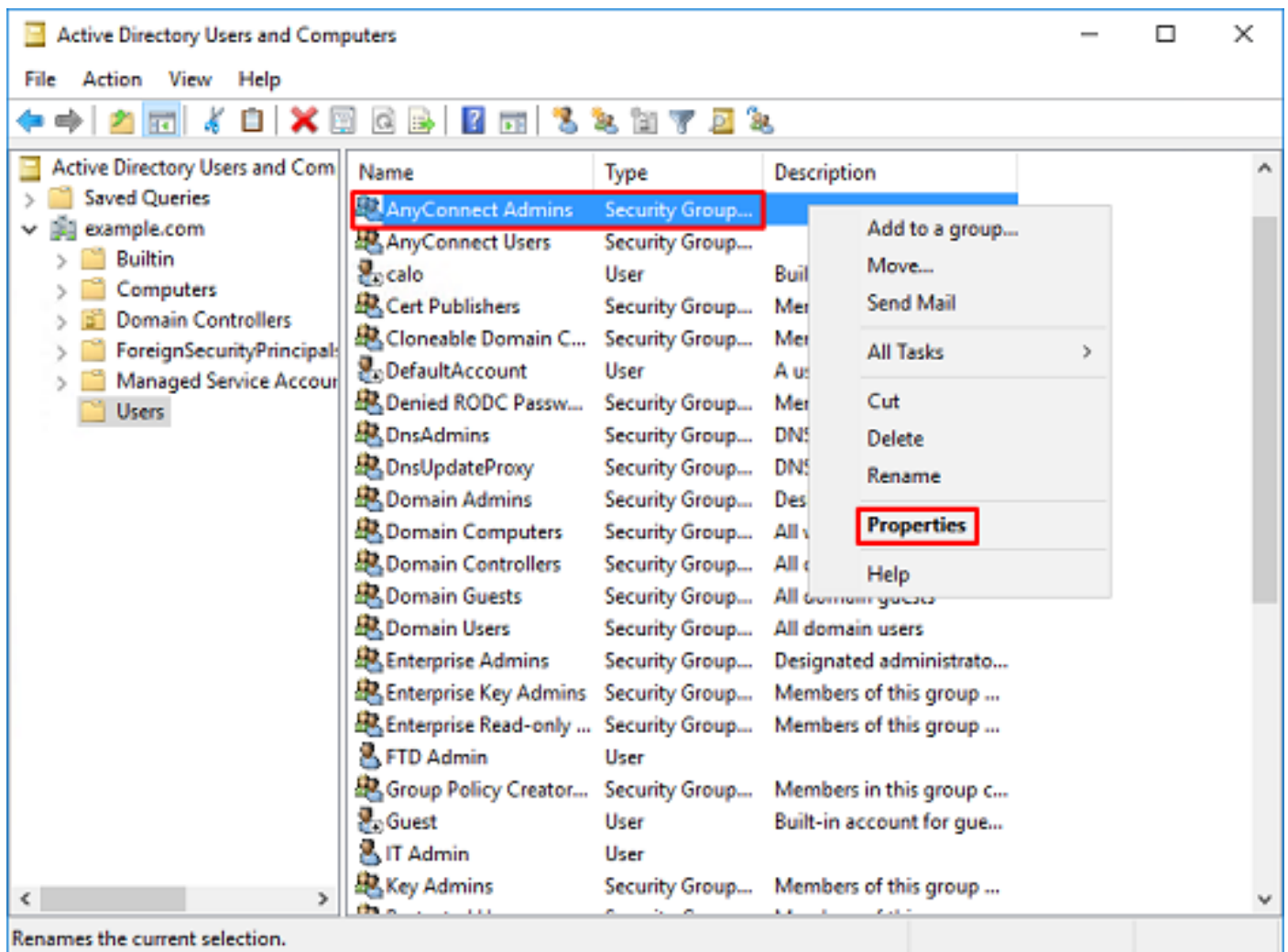
2. ةروصل الـي فـي حـضـومـهـ امـك ةومـجـمـالـا - ديـجـلـ نـئـاـكـالـ جـالـمـ لـالـخـ حـفـصـتـ.



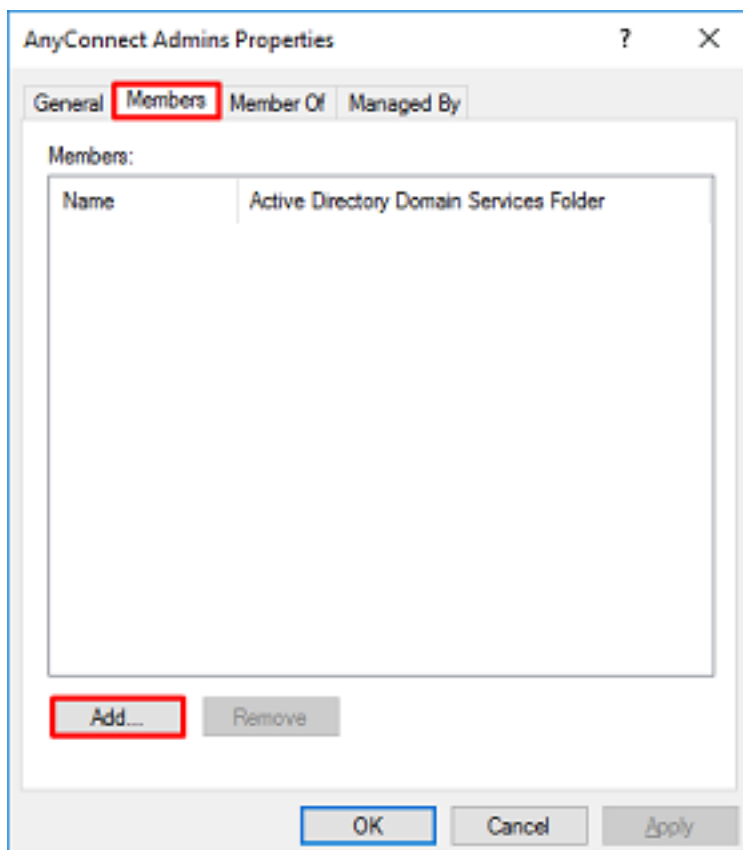
3. AnyConnect ةمـدخـتـسـم ةومـجـمـالـا ةاشـنـا ةـيـأـمـت . ةومـجـمـالـا ةاشـنـا نـمـ دـكـأتـ.



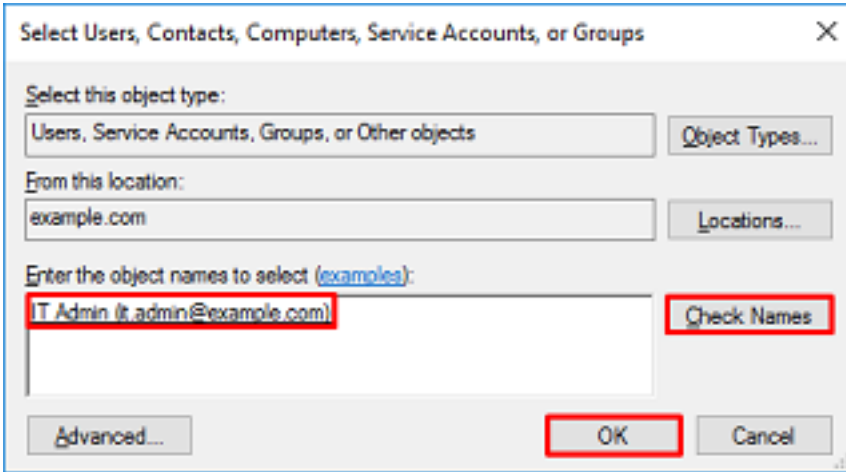
4. (نېم دځتسمال) م دځتسمال ؤفاضا م تېس ي تال ؤومجمال قوف ن مېال س وامل رزب رقنا .
 تامول عمل ؤېنقت لوؤسم ؤفاضا م تېس ، نېوكتال اذه ي ف . صئاصخ ددح م ت ، اهي ل
 ل م دځتسمال رابتخ م دځتسم ؤفاضا م تېس و AnyConnect Admins ؤومجمال ل م دځتسم ل
 ل م دځتسم AnyConnect ي م دځتسم ؤومجمال .



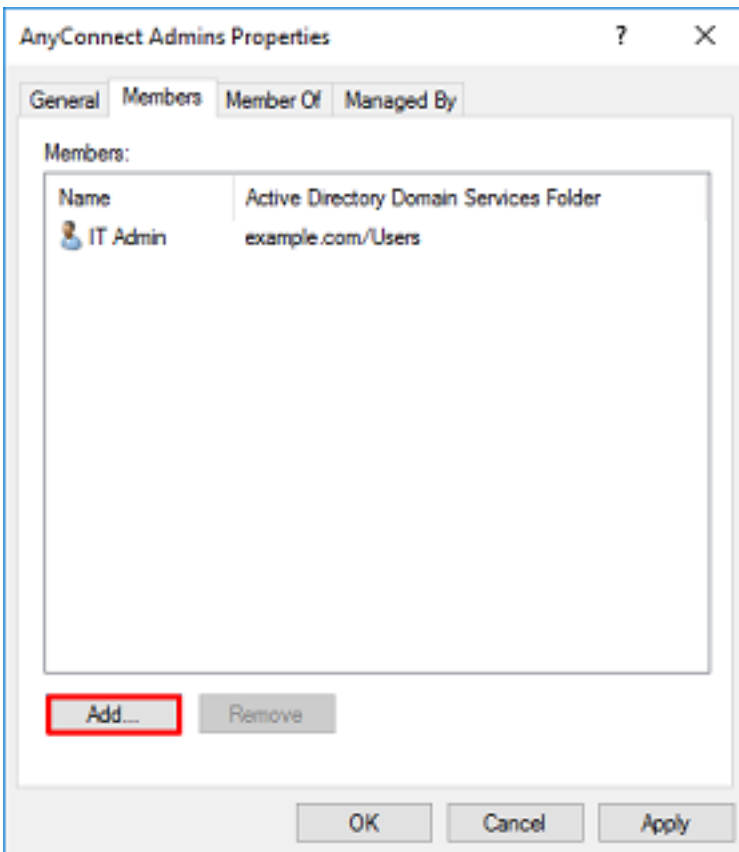
5. ةروصولا يف حضورم وه امك ةفاضل قوف رقنا م ءاضعأ بيوبتلا ةمالع قوف رقنا .



ىل ع روثعلا نم ققحتلل عامسألا نم ققحتلا رزلا قوف رقناو ل قحلا يف مدختسملا لخدأ
ت ققط، ققحتلا مت نإ ام .مدختسملا OK.

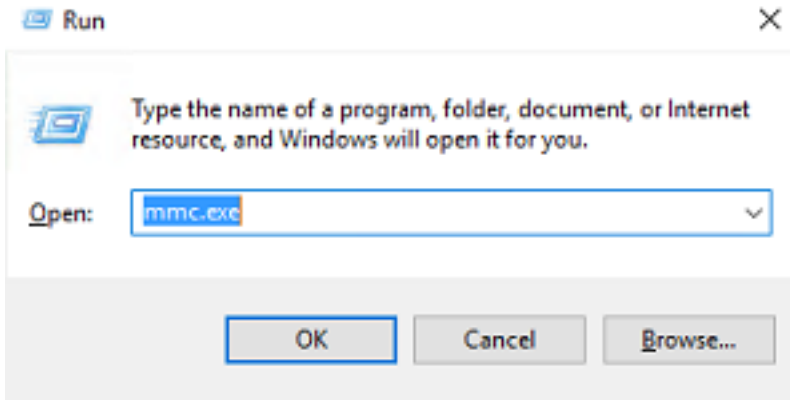


مدختسم" ةفاضلا مت امك .قف اوم رزلا قوف رقنا م ث ،حيحصلا مدختسملا ةفاضلا نم ققحت
اهسفن تاوطلخا مادختساب AnyConnect يف مدختسم ةومجم ىلا "مدختسملا رابتلخا

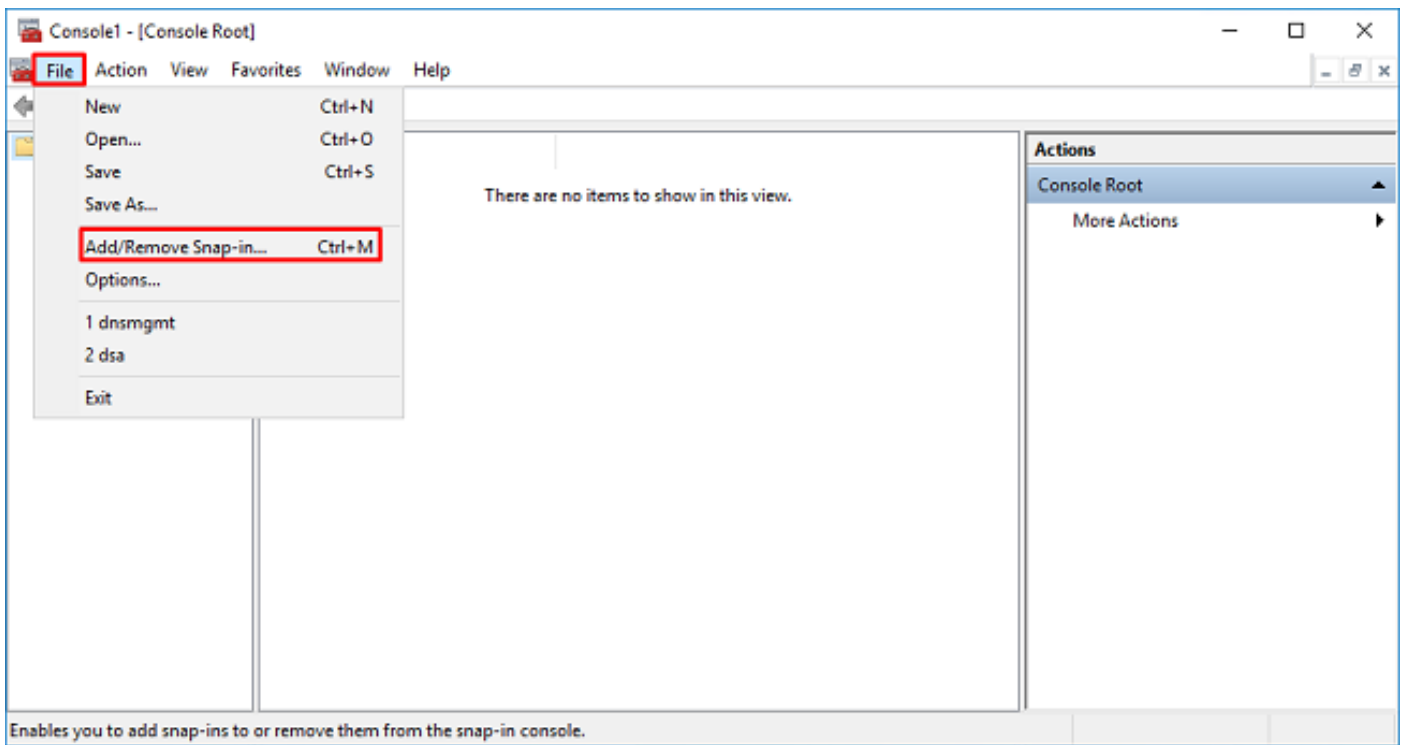


STARTTLS) و LDAPs ل طقف بولطم) LDAP ب صاخلا SSL ةداهش رذخ خسن

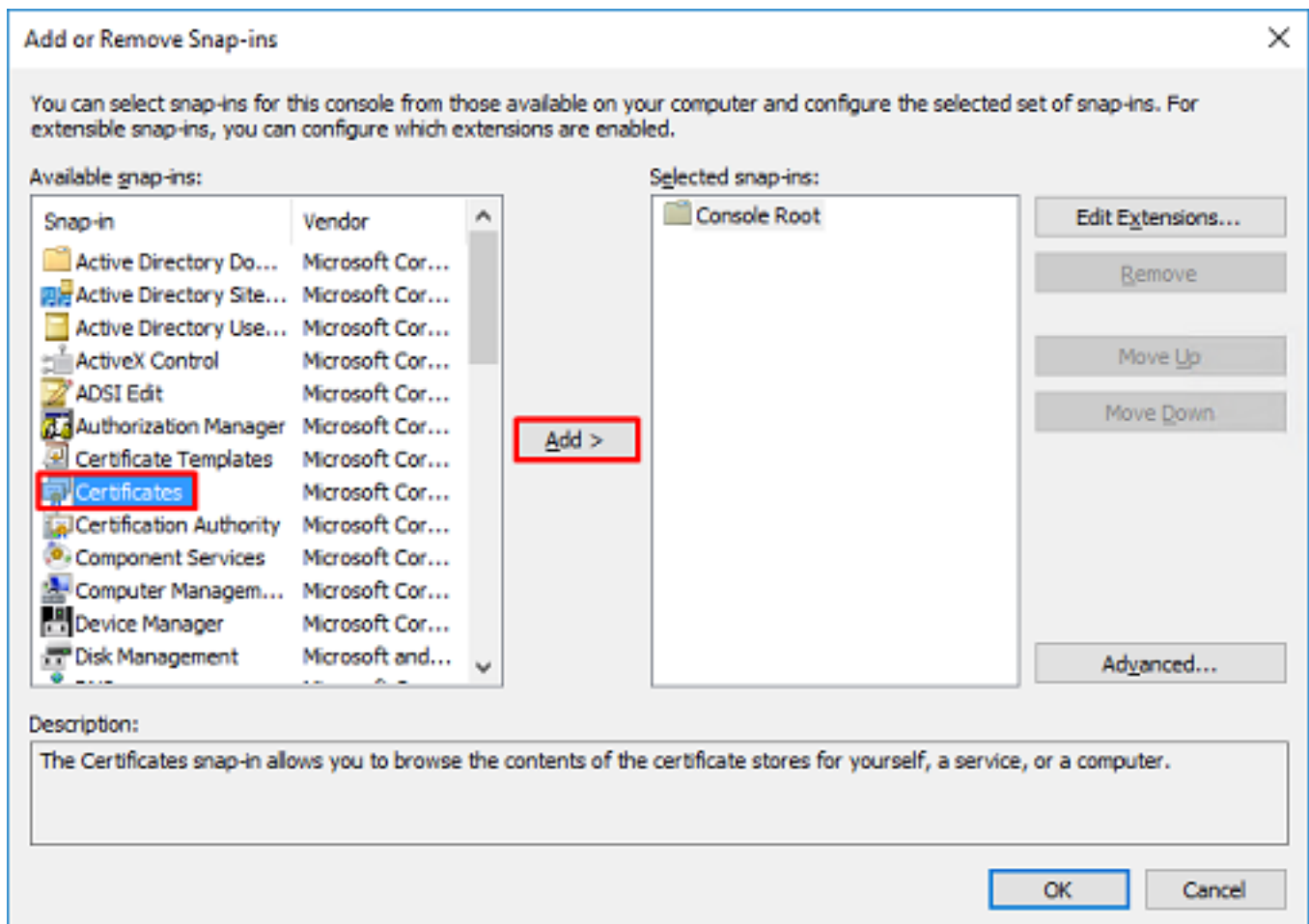
OK قوف رقناو .mmc.exe بتكاو Win+R ىل ع طغضا .1



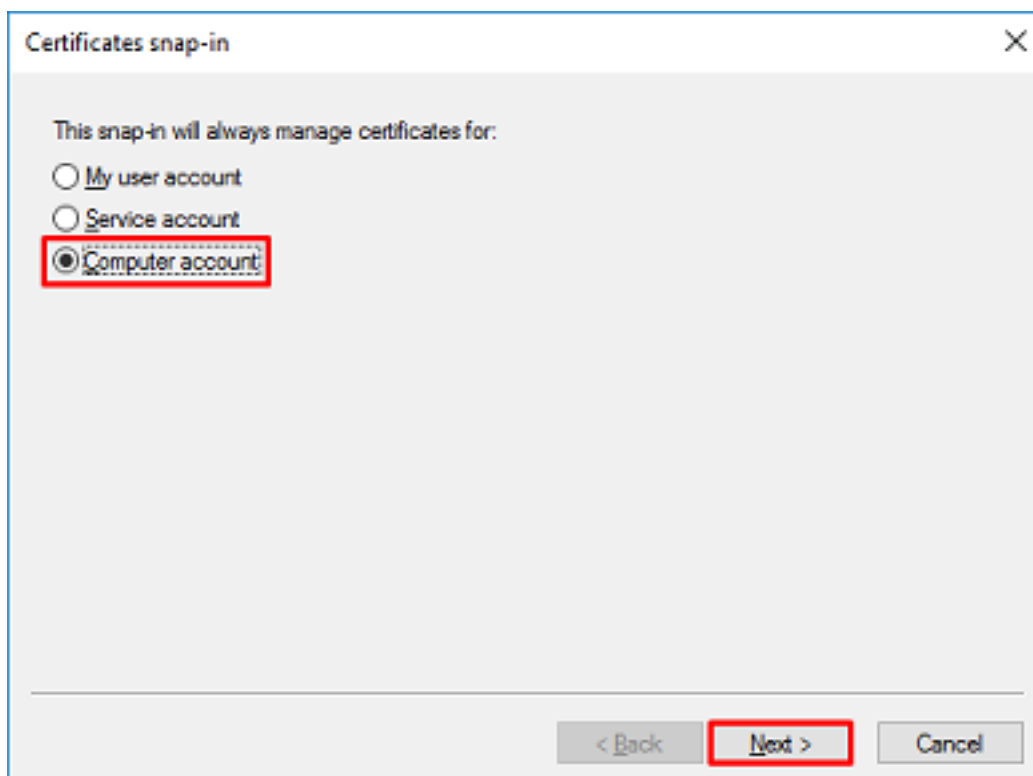
2. ةروصل الـي فـي حـضـوم وـه اـمـك ... ةـفـاضـالـا ةـأـدـالـا ةـلـازـم/ةـفـاضـالـا > فـلـم الـى لـقـتـنا .



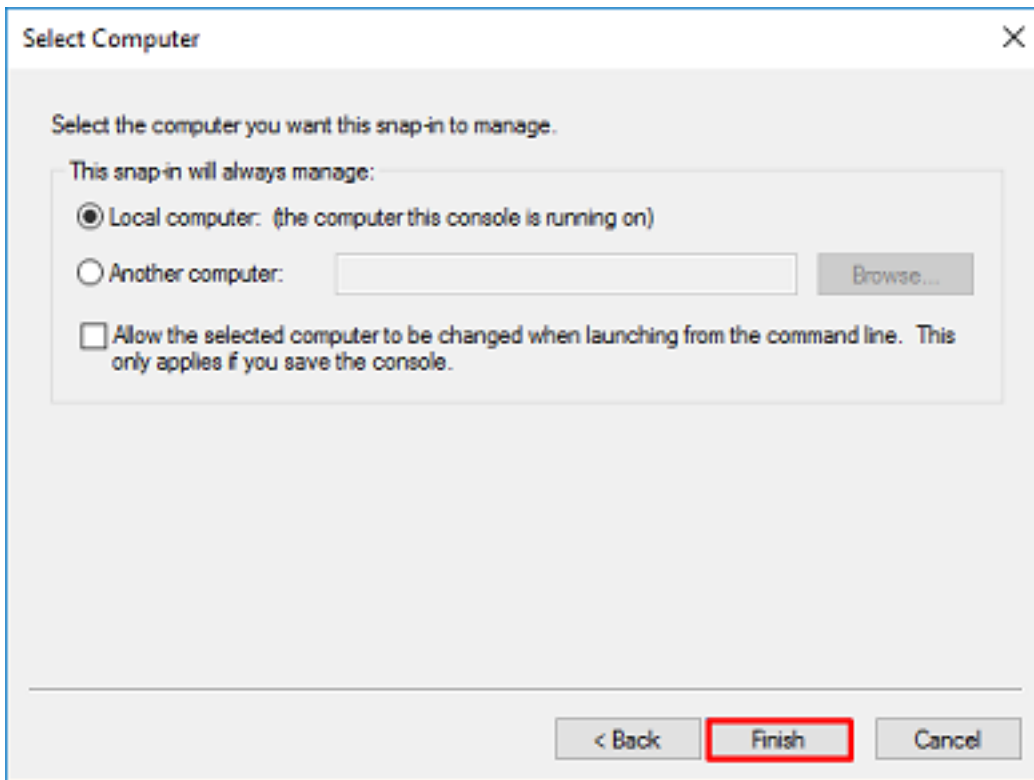
3. ةـفـاضـالـا قـوف رـقـنـا مـث ، تـأـدـاهـشـلـا قـوف رـقـنـا ، ةـحـاتـمـلـا ةـفـاضـالـا تـاـوـدـالـا تـحـت .



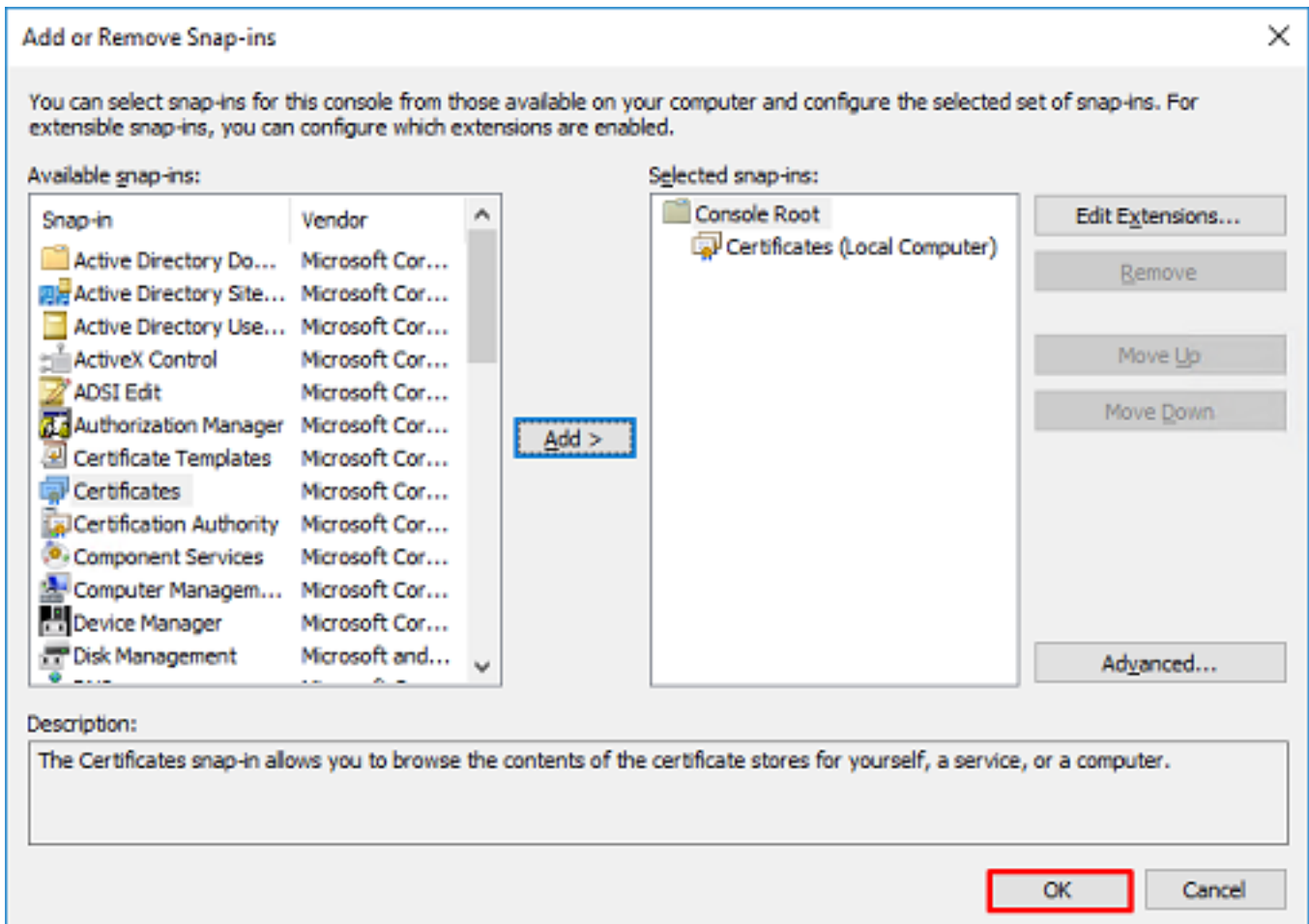
4. ةروصل ال ف حضورم وه امك يلاتل قوف رقنا م، رتوي بمكك ل باسح دح.



ءاهن| قوف رقنا



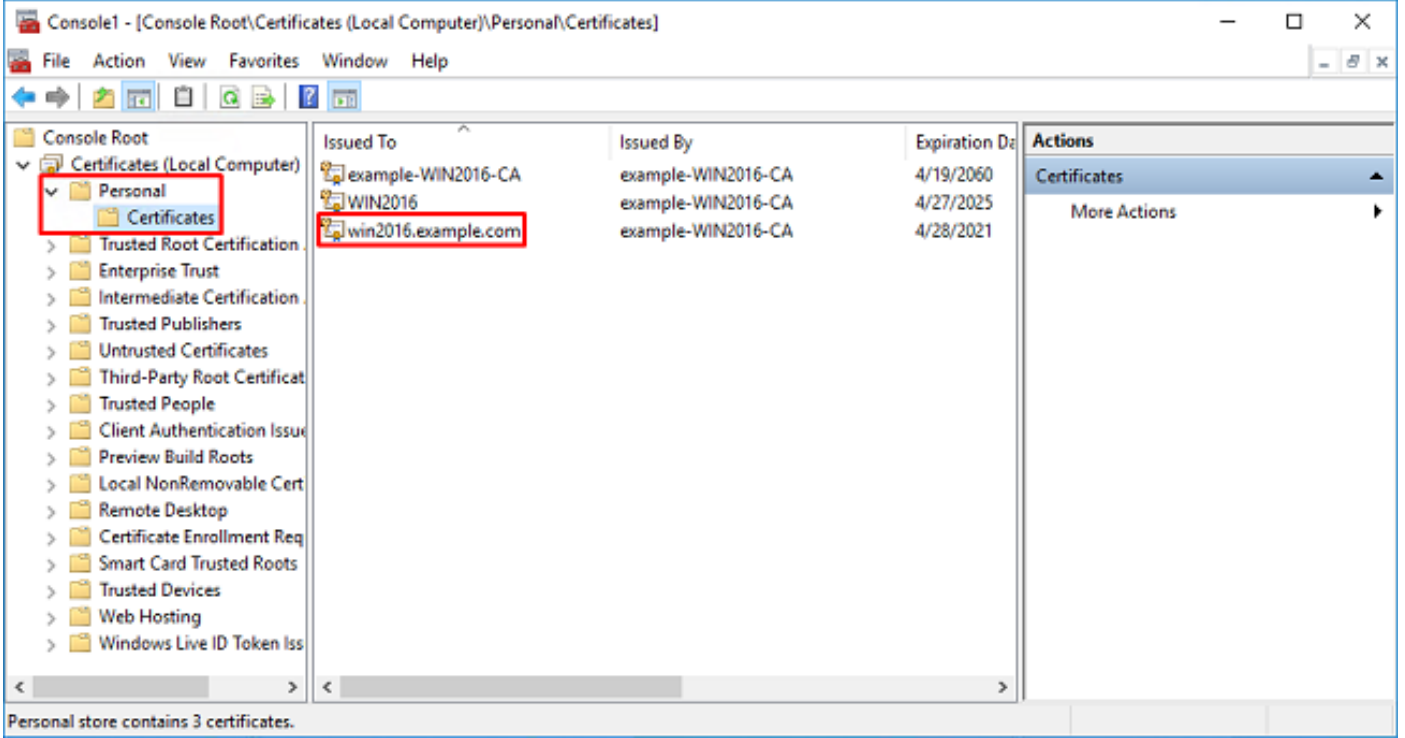
5. قوف رونا OK.



6. مدهتسملا ةداهشلا رادصا بجي .تاداهشلا قوف رونا مٲ ،ي صخشلا دلجملا عيسوتب مق 6. 3 دجوي . Windows مداخب صاخلا (FQDN) لمكلا ب لهؤملا لاجملا مسا لىا LDAPs لبق نم مداخلا اذه لىع ةجر دم تاداهش .

- WIN2016-CA لاثملاو ىلإ ةرداص ق دصم عجرم ةداهش .
- example-WIN2016-CA ةطساوب Win2016 لىغش تلالماظنل ةرداص ةيوه ةداهش .
- example-win2016-ca ةطساوب win2016.example.com ىلإ ةرداص ةيوه ةداهش .

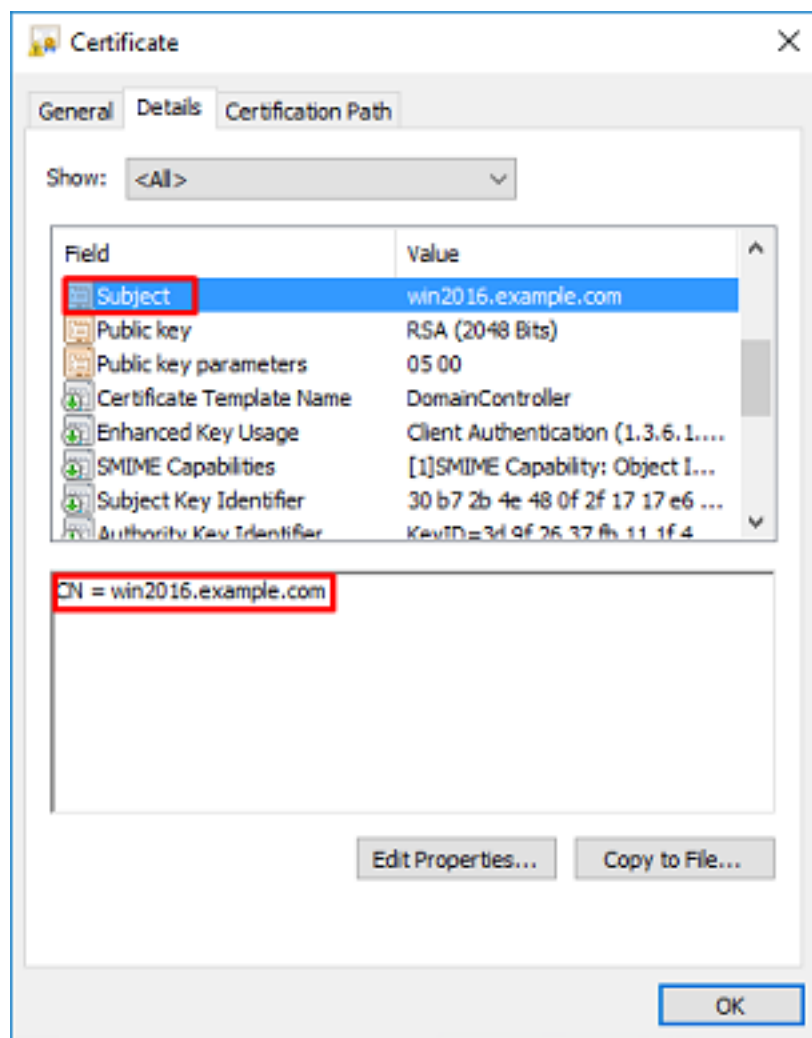
ىلوالا تاداهش للاف يلاتلابو ، win2016.example.com وه FQDN نوكي ، اذه نيوك تلال لىل دىف ىلإ اهرادص لمت ي تلال ةيوه ل ةداهش . LDAP SSL ةداهش ك مادختسالل ةحل اص رىغ ةيناثلاو ل ق دصم ل عجرم ل ةمدخ ةطساوب اىئاق لت اهرادص لمت ةداهش يه win2016.example.com لىصافتلال نم ققحتلل ةداهش لال لىع اجدزم ارقن رقنا . Windows Server .

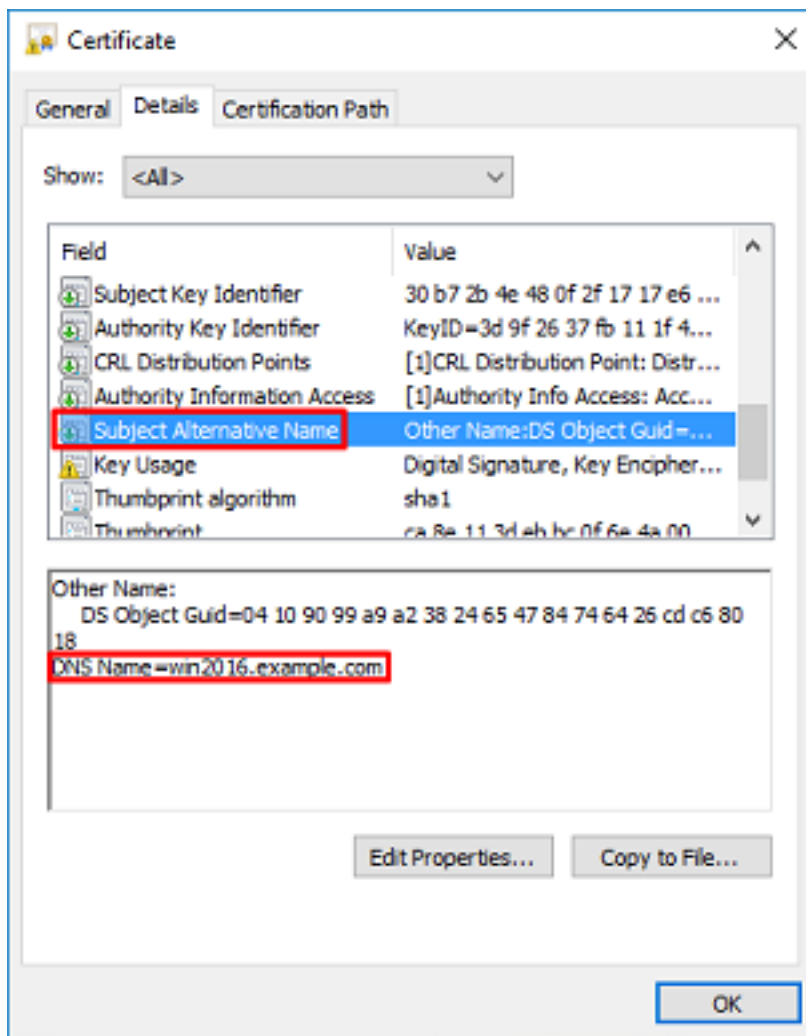


7. تابلطتملا هذه ةداهش للاف ي فوتست نأ بجي ، LDAPS ل SSL ةداهش ك اهم ادختسال ل جأ نم .

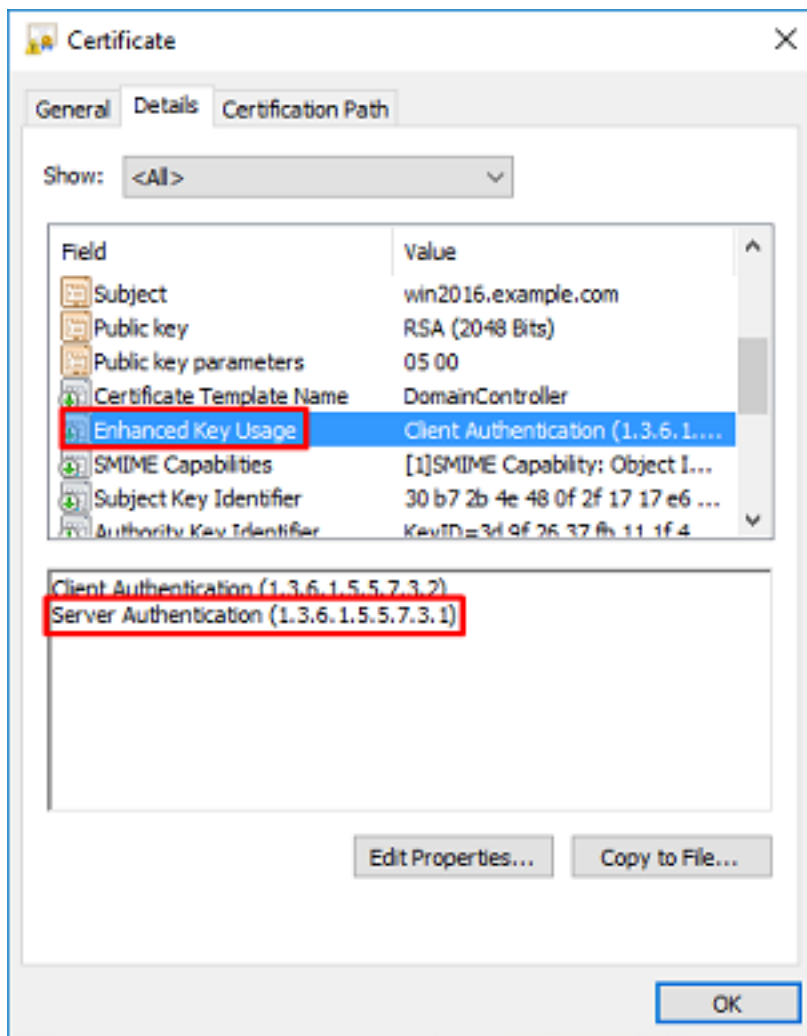
- Windows مداخل صاخلا FQDN عم DNS عوضوم لىدبلا مسالا وأ عئاشلا مسالا قباطتي .
- نسمحلا حاتفملا مادختسال ل قح نمض مداخل ةرداصم ىلع ةداهش للاف يوتحت .

نوكي ، لىدبلا عوضوم للاف عوضوم للاف يوتحت ، ةداهش للاف ي صافات بيوتتلال ةمالع تحت ادوجوم FQDN win2016.example.com .

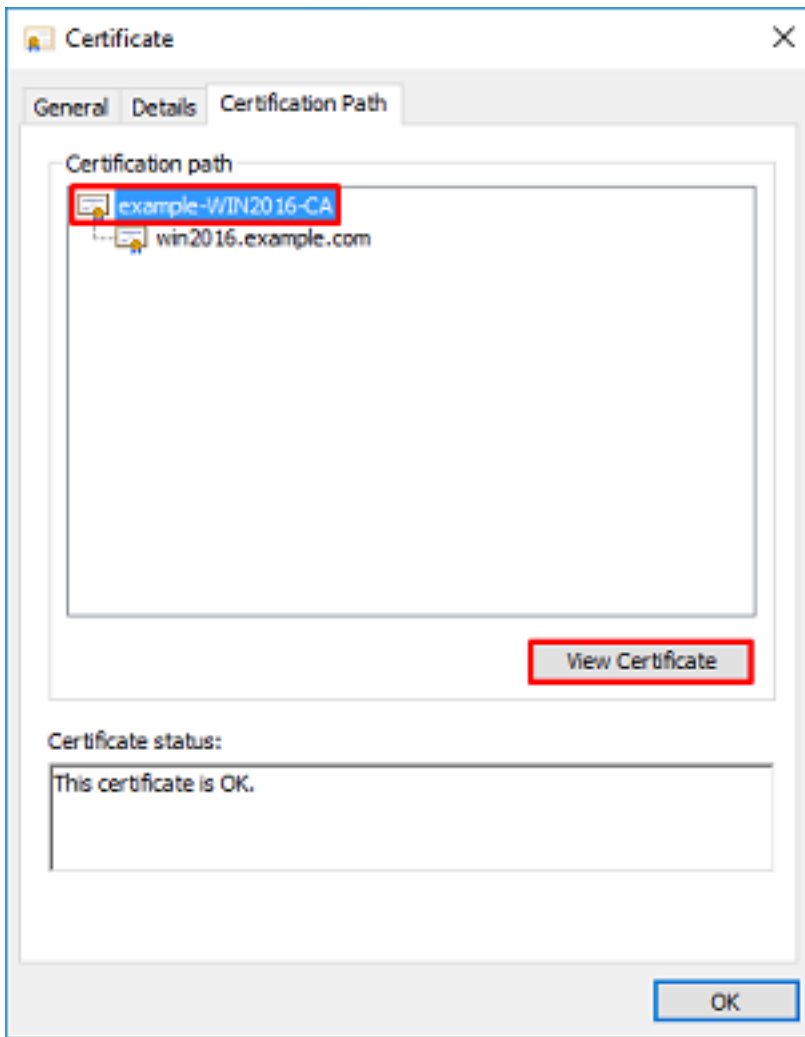




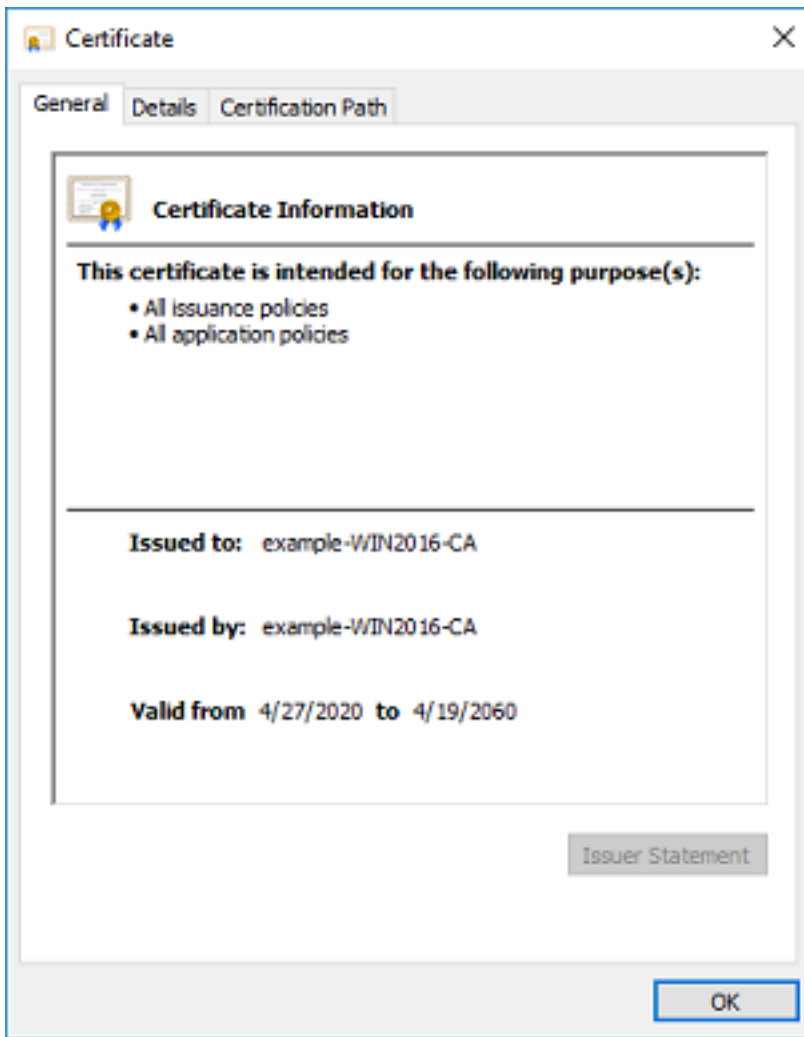
مداخله قداصم دجوت، حيت افملل نس حمل م ادخت سال تحت



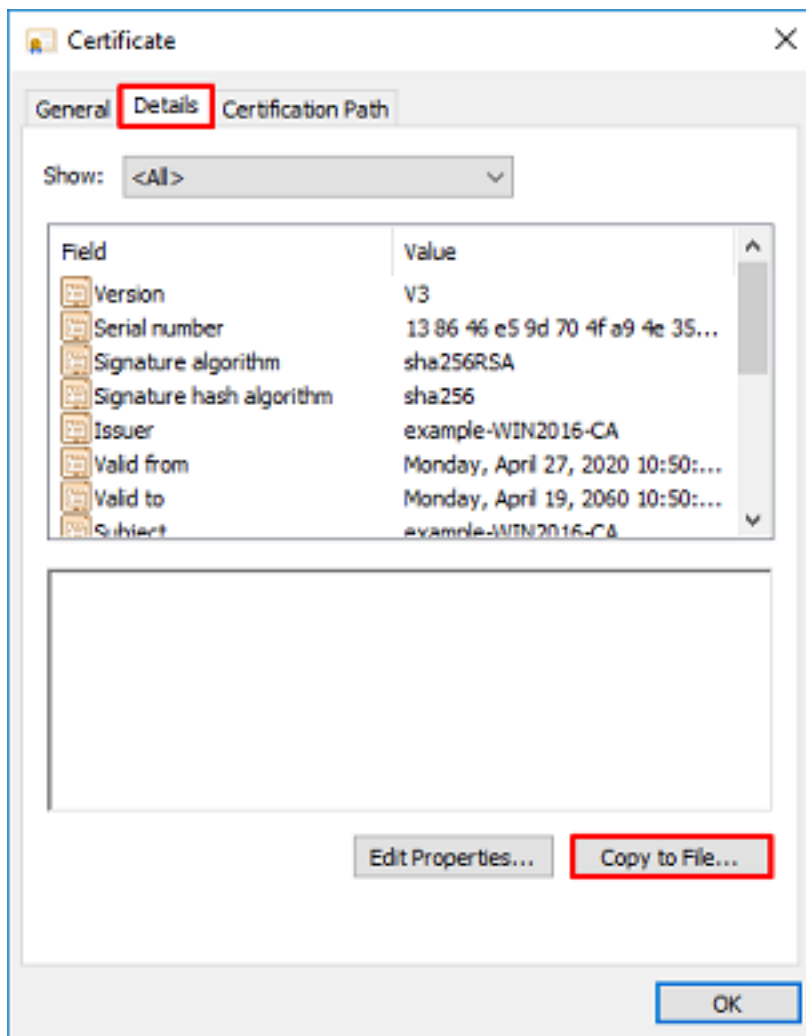
8. **داهشلا قوف رقنا . دامتعالا راسم بيوبتلا عمالع** يلى لقتنا ، كلذ نم دكأتلا درجم ب .
داهشلا ضرع رز يلع رقنا م ، رذجال قدصملا عجرملا داهش نوكت نا بجي يتلا ايلعلا



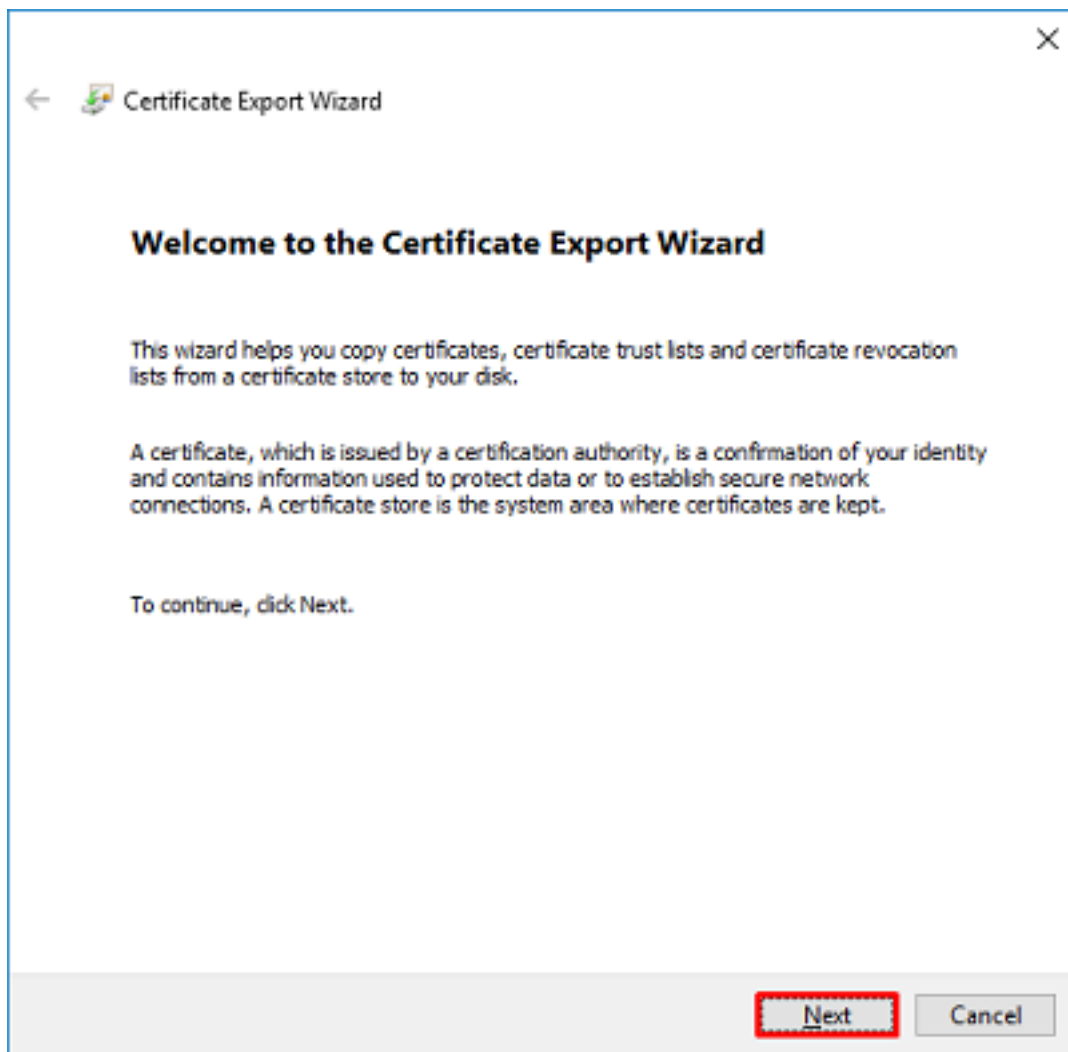
9. رذجلال قدصملا عجرملا ةداهشل ةداهشلا لىصافت حتف ىلإ كلذ يدؤيس.



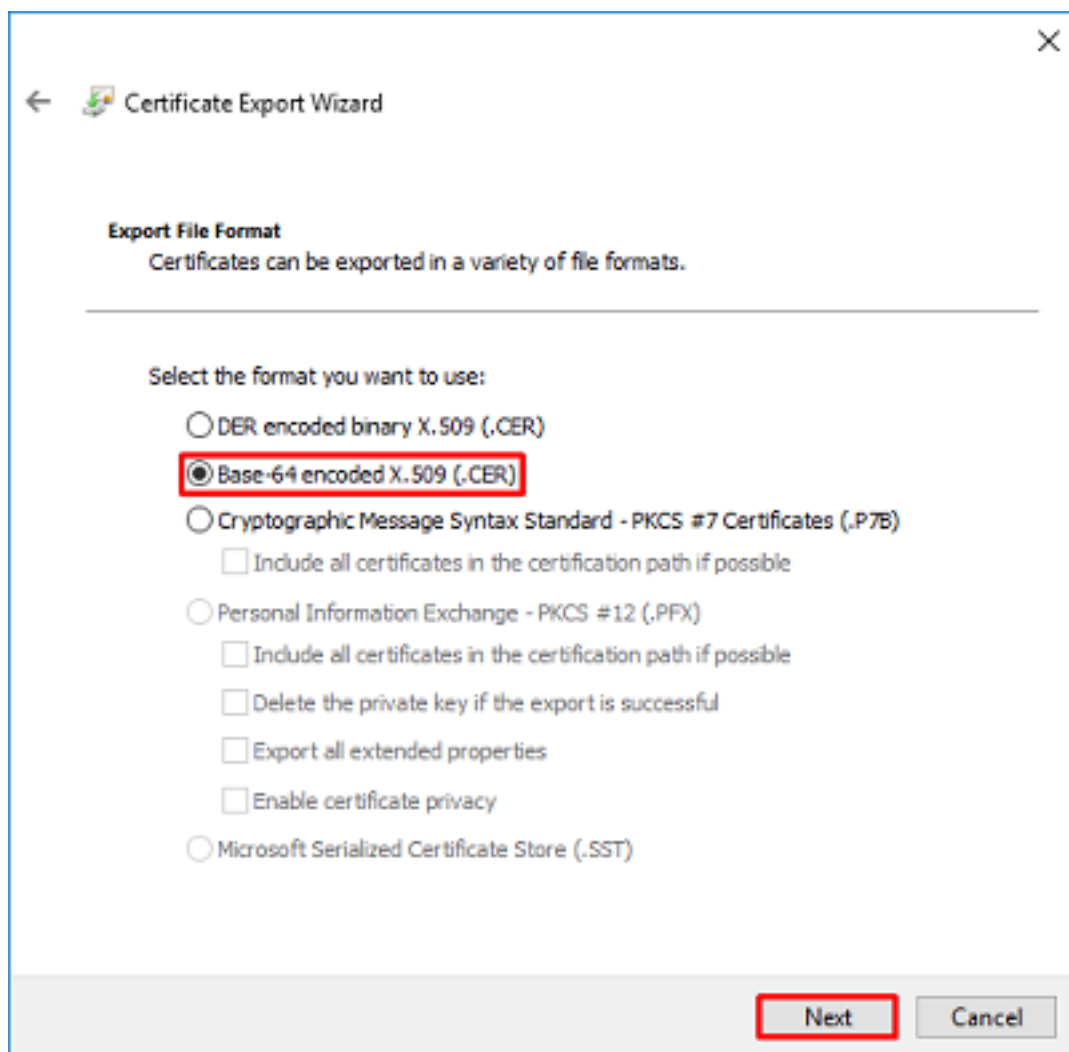
10. يف حضورم وه امك... فلم ىلإ خسن قوف رقنا م ث لي صافات بي وبت الة مالع حت فا. ةروص الة.



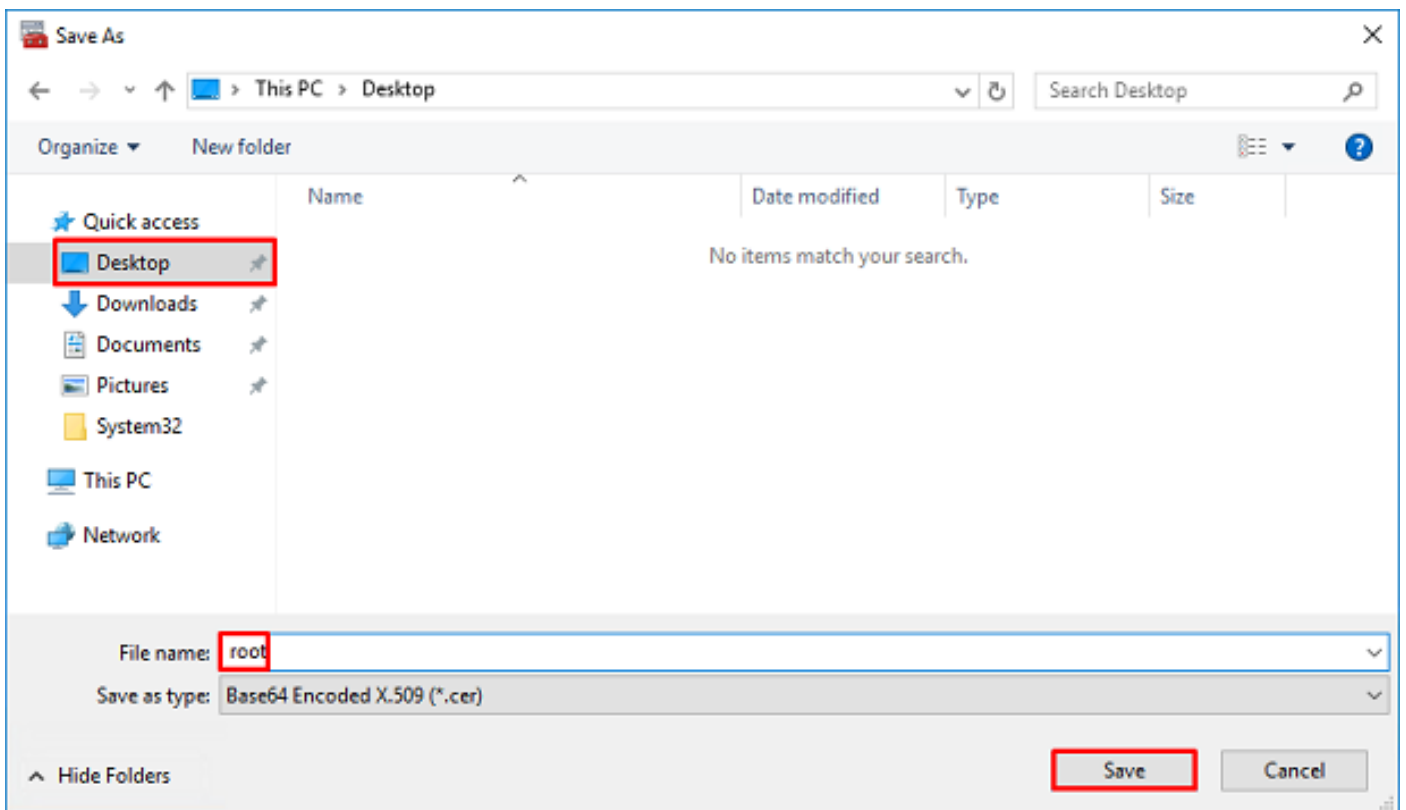
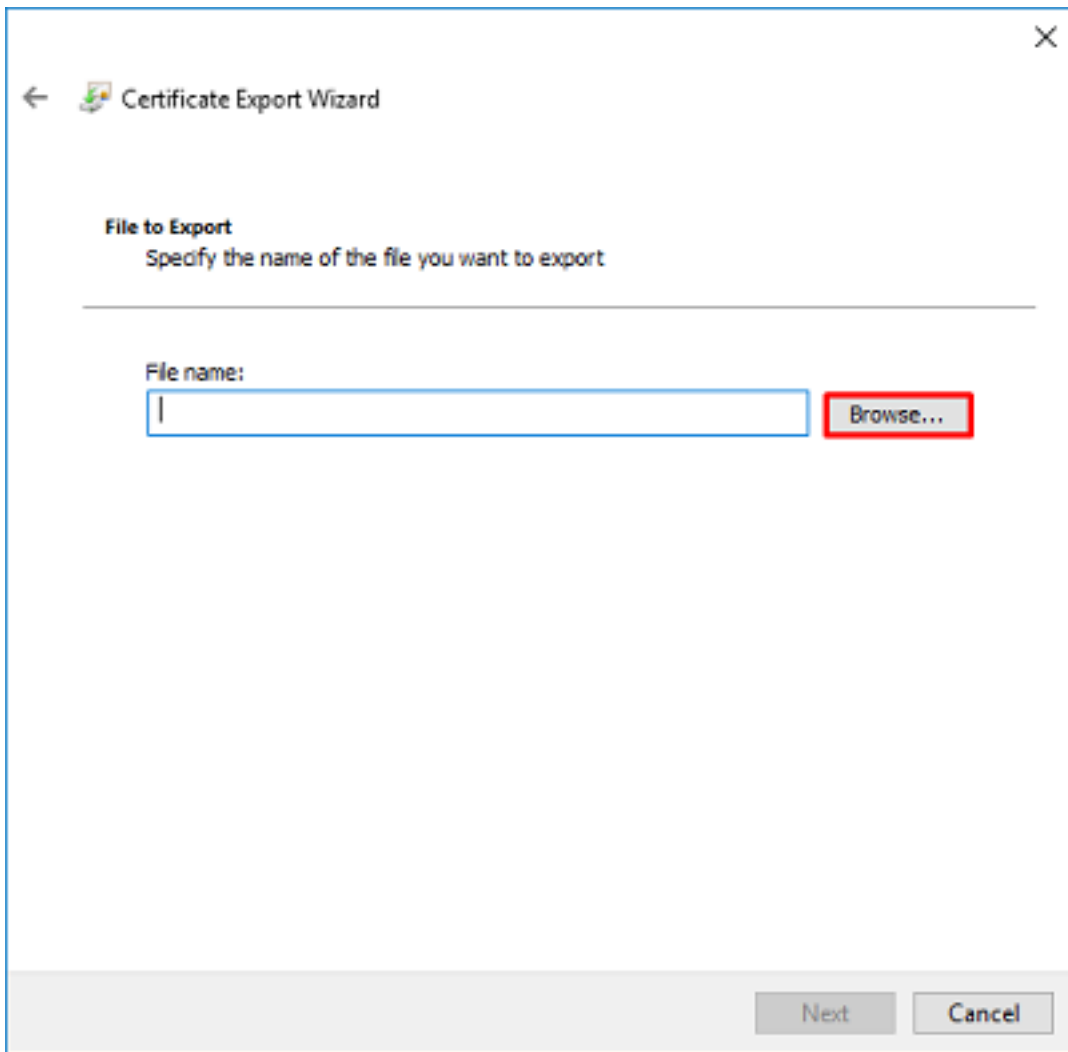
11. PEM قيسنتب رذجال قدصم لاجرم لادصي سيذلا تاداهش لادصت جالع م ربع لقتنا .

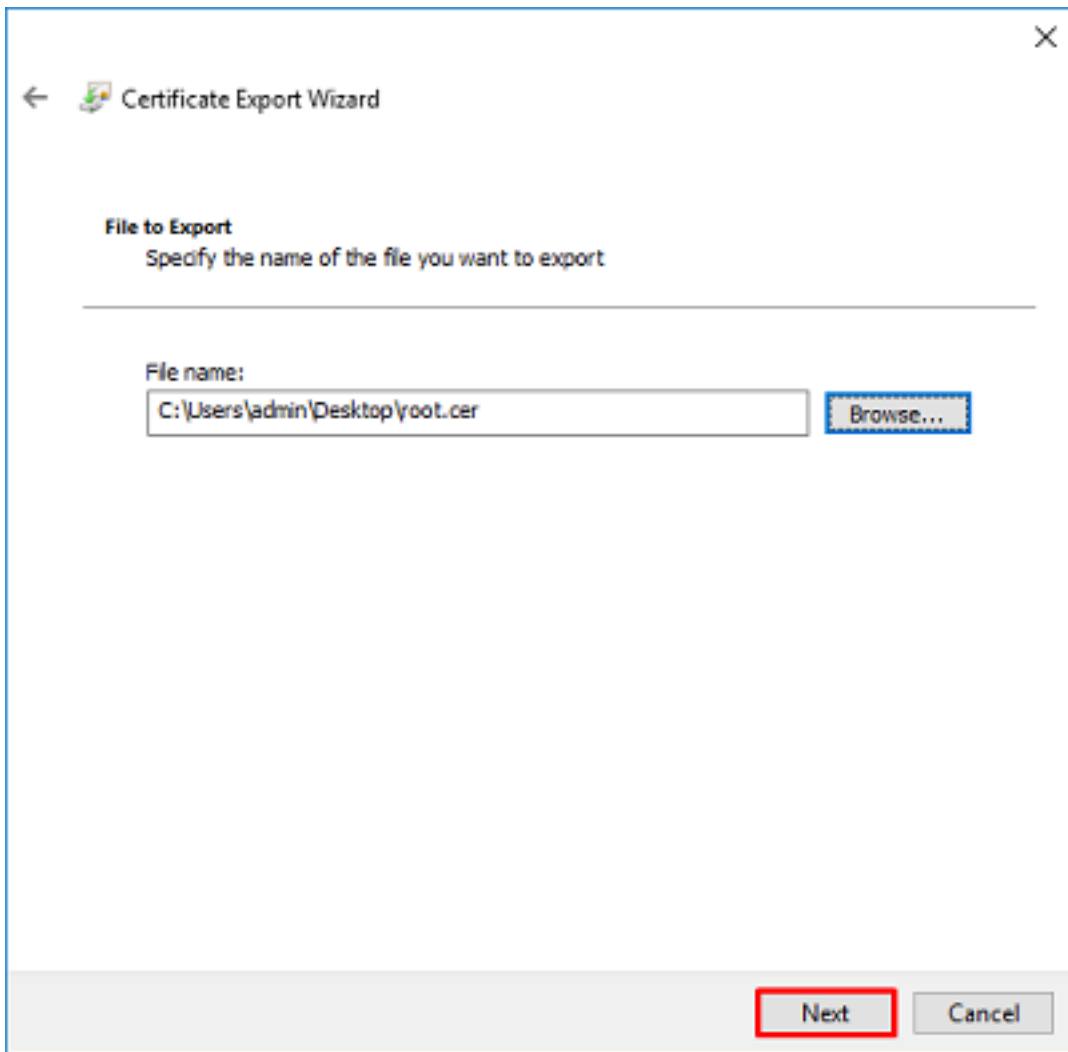


12. زمزم ل Base-64 ددح X.509.

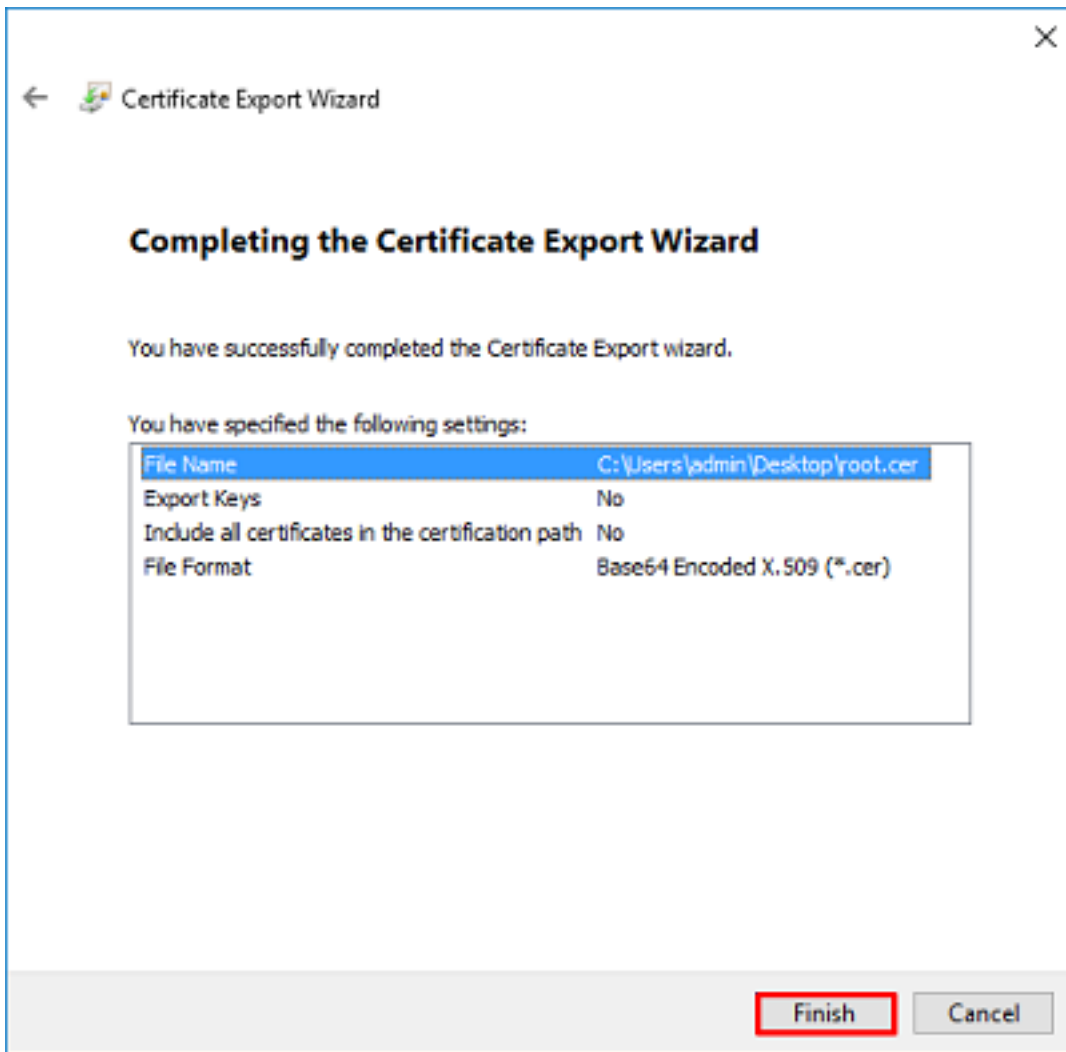


13. هـ ل هـ رـ د ص ت م تـ ي س نـ ي أ و ف ل م ل ا م س ا د د ح .





14. ماهن قوف رقنا .



رهظيس .رخآ صوصن ررحم يأ وأ ةركفم مادختساب ةداهشلا حتفاو عقوملا ىلإ لقتنا ،نآلاو .15 قحالح تقول اذه ظفاح . PEM قيسنتب ةداهش اذه

```

-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBqkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeXleGFtcmVudDQwMTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YXN1eDQw
ASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbADO6zMHbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----

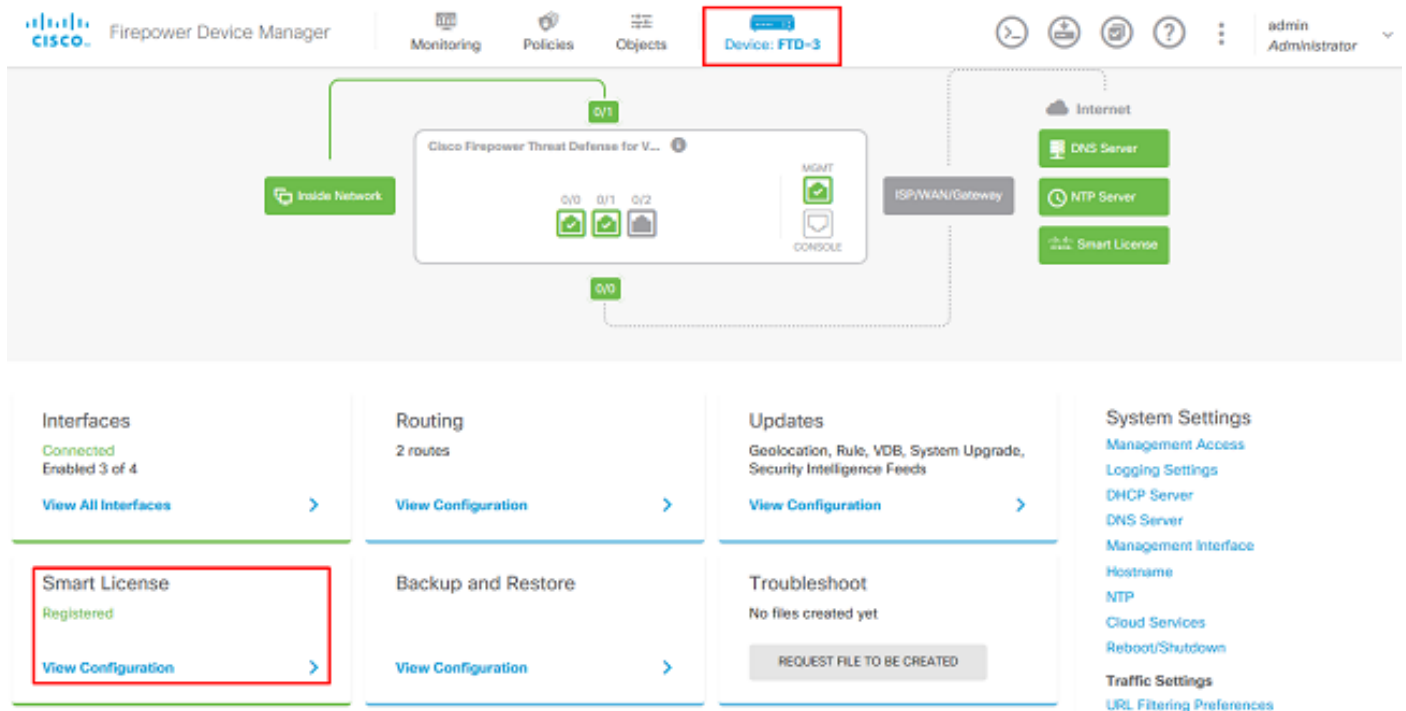
```

FDM تانويكت

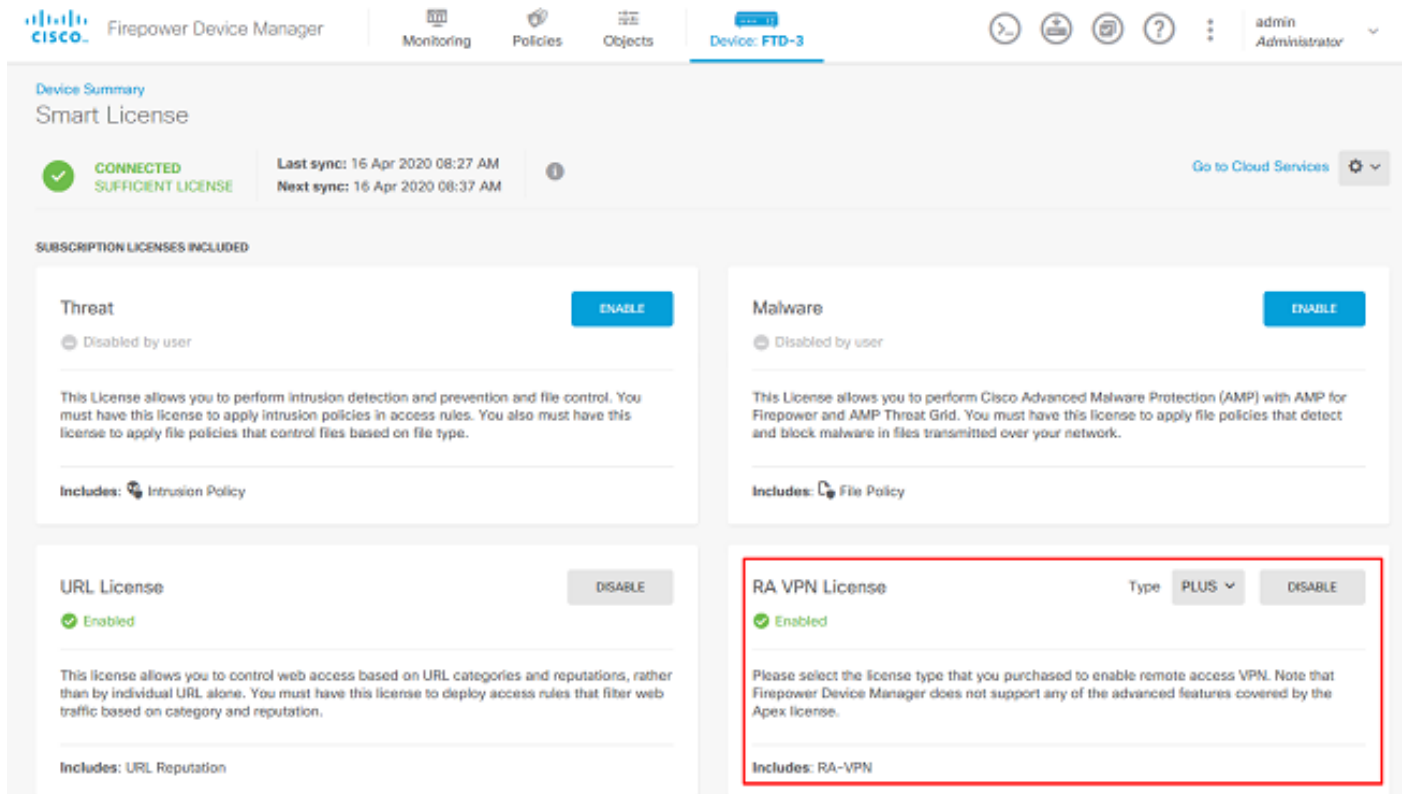
صخرتلا نم قححتلا

بجيو ويكذل صيخرتللا مداخل عم ليجستللا لىل فTD اجاتحيس ، فDM لىل AnyConnect نيوكتل زاهلال لىل عطق حل اص VPN و Apex و Plus صيخرت قيبطت

1. ةروصلال يف حضورم وه امك يكذل صيخرتللا > زاهلال لىل لقتنا .



2. و AnyConnect Plus صيخرت نيكم نم ويكذل صيخرتللا مداخل لىل فTD ليجست نم ققحت .



تانالعال ةيوه ردصم دادع

1. يف حضورم وه امك AD ددحو زمرلا + قوف رقنا م، ةيوهلال رداصم > تانئاكل لىل لقتنا .

ةروصل

The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects' (highlighted with a red box), and 'Device: FTD-3'. The left sidebar lists various object types, with 'Identity Sources' highlighted. The main content area is titled 'Identity Sources' and shows a table with one object: 'LocalIdentitySource' of type 'LOCAL'. A dropdown menu is open, showing options: 'RADIUS Server', 'RADIUS Server Group', 'AD' (highlighted with a red box), and 'Identity Services Engine'.

2. تقويف اهعيمجت مت يتل تامولعملاب Active Directory مداخل ةبسانملا تادادعإلألما. نم دكأتف، IP ناونع نم ال دب Microsoft مداخل (FQDN) فيضملا مسا مادختسا مت اذإ. قباس هذه ةعومجم قيبتب مق م. DNS ةعومجم قيبطت، DNS مداخل > ماظنلا تادادعإ > زاوجلإ لإ لاقتنالاب FTD لىع ةهجاو تحت DNS ةعومجم قيبتب، DNS مداخل > ماظنلا تادادعإ > زاوجلإ لإ لاقتنالاب FTD لىع رز قوف رقنا. DNS تامالعتسال ةبسانملا جورخلا ةهجاو ددح م، تانايللا ةهجاو ةرادإلا هذه نأ امب. FTD ةرادإ ةهجاو نم لوصولا ةيناكماو نيوكتل حاجن نم ققحتلل رابتخالإ يتللا هيجوتلل ةلباقلا تاهجاو لإ دحل لإ لىع نم سيلو FTD ةرادإ ةهجاو نم اهؤدب متي تارابتخالإ نمضي ال (لشافلا وأ) حجانلا لاصتالإناف، (DMZ، جراخلا، لخدلا لثم) FTD لىع اهنيوكت مت AnyConnect ةقداصم تابلط ادب متيس هنأل ارظن AnyConnect ةقداصم ل ةجيتنللسفن LDAP تالاصتإ رابتخالإ لوح تامولعملال نم ديزمل. هيجوتلل ةلباقلا FTD تاهجاو دحل نم LDAP. اهالصلإو عاطخالإ فاشكتسا ةقطنم في Packet Capture و Test AAA مسق عجار، FTD نم

Add Identity Realm



! Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name

LAB-AD

Type

Active Directory (AD)

Directory Username

ftd.admin@example.com

e.g. user@example.com

Directory Password

••••••••

Base DN

DC=example,DC=com

e.g. ou=user, dc=example, dc=com

AD Primary Domain

example.com

e.g. example.com

Directory Server Configuration

win2016.example.com:389

Hostname / IP Address

win2016.example.com

e.g. ad.example.com

Port

389

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

✓ Connection to realm is successful

[Add another configuration](#)

CANCEL

OK

قوتوم ال CA ةداهش ددح م ث بسانم لاري فشت لاددح، STARTTLS و LDAP مادختس اءلاحي ف قءصم عءرم ةداهش ءاشن اءل ع رقا، لءف ل اء رءال قءصم ل عءرم ل ةفاضا م ت مل اذا. اءب قءصم ل عءرم ل ةداهش قءصم ل م ث رءال قءصم ل عءرم ل ةداهش ل مسا رءفوت ب مق. ةءءء قءصم ل اءب اس اء عءمء م ت ل PEM قءصم ل رءال

Add Trusted CA Certificate



Name

LDAPS_ROOT

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

-----BEGIN CERTIFICATE-----

```
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGFtcG9uLmV4YW11bWVudC5kZS5kZS5kZS5kZS5kZS5k
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW11bWVudC5kZS5kZS5k
ASwDQYJKoZIhvcNAQEFBQADQgEPADCCAQoCggEFRAI8chT719NzS0ncOPh0YT67h
```

CANCEL

OK

Directory Server Configuration

win2016.example.com:636

Hostname / IP Address

win2016.example.com

e.g. ad.example.com

Port

636

Encryption

LDAPS

Trusted CA certificate

LDAPS_ROOT

TEST

✓ Connection to realm is successful

مقيال هذه مادختسا مت، نيوكتلا اذه في:

- ماسالا: Lab-ad
- لي لدلا مدختسم مسا: ftd.admin@example.com
- ةيساسالا DN ةكباش: DC=example,DC=com
- نالعالاب صاخلا يساسالا لاجملا: example.com
- ناونع/فضملا مسا IP: win2016.example.com
- ذفنملا: 389

3. ةروصلا في حضوم وه امك ني ميالا لعلأ في ةقولعملل تاريخيغلتل رزرقنا.

Object Types

- Networks
- Ports
- Security Zones
- Application Filters

Identity Sources

2 objects

#	NAME	TYPE	VALUE	ACTIONS
1	LocalIdentitySource	LOCAL		
2	LAB-AD	AD	win2016.example.com	

4. نآلآ رشن رزلا قوف رقنا.

Pending Changes

✓ Last Deployment Completed Successfully
01 May 2020 12:54 PM. [See Deployment History](#)

Deployed Version (01 May 2020 12:54 PM)	Pending Version
	LEGEND Removed Added Edited
+ Active Directory Realm Added: LAB-AD	
	<pre>dirPassword.masked: false dirPassword.encryptedString: *** directoryConfigurations[0].port: 389 directoryConfigurations[0].hostname: win2016.example.com directoryConfigurations[0].encryptionProtocol: NONE adPrimaryDomain: example.com dirUsername: ftd.admin@example.com baseDN: DC=example,DC=com enabled: true realmId: 9 name: LAB-AD</pre>

MORE ACTIONS CANCEL DEPLOY NOW

AD ةقداصلم ل AnyConnect نيوكت

AnyConnect نيوكت لىل عهقيبطت بجي، هنيوكت مت يذلا AD ةي وه ردصم مادختسال

1. ةروصلال ي ف حضورم وه امك Remote Access VPN > زاغ لىل لقتنا.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

0/0

Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Device Administration Audit Events, Deployment History, Download Configuration View Configuration
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Configured 1 connection 2 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	

2. ةروصلال ي ف حضورم وه امك لاصتا فيرعت فلم عاشن| وأ + رز رقنا.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
<p>There are no Remote Access Connections yet. Start by creating the first Connection.</p> <p>CREATE CONNECTION PROFILE</p>				

3. مق اقبسم هؤاشنإ مت يذلا AD ةيوه ردصم ددح ،"للمعمل نيوكتولاصتال" مسق تحت 3. نبيعتولاصتال فيرت فلم مسلك لذي في امب يرخال ماسق لال بسانم لميقل دادع اب اعاهتال دنع مالعستال لاسرل قوف رونا .اعالمعل نيوانع عمجت

Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

General

Group Alias

General

Group URL

Add Group Alias

Add Group URL

Primary Identity Source

Authentication Type

AAA Only Client Certificate Only AAA and Client Certificate

Primary Identity Source for User Authentication

Filter

LocalIdentitySource

LAB-AD

Special-Identities-Realm

Create new

Fallback Local Identity Source ⚠

Please Select Local Identity Source

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



AnyConnect-Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

SUBMIT QUERY

4. يضاف لك ش ب. بس ان مل اة و م جم لا جهن دح، دع ب نع مدخت س مل اة ب رج ت مس ق تحت 4.،
ة. فل تخم ة سايس اشن ان كم ي، كلذ عم و، **DfltGrpPolicy** مادخت سا متيس

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER		Edit
DNS Server	None	
Banner Text for Authenticated Clients	None	
SESSION SETTINGS		
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes	
Idle Time / Alert Interval	30 / 1 Minutes	
Simultaneous Login per User	3	
SPLIT TUNNELING		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
ANYCONNECT CLIENT		
AnyConnect Client Profiles	None	

BACK

SUBMIT QUERY

5. AnyConnect مزج و، ةجراخ ل ةه جاول او، SSL ةداهش دح، لقأل ىل، ةماع ل تاداع ل مسق نمض. ةيضا رتفا ايتاذ ةعقوم ةداهش ديدحت نكمي، اقباس ةداهش ءاشن ا متي مل اذا باع ل بجي. اهب قووم ريغ مداخ ةداهش ةلاس رهظتس ل احي ا ىل (DefaultInternalCertificate) اري فشت ك ف مت يت ل رورم ل ةكر ل يف اف ل ل ل و صول اب مكحت ل ةسايس ديدحت نكمي. اقح ال ذي فنن ل ل زيح مدختس م ل ةيوه ل ل و صول ا جهن دعاق ل خدت ثيحب (sysopt allowed-vpn) ةه جاول نم IPv4 رورم ةكر عي مج نوكت، نيوكت ل اذ ه يف. اضي ا انه NAT ءانثتس ل نيوكت ةبس ن ل اب. NAT نم ءانثتس اب AnyConnect ل ي م ع ل IP نيوان ع ل ل ل قتنن يت ل ل ةي ل خاد ل دعاق جاتحتس، جراخ ل ل جراخ ل نم رفاظ ل م ل قوت لثم اديق عت رثك ل ا تان يي عت ل Cisco معد عقوم ىل ع AnyConnect مزج ىل ع روثع ل نكمي. NAT ةسايس راط ل يف ةي فاض ل ل يزنن ل حل اص Apex و Plus صيخرت رفوت مز ل ي. <https://software.cisco.com/download/home>. ةمزج AnyConnect.

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

FTD-3-Manual

Outside Interface

outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

ftd3.example.com

e.g. ravpn.example.com

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks

+

inside (GigabitEthernet0/1)

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.

+

any-ipv4

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com.

You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.03052-webdeploy-k9.pkg

Linux: anyconnect-linux64-4.7.03052-webdeploy-k9.pkg

BACK

NEXT

6. لاسرل قوف رونا مٲ ،بسانم لكشب AnyConnect دادع| نم ققحت ،صخلملما مسق نمض .مالعتسال

^ Summary

Review the summary of the Remote Access VPN configuration.

General

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type AAA Only

Primary Identity Source LAB-AD

Fallback Local Identity Source -

Strip Identity Source server from username No

Strip Group from Username No

Secondary Identity Source

Secondary Identity Source for User Authentication -

Fallback Local Identity Source -

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool

BACK SUBMIT QUERY

7. ةروصلال يف حضوم وه امك نيميلال لىلعأ يف ةقلعملال تاريقيغتلال رز رقنا .

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

#	NAME	AAA	GROUP POLICY	ACTIONS
1	General	Authentication: AAA Only Authorization: None Accounting: None	DfltGrpPolicy	

8. نآلال رشن قوف رقنا .

Pending Changes ? X

✔ Last Deployment Completed Successfully
16 Apr 2020 12:41 PM, [See Deployment History](#)

Deployed Version (16 Apr 2020 12:41 PM)	Pending Version LEGEND Removed Added Edited
+ Network Object Added: AnyConnect-Pool	
-	subType: Network
-	value: 10.10.10.0/24
-	isSystemDefined: false
-	dnsResolution: IPV4_AND_IPV6
-	name: AnyConnect-Pool
+ RA VPN Added: NGFW-Remote-Access-VPN	
-	vpnGatewaySettings[0].exemptNatRule: true
-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com
-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...
-	name: NGFW-Remote-Access-VPN
anyconnectPackageFiles:	
-	anyconnect-win-4.7.03052-webdeploy-k9.pkg
vpnGatewaySettings[0].serverCertificate:	
-	FTD-3-Manual
vpnGatewaySettings[0].outsideInterface:	
-	outside
vpnGatewaySettings[0].insideInterfaces:	
-	inside
vpnGatewaySettings[0].insideNetworks:	

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

مدخستسمال ٲوهل نامأل تاسايس نيوكتو ٲوهل جهن نيكمت

دق نكلو، حاجنب لاصتالال ىلع نيرداق AnyConnect ومدخستسم نوكي نأ بجي، ٲطقنلال هذه دنع ٲوه نيكمت لال ٲوطخالل هذه يدؤتس. ٲني عم دراوم لال لوصولال ىلع نيرداق اونوكي ال دراوملاب لاصتالال AnyConnect يلوؤسم نمض نيمدخستسملل ٲطقف نكمي شيحب مدخستسمال لاصتالال ٲومجملال نمض AnyConnect يمدخستسملل ٲطقف نكمي و RDP مادختساب ٲيلخالل دراوملاب HTTP مادختساب ٲيلخالل دراوملاب.

ٲوهل جهن نيكمت قوف رقناو ٲوهل > تاسايسلال لال لقتنا 1.

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

Establishing User Identity

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

How Identity policies work

Passive authentication Active authentication

USERS → PASSIVE AUTHENTICATION → LEVERAGE IDENTITY

MULTIPLE IDENTITIES → IDENTITY SOURCES

ENABLE IDENTITY POLICY

يُفَاك رِيصِقْت عَارِجِإِلْأَوْ بُولَطْم يِفَاضِإ لِيكْشْت نَم ام، لِيكْشْت اذَه ل

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

Identity Policy

Search

#	NAME	AUTHENTICATION	AUTH. TYPE	SOURCE ZONES	NETWORKS	PORTS	DESTINATION ZONES	NETWORKS	PORTS/PROTO...	ACTIONS
There are no Identity rules yet. Start by creating the first identity rule.										

CREATE IDENTITY RULE

Default Action **Passive Auth** Any Identity Source

2. NAT عَانْتَسِإ نَاك اذِإ .بَسَانَم لِكْشَب تَلِكْش NAT نَأ دَكْأَتُو NAT > تَاسَايَسِلْأ يِلْإ لِقْتْنَا 2. يِفَاضِإ نِيوَكْت يِلْإ ةَجَاح كَانَه نُوَكْت نَلَف، اِيْفَاك AnyConnect تَادَادِعْ يِف هِنِيوَكْت مَت يِذْلَا أَنَه.

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

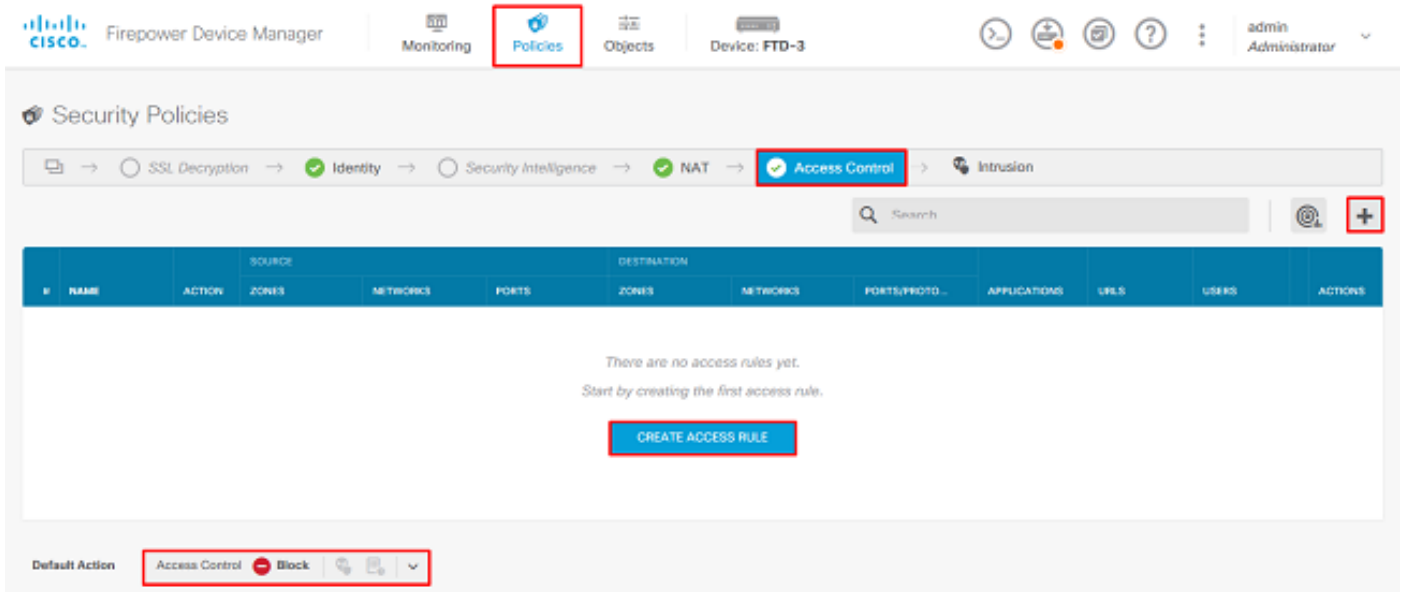
SSL Decryption → **Identity** → Security Intelligence → **NAT** → Access Control → Intrusion

1 rule

Search

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Auto NAT Rules												
>	#	Internet_PAT	DYNAMIC	ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY

3. عارجلال "نيي عت متي ،مسقلا اذ ه ي .لوصولا ي ف مكحتلا > تاسايسلا ل لقتنا 3. مدختسم لاصتا درجمب كلذل لوصول دعاوق عاشنإ متي ملو "رظحلا" لعل "يضارتفالا دعاوق عاشنإب مق وأ زمرلا + قوف رقنا .عيش يا لوصولا لعل ارداق نوكي نل ،AnyConnect ،ةديج دعاوق ةفاضال لوصولو



4. لخد نوم مدختسم لاعت متي نأ بجي ،نيوكتلا اذ ه ي .ةبسانملا ميقلاب لوقحلا ألما .ةيلخادلا ةكبشلا ي ف Windows مداخ لوصولو قحب AnyConnect ي لوؤسم ةعومجم متيس يتلا ةيجراخلا ةهجاولا يه ةيجراخ ةقطنمك ةقطنملا نيوكت مت ،ردصم لل ةبسنلاب مت يذل AnyConnect-Pool نئاك ةكبشلا نيوكت مت واهب AnyConnect ي مدختسم لاصتا ي ف مدختسملا ةيوهل ةبسنلاب .AnyConnect عالعمل IP نيوانع نيي عت لاقبسم هنيوكت لاصتالا ادبب مدختسملا موقيس يتلا ةكبشلا او ةقطنملا وه ردصملا نوكي نأ بجي ،FDM ،يتلا ةيلخادلا ةهجاولا وه zone لخد وه امك ةقطنملا نيوكت متي ،ةهوجلل ةبسنلاب .اهنم فرعي نئاك وه يذل Inside_Net نئاك ةكبشلا نيوكت متي و ،Windows مداخ اهيلي عقي لعل تالوكت ووربلا/ذفانملا نيي عت متي و ،Windows مداخ اهيلي دجوي يتلا ةيعرفلا ةكبشلا ل TCP 3389 و UDP 3389 لوكوتورب ربع RDP لوصولو حامس لل ةصصخملا ذفانملا نم نيئاك

Edit Access Rule

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP

Show Diagram | Not hit yet | CANCEL | OK

م تي شي حبة وعومجملل AnyConnect يلوؤسم ةفاضل متتس ، "نومدختسمل" مسق تحت
 Windows مداخل ل RDP لوصوب ةوعومجملل هذه نع نولصفي نيذلا نيمدختسملل حامسلا
 م، ةبسانملا ةوعومجملل قوف رقناو، تاعومجم بيوتلا ةمالع قوف رقناو، زمرلا + قوف رقنا
 لكذ ةيوهلا ردصموني درف نيمدختسمل ديحت نكمي هنا طحال. قفاوم قوف رقنا

Add Access Rule

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

AVAILABLE USERS

Filter: []

Identity Sources: **Groups** | Users

- LAB-AD \ Account Operators
- LAB-AD \ Administrators
- LAB-AD \ Allowed RODC Password Replication Group
- LAB-AD \ AnyConnect Admins**
- LAB-AD \ AnyConnect Users

Create new Identity Realm | CANCEL | OK

CONTROLLING ACCESS FOR USERS AND USER GROUPS

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram: | CANCEL | OK

قفاوم قوف رقنا ،ةبسانملا تاراخال ديحت درجمب

Add Access Rule

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

AVAILABLE USERS

- LAB-AD \ AnyConnect Admins

CONTROLLING ACCESS FOR USERS AND USER GROUPS

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram: | CANCEL | OK

ةدعاق عاشنإ متي ،نيوكتلا اذه يف .رمأل مزلا اذا لوصولا دعاقو نم ديزملا عاشنإب مق 5.

HTTP إلى لوصول اب AnyConnect يمدختم ةومجم نمض نيمدختسملل حامس لل لى رخأ لوصولو
 م داخ نم Windows.

Edit Access Rule

Order: 2 | Title: AC HTTP Access | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE

Zones	Networks	Ports
outside_zone	AnyConnect-Pool	ANY

DESTINATION

Zones	Networks	Ports/Protocols
inside_zone	Inside_Net	HTTP

Show Diagram | Not hit yet | CANCEL | OK

Edit Access Rule

Order: 2 | Title: AC HTTP Access | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

AVAILABLE USERS

- LAB-AD \ AnyConnect Users

CONTROLLING ACCESS FOR USERS AND USER GROUPS

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram | Not hit yet | CANCEL | OK

نيميل لى لى ف ةقل عمل ا تاريخي غت لل رز قوف رقنا م لوصول ةدعاق نيوك نم ققحت 6.

ةوصول ايف حضوم وه امك

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

2 rules

#	NAME	ACTION	SOURCE			DESTINATION					ACTIONS	
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	APPLICATIONS	URLS		USERS
> 1	AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne...	
> 2	AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne...	

Default Action: Access Control - Block

7. نآلا رشن قوف رقنا مٲ ،تارييغتل نم ققحت

Pending Changes

✓ Last Deployment Completed Successfully
28 Apr 2020 01:35 PM. [See Deployment History](#)

Deployed Version (28 Apr 2020 01:35 PM) Pending Version

LEGEND Removed Added Edited

+ Access Rule Added: AC HTTP Access

- users[0].name: AnyConnect Users
- logFiles: false
- eventLogAction: LOG_NONE
- ruleId: 268435467
- name: AC HTTP Access

sourceZones:

- outside_zone

destinationZones:

- inside_zone

sourceNetworks:

- AnyConnect-Pool

destinationNetworks:

- Inside_Net

destinationPorts:

- HTTP

users[0].identitySource:

- LAB-AD

+ Access Rule Added: AC RDP Access

MORE ACTIONS ▼ CANCEL DEPLOY NOW ▼

ةحصلال نم ققحتلا

ححص لكشب نيوكتل لمع ديكأتل مسقلا اذه مدختسا

يئاهنل بيترتل

AAA نېوكت

```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

AnyConnect نېوكت

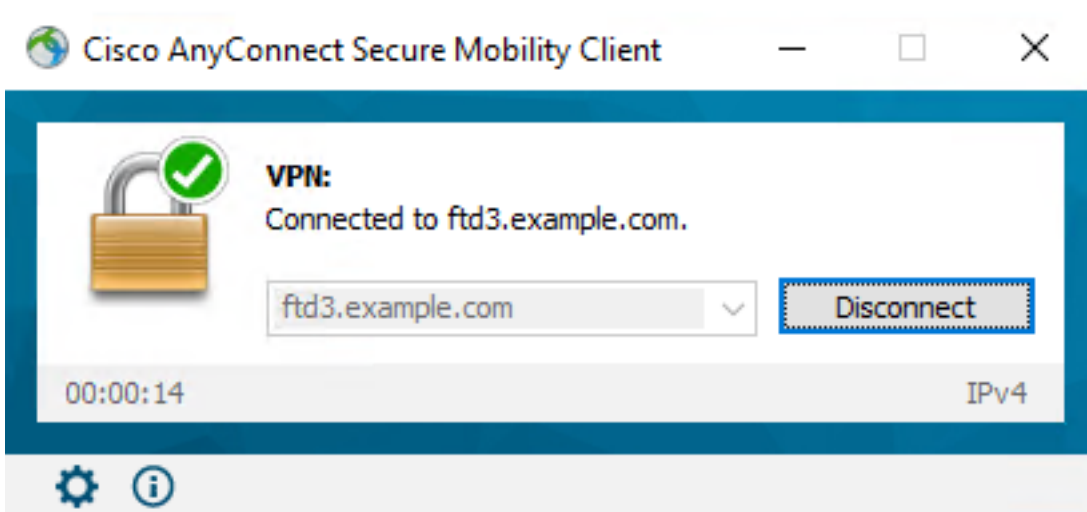
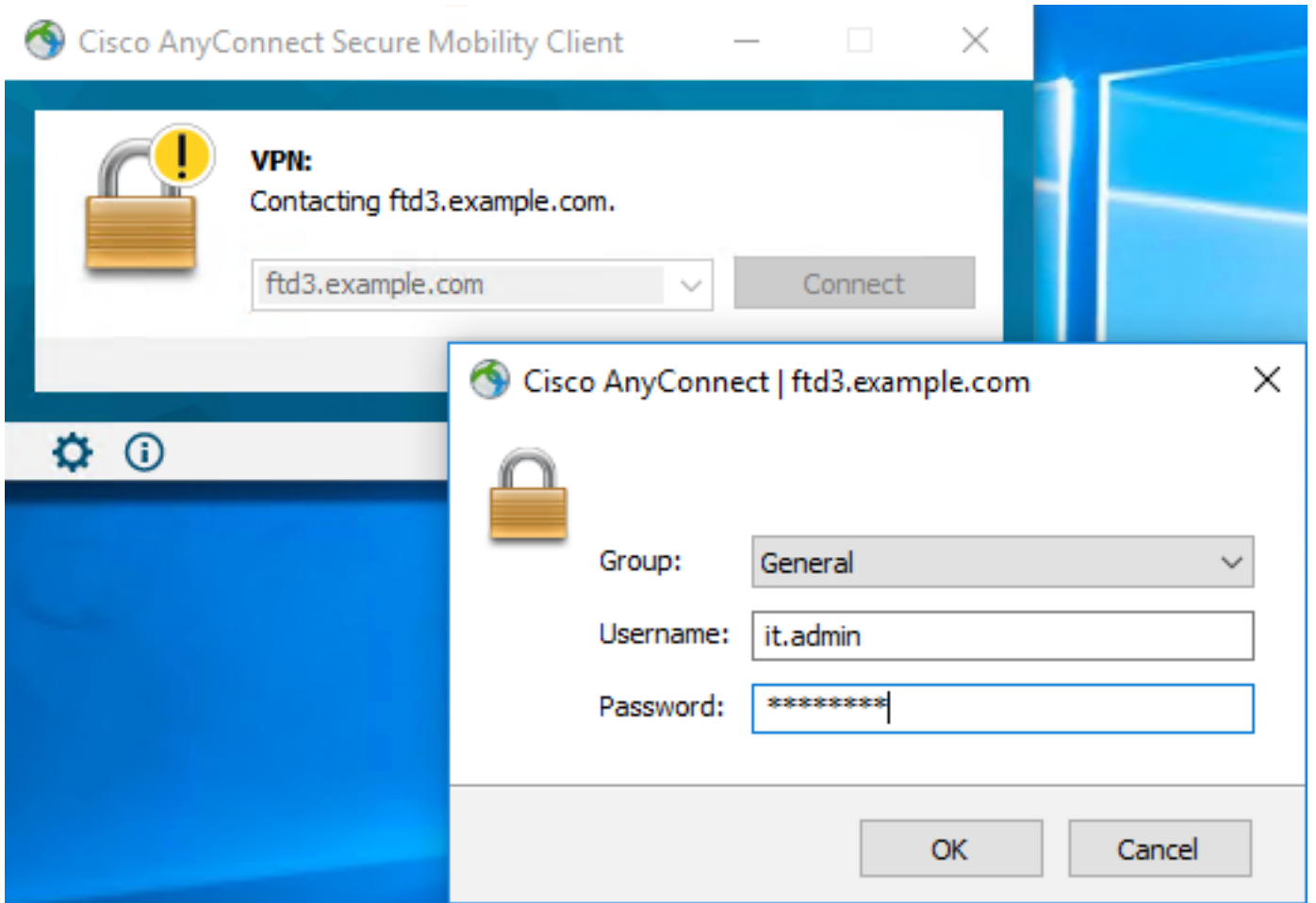
```
> show running-config webvpn
webvpn
  enable outside
  http-headers
    hsts-server
      enable
      max-age 31536000
      include-sub-domains
      no preload
    hsts-client
      enable
  x-content-type-options
  x-xss-protection
  content-security-policy
  anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
  anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
  anyconnect enable
  tunnel-group-list enable
  cache
    disable
  error-recovery disable
```

```
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable
```

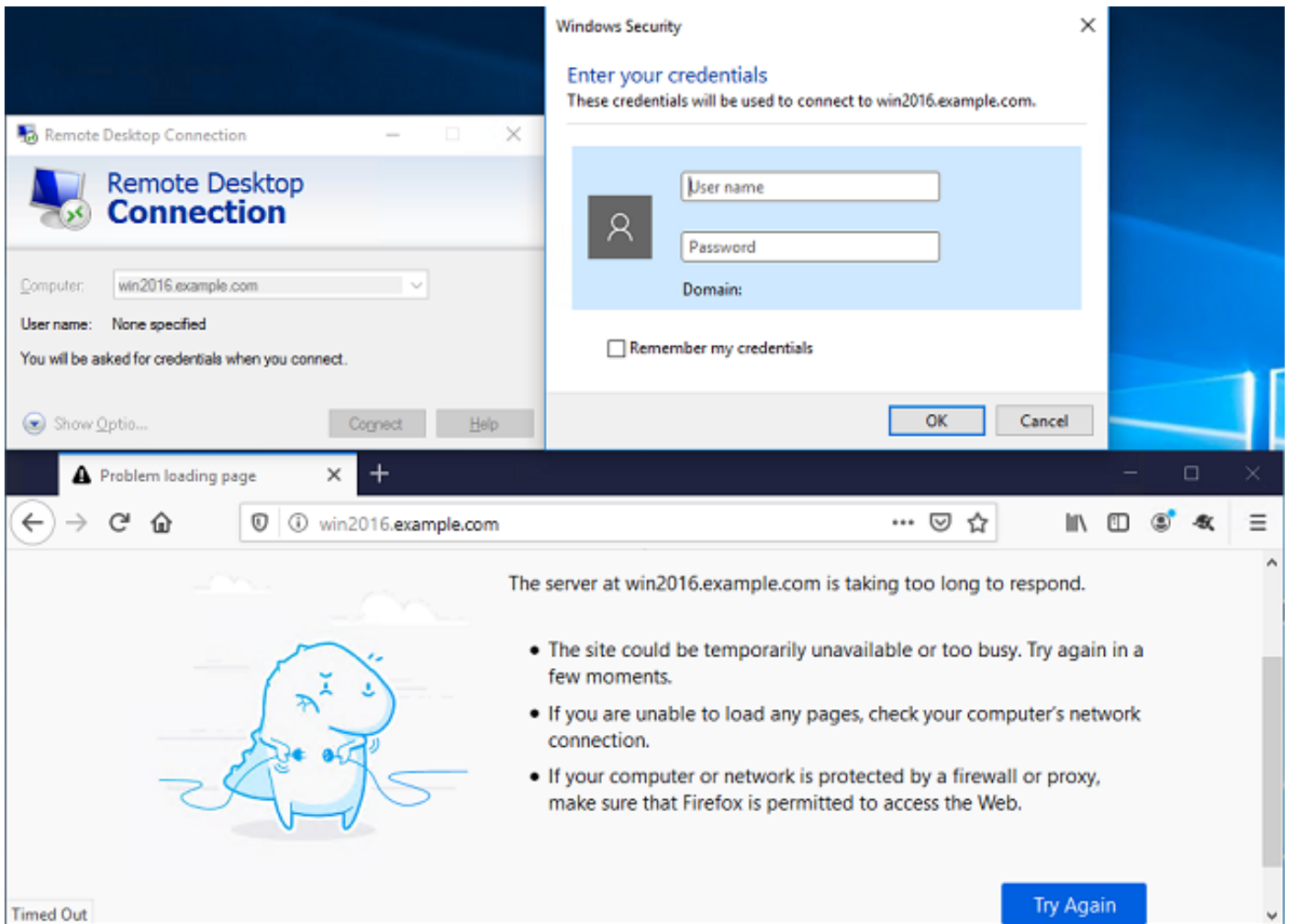
```
> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
  anyconnect ssl dtls none
```

```
> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

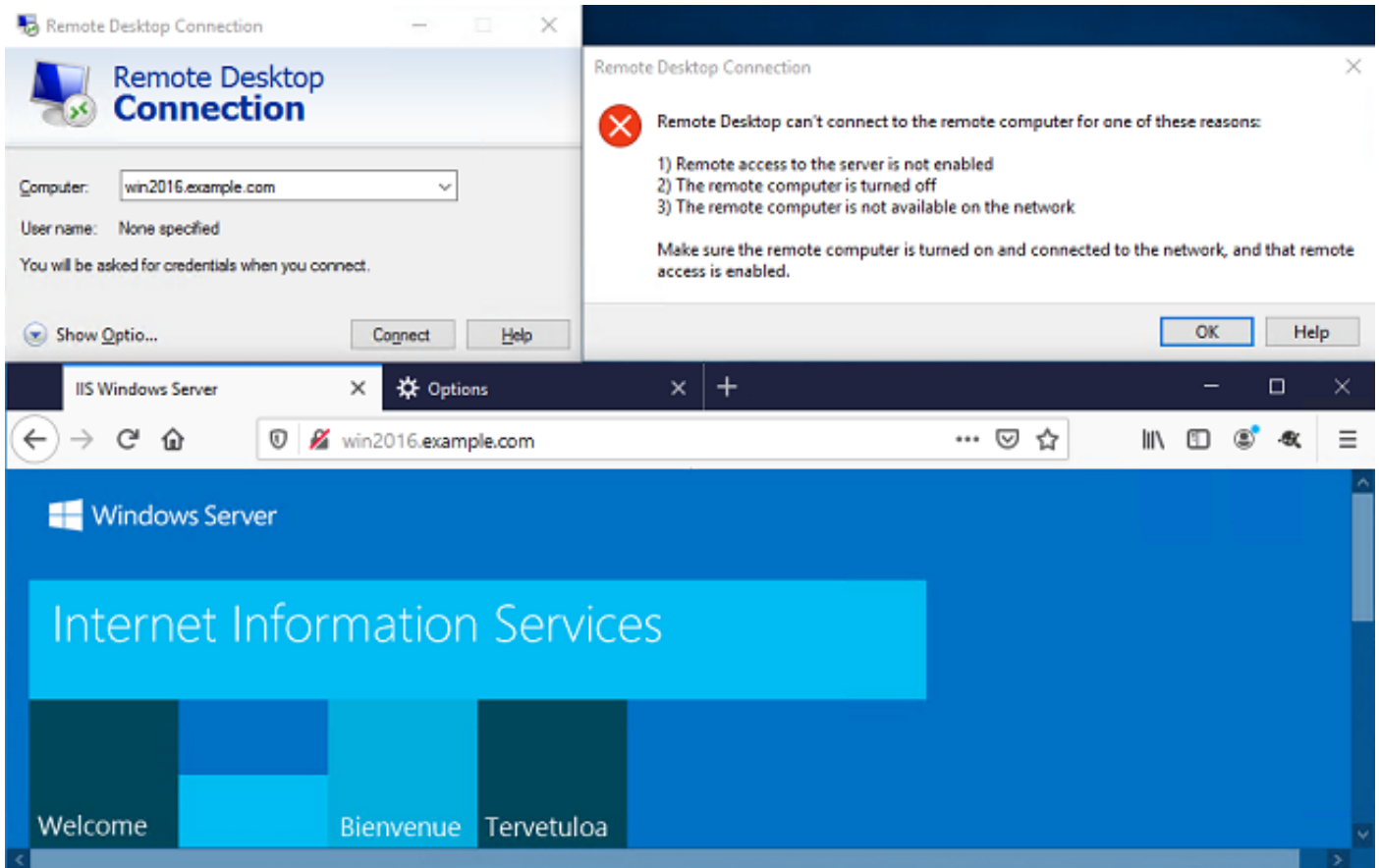
اهنم ققحتلاو AnyConnect نم لوصولا يف مكحتلا ةسايس دعاوقب لاصتالا



User IT Admin لوصول RDP إلى Windows Server، مداخل اذهل Firefox و RDP لمع ةسلج حتف ن. HTTP إلى لوصول اهيدل سيل كلذ عمو، مداخل RDP ربع مداخل إلى لوصول اه نكمي مدختس مل اذه نأ نم ققحتي.



AnyConnect يمدختمسم ةوعومجم يف دوجوم رابتخ| مدختمسم مادختساب لوخدلا ليجستب تمق اذا ةسايس دعاوق نا نم ققحتلا كنكم يف ، RDP لوصو سيلو HTTP لوصو مهيدل نيدلا لوعفملا ةيراس تحبصأ لوصولا يف مكحتلا



اهحال صإو ءاطخأل فاشكتسا

ححص لكشب نيوكتل لمع ديكأتل مسقلا اذه مدختسا

ءاطخأل ححصت

LDAP ةقداصم ءاطخأ فاشكتسال في صيخشت CLI في اذه ءاطخأل ححصت ليغشت نكمي
 اهحال صإو: `debug ldap 255`.

ليغشت نكمي، اهحال صإو مدختسملا ةيوهل لوصول في مكحتل ءسايس ءاطخأ فاشكتسال
 ببس ديدحتل مكحتل ءمئاق في ماظنل لمعدب صاخأل ءاطخأل ححصت كرحم ةيماح راج
 عقوقم ريغ لكشب اهعنم وأ رورملا ءكرحب حامسلا

ةلماعل LDAP ءاطخأ ححصت

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
      Base DN = [DC=example,DC=com]
      Filter = [sAMAccountName=it.admin]
```

```

Scope = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]   objectClass: value = top
[53]   objectClass: value = person
[53]   objectClass: value = organizationalPerson
[53]   objectClass: value = user
[53]   cn: value = IT Admin
[53]   sn: value = Admin
[53]   givenName: value = IT
[53]   distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]   instanceType: value = 4
[53]   whenCreated: value = 20200421025811.0Z
[53]   whenChanged: value = 20200421204622.0Z
[53]   displayName: value = IT Admin
[53]   uSNCreated: value = 25896
[53]   memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]   uSNChanged: value = 26119
[53]   name: value = IT Admin
[53]   objectGUID: value = &...J..O..2w...c
[53]   userAccountControl: value = 512
[53]   badPwdCount: value = 6
[53]   codePage: value = 0
[53]   countryCode: value = 0
[53]   badPasswordTime: value = 132320354378176394
[53]   lastLogoff: value = 0
[53]   lastLogon: value = 0
[53]   pwdLastSet: value = 132319114917186142
[53]   primaryGroupID: value = 513
[53]   objectSid: value = .....{I...;.....}...
[53]   accountExpires: value = 9223372036854775807
[53]   logonCount: value = 0
[53]   sAMAccountName: value = it.admin
[53]   sAMAccountType: value = 805306368
[53]   userPrincipalName: value = it.admin@example.com
[53]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]   dSCorePropagationData: value = 16010101000000.0Z
[53]   lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End

```

LDAP مداخل لاصتا عاشن | رذعت

```

[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End

```

ةلمتحملا لولحل:

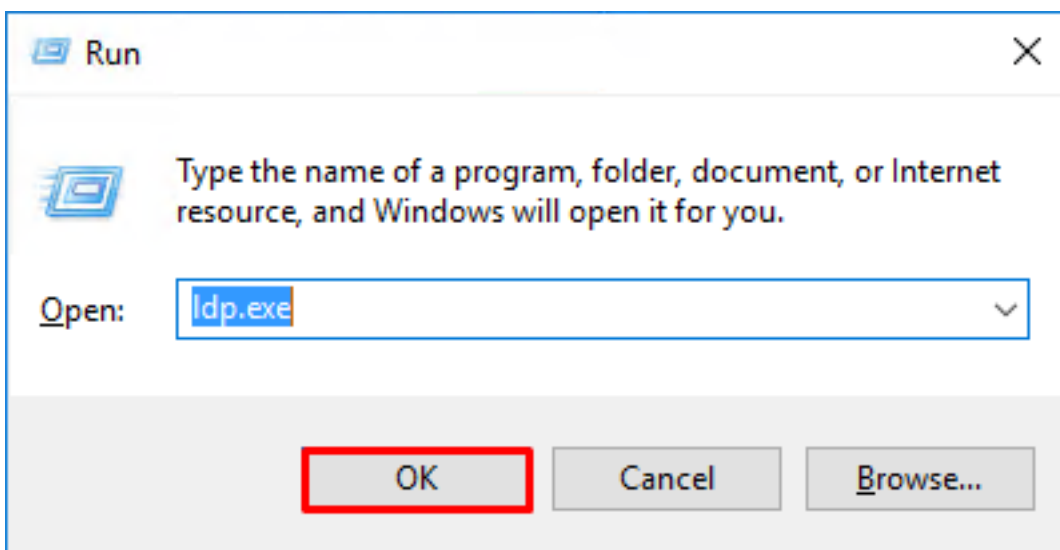
- LDAP مداخ نم ةباجتسا ىقلى تي FTD نأ نم دكأتو هي جوتلا نم ققحت
- اهب قووثوم ةحيجصل رذجل CA ةداهش نأ نم دكأت، STARTTLS وأ LDAP مادختسا ةلاح يف
- حاجنب SSL ةحفاصم لامك إنكمي شيحب
- نم ققحتف، فيضملا مسا مادختسا مت اذا. حيجص ءانيمو ناونعلا لمعتسي نأ تققد
- حيجصل IP ناونع ىل هلح ىلع DNS ةردق

ةحيجص ريغ طبزل رورملا ةملك وأ DN

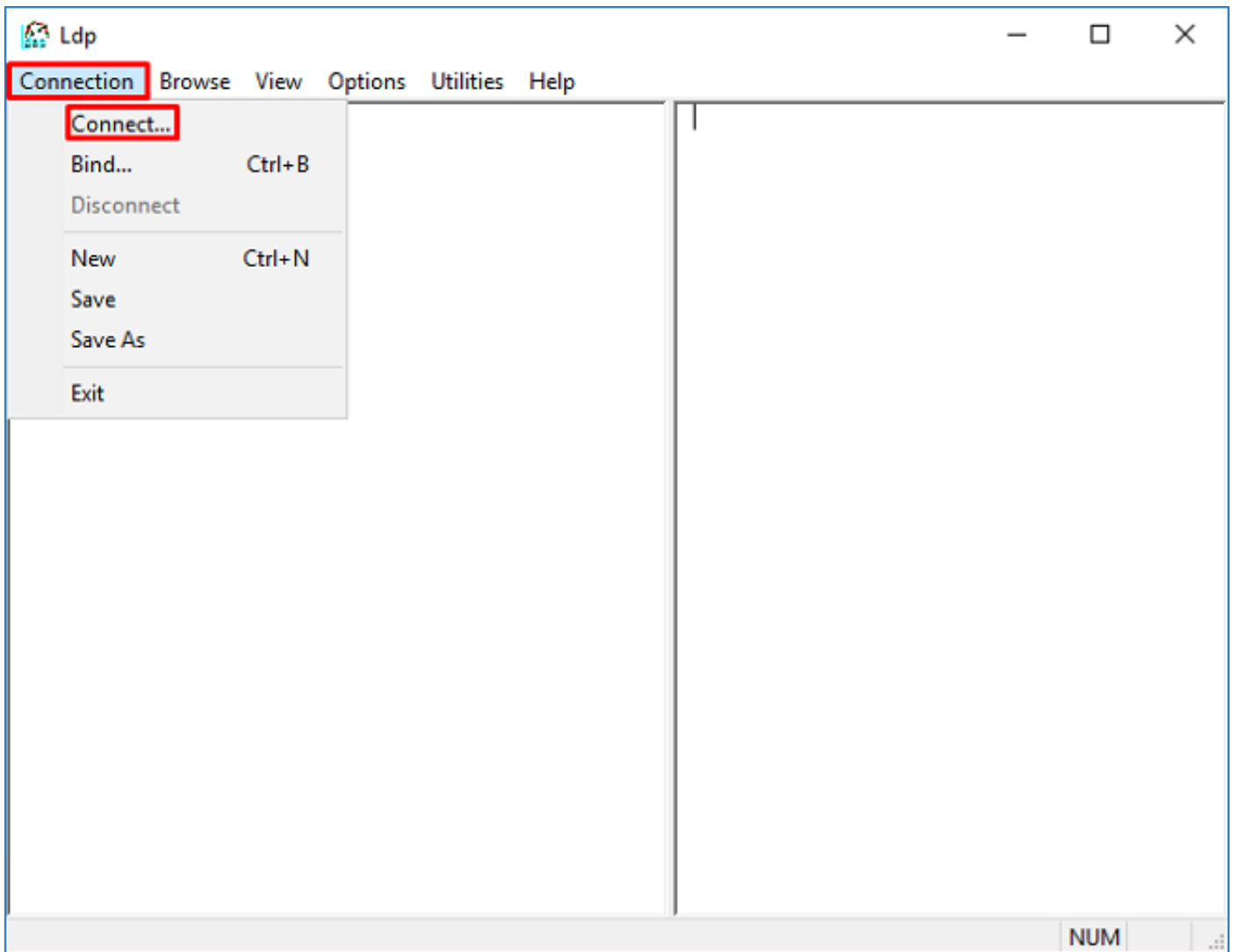
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

ليجست رورم ةملك و لوخدلا ليجستب ةصاخلا DN ةكبش نيوكت نم ققحت: لمتحملا لولحل
ققحتلل **ldp.exe** مادختساب AD مداخ ىلع ءارجإل اذه نم ققحتلا نكمي. حيجص لكشب لوخدلا
ةيلاتلا تاوطلخال ربع لقتنا، LDP مادختساب حاجنب باسح طبر ةيناكم!

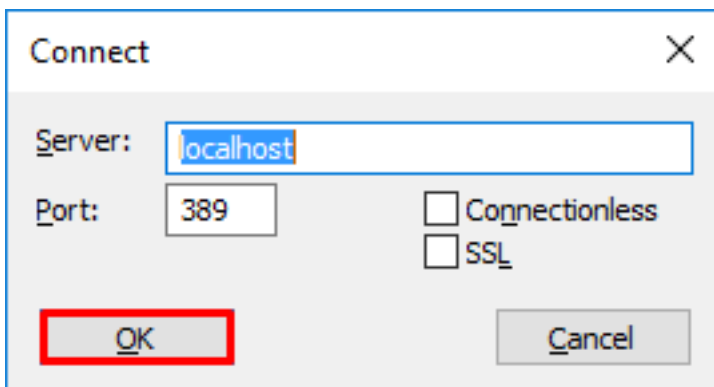
1. **ldp.exe** ن عثحاب او **Win+R** ىلع طغضا، AD مداخ ىلع.



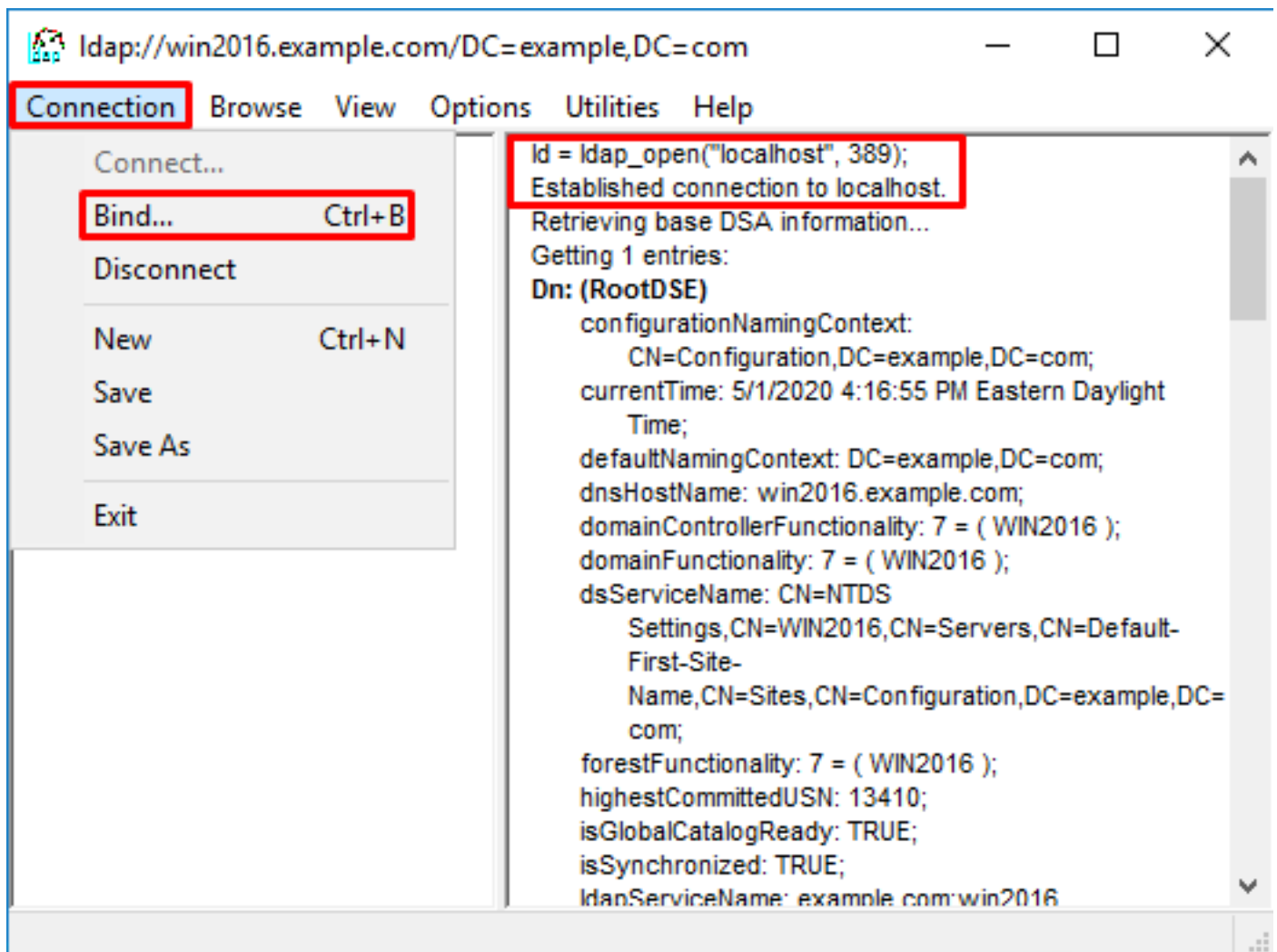
2. ةروصل يف حضوم وه امك... لاصتا > لاصتا قوف رقنا.



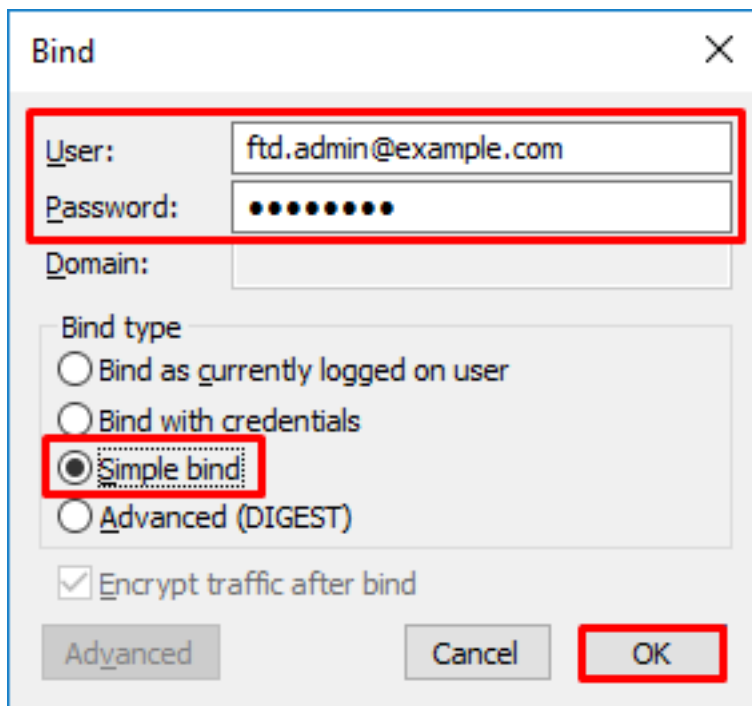
3. قفاوم قوف رقنا م ث ، بس انم لا ذفنم لا و مداخل ل يلحم في ضم دح .



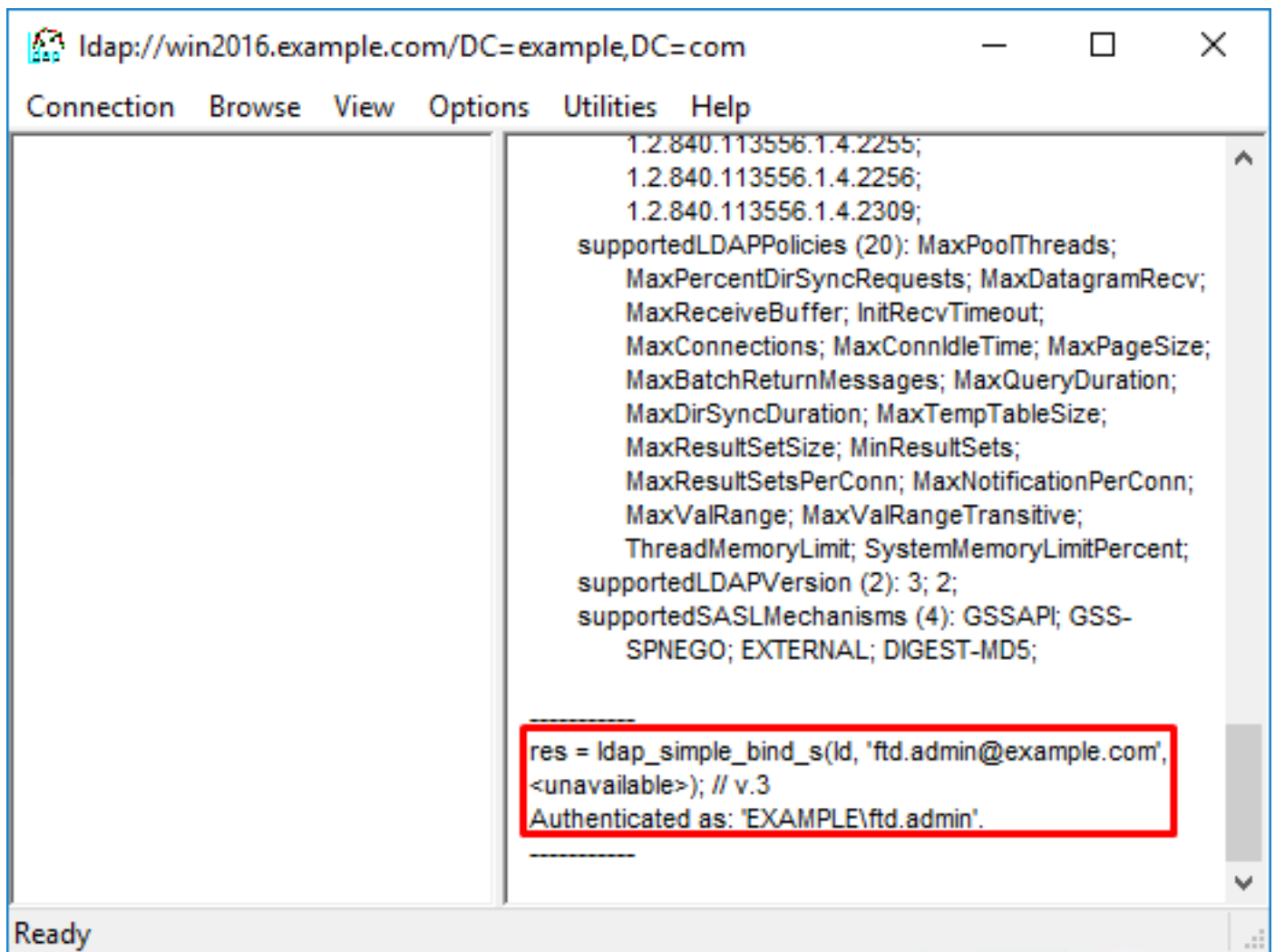
4. وه امك ... طبر > لاصتا يلع رقنا . حجان لاصتا يل ريشي يذلا صنلا نمي ال ا دومعلا رهظي .
ةروصلال يف حضورم .



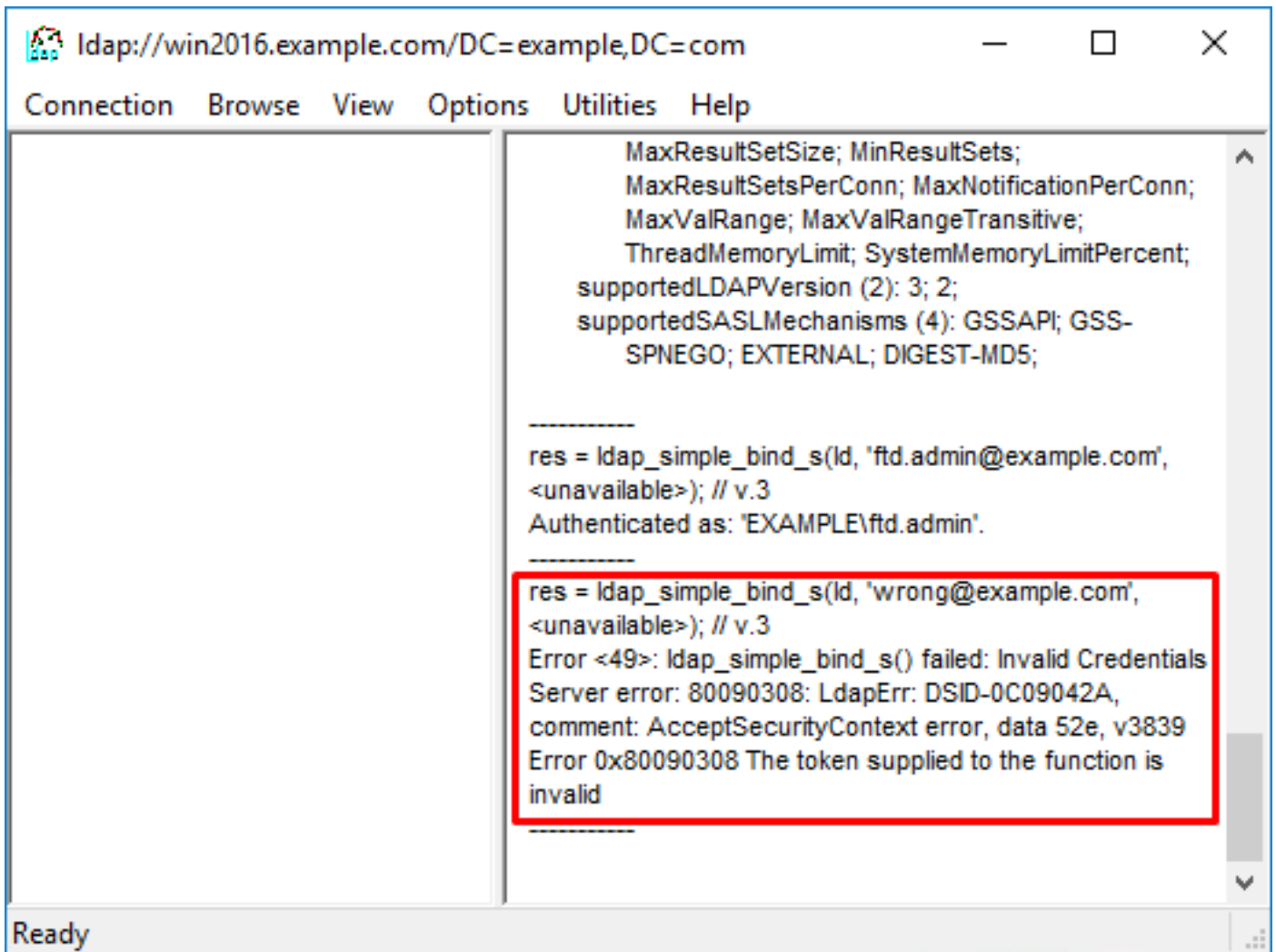
5. OK قوف روناو. رورملا ةم لك و لول دللا باسح مدختسم مسا دح م ث ، طيسب طبر دح .



DOMAIN\username. ك هيلع قوصم LDP ره طيس ، حجان طبر مادختساب



اذه لثم لشف ىل ك لذ يدؤيسف ،ةحيص ريغ رورم ةملك وأ مدختسم مسا طبر تلواح اذا



مدخستسم ال مسال ع روثع ال LDAP مداخ ع رذعت

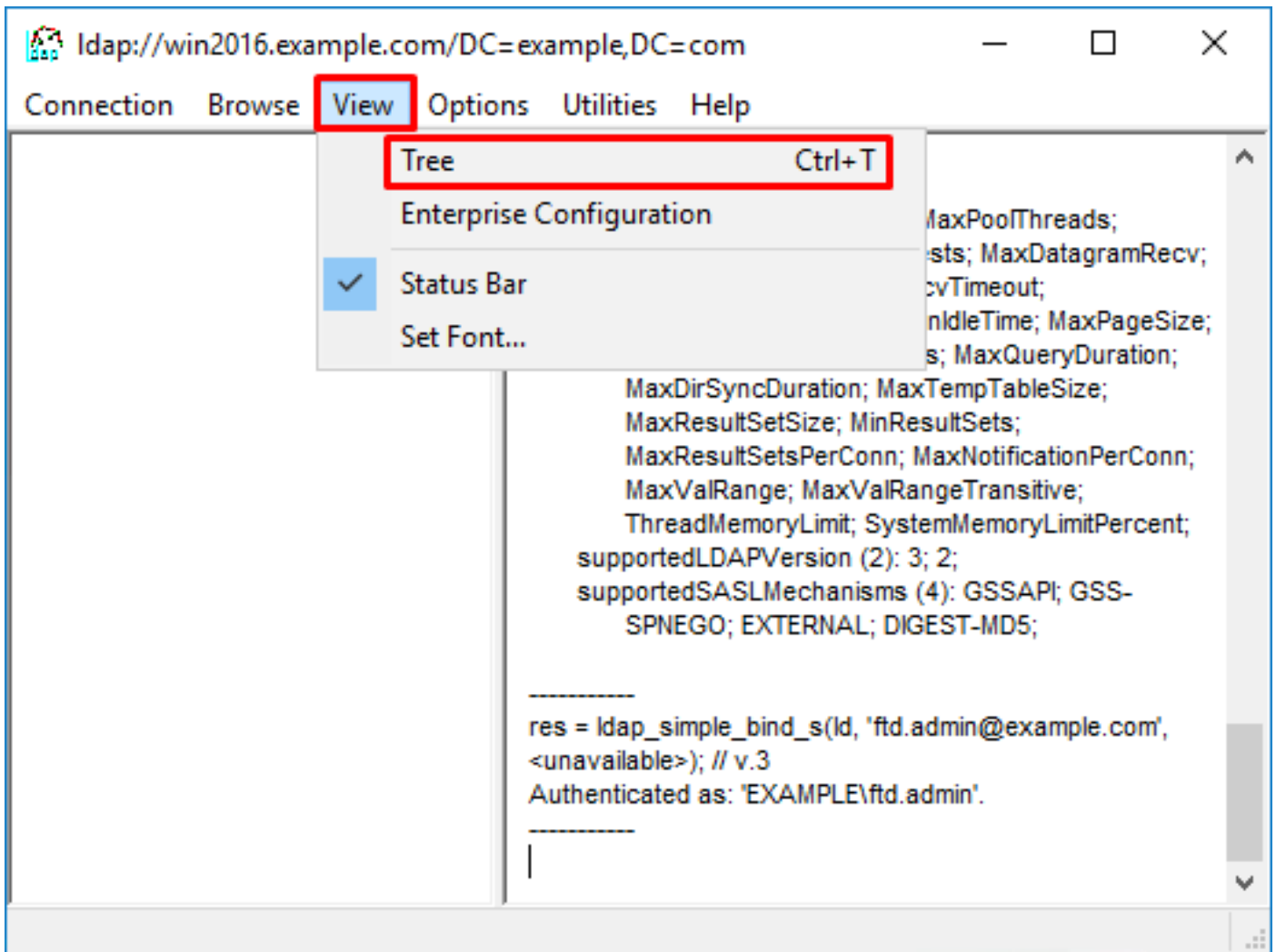
```

[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
      Base DN = [dc=example,dc=com]
      Filter  = [samaccountname=it.admi]
      Scope   = [SUBTREE]
[-2147483612] Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End

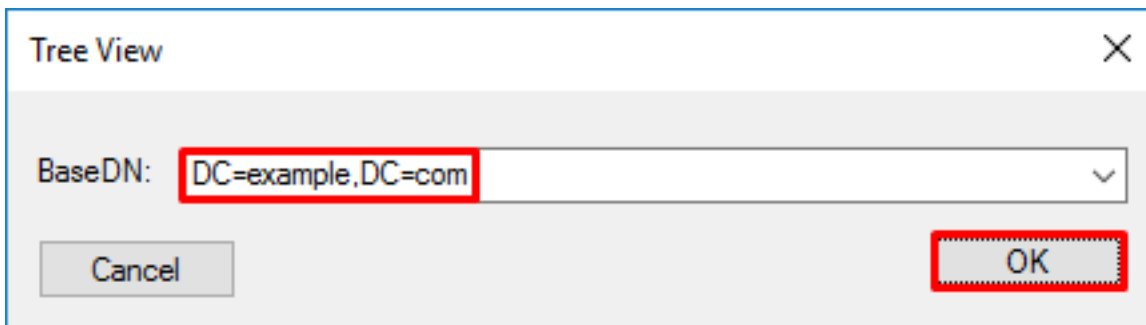
```

ةطساوب مت يذلا ثحبالا عم مدخستسم ال ع روثع ال هنكمي AD نأ نم ققحت :لمتحمل ال لجال
FTD.exe. عم اضيا كلذب مايق ال لنكم و.

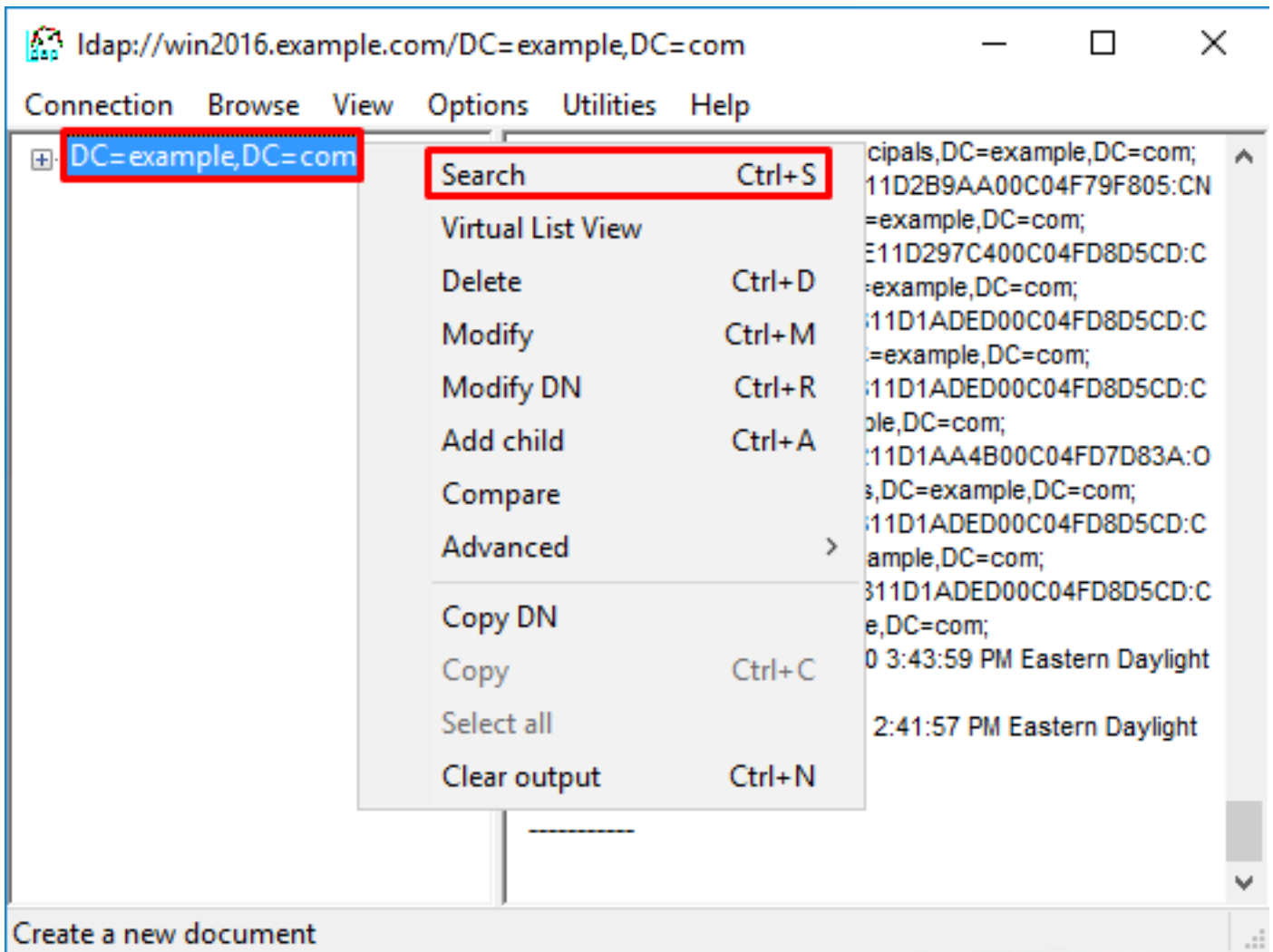
ةروصل ال ي ف حضوم وه امك ةرغش > ضرع ال لقتنا ،حاجنب طبرلا دع ب .1



2. قفاوم قوف رقنا مٲ FTD ىلع هنىوكت مت ىذلا ىساسأل DN ددح.

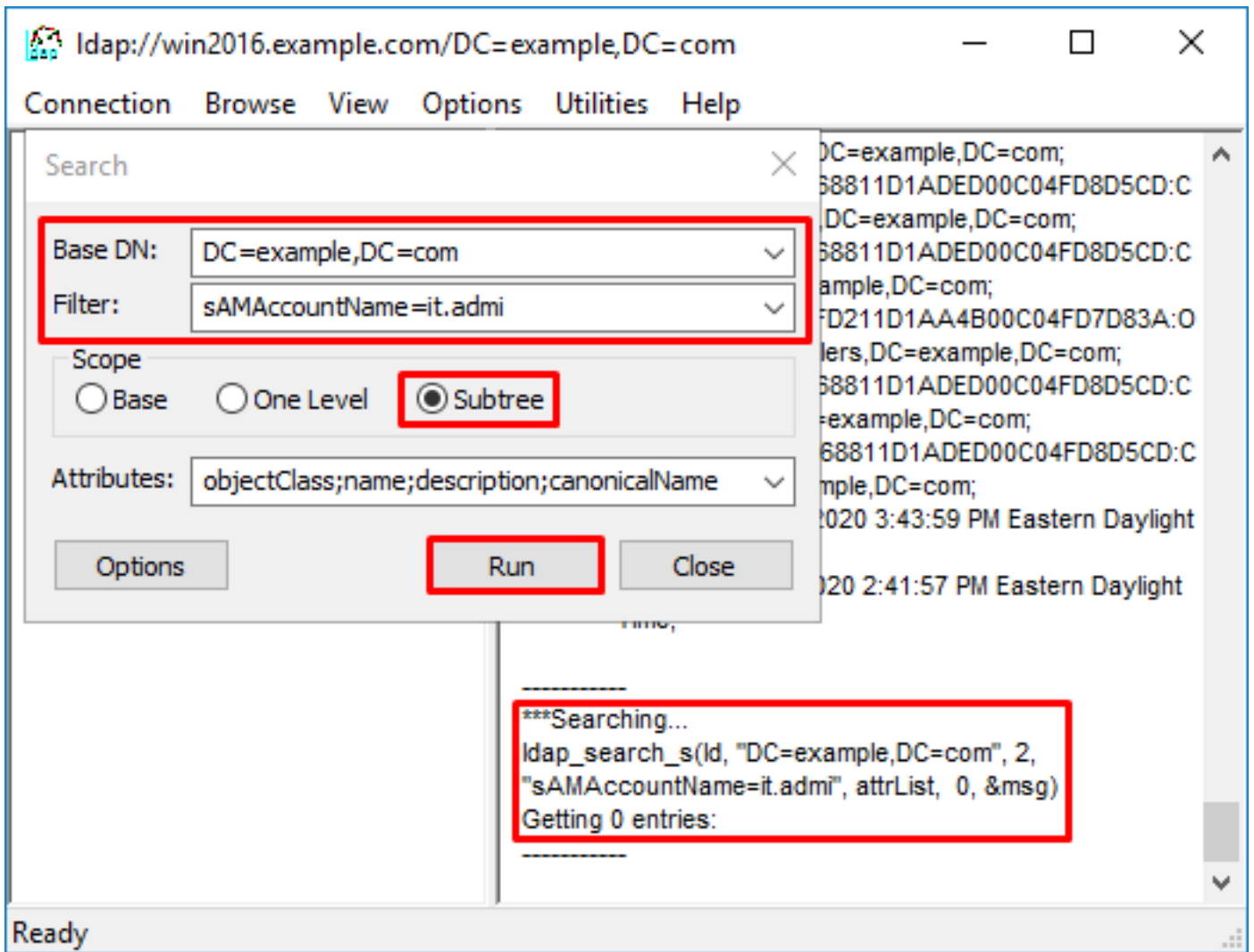


3. ةروصلال ىف حضوم وه امك شحب قوف رقنا مٲ ىساسأل DN قوف نمىأل سواملال رزب رقنا.



4. في رهظت امك ةيساسأل قاطنل او ةيفصت ل لماع و (DB) تانايب ل ةدعاق مي ق س فن دح . هذه ، ل اثل م ل اذه في . ءاطخأل احيصت

- ةيساسأل ال DN ةكبش : `dc=example.dc=com`
- ةيفصت ل لماع : `samaccountname=it.admi`
- ةعرف ل ةرشل : قاطن ل



مساب م دختسم باسح دوجو مدعل ارظن تال ا خ دا 0 ن ع LDP ش ح ب ي
 samaccountName=it.admi م س ا س ا ل ا DN ل ف س ا

ة ف ل ت خ م ة ج ي ت ن ح ي ص ل ل samaccountName=it.admin م ا د خ ت س ا ب ي ر خ ا ة ر م ة ل و ا ح م ل ا ر ه ظ ت
 م د خ ت س م ل ا ب ص ا خ ل ا DN ع ب ط ي و م س ا س ا ل ا DN ت ح ت د ح ا و ل ا خ دا 0 ن ع LDP ش ح ب ي

The screenshot shows the 'Active Directory Users and Groups' console window. A 'Search' dialog box is open, with the following configuration:

- Base DN: DC=example,DC=com
- Filter: sAMAccountName=it.admin
- Scope: Subtree
- Attributes: objectClass;name;description;canonicalName

The 'Run' button is highlighted. Below the dialog, the search results are displayed in a text box:

```

***Searching...
ldap_search_s(ld, "DC=example,DC=com", 2,
"sAMAccountName=it.admin", attrList, 0, &msg)
Getting 1 entries:
Dn: CN=IT Admin,CN=Users,DC=example,DC=com
   canonicalName: example.com/Users/IT Admin;
   name: IT Admin;
   objectClass (4): top; person; organizationalPerson;
   user;
  
```

مدخست مسال ة ححص ريغ رورم ال ة مل ك

```

[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
      Base DN = [dc=example,dc=com]
      Filter  = [samaccountname=it.admin]
      Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
  
```

```
[-2147483613] Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment:
AcceptSecurityContext error, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

ءاهتنا مدع نم وحيحص لكشب مدختسمل رورم ةملك نيوكت نم ققحت :لمتحملا لجال
مادختساب AD دض طبر ءارجاب FTD موقيس ،لوخدلا ليجستل DN عم لجال وه امكو .اهتيحالص
يلع AD ةردق نم ققحتلل ldp في طبرلا اذه ذيفنت نكمي امك .مدختسمل دامتعا تانايب
في LDP في تاوطخل رهظت .رورملا ةملك و مدختسمل مسا دامتعا تانايب سفن يلع فرعتلا
ةعجارم نكمي ،كلذ يلى ءفاضلاب .ةحيحص ريغ رورم ةملك **وأ** مسقلا طبر لوخد ليجست DN
لمتحم بلسل "Microsoft" مداخل اذح اضراع" تالجتس

رابتخ AAA

مدختسم مسا مادختساب FTD نم ةقداصم ءلواحم ءااا test رمال مادختس نكمي
وه رمال .ةقداصملا واصلتالا لشف تالاج رابتخال اذه مادختس نكمي .نيددحم رورم ةملك و
[AD IP/hostname] فيضملا [AAA-server] مداخل ةقداصم رابتخ|

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
  realm-id 7
aaa-server LAB-AD host win2016.example.com
  server-port 389
  ldap-base-dn DC=example,DC=com
  ldap-scope subtree
  ldap-login-password *****
  ldap-login-dn ftd.admin@example.com
  server-type auto-detect

> test aaa-server authentication LAB-AD host win2016.example.com
Username: it.admin
Password: *****
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

مزحل طاقنلا

LDAP مزح ترداغ اذ| AD مداخل يلى لوصول ءي ناكم| نم ققحتلل مزحلا تاعومجم مادختس نكمي
فهيوتل في ءلكشم يلى كلذ ريشي دقف ،ةباجتس اذوت ال نكلو ،FTD

LDAP رورم ءكرح هاجت ائيئانث يدي نأ مت طاقنلا انه

```
> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via inside
    Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap
```



```
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
*****
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

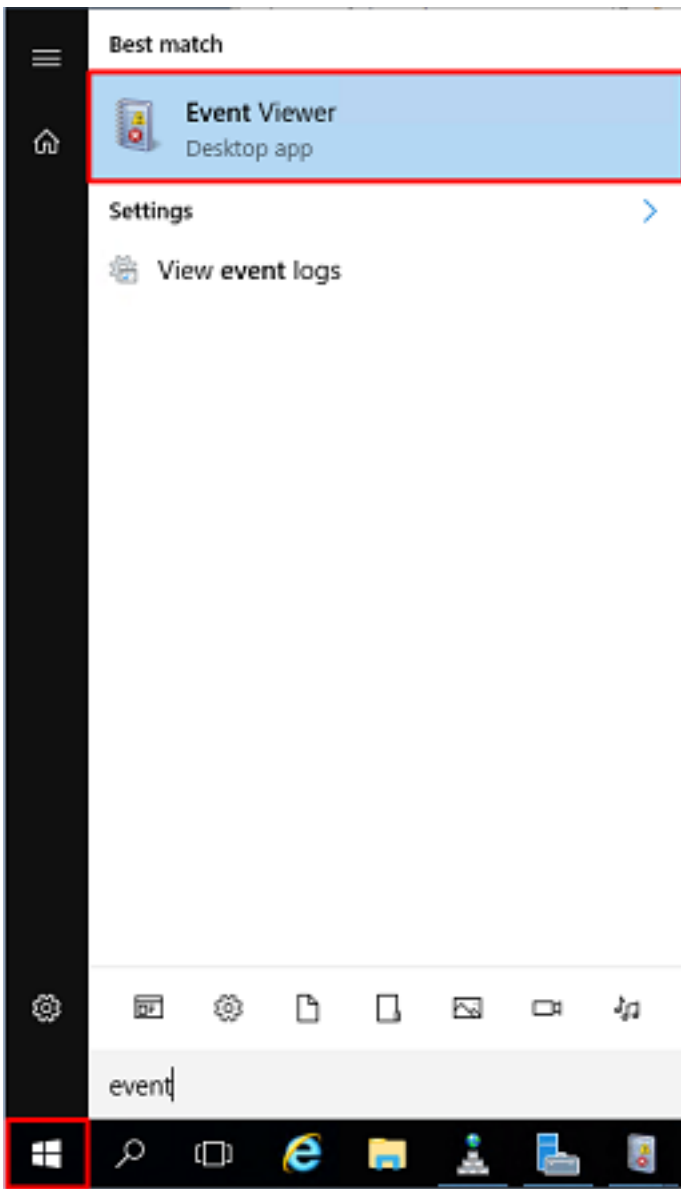
54 packets captured

  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
  3: 23:02:16.772039      192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
<nop,nop,timestamp 1061373058 762393884>
  4: 23:02:16.772482      192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
  5: 23:02:16.772924      192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
  6: 23:02:16.772955      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
  7: 23:02:16.773428      192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
  8: 23:02:16.775030      192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
  9: 23:02:16.775075      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
```

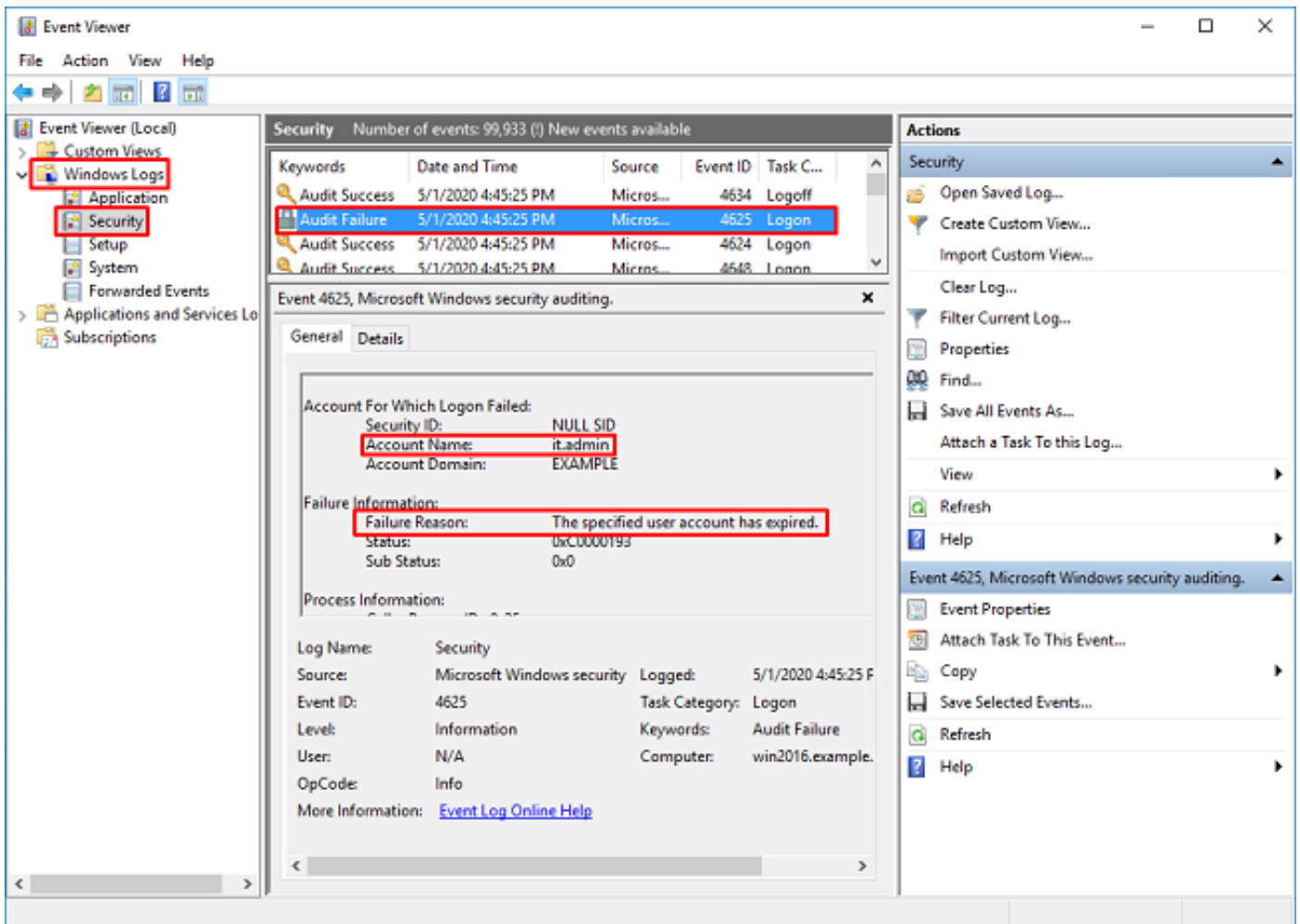
Windows Server شادحاً ضراع تالچس

الڤصفت رثكأ تامولعم رڤفوتب "AD مڤاخ" ةبرع ىلع ةدوچومل "شادحأل ضراع" تالچس موقت لقطع شودح بڤس لوح.

1. هجاتت فاو شادحأل ضراع نع شحبلا.



مسا م ادختساب قي قدتلا لشف نع شحبا . نامألا قوف رقناو Windows تالچس عيسوتب مق 2. ةروصلال ي ف حضوم وه امك لشفلا تامولعم عجارو مدختسملال باسح



An account failed to log on.

Subject:

Security ID:SYSTEM
Account Name:WIN2016\$\nAccount Domain:EXAMPLE
Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed:

Security ID:NULL SID
Account Name:it.admin
Account Domain:EXAMPLE

Failure Information:

Failure Reason:The specified user account has expired.
Status:0xC0000193
Sub Status:0x0

Process Information:

Caller Process ID:0x25c
Caller Process Name:C:\Windows\System32\lsass.exe

Network Information:

Workstation Name:WIN2016
Source Network Address:192.168.1.17
Source Port:56321

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل