

مدخلت سملاء AD (LDAP) ئىوھو ئىوكت عالمعل FDM ئىلۇ ئارادملا ئىلۇ AnyConnect

تاييەت حملاء

ئەم دەقەملە

ئىس اس ألا تابىل طەتمەلە

تابىل طەتمەلە

ئەم دەخەتسەملە تانىوكىمەلە

نىوكىتلە

ويەرانىسىلى او ئەك بىشىلل يەطىەت خەتلە مەسىرلە

تانىيەت AD

ئىس اس ألا LDAP DN دىدەت

باىسەح ئاشنە FTD

(يەرىايت خە) تانالىغا تاعومىجىلى ئەنەم دەخەتسەم ئەفاض او تانالىغا تاعومىجىم ئاشنە

مەدخەتسەملە ئىوھل نام ألا تاس ايس نىوكىت و ئىوھل اچەن نىكەمت LDAP وا ئەل طققى بولطم) LDAP بىچەلە STARTTLS)

تانىيەت FDM

صىخەرتلە نەم قىقەتلى

تانالىغا ئىوھ رەدىم دادعە

ئەم دەقەملە AnyConnect ئىوكت

مەدخەتسەملە ئىوھل نام ألا تاس ايس نىوكىت و ئىوھل اچەن نىكەمت

قىچىلە نەم قىقەتلى

يەئەنلە بېتىرتلى

اھنم قىقەتلى او AnyConnect نەم لوصولى يەف مەكتەلە ئەس ايس دەعاؤقپ لەصەتالا

اھھالىص او ئاطخىلە فاش كەتسە

ئاطخىلە حېحىصىت

قىلماعلە LDAP ئاطخىلە حېحىصىت

قىچىلە LDAP مەداخىلە ئاشنارذۇعەت

قىچىلە LDAP مەداخىلە رۈرمەلە ئەملىك وأ/و DN

مەدخەتسەملە مەسائىلە رۇثىغىلە LDAP مەداخىلە رۇذۇعەت

مەدخەتسەملە مەسالە قىچىلە رۈرمەلە ئەملىك

رابىت خە AAA

مۇزىلە طاققىتلە

ئادىجەن ئەنۋەن ئەلەجىس Windows Server

ئەم دەقەملە

عالمعل Active Directory (AD) ئەق دەاصم نىيوكت ئەي فيك حېي ضوت وە دەنەتسەملە اذە نەم ضرغىلە ئەطس اوپ ئارادملا Cisco نەم FirePOWER (FTD) دىدەت نەع افادب نۇلۇشتى ئەنەم دەقەملە AnyConnect لوصولى تاس ايس يەف مەدخەتسەملە ئىوھ مادختسەم تىيىس. زاھەن ئەرادا ئەنەم دەقەملە AnyConnect ئەنۋەن عەپ IP نىيەن دەقەملە.

ةيسيس اس ألا تاب لطتملا

تاب لطتملا

ةيلاتلا عيضاً اوملاب ةفرعم كيدل نوكت نأب Cisco يصوت:

- ىلع RA VPN نيوكتب ةيسيس اسأ ةفرعم
- ىلع LDAP مداخل نيوكتب ةيسيس اسأ ةفرعم
- نالع إلاب ةيسيس اسأ ةفرعم

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربلا تارادصا ىلا دنتسملا اذه يف ةدراولا تامولعملاء دنتسـت:

- Microsoft 2016 مـداخـ
- FTDv 6.5.0 ليغـشتـ

ةـصـاخـ ةـيـلـمـعـمـ ةـيـيـبـ يـفـ ةـدوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاـشـنـاـ مـتـ
تنـاكـ اذاـ (ـيـصـارـتـفـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ
رمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

نيوكتلا

ويرانيسـلـاوـ ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



حـطـسـ لـوـكـوـرـبـوـ (ـIISـ)ـ تـنـرـتـنـإـلـاـ تـامـوـلـعـمـ تـامـدـخـ مـادـخـتـسـابـ اـقـبـسـمـ Windowsـ مـداـخـ نـيـوـكـتـ مـتـ
عـاـشـنـاـ مـتـيـسـ ،ـاـذـهـ نـيـوـكـتـلـاـ لـيـلـدـ يـفـ .ـمـدـخـتـسـمـلـاـ ةـيـوـهـ رـاـبـتـخـاـلـ (ـRDPـ)ـ دـيـعـبـلـاـ بـتـكـمـلـاـ
نـيـتـعـوـمـجـمـوـ نـيـمـدـخـتـسـمـ تـابـاسـحـ ةـثـالـثـ.

نـيـمـدـخـتـسـمـلـاـ تـابـاسـحـ:

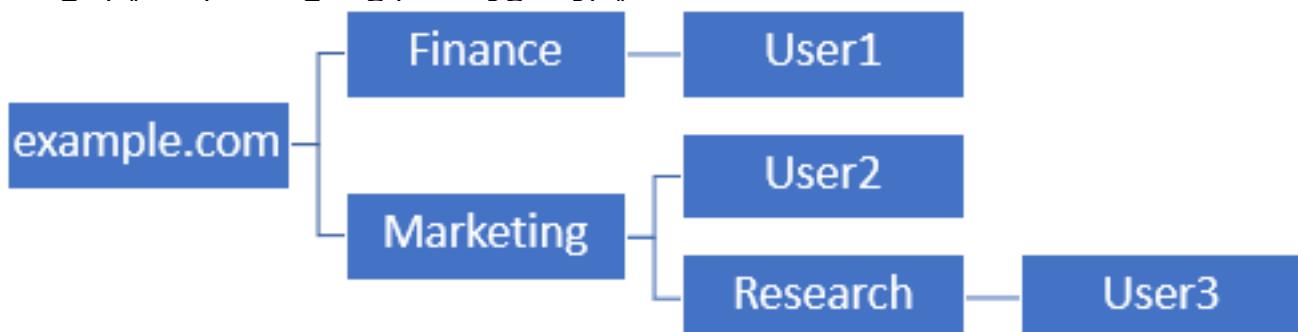
- مـداـخـ طـابـتـرـالـاـ FTDـ لـ حـامـسـلـلـ لـيـلـدـ بـاسـحـكـ اـذـهـ مـادـخـتـسـاـ مـتـيـسـ:ـ ADـ لـوـؤـسـمـ
 - مـدـخـتـسـمـلـاـ ةـيـوـهـ رـاـبـتـخـاـلـاـ لـوـؤـسـمـ بـاسـحـ مـدـخـتـسـيـ:ـ تـامـوـلـعـمـلـاـ ةـيـنـقـتـ لـوـؤـسـمـ
 - مـدـخـتـسـمـلـاـ ةـيـوـهـ رـاـبـتـخـاـلـ مـدـخـتـسـيـ رـاـبـتـخـاـلـ مـدـخـتـسـمـ بـاسـحـ:ـ رـاـبـتـخـاـلـاـ مـدـخـتـسـمـ
- تـاعـوـمـجـمـلـاـ:

- AnyConnect Admins: رـاـبـتـخـاـلـاـ لـوـؤـسـمـ ىـلـاـ رـاـبـتـخـاـلـ ءـعـوـمـجـمـ ةـفـاضـاـ مـتـيـسـ:ـ Windowsـ طـقـفـ RDPـ مـداـخـ ىـلـاـ
- ةـيـوـهـ رـاـبـتـخـاـلـ مـدـخـتـسـمـلـاـ ىـلـاـ رـاـبـتـخـاـلـ ءـعـوـمـجـمـ ةـفـاضـاـ مـتـتـسـ:ـ AnyConnectـ طـقـفـ
- HTTPـ لـوـصـوـقـحـ ءـعـوـمـجـمـلـاـ ىـلـاـ Windows~ Serverـ نـوـكـيـسـ .ـمـدـخـتـسـمـلـاـ ةـيـوـهـ

تـانـيـوـكـتـ AD

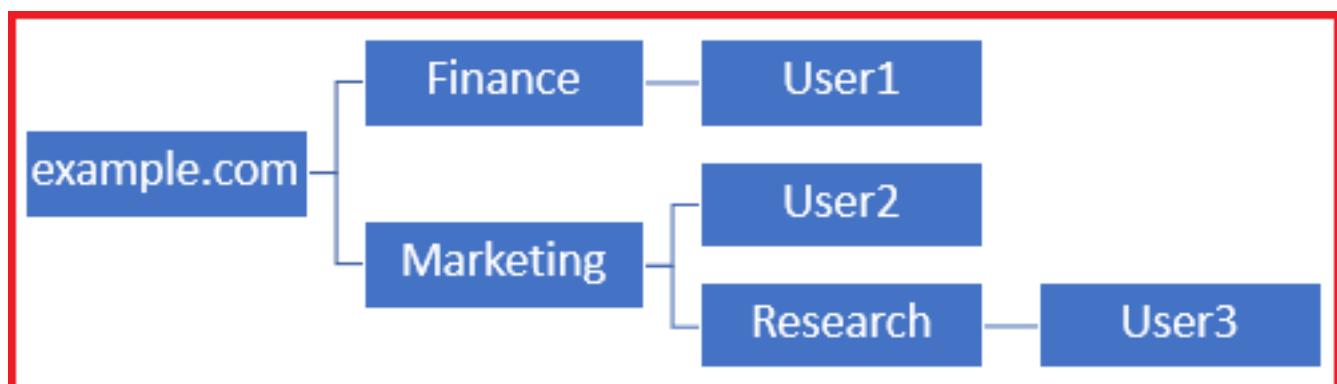
نم ليلق ددع رفوت مزلي، ىلع بسانم لكشب مدخلتسملا ئي وهو AD ۋە قاداصم نىوكتل نىوكتللا ئارجى لبىق Microsoft مداخلىع اهعېمجت وألىيصافتلا هذه عېمج ئاشنابىجى. مىقلالا يىھ ئيسىئرلا مىقلالا (FDM) لوحملاتانايىب ۋە دعاق ۋارادى ىلع:

- مسا وە example.com، اذه نىوكتللا ليلىدىف. مداخللىاجملامسا وە اذه: لاجملامسا لاجملام.
- مت اذا Microsoft مداخلىل لوصولل مدخلتسملا FQDN وأ IP ناونع: مداخللىل FQDN ناونع نىوكتللا ليلىدىف. FQDN و لخاد FDM مداخنىوكت بجىف، FQDN مادختسإ 192.168.1.1 ىلىلچىلا مىتىي ىذلا win2016.example.com يىھ مىقلالا هذه نوكت، اذه.
- مدخلتسىس، يضارتفا لكشب LDAP. ۋە مدخلتسىس اوب مدخلتسملا ذفنملا: مداخللا ذفنم LDAP، يضارتفا لكشب LDAP ۋە مادرختسى TCP 389 ۋە LDAP SSL (LDAPs) و STARTTLS.
- عجملا مادرختسى مزلى، LDAP ۋە STARTTLS مادرختسى ۋە لاح يىف: رذجلا قدصملاملا عجملا.
- عجملا مادرختسى ۋە مادرختسى SSL ۋە مادرختسى LDAPs.
- FDM و FTD لبىق نم مدخلتسىملا باسحلا وە اذه: رورملامىللىكولىلىدىلا مادرختسم مسا.
- ماتىس. تاعومجم و نىم مادرختسىم نع ثحبلا او نىم MDR ئەنلىك دەرىپللىك طېرىلىللىك، مادرختسى LDAP ۋە مادرختسى TCP 636.
- نم FDM بىلطيسى و FDM ئەدبىلا ئەطاقن يىس اسألا DN لىثمى: يىس اسألا زىمملا مسا الا Active Directory.
- ماتىس، اذه نىوكتللا ليلىدىف. نىم مادرختسىم نع ثحبلا دەرىپللىك، جاتنالا ئىيېبل، كىلذۇمۇ، يىس اسألا DN ھەنأىلۇ example.com رذجلا لاجملامادرختسى ىلىع. لصفا LDAP ل يىمرەلا جىرتلار خادىفاضا لكشب يىس اسألا DN مادرختسى نوکىي اذه: يىمرەلا جىرتلار مادرختسى، لاثمىلار لىبسىن.



ىلىع نىرداق ئيمى ئەنلىلا قىيىستىلا ۋە دەرىپللىك ئەنلىلا نوکىي نأ دىرىي لوفوسىملا ناك اذىكىلذنىاف، ىلىع هنىيەت نىكمىي ئەنلىلا يىس اسألا DN ىلىع ئەقاداصملا اضىأ لوخدىلا لىچىستىپ ئەيلاملا ئيمى ئەنلىلا ۋە دەرىپللىك ئەنلىلا User1 ل اضىأ حەمسىس ثحبلا او قىيىستىلا او ئەيلاملا ىلىا ھەجتىي و رذجلا نم أدبىس مادرختسىملا ثحب ناك ارظن.

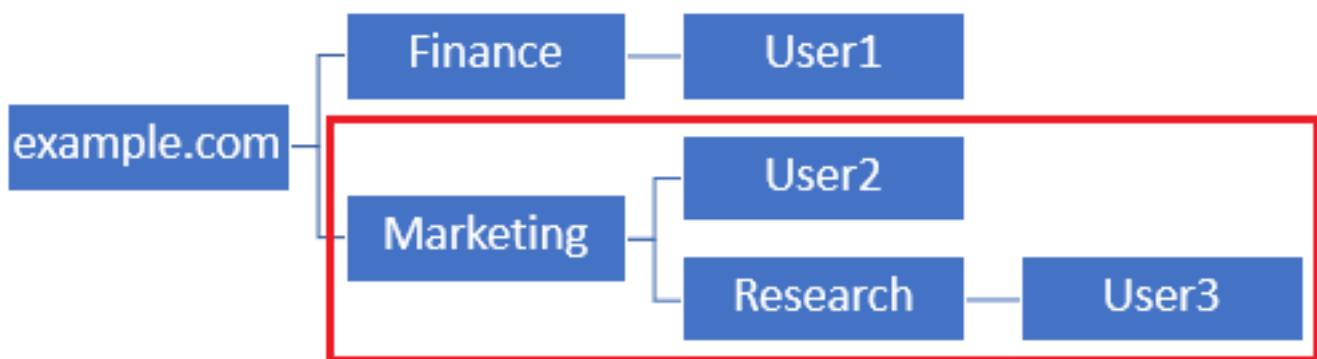
ىلىع يىس اسألا DN نىيىعت ماتىس.



وا قىيىستىلا ئاسسۇم ۋە دەرىپللىك ئەنلىلا لىچىستىپ ئەنلىلا ناك اذىكىلذنىاف، ىلىع يىس اسألا DN نىيىعت كىلذ نم الدب لوفوسىملىك ئەندا.

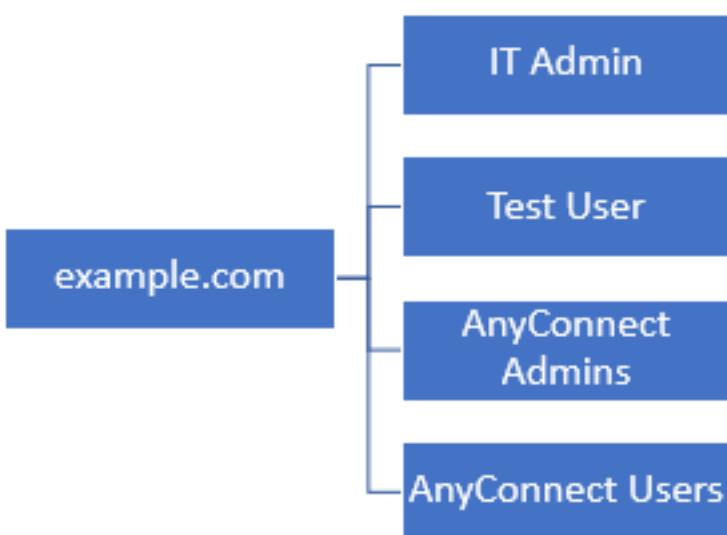
"قیوستلا" يف أدبیس ثحبلا نأ ئقداصلما طقف User2 و User3.

قیوستلا ىلع يساسألا DN نیيغت:



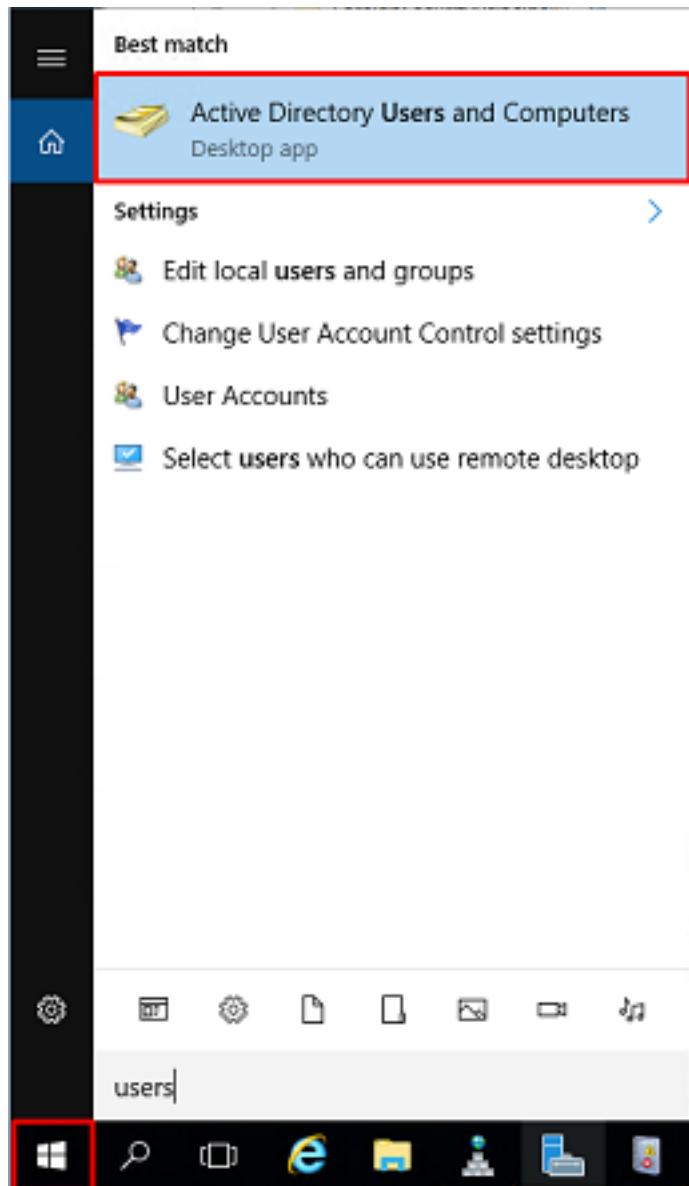
نیم دختسملل حامسلما متیس يذل او FTD لخاد تایوتسملا ددعتم مکحتلا نم دیزممل هنأ ظحال، مهباً ۋە ئەنلىك AD تامس ىلا ادانتسا نیم دختسملل فلتاخم ضيوفت نیيغت وا لېصوتپ ضيوفت ۋە طېرخ نیوكت نیيغتیس LDAP.

مادختسما متیسو اذه نیوكتلا لىلد يف طسبملا LDAP ل يمرهلا جردتلا اذه مادختسما متی يساسألا DN رذجلل example.com ل DN.

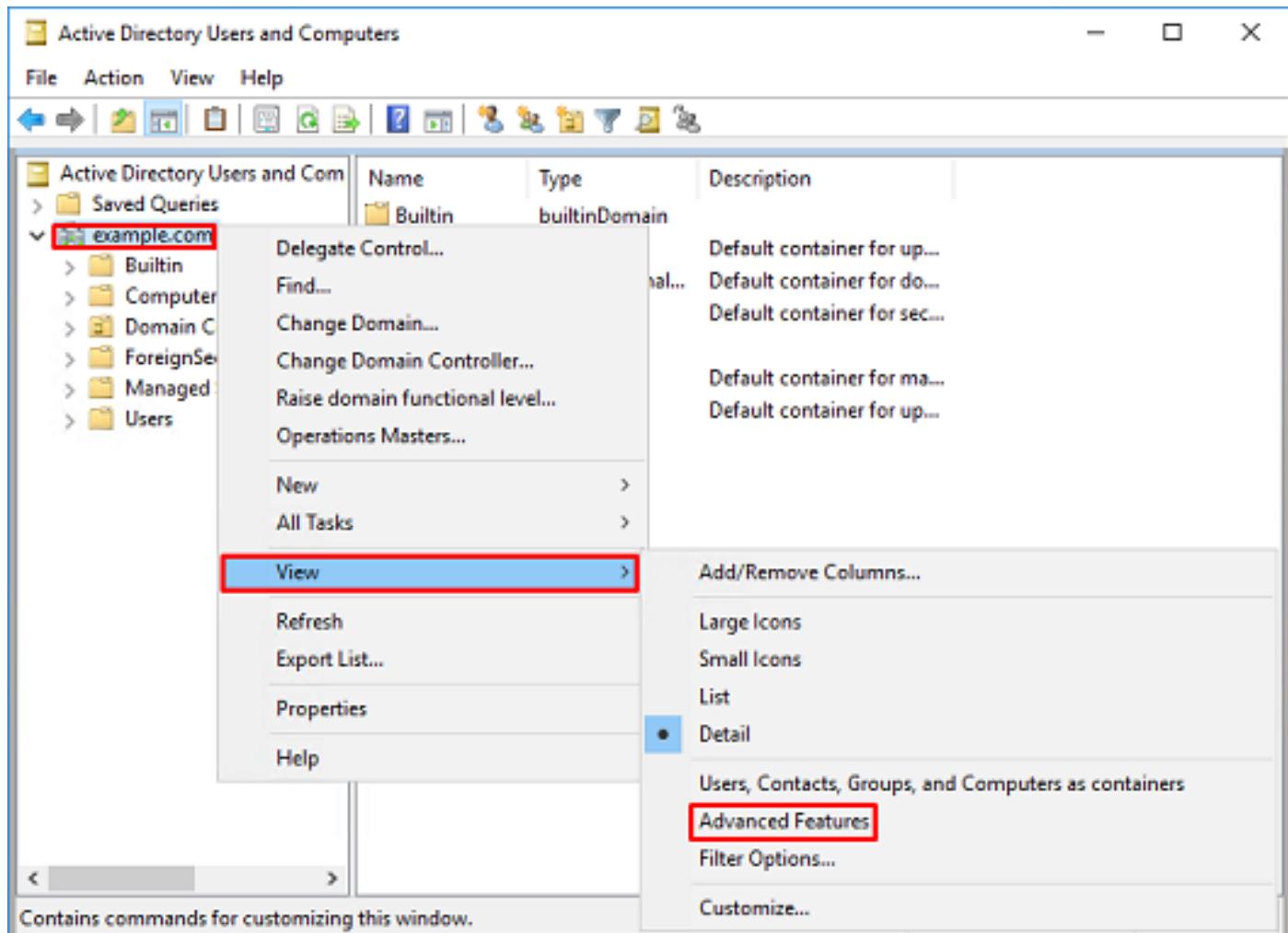


يساسألا DN ديدجت

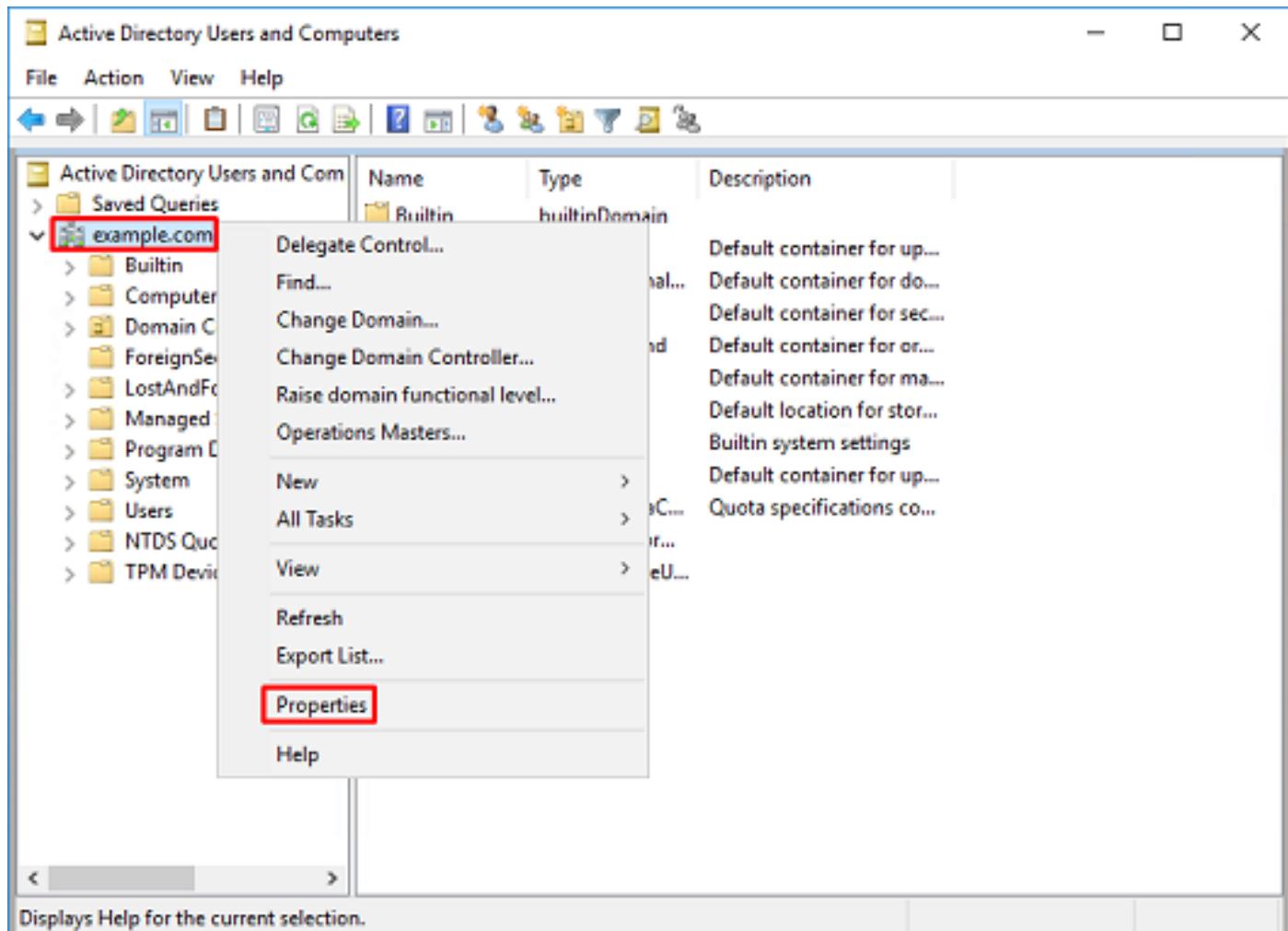
1. رتويي بمكلا ۋە حوت فملانالعىلا و مادختسم.



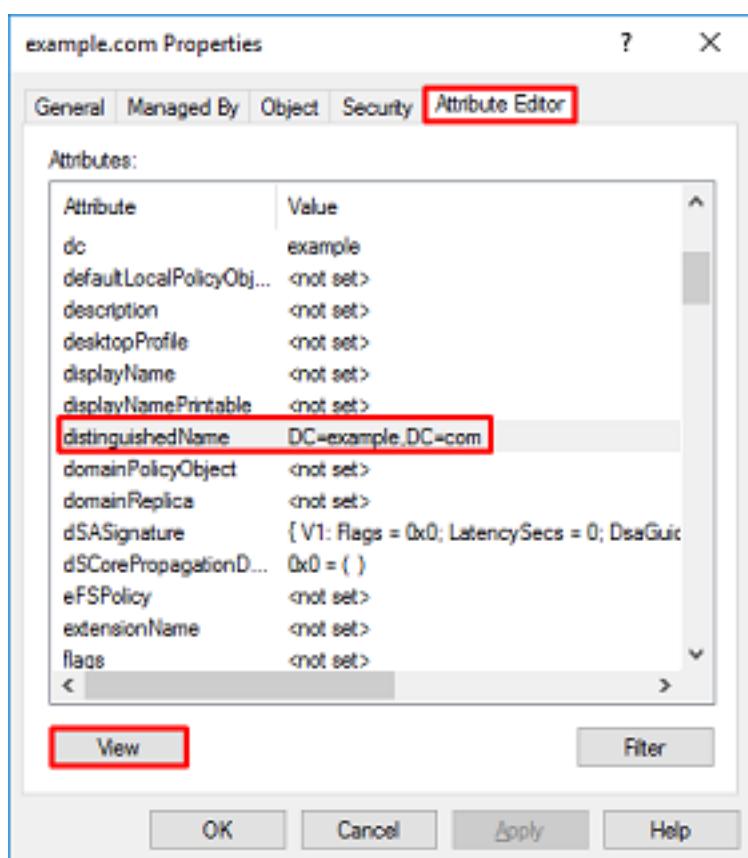
نميألا سواملا رزب رقنا مث ،(ةيواحلا حتفل) رذجلالاجملالا قوف نميألا سواملا رزب رقنا 2.
ةمدقتم تازيم قوف رقناو ضرع ىلإ لقتنا مث ،رذجلالاجملالا قوف.



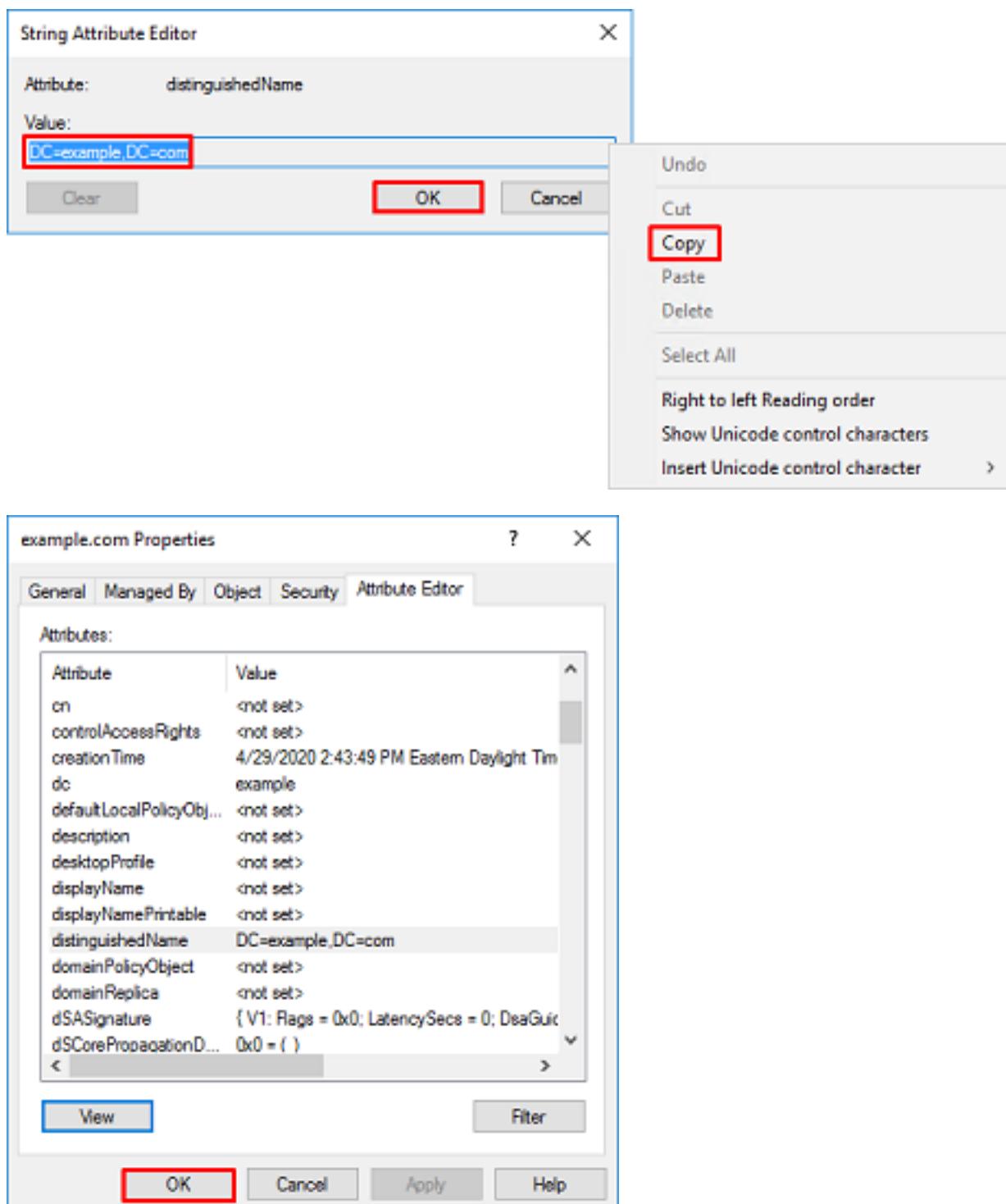
روث عل لاثملا ليبس ىلع AD تانئاک تحت ئيفاضلا صئاصخلا ضرع كلذ حيتيس. قوف نميألا سوامل رزب رقنا example.com يسيئرلا رذجلاب ئصاخلا DN ئكبس ىلع example.com مث لقتنا مث.



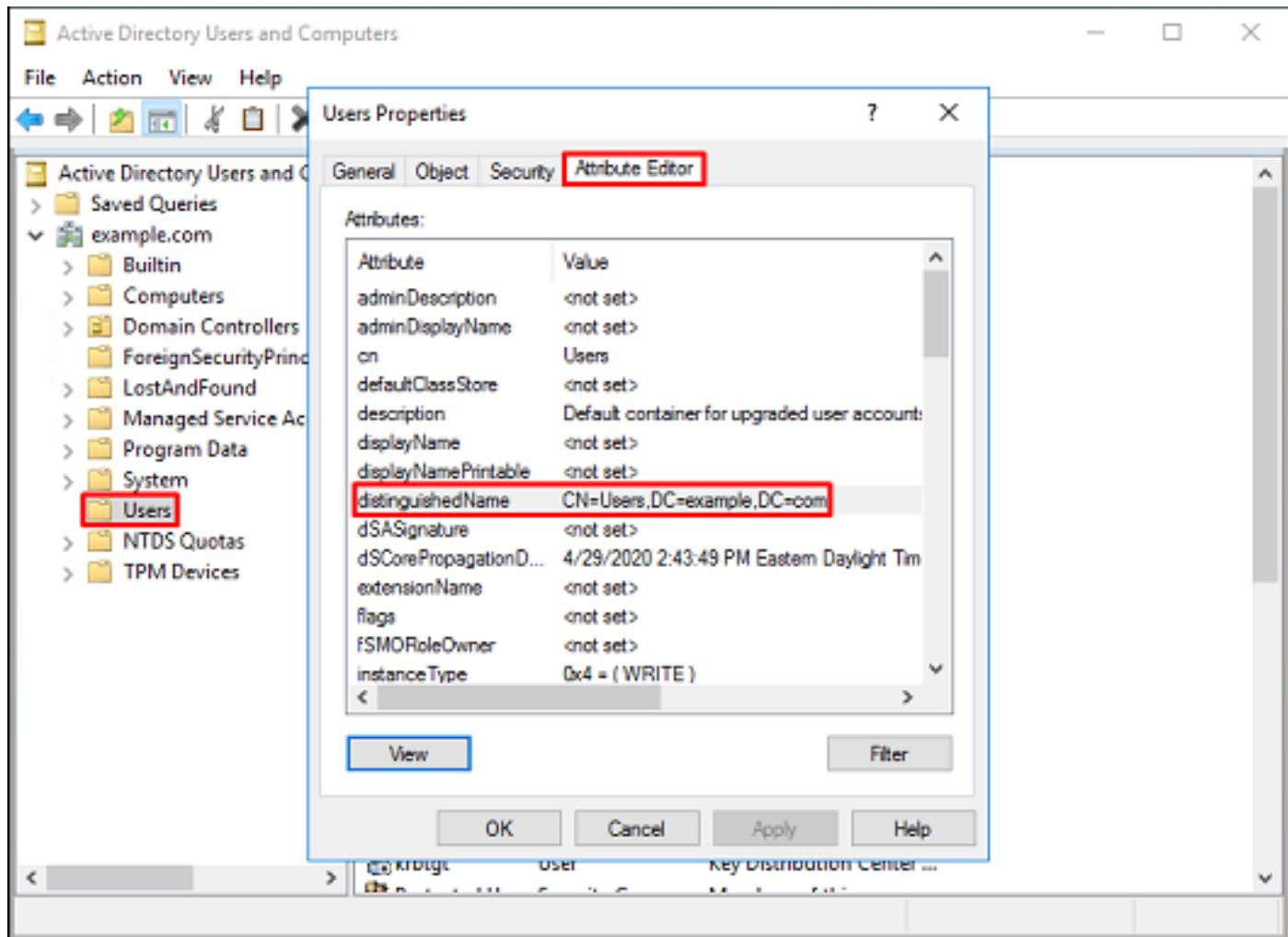
تامسلا تحت زيمم مسا نع ثحبا. تامسلا رحم بيوبتل اقامالع قوف رقنا، صياصخ تحت ضرع قوف رقنا مث.



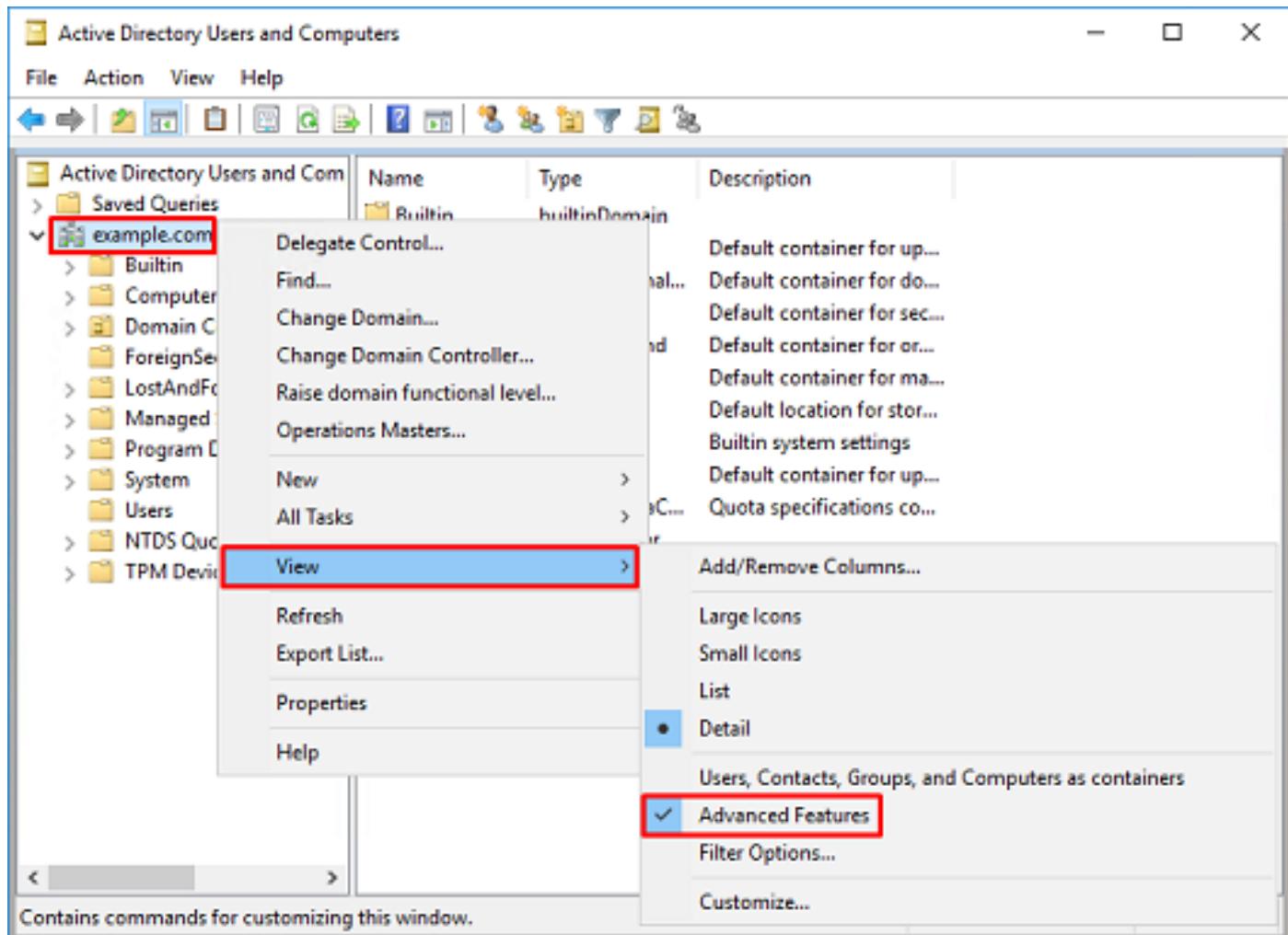
اده يف .اقحال FDM يف هقصل و DN خسن نكمي ثيح ةديج ةذفان حتف ىلا كلذ يدؤي س. نم جورخ لل **قف اوم قوف** رقنا .ةمميقلا خسن ا DN نوكى ،لاثملأا صئاصخلا نم جورخ لل ئرخأ ةرم **قف اوم قوف** رقنا او ،ةلسسلأا تامس ررحم ةذفان.



مادختسإ متى ،لاثملأا ليبس ىلع .AD لخاد ةددعتم تانئاكل ةبسنلاب كلذب مایقلا نكمي مادختسملا ةيواحصا داخل DN ىلع روطخلل تاوطلخا ھذه:



رذجلا DN ۋە كېشىلۇن نەمىيەلە سواملا رزب رقنا. ۋە مۇقتىملا تازىملا ضرعە قىيرط ئەلا زىنلىكىمى. يىخا ئەرمىمۇقتىملا تازىملا قوف رقنا او، ضرعە لە حفصىت.



باسح عاشنا FTD

نیم دختسملاء نع ثحب ل AD ع م طبارتلاب FTD و FDM ل اذه م دختسملاء باسح حمسیس حرصملاء ریغ لوصلوا عنم وہ لصفنم FTD باسح عاشناء نم ضرغلاء. مهتقا صم و تاعو مجملا و نا مزلي ال. طبرلل ڈمدختسمملاء دامتعالا تاناياب قارت خا مث اذا ڈک بشل لخادر آنا کم یلإ هب یسا سألا DN قاطن نمض باسحلا اذه نوكی.

ڈمظنمملاء ڈيوا جل اقوف نميألا سواملاء رزب رقنا، **Active Directory Users and Computers** يف 1. نمض FTD باسح ڈفاصن متنس، نيوكتلاء اذه يف. اهيل FTD باسح ڈفاصن متنس يتلا نميألا سواملاء رزب رقنا. ftd.admin@example.com. نومدختسمملاء "نومدختسمملاء" ڈيوا جل مدختسملاء > ديدج قوف رقنا مث، نيم دختسملاء قوف.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
Saved Queries
example.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users

Name Type Description

DefaultAcco... User A user account manage...

Denied ROD... Security Group... Members in this group c...

DnsAdmins Security Group... DNS Administrators Gro...

DnsUpdateP... Security Group... DNS clients who are per...

Domain Ad... Security Group... Designated administrato...

Domain Co... Security Group... All workstations and ser...

n... Security Group... All domain controllers i...

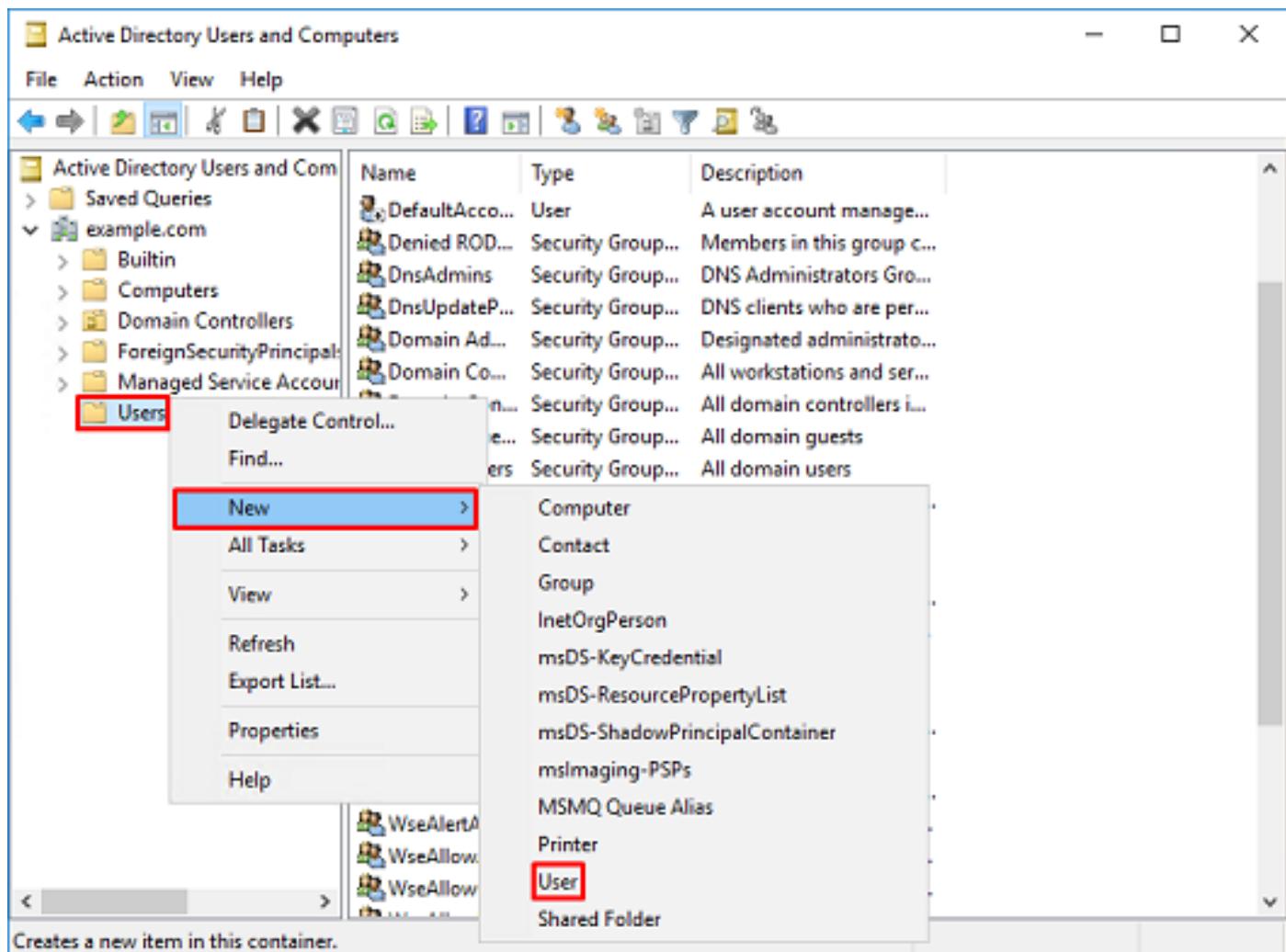
e... Security Group... All domain guests

ers Security Group... All domain users

New All Tasks View Refresh Export List... Properties Help

Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder

Creates a new item in this container.



م دختس م - ديج نئاڭ جلاغم رباع لقنتلا.

New Object - User

Create in: example.com/Users

First name: FTD Initials:

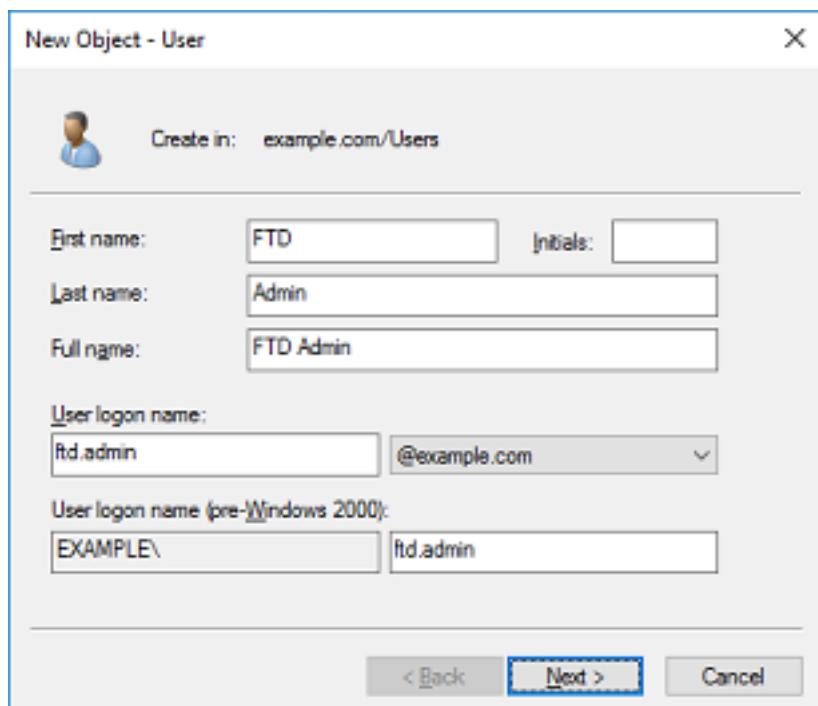
Last name: Admin

Full name: FTD Admin

User logon name:
ftd.admin @example.com

User logon name (pre-Windows 2000):
EXAMPLE\ftd.admin

< Back Next > Cancel



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

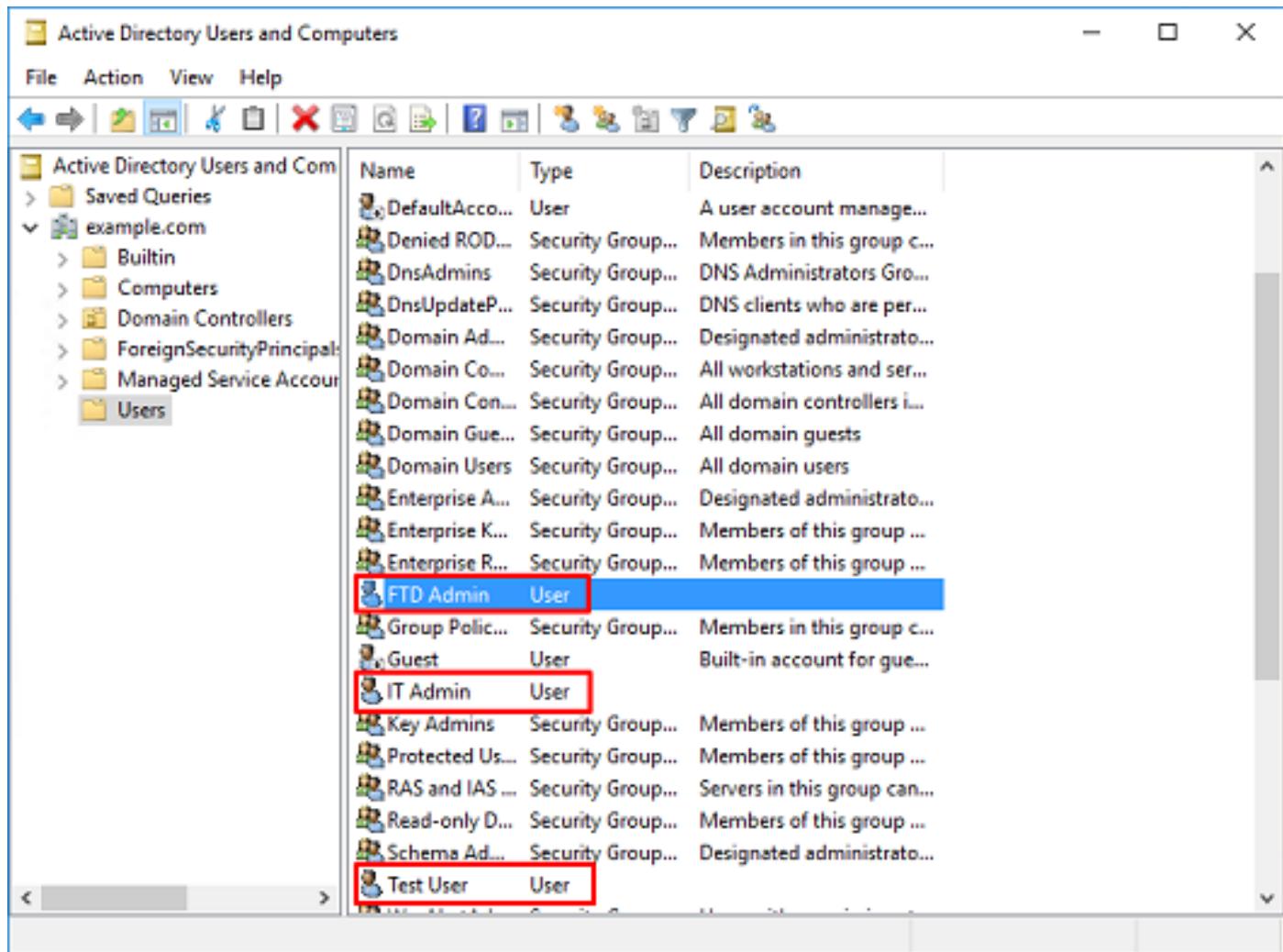
Create in: example.com/Users

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

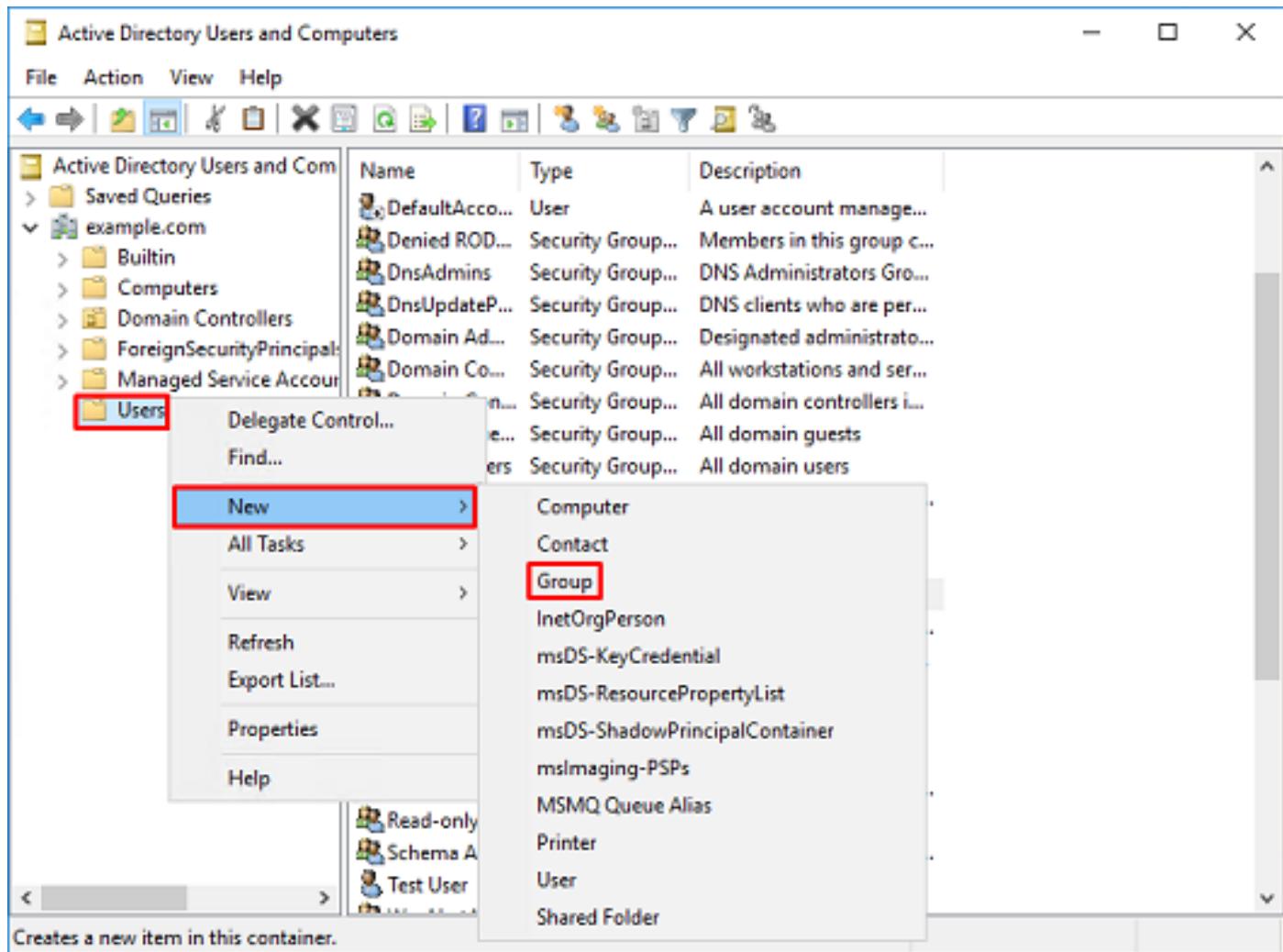
امهه، نويي فااض! نوي باسح عاشن! مهت، كل ذيل! ةفاض إلابو. FTD باسح عاشن! نم ققحت.
رآبت خالا مدخلتس مو تامولعملا ةينقت لوفسم.



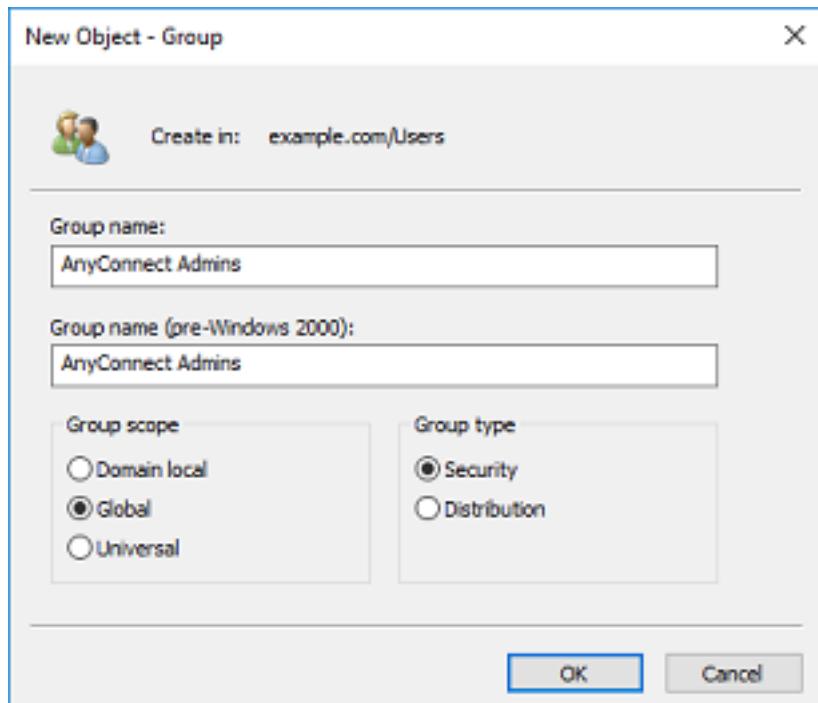
(يرايتخ) تانالع| تاعومجم ىل| نيمدختسم ۋفاض| أو تانالع| تاعومجم عاشن|

قىبىطت ليھستل تاعومجملا مادختس| نكمى، ۋەقداصلما ىل| ۋەچاھلا مدع نم مغىرلا ىلىعو نىۋەكتىلا لىلد يف LDAP. ضىيوفت ىل| ۋەفاض| إلاب نىمىدختسم ۋەدع ىلۇ لوصولاناسايىس ۋەيە لالخ نم اقحال لوصولاب مكەحتىلا جەن تادادع| قىبىطتل تاعومجملا مادختس| مەتىيىس، اذە لىخاد مادختسمىلما FDM.

ۋەسسىمۇملا/ۋەيواھلا قوف نمىيألا سوامىلا رزب رقنا، Active Directory Users and Computers، يىلۋەفسىم ۋەفاضا مەتتس، لاثمەلما اذە يف. اهىل| ۋەدىدجلا ۋەعومجملا ۋەفاضا مەتتس يىتلە قوف نمىيألا سوامىلا رزب رقنا. نىمىدختسم ۋەيواھلا نەمض ۋەعومجملا يىل AnyConnect فەرمۇنىڭ دىدجىق قوف رقنا مىث، نىمىدختسمىلما.



ةروصل اي ف حضوم و هامك ئەعومجملا - دىدجىلا نىاكلالا جلاعىم لالخ حفصىت.



3. ئەعومجم ئەم دىختسىم ئەعومجم ئاشنۇدا ئېمدىن ئەن دىكأت.

Name	Type	Description
AnyConnect Admins	Security Group...	
AnyConnect Users	Security Group...	
calo	User	Built-in account for ad...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain C...	Security Group...	Members of this group t...
DefaultAccount	User	A user account manage...
Denied RODC Passw...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only ...	Security Group...	Members of this group ...
FTD Admin	User	
Group Policy Creator...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
IT Admin	User	
Key Admins	Security Group...	Members of this group ...

نیم دختسمل (ا) مدختسمل ا ئەفاضا متىس يىتلار قۇمۇجىلار قۇمۇجىلار زىب رقنا تامولۇملا ۋىننىت لۇپسىم ئەفاضا متىس، نىيوكىتلار ازهەرىف. صىئاصىخ دەھمەت، ھەيلەرلىك دەھمەت سىپارىشىدا AnyConnect Admins و AnyConnect Users ئەفاضا متىس، نىيوكىتلار ازهەرىف. نىيوكىتلار ازهەرىف، دەھمەت سىپارىشىدا AnyConnect Admins و AnyConnect Users ئەفاضا متىس، نىيوكىتلار ازهەرىف.

Active Directory Users and Computers

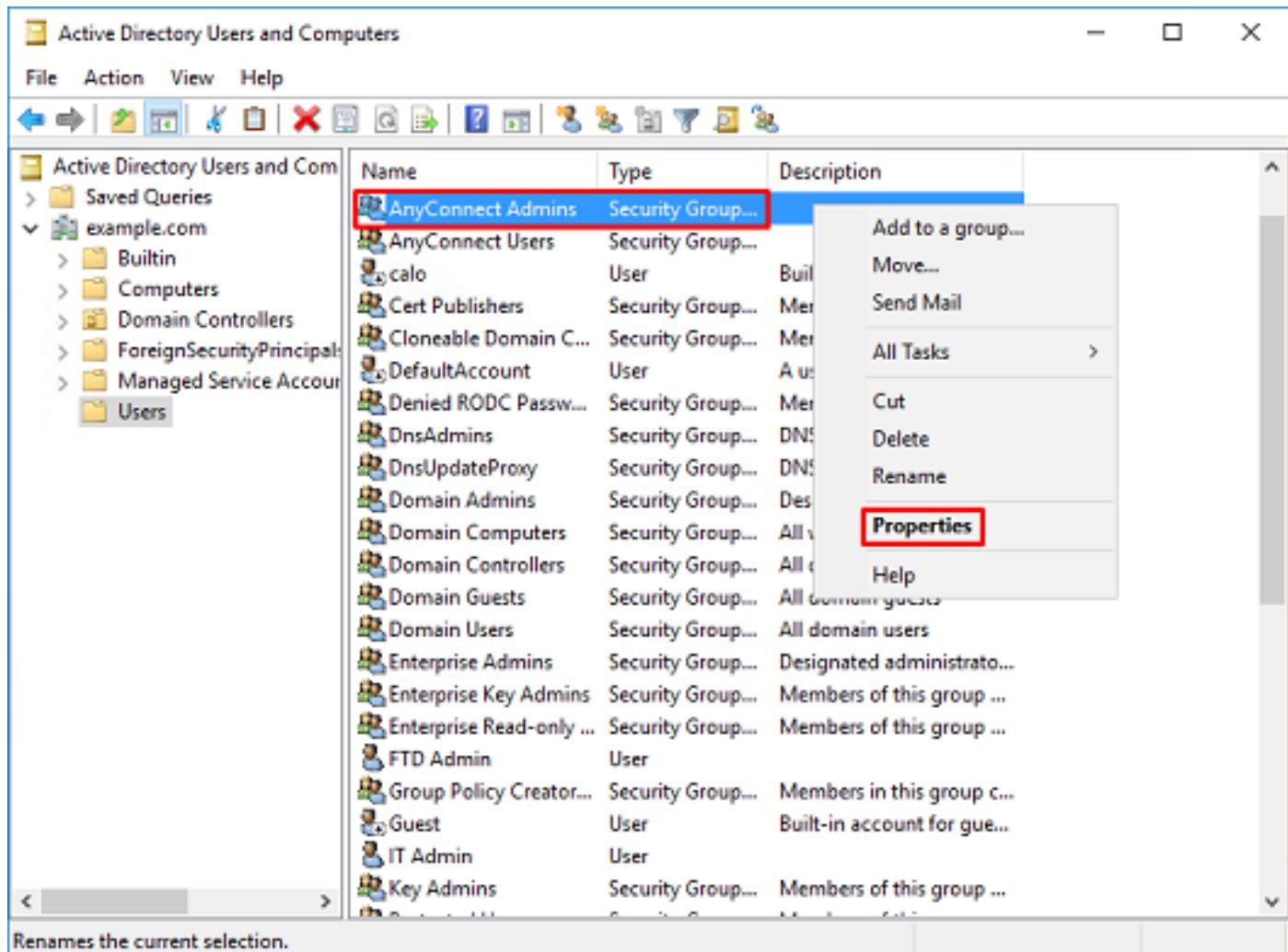
File Action View Help

Active Directory Users and Com
Saved Queries
example.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Account
Users

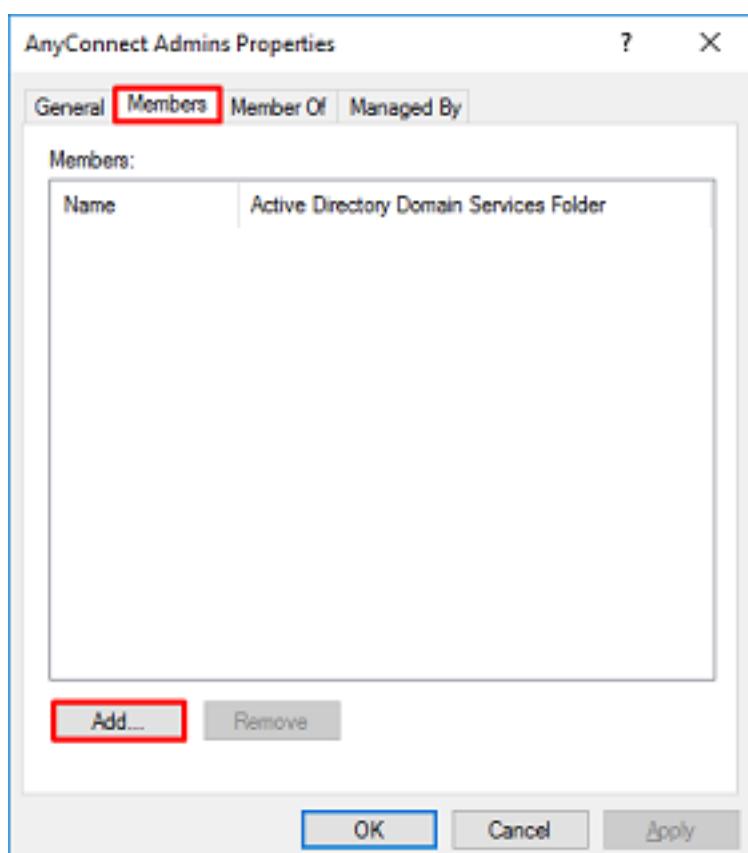
Name	Type	Description
AnyConnect Admins	Security Group...	
AnyConnect Users	Security Group...	
calo	User	Buil
Cert Publishers	Security Group...	Mer
Cloneable Domain C...	Security Group...	Mer
DefaultAccount	User	A us
Denied RODC Passw...	Security Group...	Mer
DnsAdmins	Security Group...	DNS
DnsUpdateProxy	Security Group...	DNS
Domain Admins	Security Group...	Des
Domain Computers	Security Group...	All
Domain Controllers	Security Group...	All
Domain Guests	Security Group...	All domain gues
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only ...	Security Group...	Members of this group ...
FTD Admin	User	
Group Policy Creator...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
IT Admin	User	
Key Admins	Security Group...	Members of this group ...

Add to a group...
Move...
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help

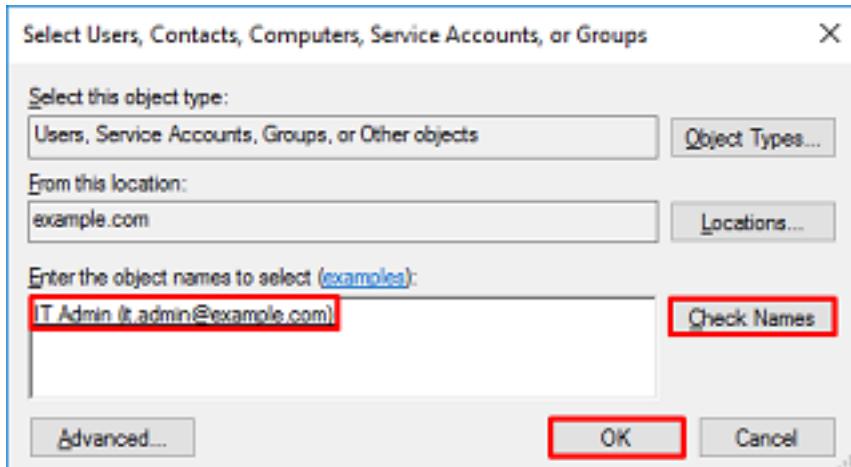
Renames the current selection.



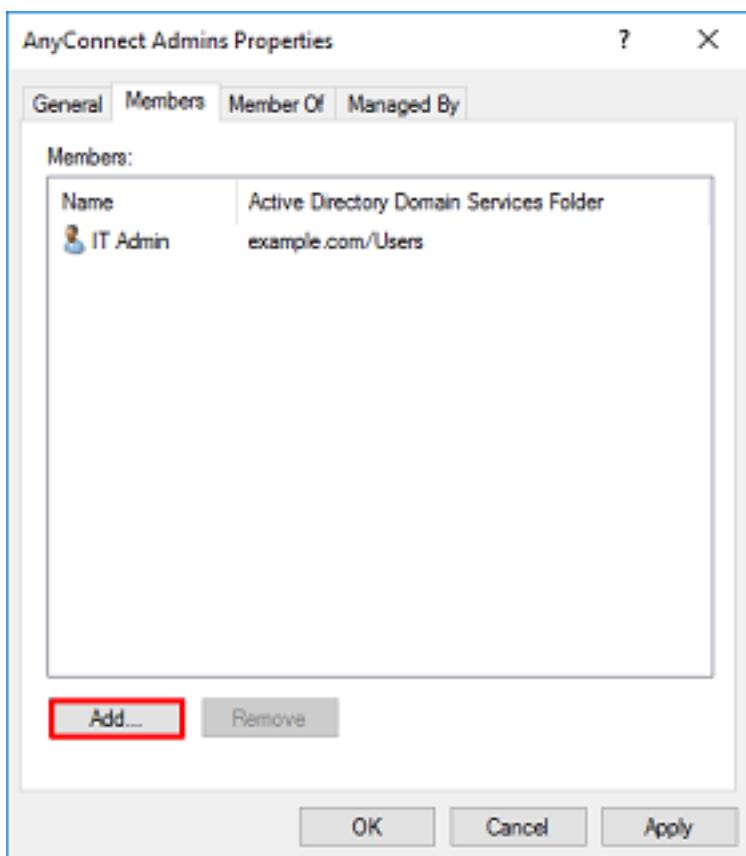
ة.روصلـا يـف حـضـوم وـه اـمـك ةـفـاضـا قـوفـ رـقـنـا مـث عـاصـعـا بـيـوبـتـلـا ةـمـالـع قـوفـ رـقـنـا.



ىلע روتعلا نم ققحتلل عامسألا نم ققحتلا رزلا قوف رقناولقحلا يف مدخلتسملالخدا ok تقطقط، ققحتلا مت نا ام. مدخلتسملال

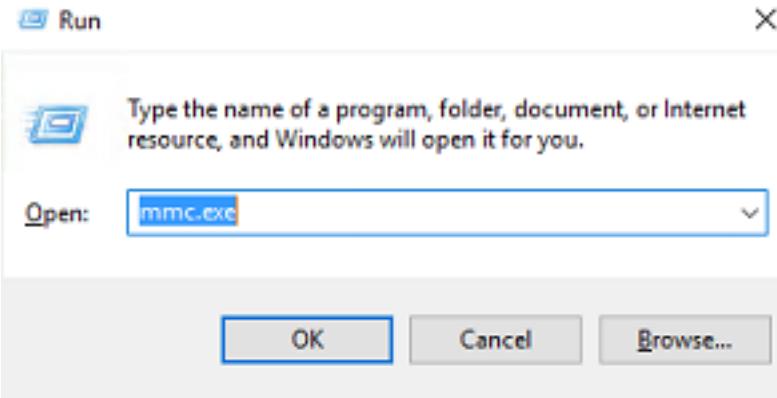


مدخلتسملالا فاضا متت امك. قفاوم رزلا قوف رقنا مت، حيحصلامدخلتسملالا فاضا نم ققحت اهسفن تاوطلخلامادخلتساب AnyConnect يمدخلتسملالا "مدخلتسملالا رابتاخا".

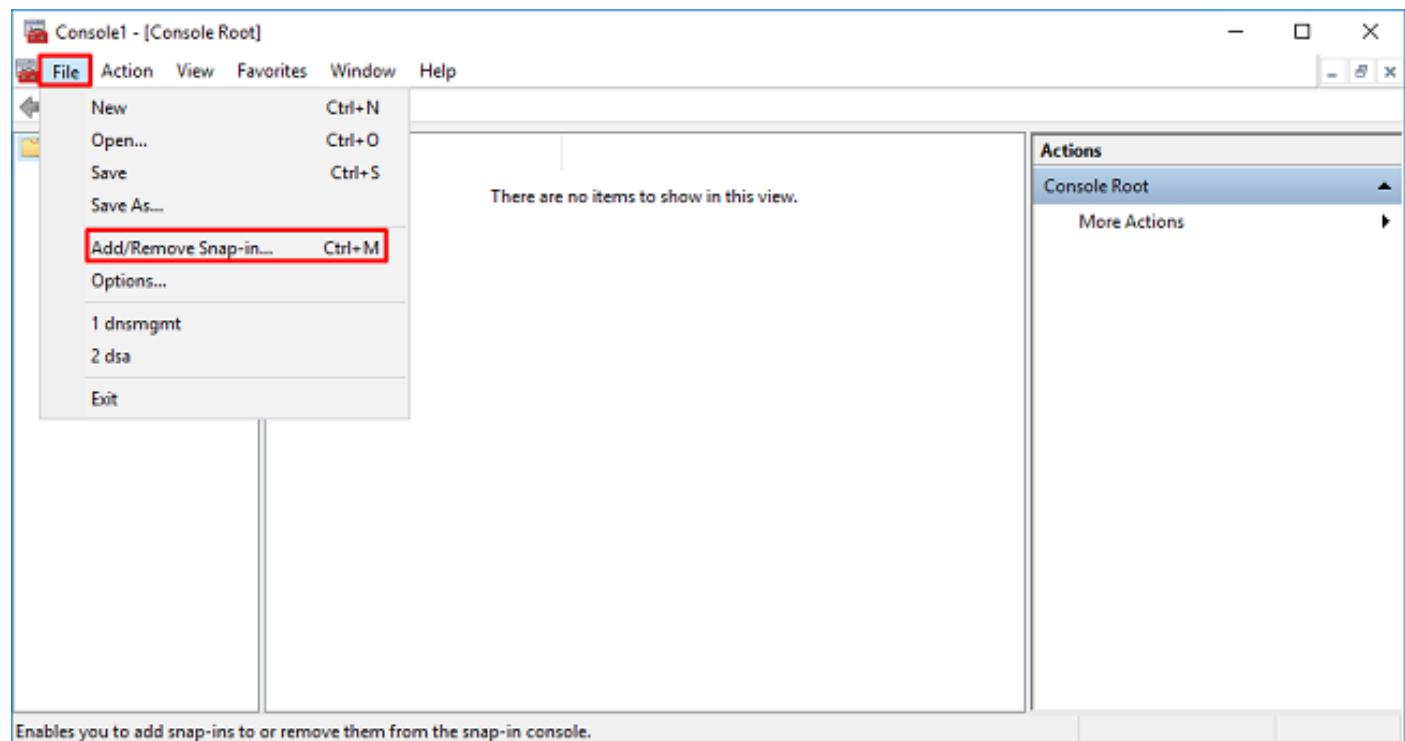


ىلع طقف بولطم) SSL لـ LDAP وـ STARTTLS) صالح LDAPs داهش رذج خسن

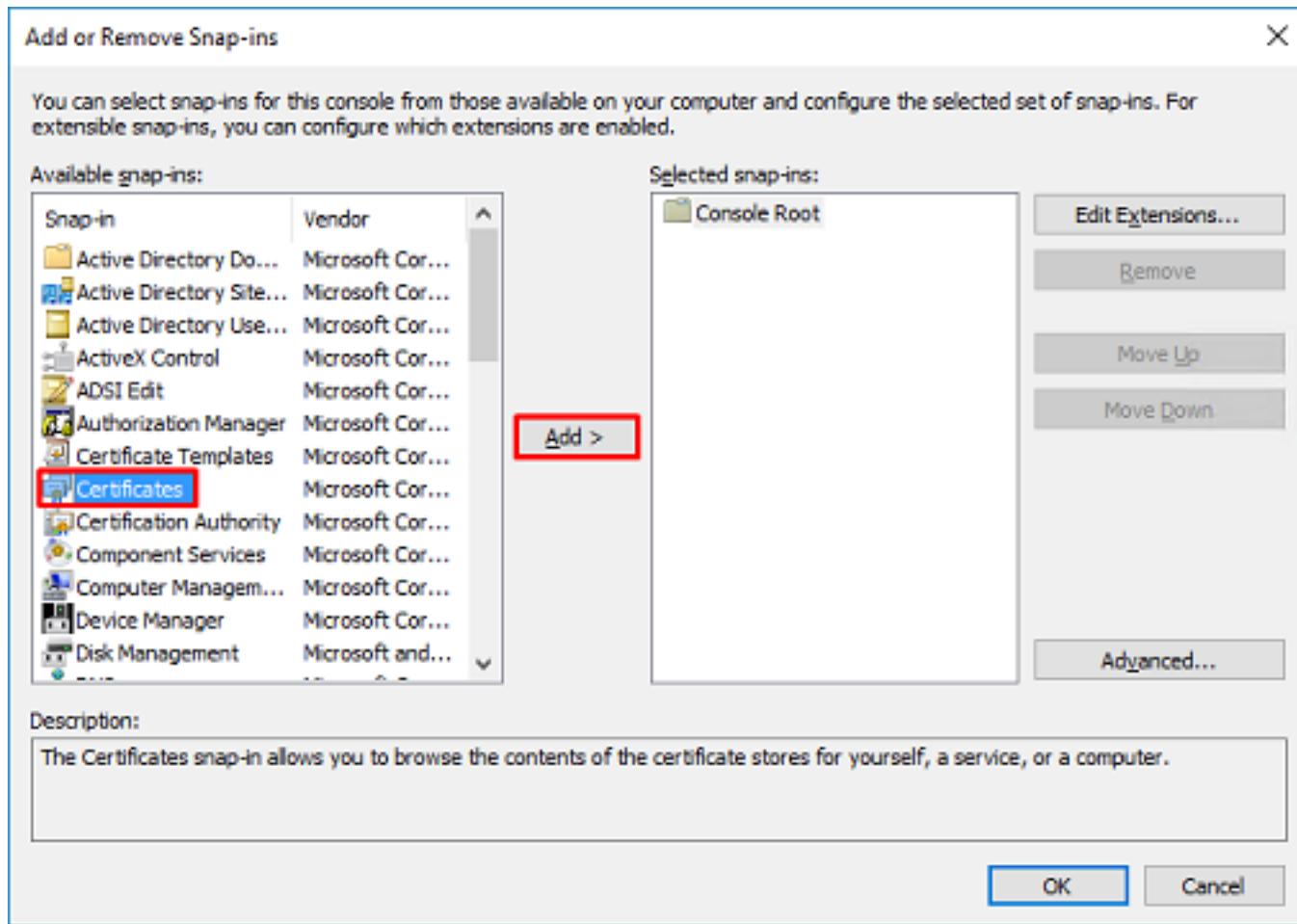
1. قوف رقناو Win+R بتكاو mmc.exe.



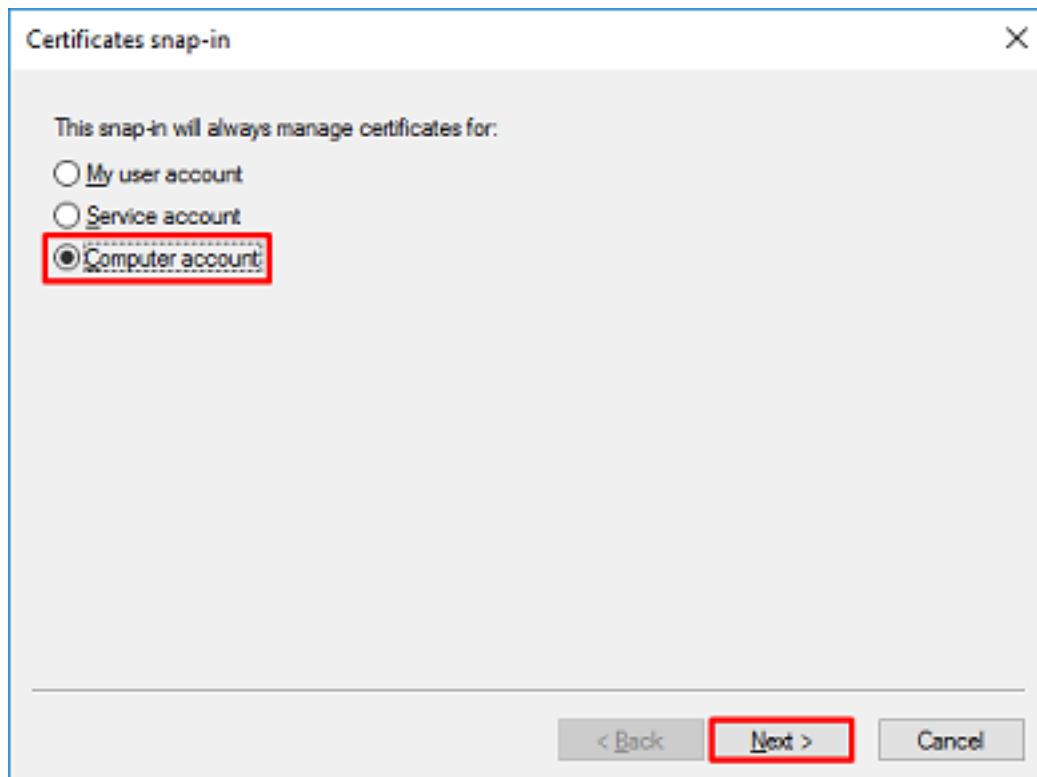
2. روصلا يف حضوم وه امك ...يفرض إلأ ةادلأا ئلانا/يفرض إلأ > فلم ئلأ لقتنا.



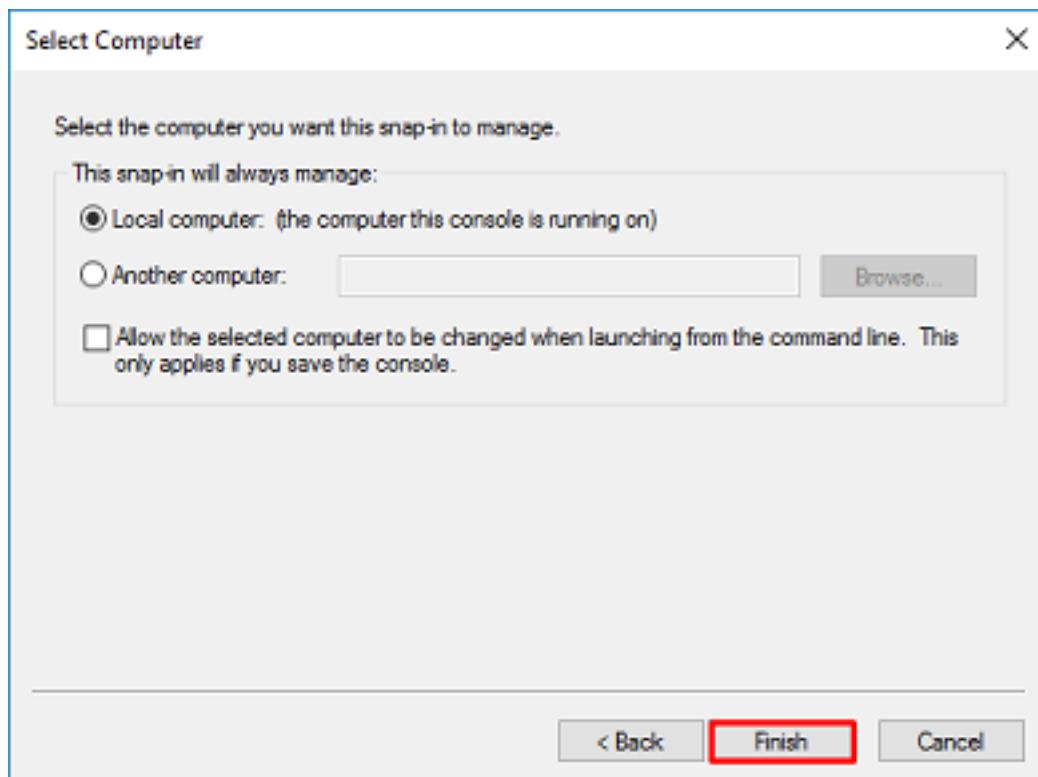
3. ةيفرض إلأ قوف رقنا مث ،تاداهشلا قوف رقنا ،ةحاتملأا ةيفرض إلأ تاودلأا تحت.



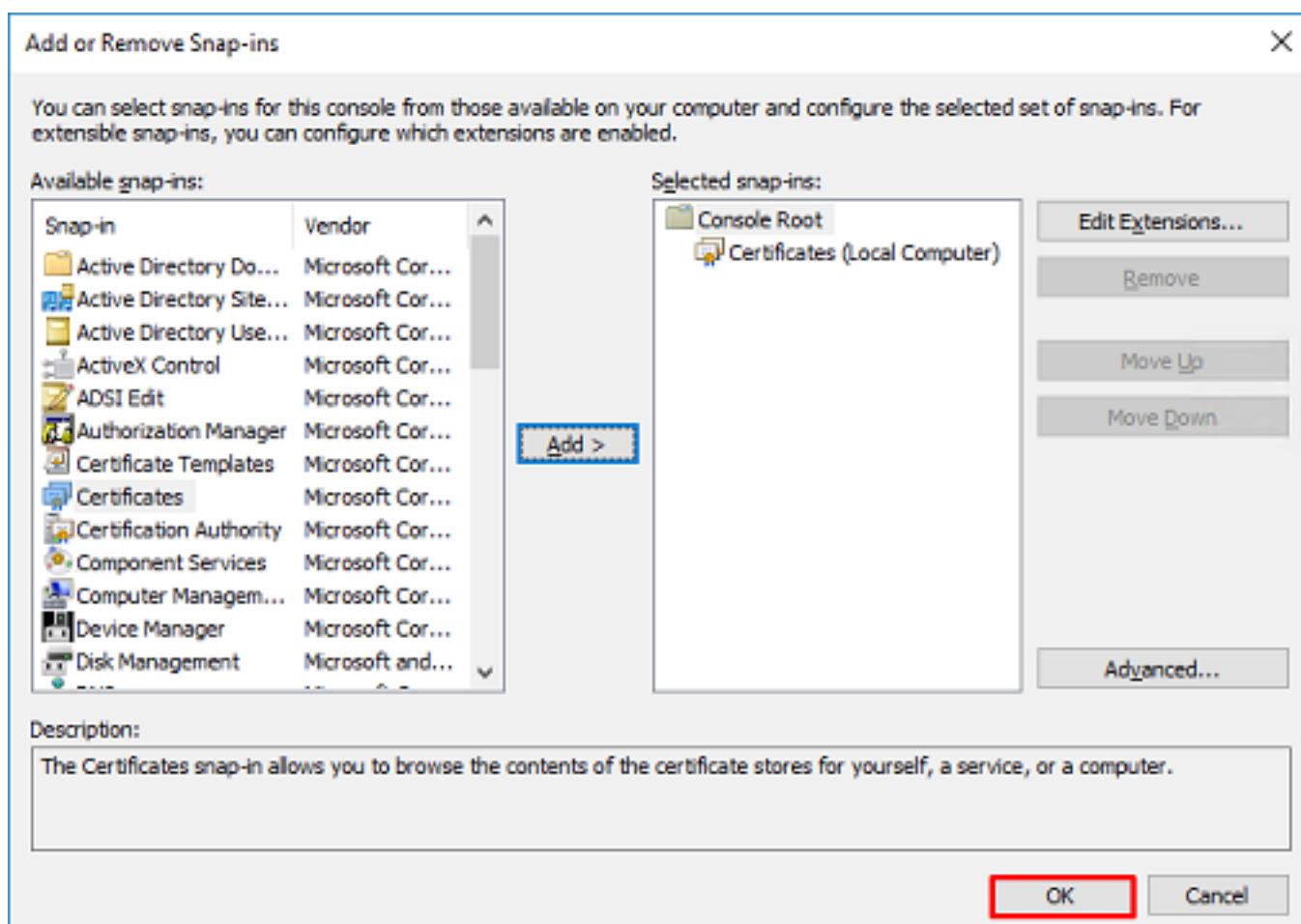
4. ۋەزىلەتلىك حىچىم وە ئامك ئىلاتلا قۇف رقنا مىت، رىت توپىب مكىلاباسىح دىدج.



عاهنە قۇف رقنا.

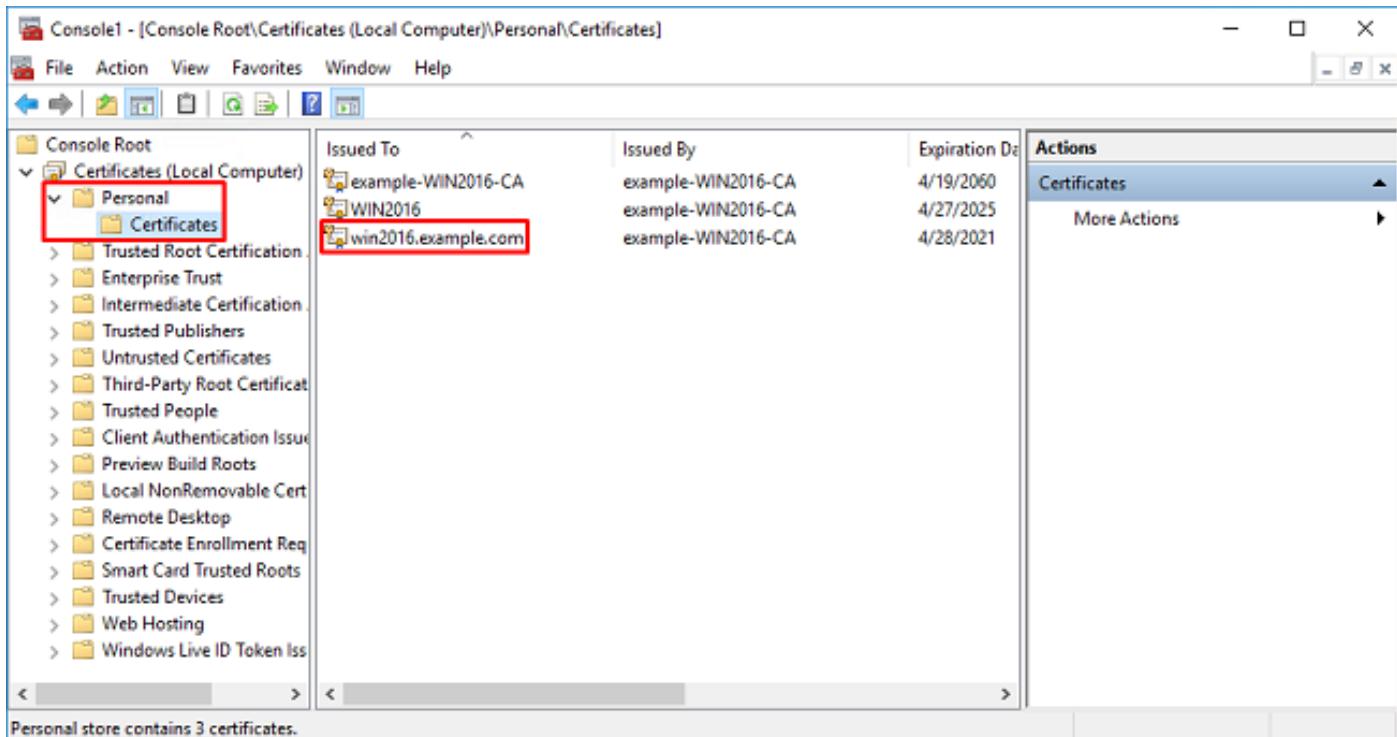


5. قوف رقنا OK.



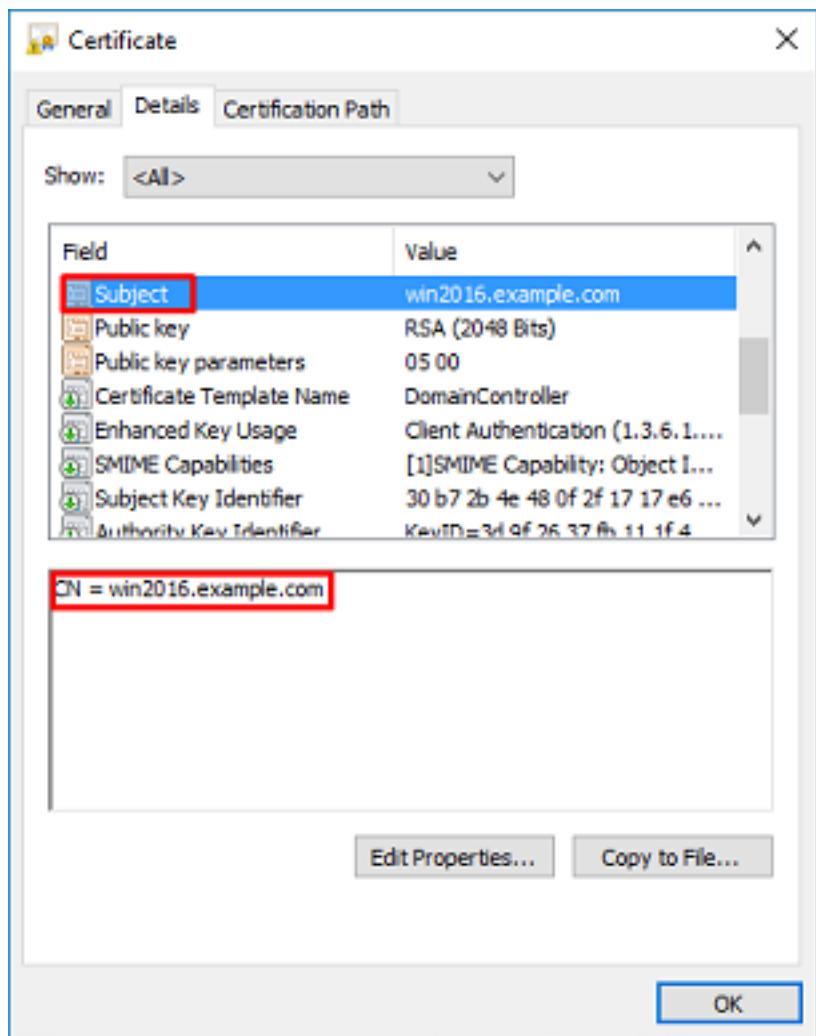
6. ةمدختسملا ةداهشلا رادصا بجي .تاداهشلا قوف رقنا مث ،يصخشلا دلجملا عيسوت بمـق .3 دجوي Windows .LDAPs لـمـاـكـلـابـ صـاخـلـاـ (FQDN)ـ لـاجـمـلـاـ لـهـفـمـلـاـ مـسـاـ ئـلـىـ مـداـخـلـاـ اـذـهـ لـعـ جـرـدـمـ تـادـاهـشـ .

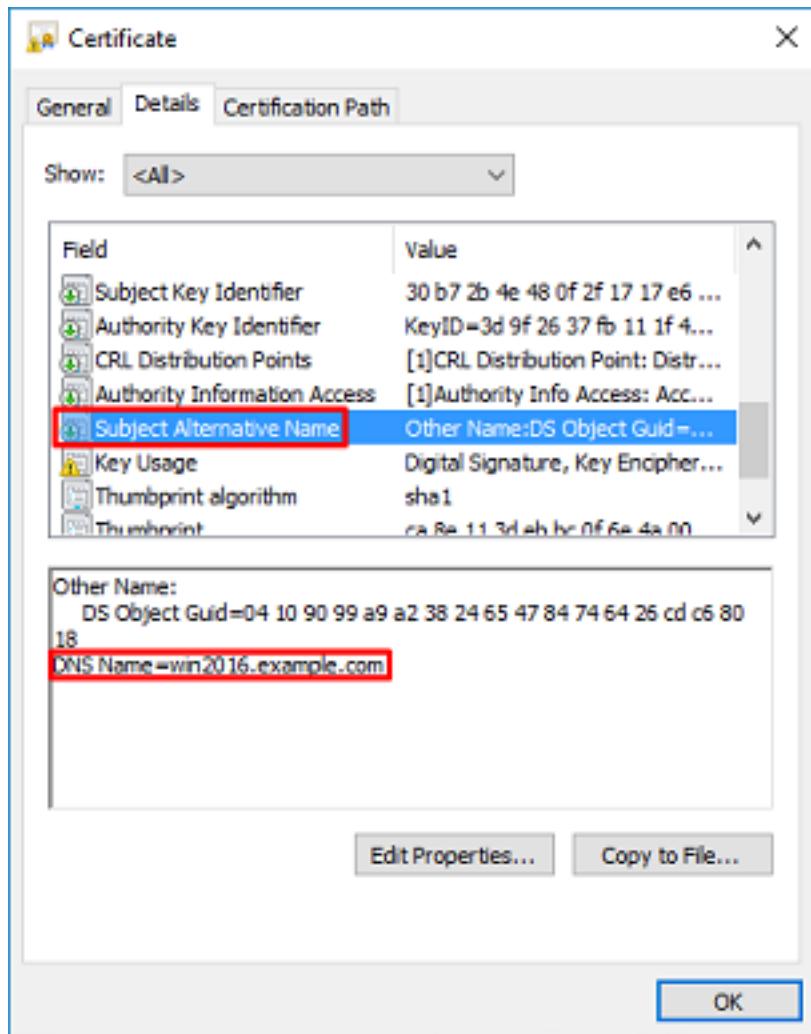
- لاثمل او لىا ئرداصل قىدىمىن عەجم ئەدەش WIN2016-CA.
 - لىغۇشلى ماظىنل ئرداصل ئىوه ئەدەش Win2016 ئەطس اوپ example-WIN2016-CA.
 - لىغا ئەدەش ئىلار ئەن ئەدەش ئەن ئەدەش win2016.example.com ئەطس اوپ example-win2016-ca.
- ىلولى تاداهشلى نإف يەلاتلىبو، اذە نېوكتلا لىيلدىف ىللا اهراصلما مەت يەتلە ئىوهلا ئەدەش LDAP SSL. ىللا اهراصلما مەت يەتلە ئىوهلا ئەدەش win2016.example.com يەن ئەدەش لىق دىمىلما عەجملىم ئەمدىخ ئەطس اوپ ايئاقلەت اهراصلما مەت ئەدەش يەن Windows Server. لىصافتلا نەم قىقەتلىل ئەدەشلى رقنى رقنى.



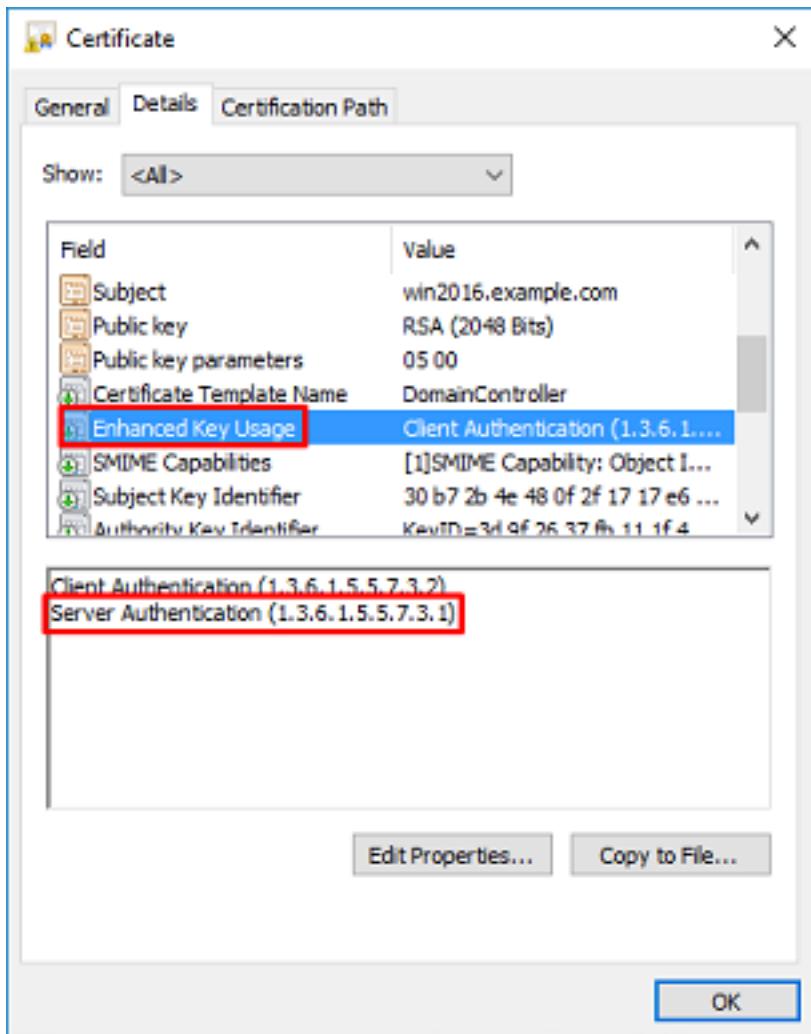
7: تابلىتلىل ئەدەشلى يەفوتسىن ئەمداختسا لىجأ نەم:

- مەدەب سەخلى FQDN عوضوملىكىيلىدىبلا مەسالا واعىاشلى مەسالا قىباشتىي Windows.
 - نەسەحملە حاتفەملە مەداختسا لىقەنەمىز مەداخلىا ئەقداصل ئەدەشلى يەوتختى.
- نېكىي، لىدىبلا عوضوملىكىيلىنىڭ ئەدەشلى ئەن ئەدەش ئەن ئەدەش ئەن ئەدەش FQDN win2016.example.com تەختى.

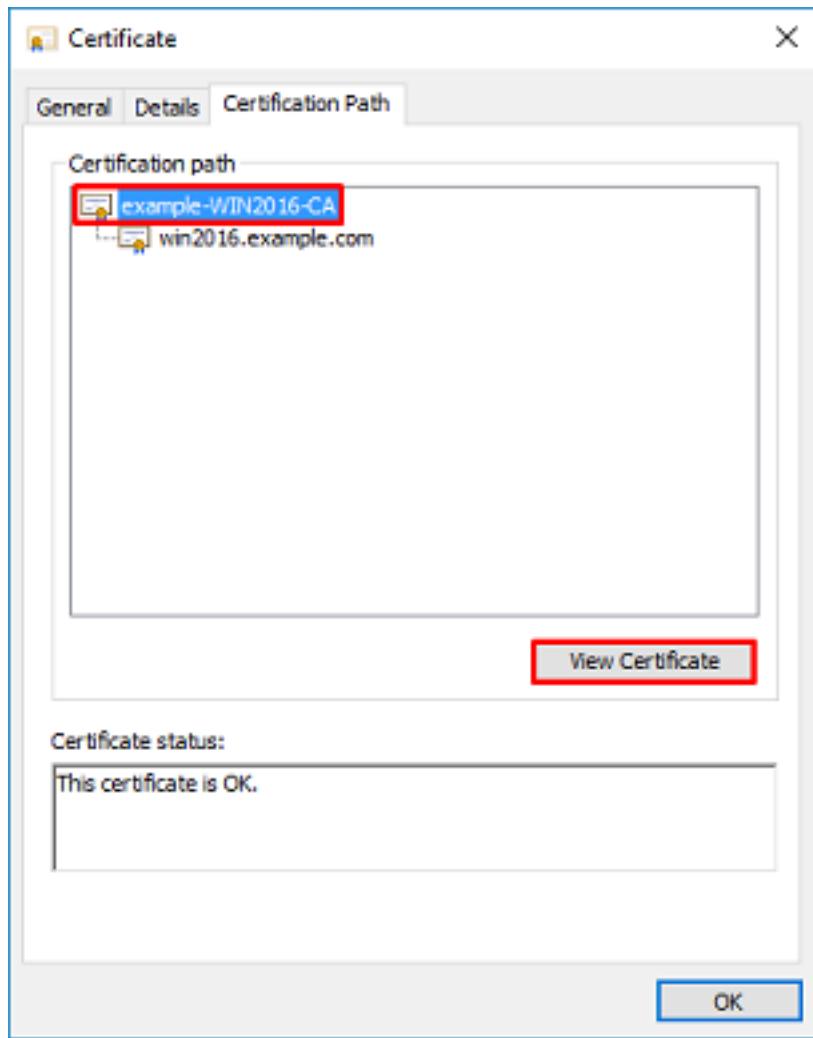




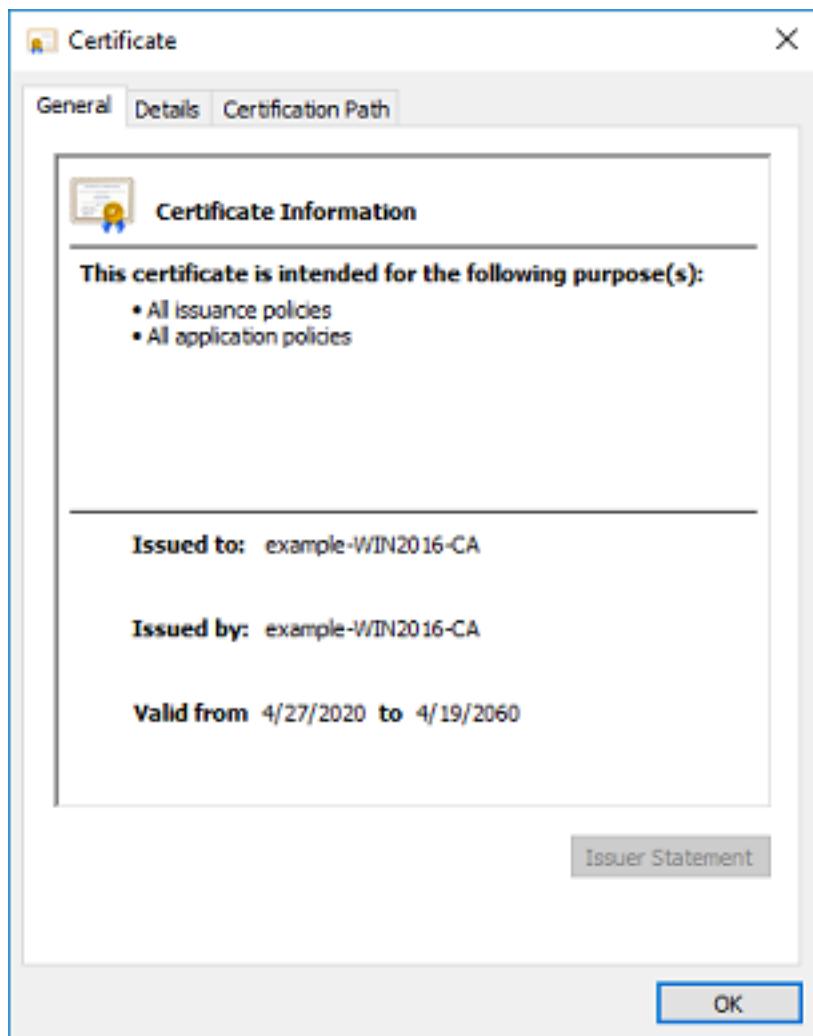
مداخلاً قداصم دجوت، حيث افملل نسحمل ما دختس الا تحت



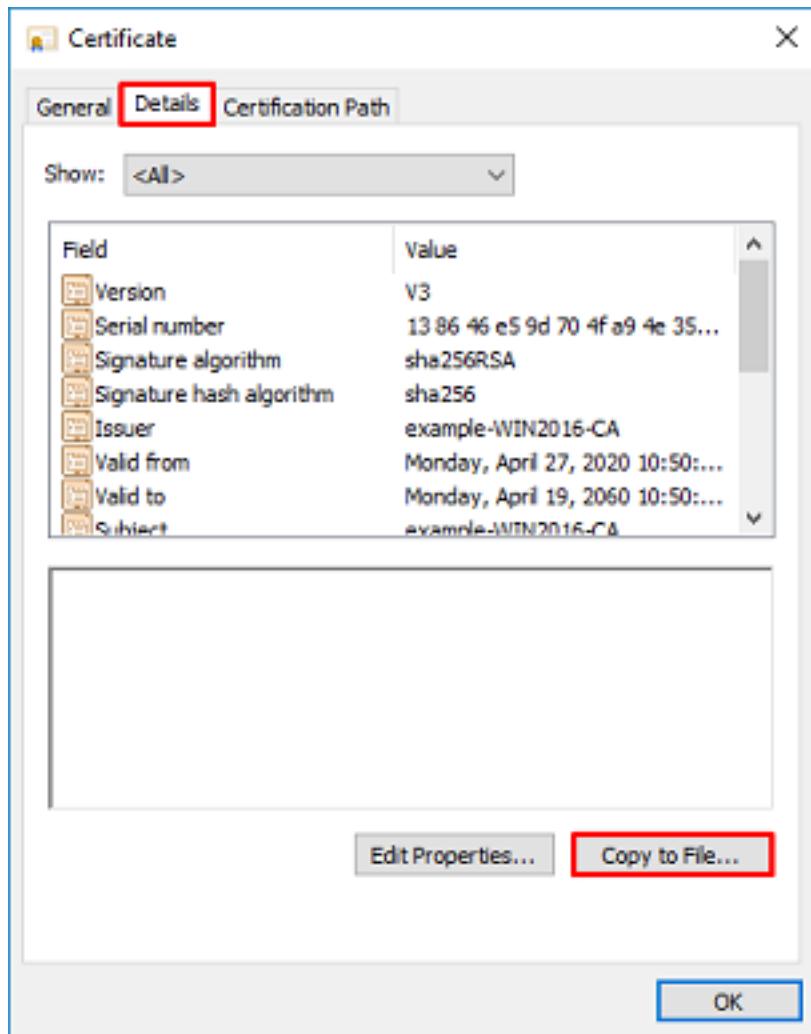
ةداهشلا قوف رقنا . دامت عالا راسم بي و بتل ا ظمالع ىل ا لقتنا ، كلذ نم دكأ تل ا درج مب .
ةداهشلا ضرع رزىل ع رقنا مث ، رذجل ا قدص مل ا ع جرم ل ا ةداهش نوكت نأ بجي ي يتل ا اي لعل ا



رذجل ا قدص ملأ عجرمل ا ئدابهش ل ا ليص افت حتف ئىلا كىل ذي دؤيىس.



يەھىچوم وە امك ...فلم ىلإ خسن قوف رقنا مث ليصافت بىوبتلا ۋەممالۇ حەتفا 10. ۋەرسىلى.



11. PEM قيسمتىب رىجىلا قدصىمىلا عجمىلدا رىدىصت جىلاعىم رباع لقتنىا.



← Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next

Cancel

12. دفع Base-64 لـ X.509.



← Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

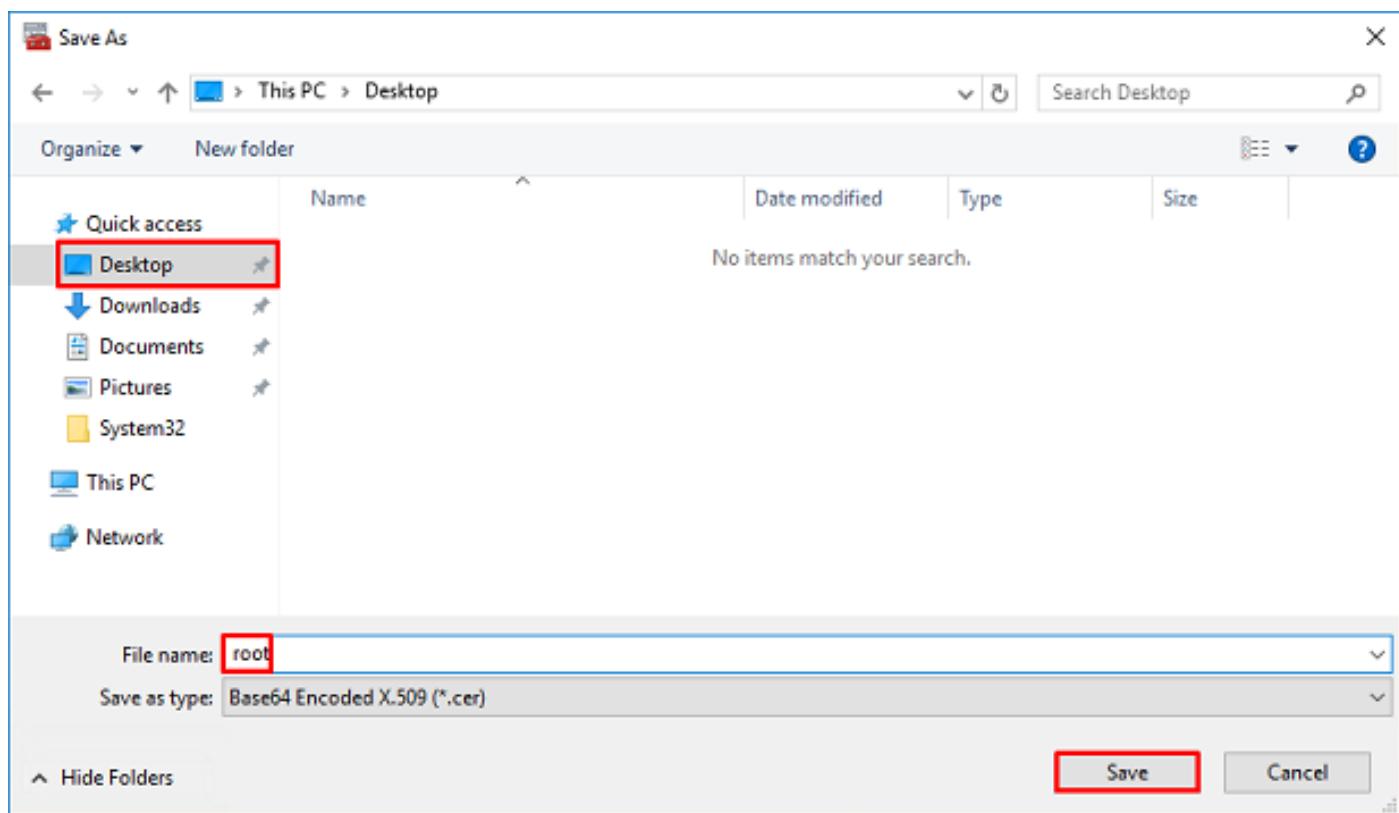
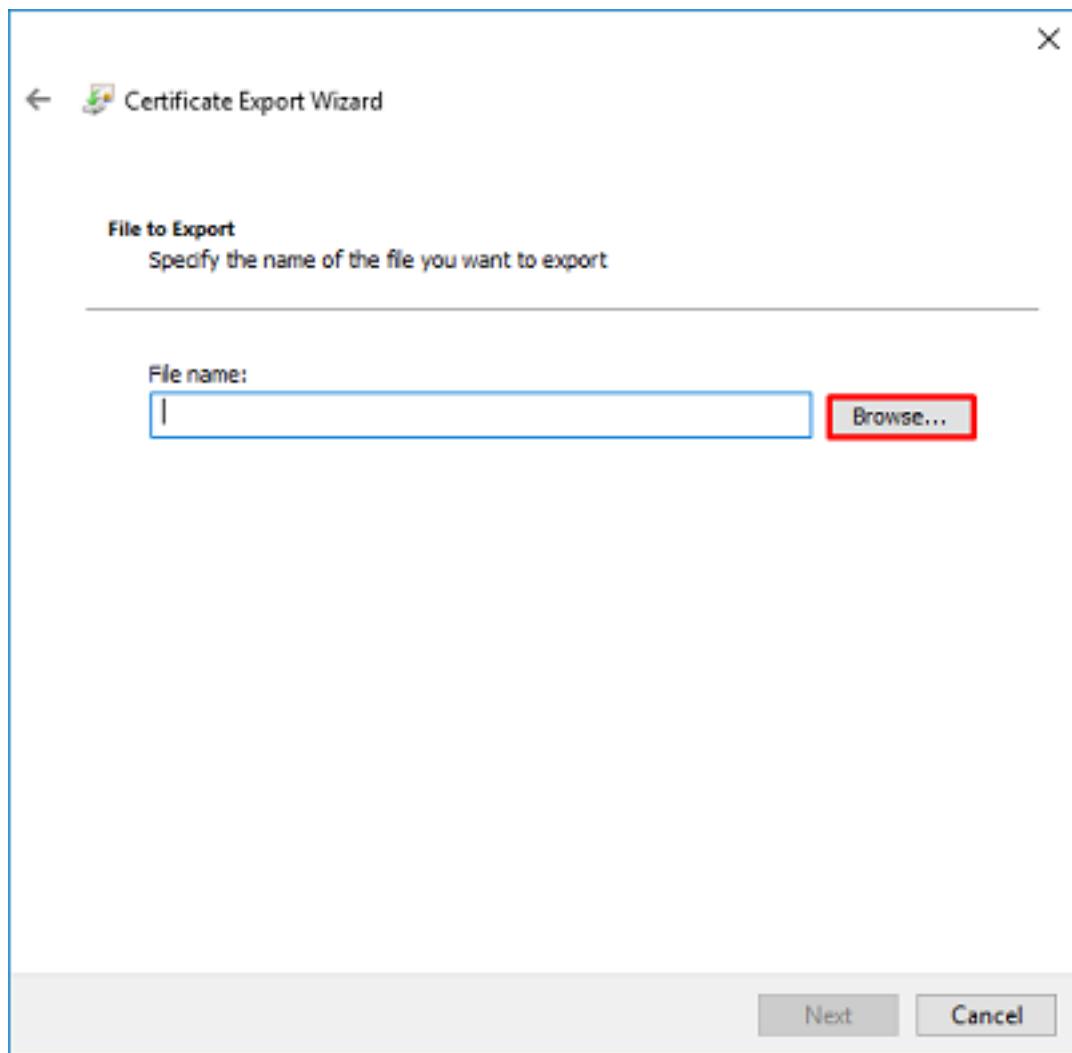
Select the format you want to use:

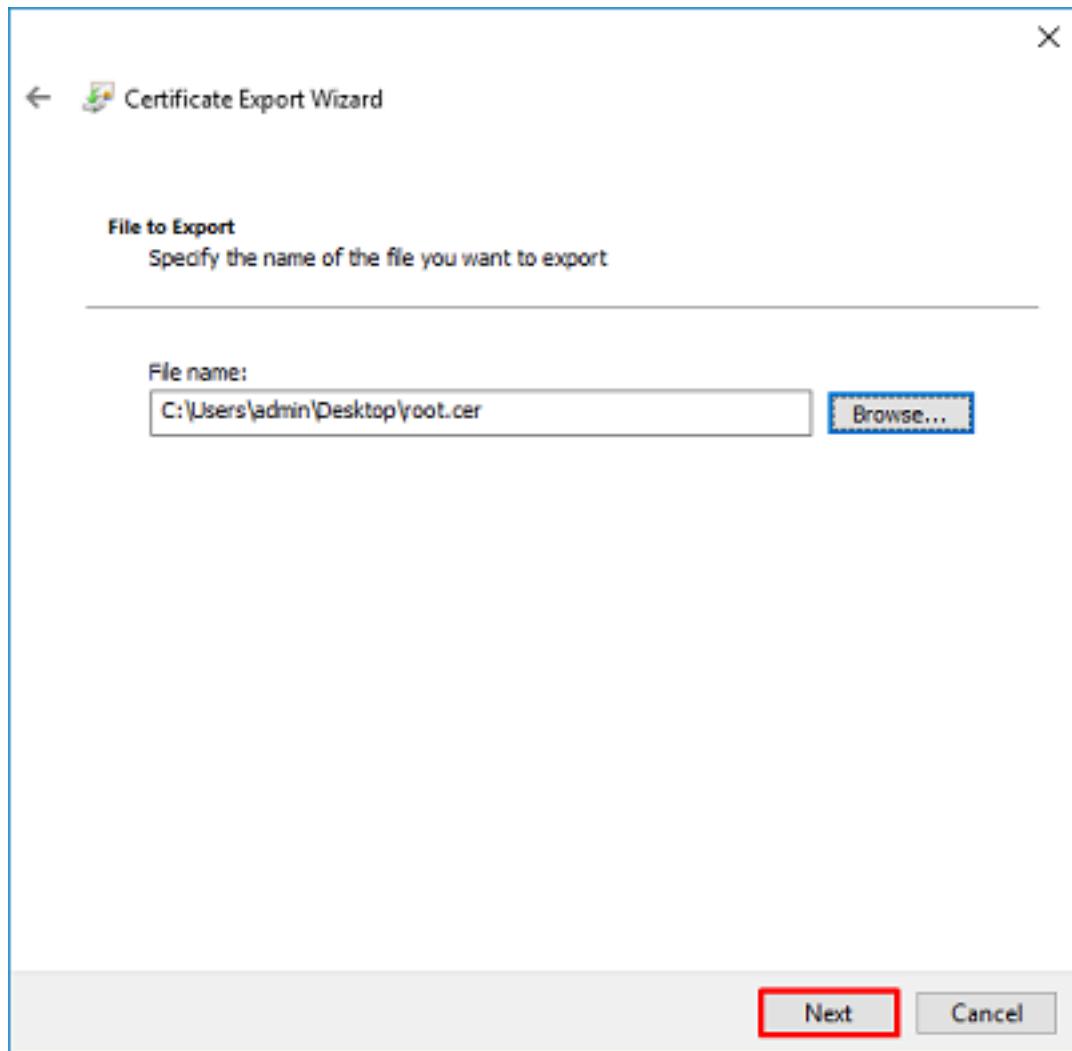
- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
 - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

Next

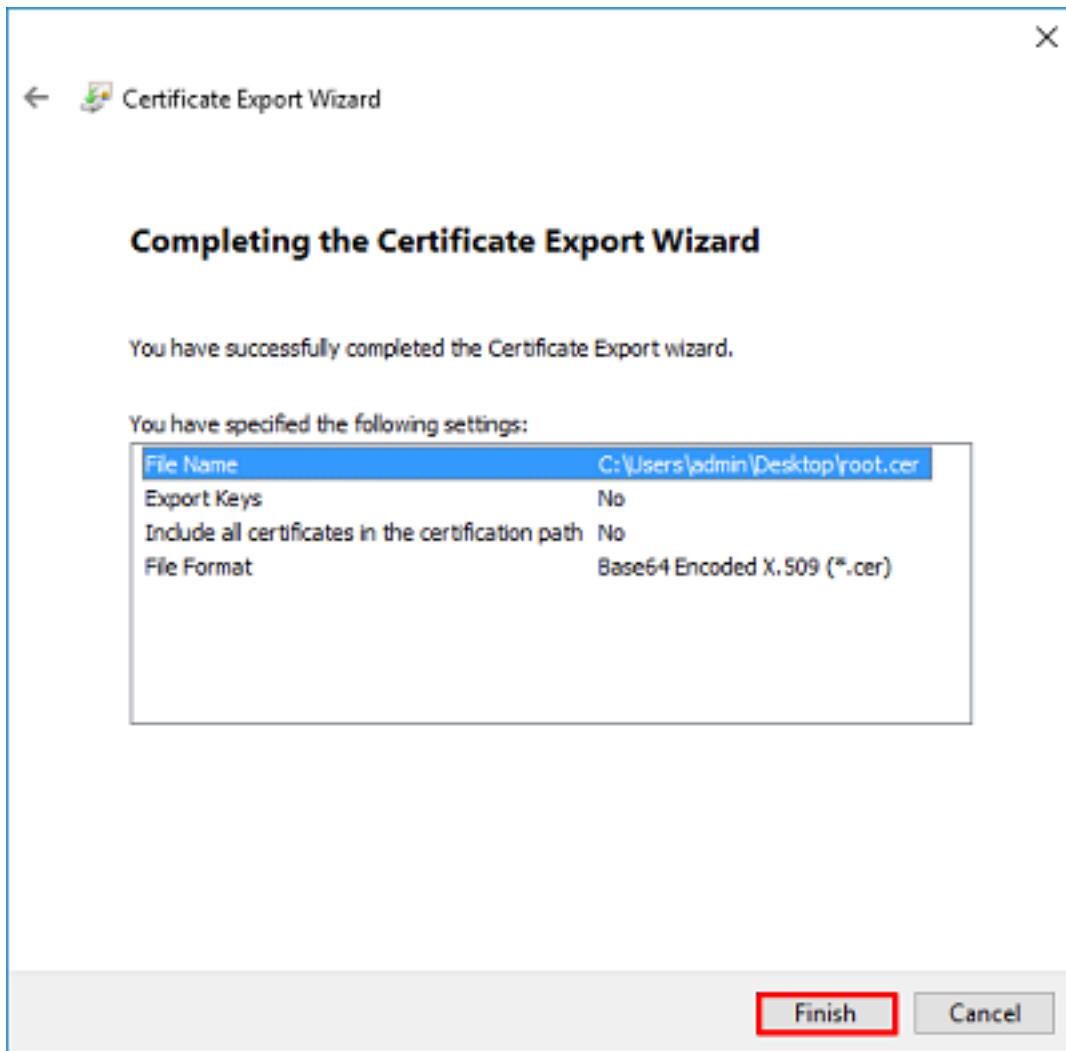
Cancel

13. ددح مسا فلملأا نيأو متييس دري دصت ليلإ.





عاهن| قوف رقنا. 14.



رهظیس .رخ آ صوصن ررحم یا و ا ئركفم مادختساب ۋەداھشلا حتفاوعقۇملا ىلى لقتنا ،نآل او 15. قحال تقول ادھ ظفحى PEM. قىسنتب ۋەداھش ادھ.

-----BEGIN CERTIFICATE-----
MIIDCDCCAFBgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJ1eGFtcGx1LVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBqNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVKEKSGoY+v940S23161zdwReMOFhgbc2qMertiOficrRhihonuu
Cjyeub3CO+meJUUKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPum
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHW1RnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPPfMA3u8C
AwEAAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIxW2dTsjenAEt7r
phFIHZoCoSyjbjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscbubR1+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFFQV3DgZg+R96
9WLKR3Obig6xyo9Zu+1ixcWpdrbADO6zMhbEYEHkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----

تاني وكت FDM

صيخرتلا نم ققحتلا

بجي و يكذلا صيخرتلا مدادع ليجستلا ايل FDM، اتحيس FTD جاتحيس، ايل AnyConnect FDM، ايل اپيکس Plus، او ايل اپيکس Apex، او ايل اپيکس VPN.

رةوصلا يف حضوم و امك يكذلا صيخرتلا > زاهجلا ايل لقتنا.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3 admin Administrator

Inside Network

Cisco Firepower Threat Defense for V...

0/0 0/1 0/2

MGMT CONSOLE

Internet

DNS Server

NTP Server

Smart License

Interfaces

Connected Enabled 3 of 4

View All Interfaces

Smart License Registered

View Configuration

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

وا AnyConnect Plux او Apex او VPN طقف حضوم نيكتمت نمو يكذلا صيخرتلا مدادع ليجست نم قيقحت.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3 admin Administrator

Device Summary

Smart License

CONNECTED SUFFICIENT LICENSE Last sync: 16 Apr 2020 08:27 AM Next sync: 16 Apr 2020 08:37 AM Go to Cloud Services

SUBSCRIPTION LICENSES INCLUDED

Threat

Malware

URL License

RA VPN License

دانالعالا ئيه وه ردهنم دادعا

يف حضوم و امك AD ددحو زمرلا + قوف رقنا مث، ئيه وهلا رداضم > تانئاك ايل لقتنا.

ةروصلـا.

The screenshot shows the Firepower Device Manager interface. The top navigation bar includes 'Firepower Device Manager', 'Monitoring', 'Policies', 'Objects' (which is highlighted with a red box), and 'Device: FTD-3'. The right side shows the user 'admin' and 'Administrator'. The left sidebar under 'Object Types' has 'Identity Sources' selected (also highlighted with a red box). The main content area is titled 'Identity Sources' and shows a table with one row: '1 object'. The table columns are 'NAME', 'TYPE', and 'VALUE'. The single entry is 'LocalIdentitySource' with 'LOCAL' in the TYPE column. To the right of the table is a context menu with options: 'RADIUS Server', 'RADIUS Server Group', 'AD' (which is highlighted with a red box), and 'Identity Services Engine'. A search bar at the top right says 'Search'.

تقـوـيـفـ اـعـيـمـجـتـ مـتـ يـتـلـاـ تـامـولـعـمـلـابـ Active Directoryـ مـداـخـلـ ئـبـسـانـمـلـاـ تـادـادـعـلـاـ أـلـمـاـ. نـمـ دـكـأـتـفـ ، IPـ نـاوـنـعـ نـمـ الـدـبـ Microsoftـ مـداـخـلـ (FQDN)ـ فـيـضـمـلـاـ مـسـاـ مـادـخـتـسـاـ مـتـ اـذـاـ. قـبـاسـ هـذـهـ DNSـ ئـعـوـمـجـمـ قـيـبـطـبـ مـقـ مـثـ. DNSـ ئـعـوـمـجـمـ > تـانـىـاـكـلـاـ تـحـتـ ئـبـسـانـمـ ئـعـوـمـجـمـ عـاشـنـاـ ھـجـاـوـ تـحـتـ DNSـ ئـعـوـمـجـمـ قـيـبـطـ، DNSـ مـداـخـ > مـاـظـنـلـاـ تـادـادـعـ > زـاهـجـلـاـ ىـلـاـ لـاقـتـنـالـاـبـ ىـلـعـ رـزـ قـوـفـ رـقـنـاـ. تـامـالـعـتـسـالـ ئـبـسـانـمـلـاـ جـوـرـخـلـاـ جـوـرـخـلـاـ ھـجـاـوـ دـدـحـ مـثـ، تـانـاـيـبـلـاـ ھـجـاـوـ وـرـادـإـلـاـ ذـهـ نـأـ اـمـبـ. FTDـ ھـرـادـإـ ھـجـاـوـ نـمـ لـوـصـوـلـاـ ھـيـنـاـكـمـاـوـ نـيـوـكـتـلـاـ حـاجـنـ نـمـ قـقـجـتـلـلـ رـابـتـخـالـاـ يـتـلـاـ ھـيـجـوـتـلـلـ ۋـلـبـاـقـلـاـ تـاهـجـاـوـلـاـ ىـدـحـإـ لـالـخـ نـمـ سـيـلـوـ FTDـ ھـرـادـإـ ھـجـاـوـ نـمـ اـھـؤـدـبـ مـتـيـ تـارـابـتـخـالـاـ نـمـضـيـ اـلـ (لـشـافـلـاـ وـاـ)ـ حـجـانـلـاـ لـاـصـتـالـاـ نـإـفـ، DMZـ، جـرـاخـلـاـ، لـخـادـلـاـ لـثـمـ)ـ ىـلـعـ اـھـنـيـوـكـتـ مـتـ AnyConnectـ ۋـقـدـاصـمـ تـابـلـطـ عـدـبـ مـتـيـسـ هـنـأـلـ اـرـظـنـ AnyConnectـ ۋـقـدـاصـمـلـ ۋـجـيـتـنـلـاـ سـفـنـ LDAPـ تـالـاـصـتـاـ رـابـتـخـإـ لـوـحـ تـامـولـعـمـلـاـ نـمـ دـيـزـمـلـ. ھـيـجـوـتـلـلـ ۋـلـبـاـقـلـاـ تـاهـجـاـوـ ىـدـحـإـ نـمـ اـھـحـالـصـ اوـعـاطـخـأـلـاـ فـاشـكـتـسـأـ ۋـقـطـنـمـ يـفـ Test AAAـ وـ Packet Captureـ مـسـقـ عـجـارـ، FTDـ نـمـ

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

قوثومل CA ۆدەش دەح مى بسانملا ريفشتلا دەح، LDAP و/or STARTTLS ۆدەش عەشەنە لىع رقنا، لەفلىاب رذجلە قىدىملا عەرمەلە ۆفاضە مەتت مل اذا. ەب قىدىملا عەرمەلە ۆدەش قىسىلا مى رذجلە قىدىملا عەرمەلە ۆدەش مىسا ريفوتپ مۇق. ۆدېدەج ۆققىت اقىباس اھىيەمىجىت مى يتلا PEM قىسىنىت رذجلە.

Add Trusted CA Certificate

Name
LDAPS_ROOT

Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.

```
-----BEGIN CERTIFICATE-----
MIIDCDBCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxILVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASImD0V.IKoZIhucNAOFRR0ADnqFRADCC4OoOoqFRAlRohT719NzSOnnOPh0VT67h
-----END CERTIFICATE-----
```

CANCEL **OK**

Directory Server Configuration

win2016.example.com:636

Hostname / IP Address	Port
win2016.example.com	636
e.g. ad.example.com	
Encryption	Trusted CA certificate
LDAPS	LDAPS_ROOT

TEST ✓ Connection to realm is successful

میقل لىا هذى مادختسى مىت، نىوكتل اذى يف:

- مىسالا: Lab-ad
- مىسالا: ftd.admin@example.com
- ئىساس ئىنلىك: DC=example,DC=com
- ئىساس ئىنلىك: example.com
- IP: win2016.example.com
- مىسالا: 389

3. روصىل ايف حضوم وە امك نىميلىا ئىلعأ يف ۋەقىلەتلى تارىيەتلى رز رقنا.

The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Firepower Device Manager', 'Monitoring', 'Policies', 'Objects' (which is the active tab), and 'Device: FTD-3'. The user is 'admin' with the role 'Administrator'. On the left, there's a sidebar titled 'Object Types' with options: Networks, Ports, Security Zones, and Application Filters. The main content area is titled 'Identity Sources' and shows a table with two objects:

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

نآل 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

نیوکت AD ڈاچس مل AnyConnect

نیوکت یل ع هقیب طت بجی، ہنیوکت مت یذلا AD ڈی یوکت مادھم مادھم سال AnyConnect.

1. روصلایف حضوم وہ امک زاہج یلا لقتنا.

Cisco Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

Interfaces Connected Enabled 3 of 4 View All Interfaces

Smart License Registered View Configuration

Site-to-Site VPN There are no connections yet View Configuration

Routing 2 routes View Configuration

Backup and Restore View Configuration

Remote Access VPN Configured 1 connection | 2 Group Policies View Configuration

Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration

Troubleshoot No files created yet REQUEST FILE TO BE CREATED

Advanced Configuration Includes: FlexConfig, Smart CLI 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

Device Administration Audit Events, Deployment History, Download Configuration View Configuration

2. روصلایف حضوم وہ امک لاصتا فیرعت فلم عاشن اوا + رز رقنا.

مق. اقبسم هؤاشن ام ت يذلا AD ئي ووه ردىصىم ددح ، "لي مىع لالا نى يوكتول اصتالا" مسق تتحت. 3. نى يي عتول اصتالا فييرعت فلم مس اك لذ يف امب يرخ لالا ماسق أللل ئبسان ملما مي قىلدا دادعاب عاهتنالا دن دن ع مالعتسالا لاسرا قوف رقنا. ئالى عالمىع لالا نى وانع عمجمت.

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

[Add Group Alias](#)

Group URL

[Add Group URL](#)

Primary Identity Source

Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

Primary Identity Source for User Authentication

Fallback Local Identity Source ⚠

Filter

Please Select Local Identity Source

LocalIdentitySource

LAB-AD

Special-Identities-Realm

[Create new](#)

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

، يضارتفا لكشب . بسانمل ا ئعومجملا جهن ددج ، دعب نع مدخلتسمل ا ئبرجت مسق تتحت .
ةفلتخم ئاسايىس عاشن ا نكمي ، كلذ عم و DfltGrpPolicy مادختسا متيس .

View Group Policy

DfltGrpPolicy

Policy Group Brief Details

Edit	
DNS + BANNER	
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

AnyConnect مزح و، ةيجراخلا ةهجاول او، SSL ئدابهش ددح، لقألا ىلع، ةماعلا تادادعإلا مسق نمض. 5. ئيضاارت فا ايتأذ ٰعقوم ئدابهش ديدحت نكمي، اقباس ئدابهش عاشنامتى مل اذا
عاغلا بجي. اه قوثوم ريغ مداخ ئدابهش ئلراسر رهظتس لاح يأ ىلع
(DefaultInternalCertificate) اهريفسن كف مت يتلا رورملما ةكرحل يف افتلالا لوصولاب مكحتلا ةسايس ديدحت
نكمي. اقحال ذيفنتلا زيح مدختسملا ئيوهيلالا لوصولالا جهن دعاوق لخدت ثيحب allowed-vpn
ةهجاولما IPv4 رورم ةكرح عيجم نوكت، نيوكتتلا اذه يف. اضيأ انه NAT ءانثتسا نيوكت
ةبسنلاب NAT نم ءانثتسا ب AnyConnect ليمعل IP نيوانعيلالا لقتنت يتلا ةيلخادلا
NAT دعاوق جاتحتس، جراخلا ىلما جراخلا نم رفاظالا ميلقت لثم اديقعت رثكلأا تانيييعتلل
Cisco: معدعقوم ىلع AnyConnect مزح ىلع روشعلا نكمي. ةسايس راطإ يف ةيفاضا
ليزنل حلاص Plus Apex وأ صيخرت رفوت مزلبي
ةمزح 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

▼

Outside Interface

▼

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

▼

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

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

BACK

NEXT

لاسا قوف رقنا مث ،بسانم لکشب AnyConnect دادعا نم ققحت ،صلملما مسق نمض .
ماعتتسالا

^ 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. ةروصلـا يـف حـضـوم وـه اـمـك نـيـمـيـلـا ىـلـعـأ يـف ـقـلـعـمـلا تـارـيـغـتـلـا رـزـرـقـنـا.

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

Search

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

8. نـآلـا رـشـنـ قـوفـ رـقـنـا.

Pending Changes

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

Deployed Version (16 Apr 2020 12:41 PM)	Pending Version	
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	anyconnectPackageFiles: vpnGatewaySettings[0].serverCertificate: vpnGatewaySettings[0].outsideInterface: vpnGatewaySettings[0].insideInterfaces: vpnGatewaySettings[0].insideNetworks:	vpnGatewaySettings[0].exemptNatRule: true vpnGatewaySettings[0].outsideFqdn: ftd3.example.com vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t... name: NGFW-Remote-Access-VPN anyconnect-win-4.7.03052-webdeploy-k9.pkg FTD-3-Manual outside inside

MORE ACTIONS ▾ CANCEL DEPLOY NOW ▾

مدختسملاء اي ولهلا نامألا تاسايس نويوكتو وي وهلا جه نيكمت

دق نكلو، حاجن ب لاصتا لىلع نيرداق AnyConnect ومدختس م نوكى نأ بجي، ظقىللا هذه دنع وي وه نيكمت ىلا ووطخللا هذه يدؤتس. ةنيعم دراوم ىلا لوصوللا لىلع نيرداق اونوكى ال دراوملاب لاصتا لىلا AnyConnect يلوفسم نمض نيمدختسم ل طقف نكمي ثيحب مدختس مملأا لاصتا لىلا ًعومجملا نمض AnyConnect يمدختسم طقف نكمي و RDP مادختس اب وي خادلأا مادختس اب وي خادلأا دراوملاب HTTP.

1. نيكمت قوف رقنا وي وهلا > تاسايسلا ىلا لقتنا.

Cisco Firepower Device Manager | Policies | Objects | Device: FTD-3 | admin | Administrator

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

PASSIVE AUTHENTICATION

USERS → LEVERAGE IDENTITY → IDENTITY SOURCES

MULTIPLE IDENTITIES

ENABLE IDENTITY POLICY

يـفـاـكـ رـيـصـقـتـ عـارـجـإـلـأـوـ بـولـطـمـ يـفـاضـإـ لـيـكـشـتـ نـمـ اـمـ ،ـلـيـكـشـتـ اـذـهـ لـ.

Cisco Firepower Device Manager | Policies | Objects | Device: FTD-3 | admin | Administrator

Security Policies

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

Identity Policy **ENABLED**

Search

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

Default Action **Passive Auth** Any Identity Source

2. عـانـثـتـسـ إـنـاـكـ اـذـاـ بـسـاـنـمـ لـكـشـبـ تـلـكـشـ **NAT** نـأـ دـكـأـتـوـ > تـاسـاـيـسـلـاـ إـلـاـ لـقـتـنـاـ .ـيـفـاـضـإـ نـيـوـكـتـ إـلـاـ ـقـجـاحـ كـاـنـهـ نـوـكـتـ نـلـفـ ،ـيـفـاـكـ AnyConnectـ تـادـادـعـإـ يـفـ هـنـيـوـكـتـ مـتـ يـذـلـهـ اـنـهـ .ـ

Cisco Firepower Device Manager | Policies | Objects | Device: FTD-3 | admin | Administrator

Security Policies

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

1 rule

Search

H	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATI...	SOURCE PORT	DESTINATI...	SOURCE AD...	DESTINATI...	SOURCE PORT	DESTINATI...	
>	Internet_PAT	DYNAMIC	ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

Auto NAT Rules

عاج إلأ" نوييعدت متي، مسقلنا اذه يف **لوصولـا يـف مـكـحـتـلـا > تـاسـايـسـلـا إـلـا لـقـتـنـا**.
مـدـخـتـسـمـ لـاـصـتـا درـجـمـبـ كـلـذـلـ لـوـصـوـ دـعـاـوـقـ عـاـشـنـا مـتـيـ مـلـوـ "رـطـحـلـا" إـلـعـ "يـضـارـتـفـالـاـ"
ـدـعـاـقـ عـاـشـنـاـبـ مـقـ +ـ قـوـفـ رـقـنـاـ.ـ عـيـشـ يـأـلـاـ لـوـصـولـاـ إـلـعـ اـرـدـاقـ نـوـكـيـ نـلـ.
ـدـيـدـجـ ـدـعـاـقـ ـفـاضـلـاـ لـوـصـوـ وـ.

The screenshot shows the Cisco Firepower Device Manager web interface. The top navigation bar includes tabs for Monitoring, Policies (which is highlighted with a red box), Objects, and Device: FTD-3. On the far right, it shows the user is logged in as 'admin' with 'Administrator' privileges. Below the navigation is a breadcrumb trail: Security Policies > Access Control. A search bar and a '+' button are also present. The main content area displays a table header for 'Access Rules' with columns: #, NAME, ACTION, ZONES, NETWORKS, PORTS, ZONES, NETWORKS, PORTS/PROTOS, APPLICATIONS, URLs, USERS, and ACTIONS. A message below the table states: 'There are no access rules yet. Start by creating the first access rule.' A prominent blue 'CREATE ACCESS RULE' button is centered. At the bottom, there's a 'Default Action' dropdown set to 'Access Control' with a 'Block' option selected, and a row of small icons.

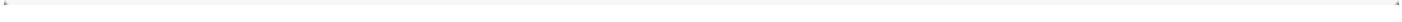
لـخـادـ نـوـمـدـخـتـسـمـلـاـ عـتـمـتـيـ نـأـ بـجـيـ،ـ نـيـوـكـتـلـاـ اـذـهـ يـفـ.ـ ظـبـسـانـمـلـاـ مـيـقـلـابـ لـوـقـحـلـاـ أـلـمـاـ.
ـيـلـخـادـلـاـ ةـكـبـشـلـاـ يـفـ RDPـ مـدـاخـلـاـ لـوـصـوـ قـحـبـ AnyConnectـ يـلـوـفـسـمـ ةـعـوـمـجـمـ
ـمـتـيـسـ يـتـلـاـ ةـيـجـرـاخـلـاـ ةـهـجـاـوـلـاـ يـهـ ةـيـجـرـاخـ ةـقـطـنـمـكـ ةـقـطـنـمـلـاـ نـيـوـكـتـ مـتـ،ـ رـدـصـمـلـلـ ةـبـسـنـلـابـ
ـمـتـ يـذـلـاـ AnyConnect-Poolـ نـيـاـكـ ةـكـبـشـلـاـ نـيـوـكـتـ مـتـ وـاهـبـ AnyConnectـ يـمـدـخـتـسـمـلـاـ لـاـصـتـاـ
ـيـفـ مـدـخـتـسـمـلـاـ ةـيـوـهـلـ ةـبـسـنـلـابـ.ـ ءـالـمـعـلـ IPـ نـيـوـانـعـ نـيـيـعـتـلـ اـقـبـسـمـ هـنـيـوـكـتـ
ـلـاـصـتـاـلـاـ عـدـبـبـ مـدـخـتـسـمـلـاـ مـوـقـيـسـ يـتـلـاـ ةـكـبـشـلـاـوـ ةـقـطـنـمـلـاـ وـهـ رـدـصـمـلـاـ نـوـكـيـ نـأـ بـجـيـ
ـيـتـلـاـ ةـيـلـخـادـلـاـ ةـهـجـاـوـلـاـ وـهـ اـمـكـ ةـقـطـنـمـلـاـ نـيـوـكـتـ مـتـيـ،ـ ةـهـجـوـلـلـ ةـبـسـنـلـابـ.ـ اـهـنـمـ
ـفـرـعـيـ نـيـاـكـ وـهـ يـذـلـاـ Inside_Netـ نـيـاـكـ ةـكـبـشـلـاـ نـيـوـكـتـ مـتـيـوـ،ـ Windowsـ مـدـاخـ اـهـيـلـعـ عـقـيـ
ـلـعـ تـالـوـكـوـتـورـبـلـ/ـذـفـانـمـلـاـ نـيـيـعـتـ مـتـيـوـ،ـ Windowsـ مـدـاخـ اـهـيـفـ دـجـوـيـ يـتـلـاـ ةـيـعـرـفـلـاـ ةـكـبـشـلـاـ
ـلـوـكـوـتـورـبـلـ رـبـعـ TCP~3389ـ وـ UDP~3389ـ لـوـصـوـبـ حـامـسـلـلـ ةـصـصـخـمـلـاـ ذـفـانـمـلـاـ نـيـنـئـاـكـ

Edit Access Rule

Order	Title	Action
1	AC RDP Access	Allow

Source/Destination Applications URLs Users Intrusion Policy 1 File policy 1 Logging

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



متي ثيحب ئەعومجمىلى AnyConnect مەتتىس ، "نۇمدختىمىلا" مىسىق تەخت
Windows مداخىلى RDP لۇصوب ئەعومجمىلا ھەذە نىع نولصىفي نىذلە نىيەمدىختىمىلى حامىسىلى
مۇ ، ئەپسانمەلە ئەعومجمىلا قوف رقنا او ، تاۋاعومجم بىيوبتىلا ئەملاع قوف رقنا او ، زەرمىلا + قوف رقنا
كەلذك ئەپەلە رەدىصەم و نىيەرىف نىيەمدىختىمى دىدەت نەكمىي ھەنأ ئەظحال . قەفاوەم قوف رقنا

Add Access Rule

Order	Title	Action
1	AC RDP Access	Allow

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

AVAILABLE USERS

+ **CONTROLLING ACCESS FOR USERS AND USER GROUPS**

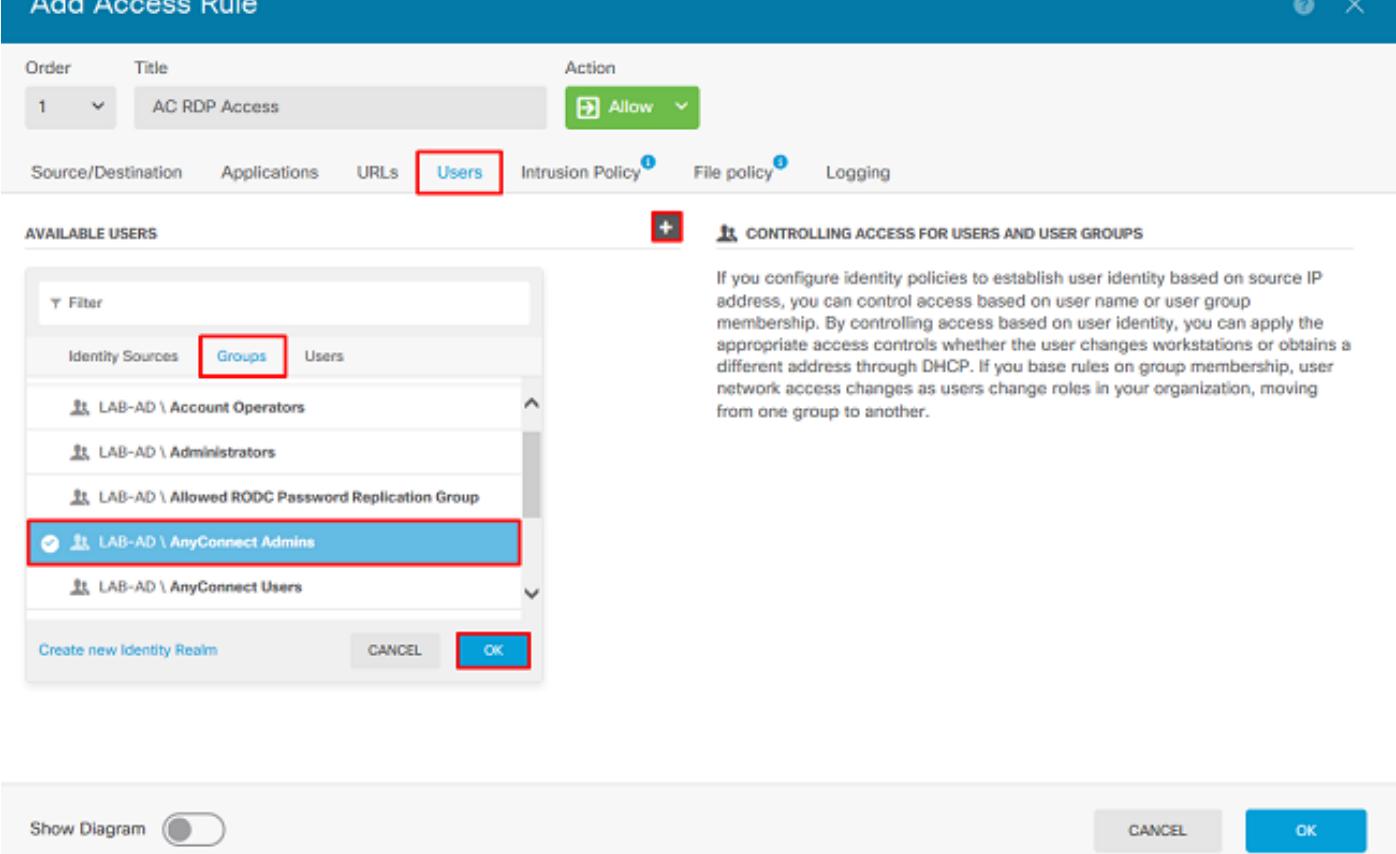
If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a 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.

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

Show Diagram CANCEL OK



قفاوم قوف رقنا، ئېسەنملە تارايىخلا دىدھت درجمب.

Add Access Rule

Order	Title	Action
1	AC RDP Access	Allow

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

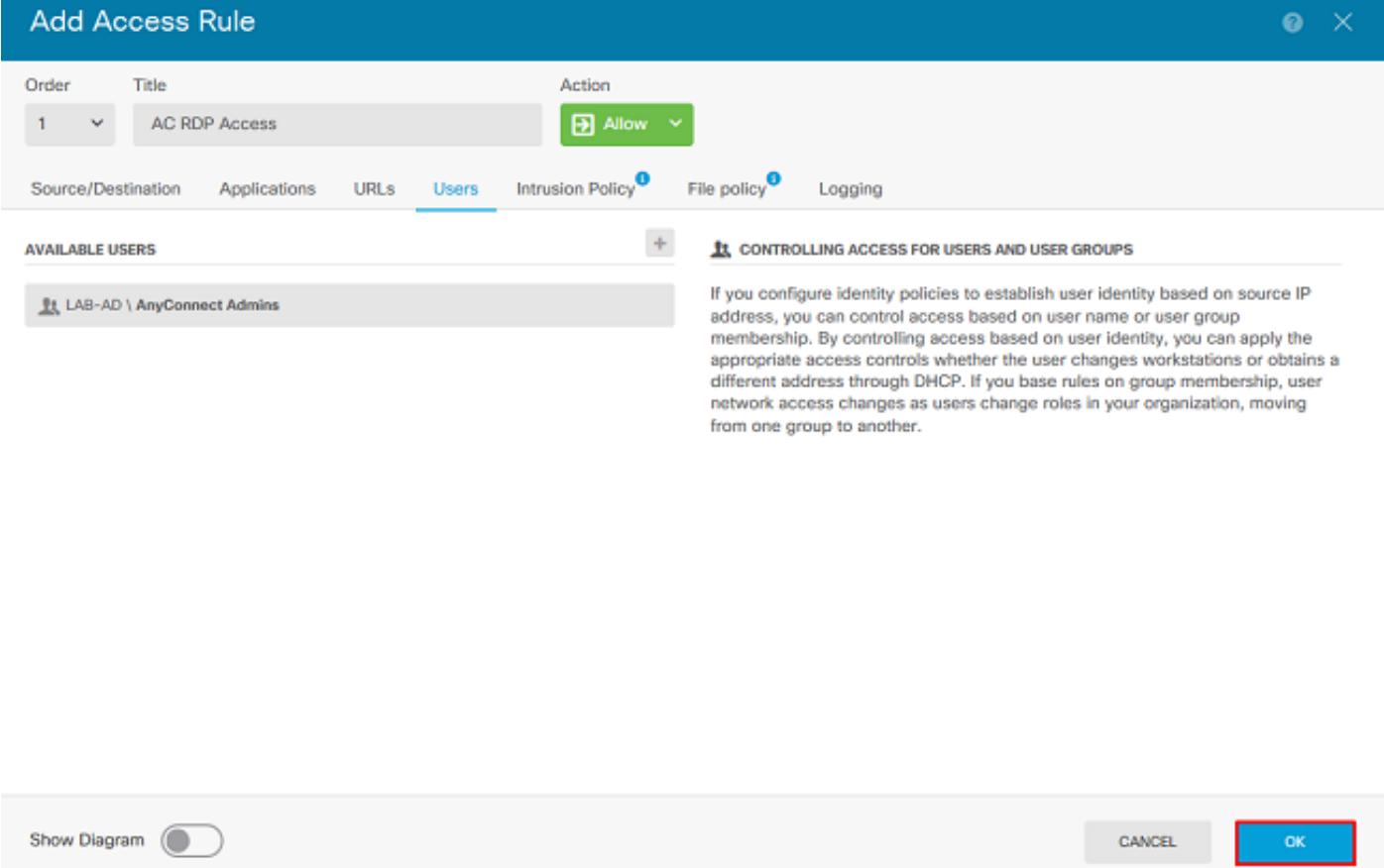
AVAILABLE USERS

+ **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.

LAB-AD \ AnyConnect Admins

Show Diagram CANCEL OK



دەعاق ئاشنە مەتى، نىوكتىلا اذە يىف. رەمألا مىزلى اذى لوصولە دعاووق نەم دىزمەلە ئاشناب مۇق.

ىلـا لـوصـلـاب HTTP AnyConnect يـمـدـخـتـسـمـعـوـجـمـنـمـضـنـيـمـدـخـتـسـمـلـلـحـامـسـلـلـىـخـأـلـوـصـوـنـمـداـخـنـمـW~ndows.

Edit Access Rule

Order	Title	Action
2	AC HTTP Access	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	HTTP

Show Diagram CANCEL OK

Not hit yet

Edit Access Rule

Order	Title	Action
2	AC HTTP Access	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 CANCEL OK

Not hit yet

نـيـمـيـلـاـىـلـعـأـيـفـةـقـلـعـمـلـاـتـارـيـيـغـتـلـاـرـزـقـوـفـرـقـنـاـمـثـلـوـصـلـاـةـدـعـاـقـنـيـوـكـتـنـمـقـقـحـتـ6.

ةروصلـا يـف حـضـوم وـه اـمـك

The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes the Cisco logo, device name 'Firepower Device Manager', and tabs for Monitoring, Policies (which is selected), Objects, and Device: FTD-3. The main content area is titled 'Security Policies' and shows a breadcrumb trail: SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion. Below this, it says '2 rules' and displays a table with two entries:

#	NAME	ACTION	SOURCE ZONES	NETWORKS	PORTS	DESTINATION ZONES	NETWORKS	PORTS/PROTOS	APPLICATIONS	URLS	USERS		ACTIONS
> 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...		

At the bottom, there are buttons for 'Default Action' (Access Control, Block), and a search bar.

نـآلـا رـشـن قـوف رـقـنـا مـثـ، تـارـيـيـغـتـلـا نـم قـقـحـتـ.

The screenshot shows the 'Pending Changes' screen. At the top, it says 'Last Deployment Completed Successfully' on '28 Apr 2020 01:35 PM'. Below this, it lists 'Deployed Version (28 Apr 2020 01:35 PM)' and 'Pending Version'.

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 ▾

ةـحـصـلـا نـم قـقـحـتـلـا

حيـحـصـ لـكـشـبـ نـيـوـكـتـلـا لـمـعـ دـيـكـأـتـلـ مـسـقـلـا اـذـهـ مـدـخـتـسـا

يـئـاهـنـلـا بـيـتـرـتـلـا

نیوکت AAA

```
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=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

نیوکت AnyConnect

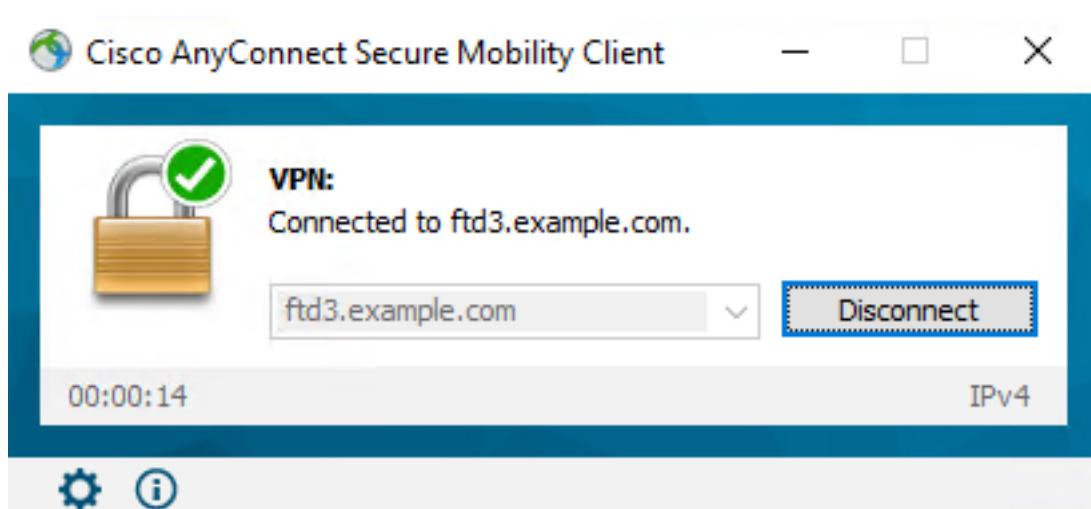
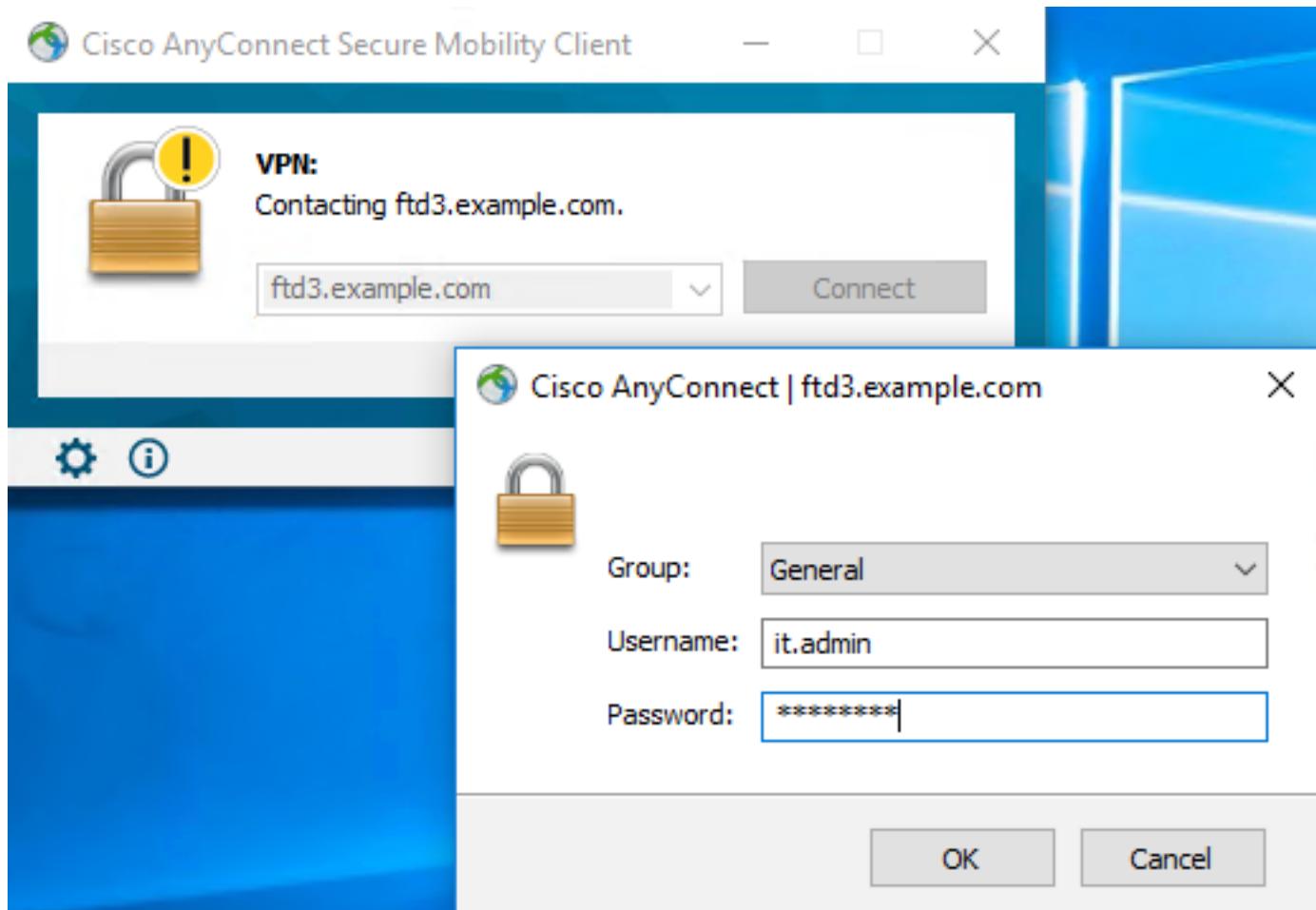
```
> show running-config webvpn
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1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

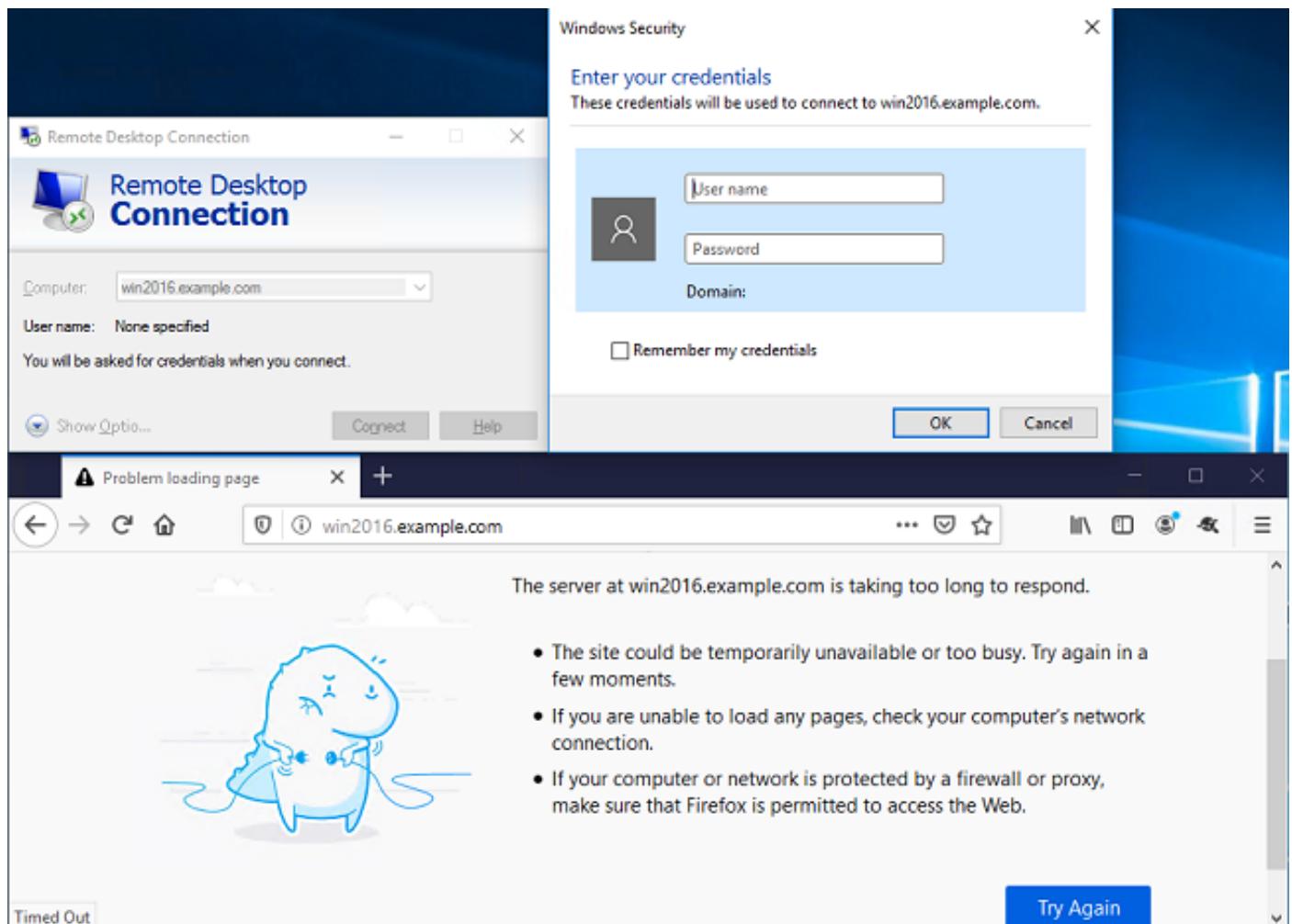
> show running-config group-policy
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
anyconnect ssl dtls none

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

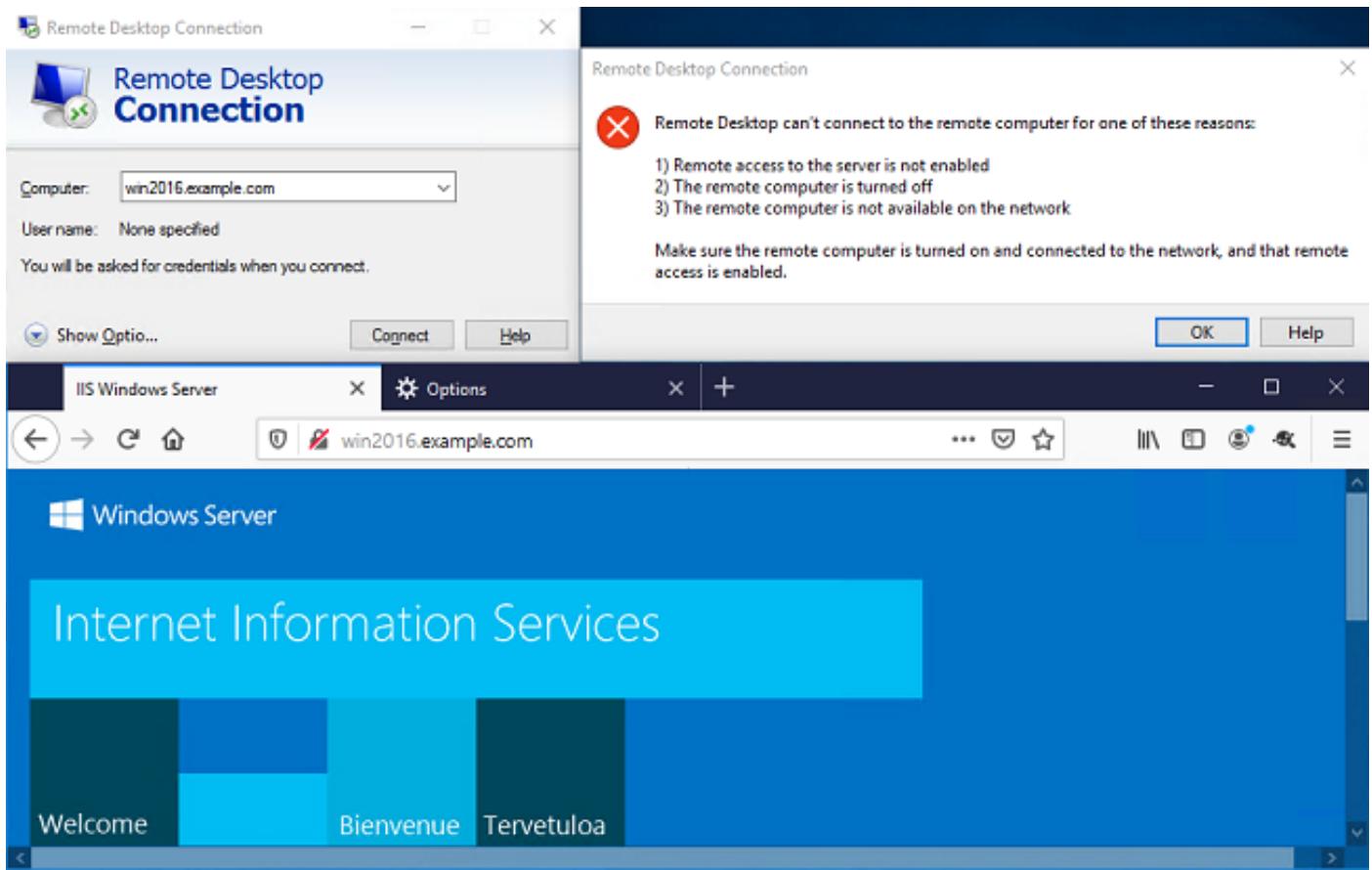
اهم ققحتل او AnyConnect نم لوصول ایف مکحتلا ئاسایس دعاوقب لاصتا



User IT Admin لوچ و اهیدل یتل ایف دوجوم AnyConnect Admins مدادخلا اذهل Firefox و RDP لمع ئسلج حتف نا. اهيدل سيل كلذ عمو. مدادخلا اذهل HTTP Server. اهيدل سيل كلذ عمو. طقق ف ربع مدادخلا یلل الوچولو هنكمي مدخلتسمل اذه ننم ققحتي.



يـمـدـخـتـسـمـ ةـعـوـمـجـمـ يـفـ دـوـجـوـمـ رـاـبـتـخـاـ مـادـخـتـسـابـ لـوـخـدـلـاـ لـيـجـسـتـبـ تـمـقـ اـذـ [AnyConnect] ئـسـاـيـسـ دـعـاـوـقـ نـأـ نـمـ قـقـحـتـلـاـ كـنـكـمـيـفـ ، RDP، HTTP، HTTPS وـمـهـيـلـوـ لـوـصـوـسـيـلـوـ لـوـصـوـمـهـيـلـوـ لـوـعـفـمـلـاـ ئـيـرـاسـ تـحـبـصـأـ لـوـصـوـلـاـ يـفـ مـكـحـتـلـاـ.



اهحالص او عاطخألا فاشكتسا

حيحص لکشب نیوکتل المع دیکأتل مسقل اذه مدخلتسا.

عاطخألا حيحصت

لیغشت نكمي، اهالص او مدخلتسمل اهیوه لوصول ایف مکحتل اسایس عاطخألا فاشكتسا يليغشت نكمي LDAP یف اذه عاطخألا حيحصت CLI يصيخت.

لیغشت نكمي، اهالص او مدخلتسمل اهیوه لوصول ایف مکحتل اسایس عاطخألا فاشكتسا ببس دیدحتل مکحتل اقمیاق یف ماظنل امعدب صاخلا عاطخألا حيحصت کرحم ڈیامح راجع. قوتم ریغ لکشب اهعنم و آرورمل اهکرحم حامسل.

ةلماعل ا عاطخألا حيحصت LDAP

```
[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...;.....j...
[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

```

مداخلہ لاصت اعاشنا 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

```

لولحلا متحمل لـ DN:

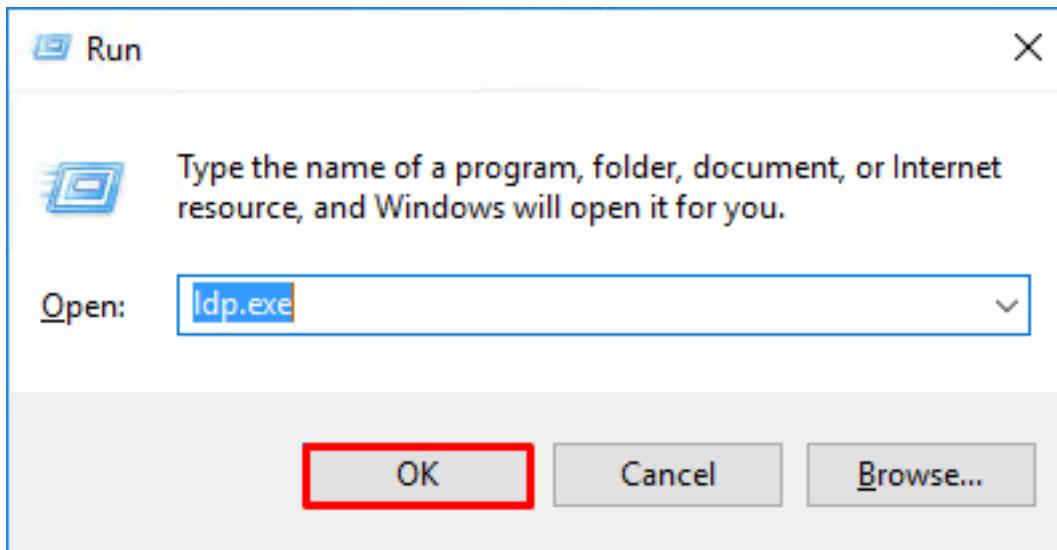
- LDAP نـم قـقـحـتـي FTD نـم دـكـأـتـو هـيـجـوـتـلـا نـم قـقـحـتـي.
- اـهـبـ قـوـثـومـ وـحـيـحـصـلـا رـذـجـلـا CA نـم دـكـأـتـ، LDAP وـأـ STARTTLS مـادـخـتـسـا ئـلـاحـ يـفـ.
- حـاجـنـبـ SSL وـحـفـاصـمـ لـامـكـاـ نـكـمـيـ ثـيـحـبـ.
- نـمـ قـقـحـتـفـ ، فـيـضـ مـلـاـ مـسـاـ مـادـخـتـسـاـ مـتـ اـذـاـ حـيـحـصـ عـانـيـمـ وـنـاـونـعـلـاـ لـمـعـتـسـيـ نـأـ تـقـقـدـ.
- حـيـحـصـلـا IP نـاـونـعـىـلـاـ هـلـحـىـلـعـ DNS ئـرـدـقـ

حـيـحـصـ رـيـغـ طـبـرـلـلـ روـرـمـلـاـ ئـمـلـكـ وـأـوـ DN

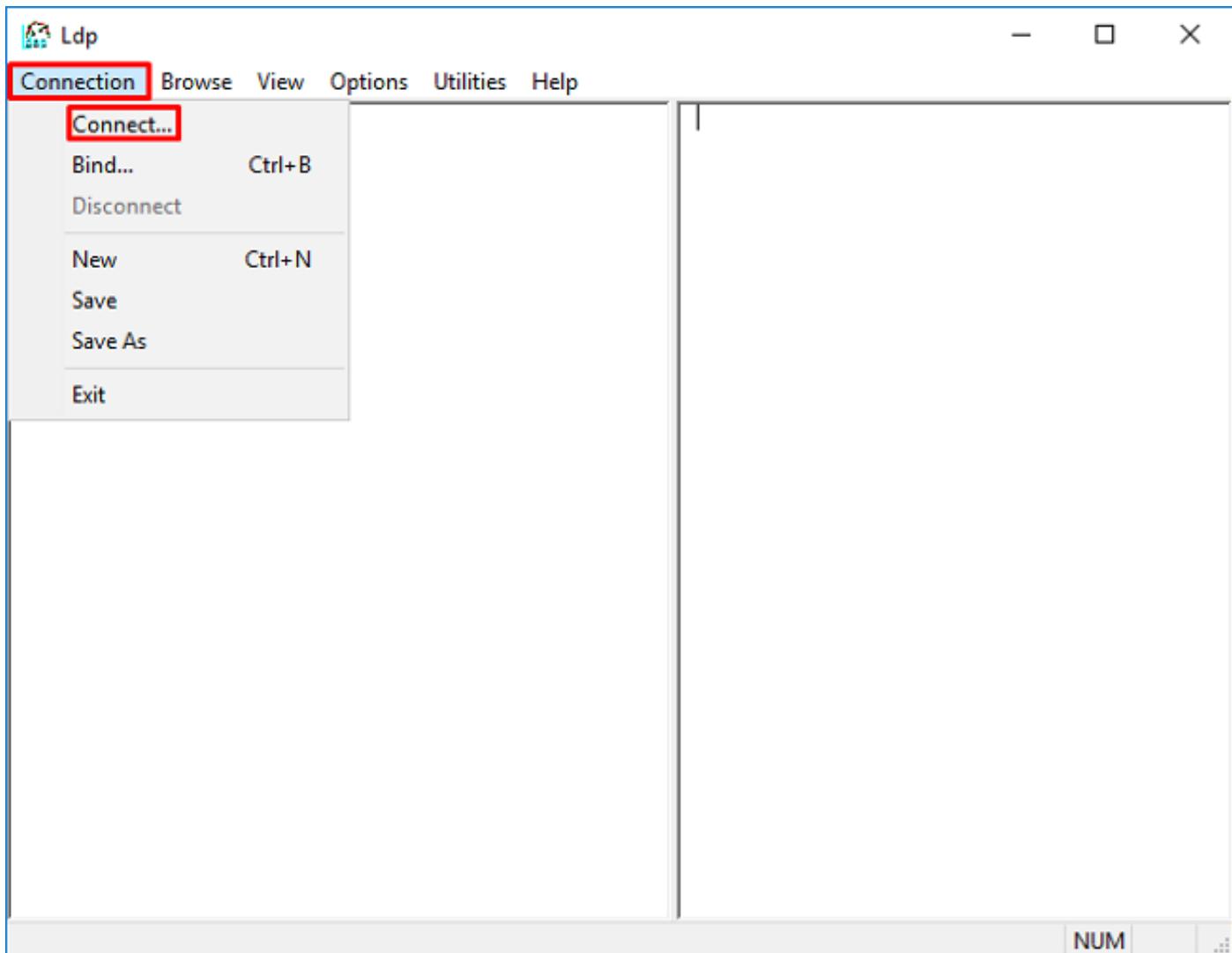
```
[ -2147483615] Session Start
[ -2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483615] Fiber started
[ -2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[ -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
```

لـيـجـسـتـ روـرـمـ ئـمـلـكـ وـلـوـخـدـلـاـ لـيـجـسـتـبـ ئـصـاخـلـاـ DN ئـكـبـشـ نـيـوـكـتـ نـمـ قـقـحـتـيـ: لـمـتـحـمـلـلـاـ لـحـلـلـاـ قـقـحـتـلـلـ. ldp.exe. مـادـخـتـسـابـ AD مـادـخـلـعـ ئـارـجـإـلـاـ اـذـهـ نـمـ قـقـحـتـلـاـ نـكـمـيـ. حـيـحـصـ لـكـشـبـ لـوـخـدـلـاـ ئـيلـاتـلـاـ تـاوـطـخـلـاـ رـبـعـ لـقـتـنـاـ، LDP مـادـخـتـسـابـ حـاجـنـبـ بـاسـحـ طـبـرـ ئـيـنـاـكـمـاـ نـمـ:

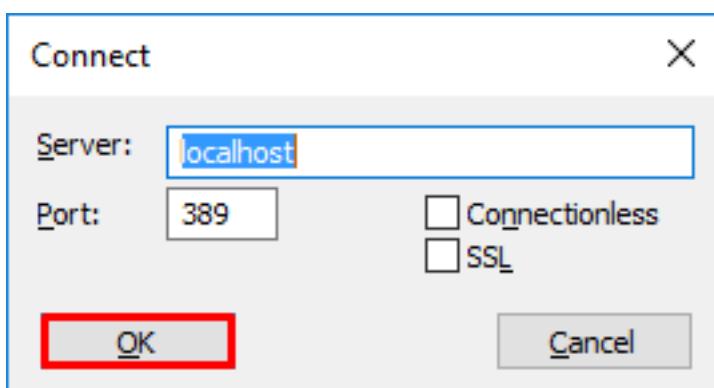
1. مـادـخـلـعـ Win+R نـعـ ثـحـبـ اوـ Win+R نـعـ ثـحـبـ اوـ ldp.exe.



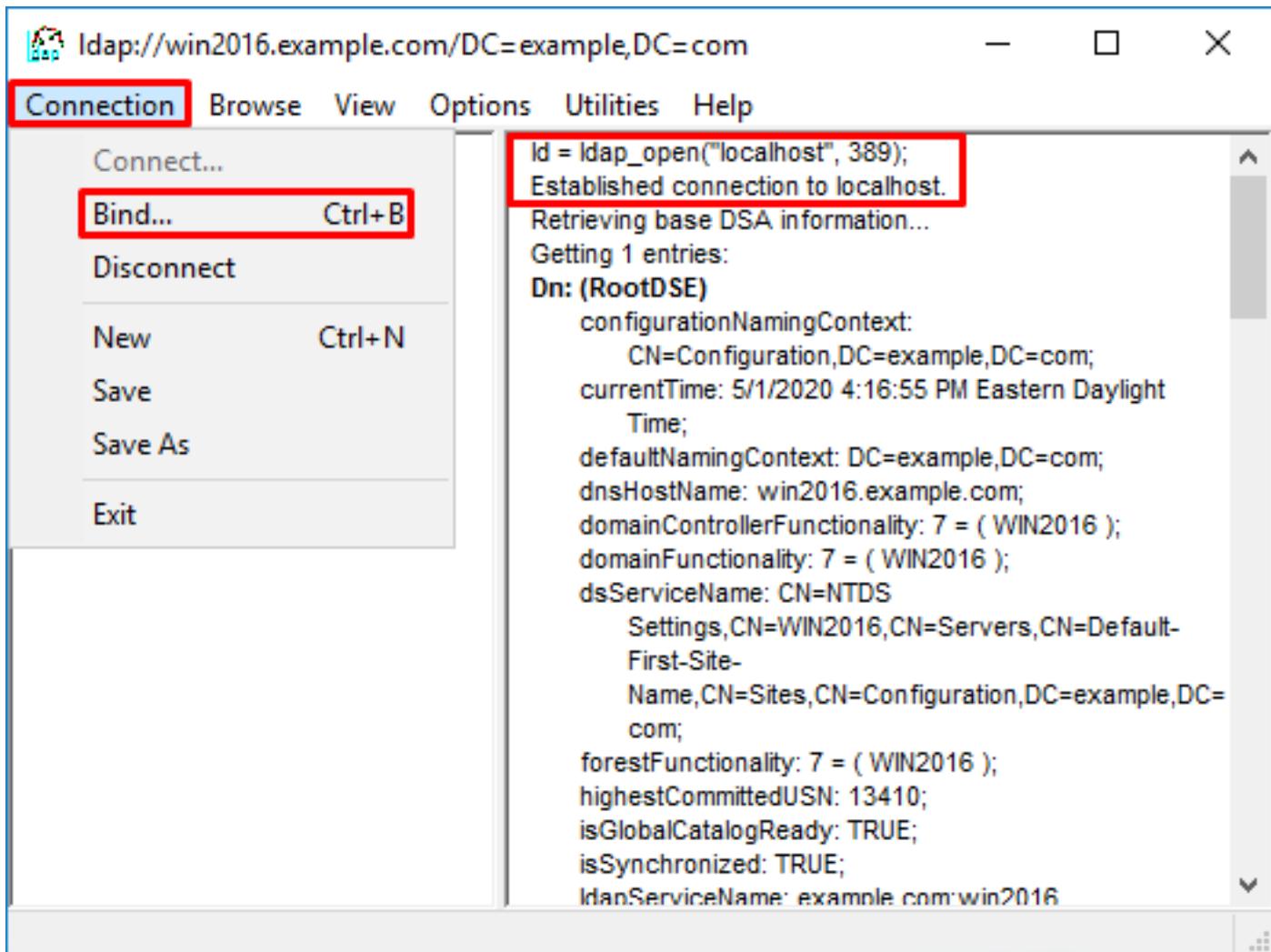
2. ئـروـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ ...ـلـاـصـتـاـ >ـلـاـصـتـاـ قـوـفـ رـقـنـاـ.



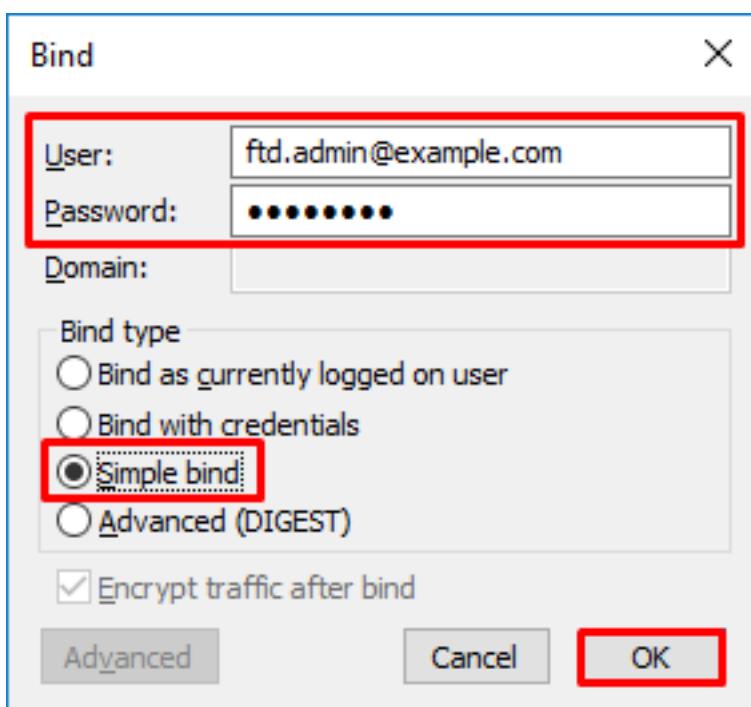
3. قف اوم قوف رقنا مث ، بسانمل ا ذفنمل او مداخلل يلحه فيضم ددح.



4. وه امك ... طبر < لاصتا ىلع رقنا . حجان لاصتا ىلا ريشي يذلا صنلا نميألا دومعلا رهظي . روصلا يف حضوم



5. قوف رقناو. رورمل ا ةملکولیل دلا باسح مدخلتسن مسا ددح مث ، طیسب طبر ددح OK.



6. یل ع قدصم LDP ره ظیس، حجان طبر مادختسن اب DOMAIN\username.

ldap://win2016.example.com/DC=example,DC=com

Connection Browse View Options Utilities Help

```
1.2.840.113556.1.4.2255;
1.2.840.113556.1.4.2256;
1.2.840.113556.1.4.2309;
supportedLDAPPolicies (20): MaxPoolThreads;
MaxPercentDirSyncRequests; MaxDatagramRecv;
MaxReceiveBuffer; InitRecvTimeout;
MaxConnections; MaxConnIdleTime; MaxPageSize;
MaxBatchReturnMessages; MaxQueryDuration;
MaxDirSyncDuration; MaxTempTableSize;
MaxResultSetSize; MinResultSets;
MaxResultSetsPerConn; MaxNotificationPerConn;
MaxValRange; MaxValRangeTransitive;
ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;
```

```
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com',
<unavailable>); // v.3
Authenticated as: 'EXAMPLE\ftd.admin'.
```

Ready

اذه لثم لشف ىل ا كل ذي دؤي سف، ٰ حيحص ريغ رورم ٰ مملک وا مدخلت سم مسا طبر تلواح اذا.

```

ldap://win2016.example.com/DC=example,DC=com
Connection Browse View Options Utilities Help
MaxResultSetSize; MinResultSets;
MaxResultSetsPerConn; MaxNotificationPerConn;
MaxValRange; MaxValRangeTransitive;
ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com',
<unavailable>); // v.3
Authenticated as: 'EXAMPLE\ftd.admin'.

-----
res = ldap_simple_bind_s(ld, 'wrong@example.com',
<unavailable>); // v.3
Error <49>: ldap_simple_bind_s() failed: Invalid Credentials
Server error: 80090308: LdapErr: DSID-0C09042A,
comment: AcceptSecurityContext error, data 52e, v3839
Error 0x80090308 The token supplied to the function is
invalid

```

Ready

مدى تسلسل اجراءات LDAP في التسجيل

```

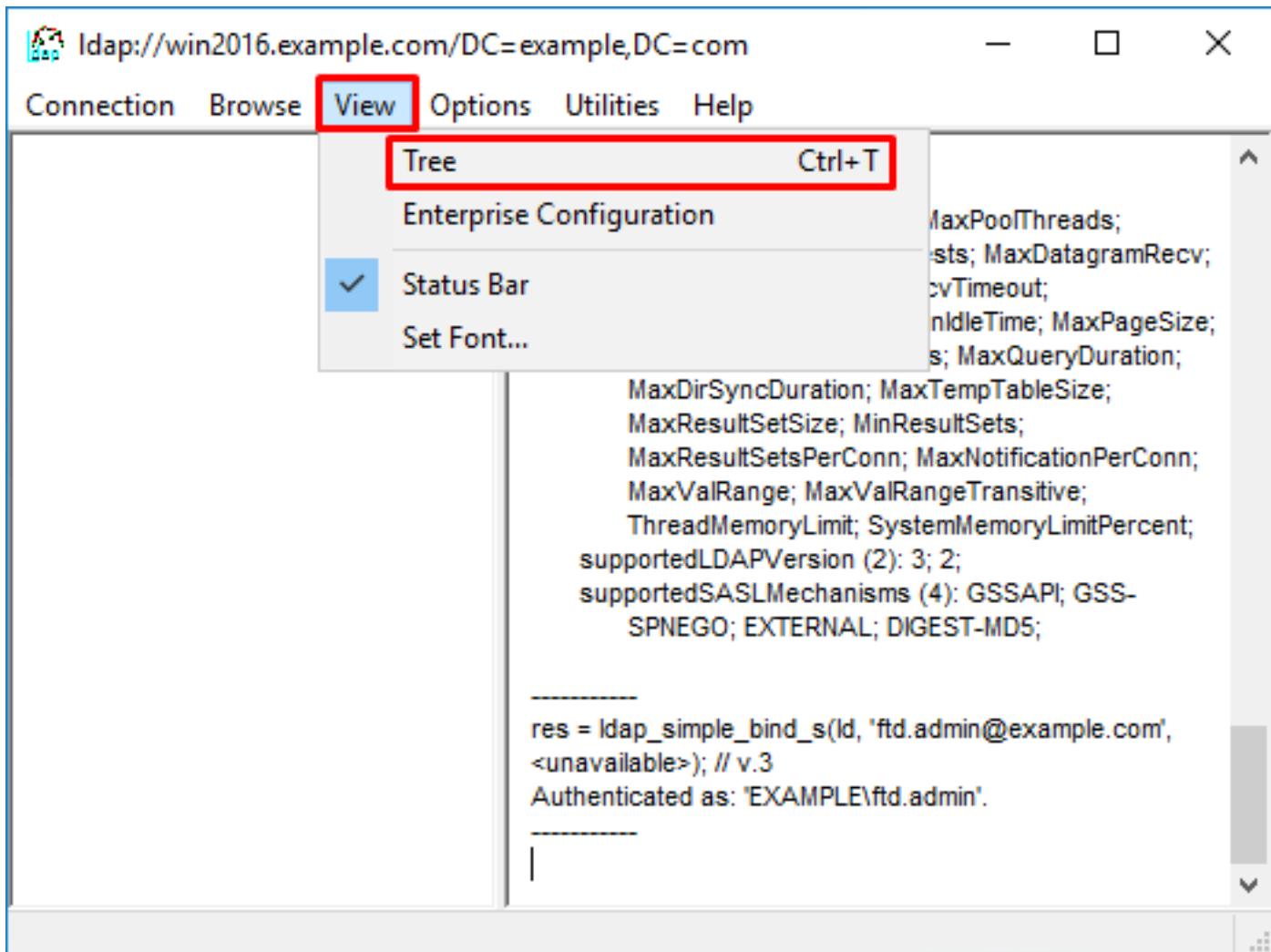
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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

```

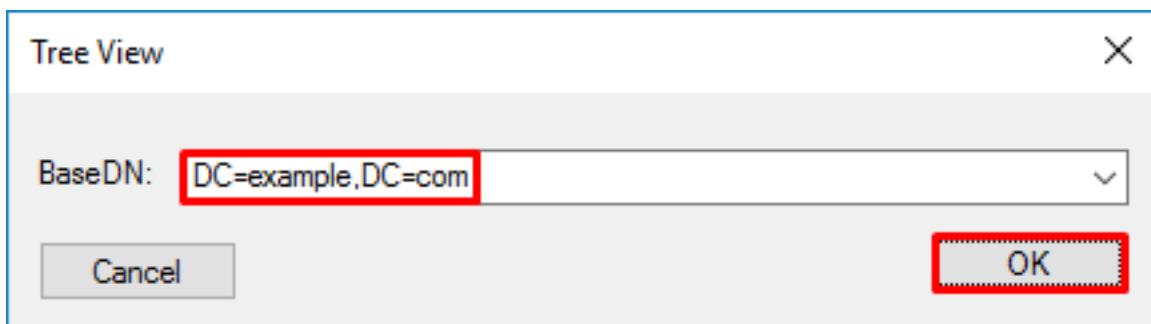
هذا هو تسلسل الأحداث في التسجيل:

- فتح الاتصال (Session Start)
- إنشاء سياق (New request Session)
- البدء في الألياف (Fiber started)
- إنشاء سياق LDAP (Creating LDAP context)
- الاتصال بالخادم LDAP (Connect to LDAP server)
- بيان دعم LDAP (supportedLDAPVersion)
- بيان دعم LDAP (supportedLDAPVersion)
- بيان عن الخادم LDAP (LDAP server)
- ال BIND (Binding)
- التحقق من كلمة المرور (Performing Simple authentication)
- البحث (LDAP Search)
- فشل تحليل النتائج (Search result parsing returned failure status)
- الاتصال بالخادم LDAP (Talking to Active Directory server)
- قراءة سياسة كلمة المرور (Reading password policy)
- ال BIND (Binding)
- التحقق من كلمة المرور (Performing Simple authentication)
- خروج الألياف (Fiber exit)
- إغلاق الاتصال (Session End)

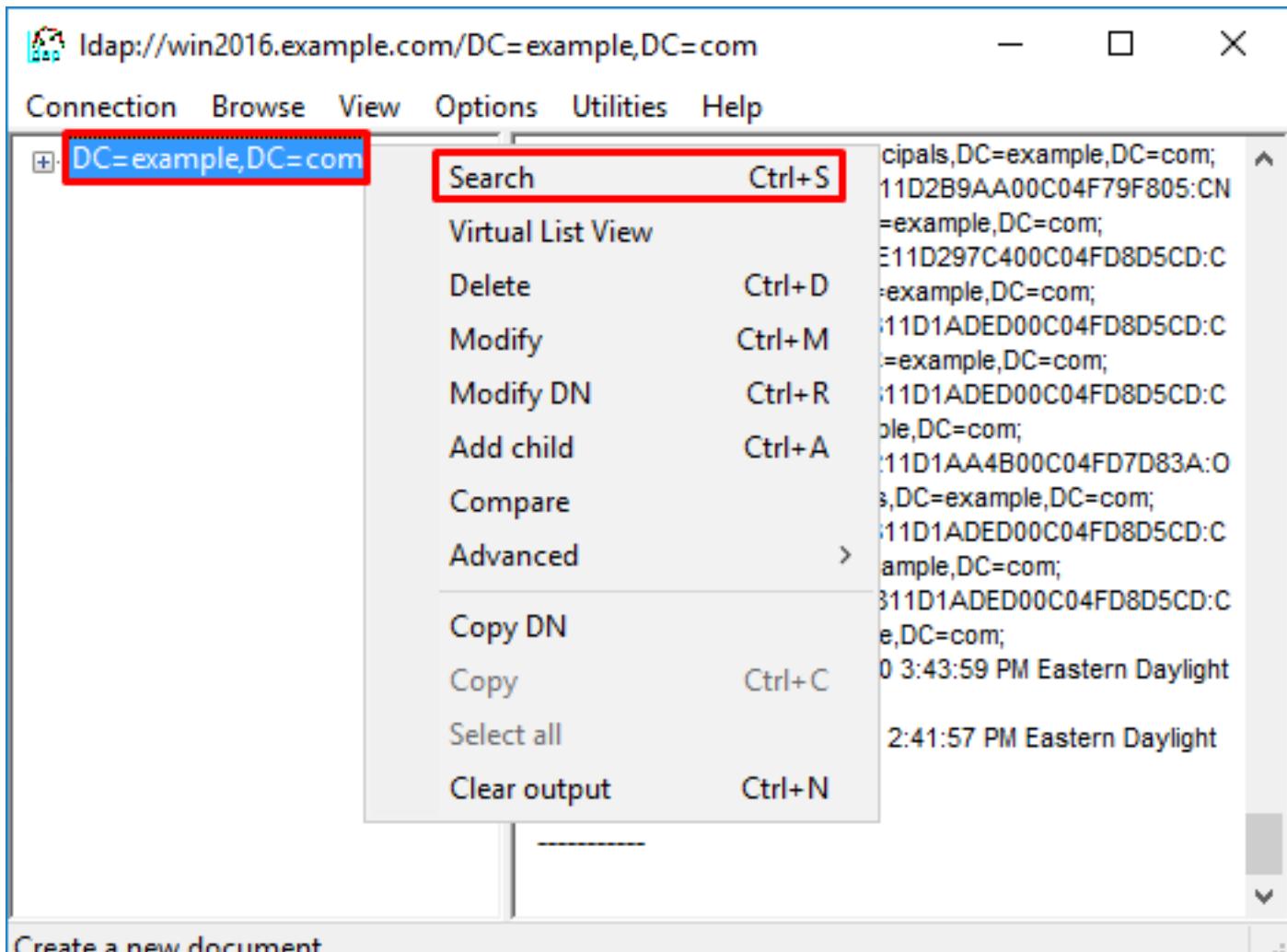
رسالة الخطأ المنشورة في الخطوة 11 تشير إلى أن التوكن المقدمة للوظيفة غير صالح.



2. قف اوم قوف رقنا مث FTD ىلع هن يوكت مت يذلا يس اس األا DN ددح.



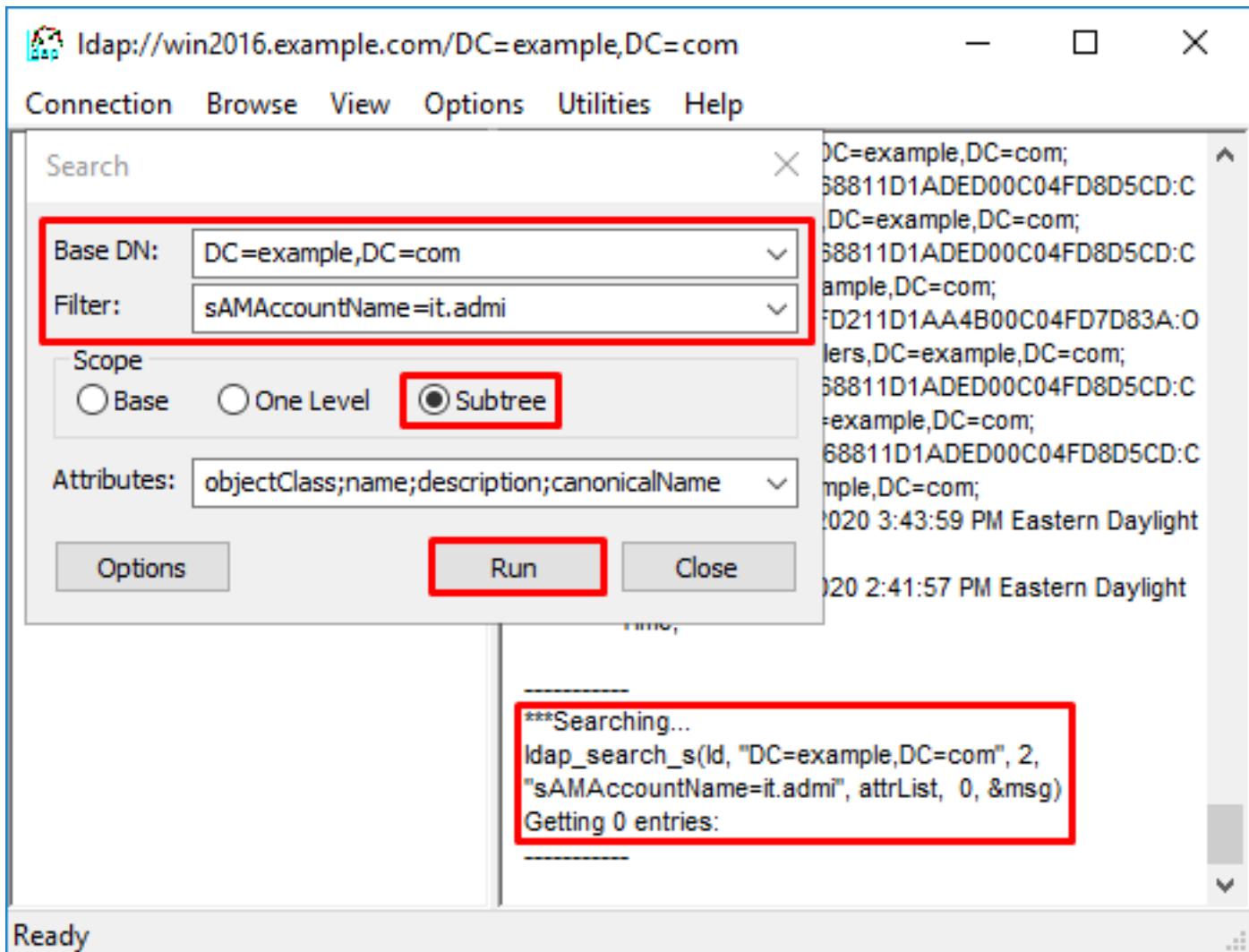
ةروصل ا يف حضوم و ه امك ثحب قوف رقنا مث يس اس األا DN قوف نمي ا س و امل رزب رقنا.



Create a new document

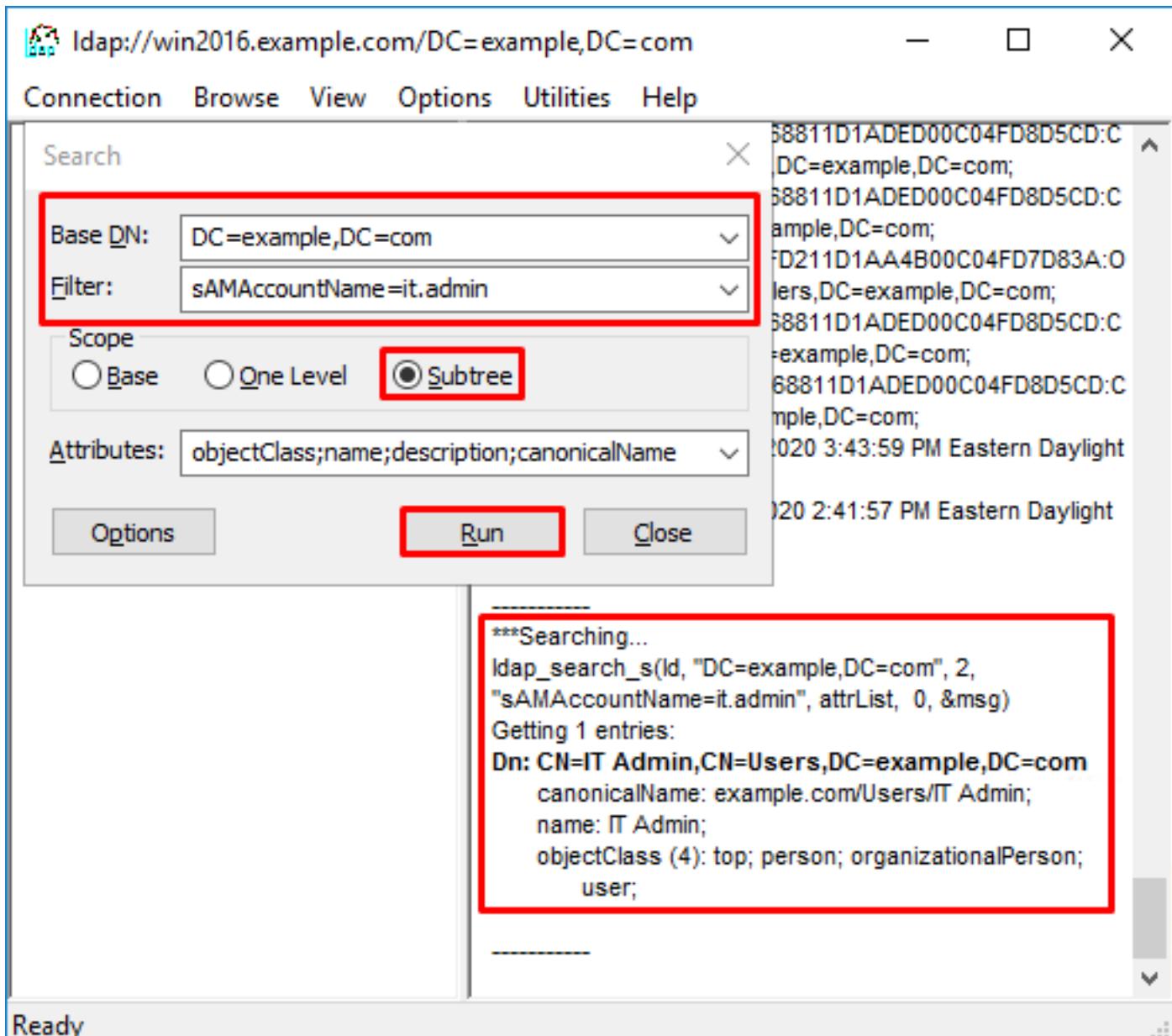
يىف رەھەت امك ئىس اسألا قاطنلار ئىفصىتلار لەماعو (DB) تانايىبلا ئەدعاق مىق سەفن دەح. هذه، لاثملا اذه يىف. ئاطخألا حىحصىت:

- ئىس اسألا DN ئەكباش: dc=example,dc=com
- ئىفصىتلار لەماع: samaccountName=it.admin
- ئىعرفىلار ئەرجىشلى: قاطنلار



مساب مدخلتسم باسح دوجو مدخل ارظن تالاخدا نع LDP ثحبی samaccountName=it.admin لفسا ایسالا DN example.dc=com.

فلت خم ۃجیتن حیح حصل ایسالا DN تحت دحاو لاخدا نع LDP ثحبی samaccountName=it.admin عبطي و example.dc=com مدخلتسلاب صالحیا.



Ready

مدخلة سمل امسال ٰ حیحص ریغ رورم لام ملک

```

[-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

```

عاهتن ا مدع نمو حي حص لكش ب مدخلت سمل رورم ظملك نويوكت نم ققحت لمحمل ا لحل ا
مادخت ساب AD دض طبر عارج اب FTD موقيس، لوح دل ا ليج ستل DN عم لاحل ا واه امك واه تي حالص
يلع AD ۀ ردق نم ققحت لـ ldap يف طبر لـ اذه ذيفنـت نكمـي اـمـكـ. مـدخلـتـسـمـلـاـ دـامـتـعـاـ تـانـاـيـبـ
يف LDP يـفـ تـاوـطـخـلـاـ رـهـظـتـ. رـوـرـمـلـاـ ظـمـلـكـ وـمـدـخـلـتـسـمـلـاـ مـسـاـ دـامـتـعـاـ تـانـاـيـبـ سـفـنـ لـيـلـعـ فـرـعـتـلـاـ
وعـجـارـمـ نـكـمـيـ،ـ كـلـذـلـىـ ۀـ فـاضـإـلـاـ. ۀـ حـيـحـصـ رـيـغـ رـوـرـمـ ظـمـلـكـ وـأـوـ مـسـقـلـاـ طـبـرـ لـوـخـدـ لـيـجـ سـتـ DNـ
لـمـتحـمـ بـبـسـلـ "ـ مـدـاخـ ثـادـحـ ضـرـاعـ"ـ تـالـجـسـ Microsoftـ.

رابـتـخـاـ AAA

مـدخلـتـسـمـ مـسـاـ مـادـخـتـسـابـ FTDـ نـمـ ۀـ قـدـاصـمـ ۀـ لـواـحـمـ ۀـ اـحـمـلـ testـ aaaـserverـ رـمـأـلـاـ مـادـخـتـسـاـ نـكـمـيـ
وـهـ رـمـأـلـاـ. ۀـ قـدـاصـمـلـاـ وـأـلـاـصـتـالـاـ لـشـفـ تـالـاحـ رـابـتـخـالـ اـذهـ مـادـخـتـسـاـ نـكـمـيـ. نـيـدـحـمـ رـوـرـمـ ظـمـلـكـ وـ
فـيـضـمـلـاـ aaaـ [AD IP/hostname].

```

> 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 ftp.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

```

مزـحـلـاـ طـاقـتـلـاـ

مزـحـ تـرـدـاغـ اـذـاـ ADـ مـدـاخـ لـلـوـصـولـاـ ۀـ يـنـاـكـمـاـ نـمـ قـقـحـتـلـلـ مـزـحـلـاـ تـاعـوـمـجـمـ مـادـخـتـسـاـ نـكـمـيـ
يـجـوـتـلـاـ يـفـ ۀـ لـكـشـمـ لـلـاـ كـلـذـ رـيـشـيـ دقـفـ،ـ ۀـ بـاجـتـسـاـ دـجـوتـ الـ نـكـلـوـ،ـ FTDـ.

رورم ۀـ كـرـحـ هـاجـتـاـ يـئـانـثـ يـدـبـيـ نـأـمـ طـاقـتـلـاـ اـنـهـ:

```

> 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

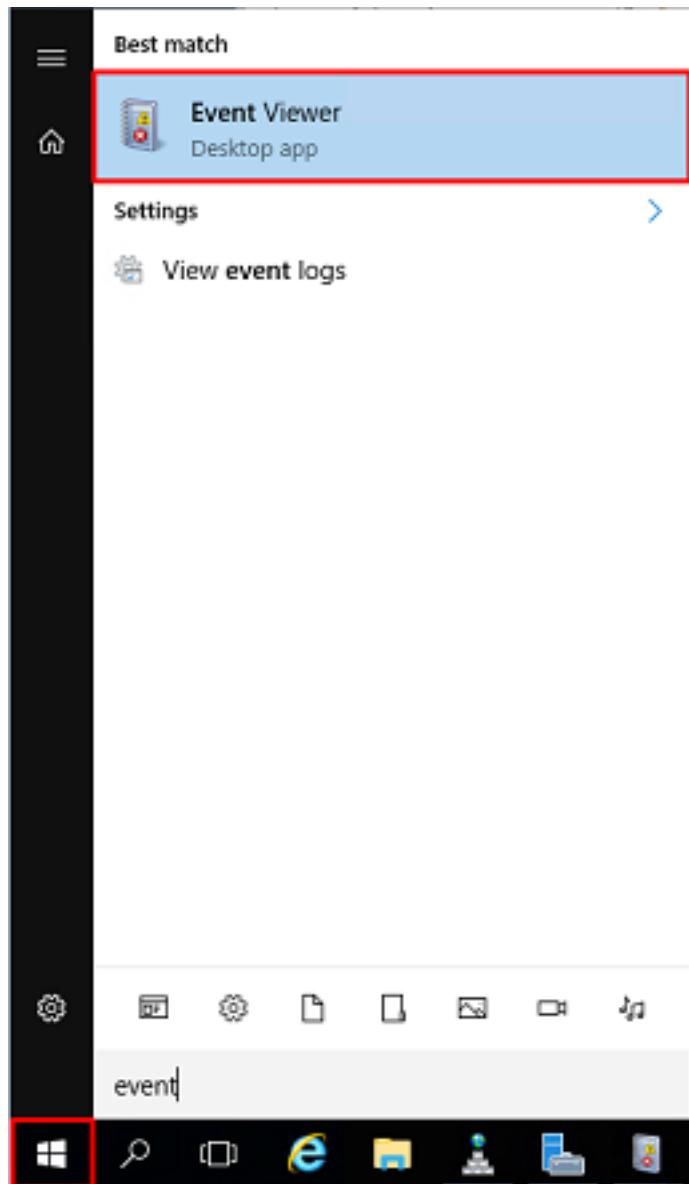
1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
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>
[...]
54 packets shown

```

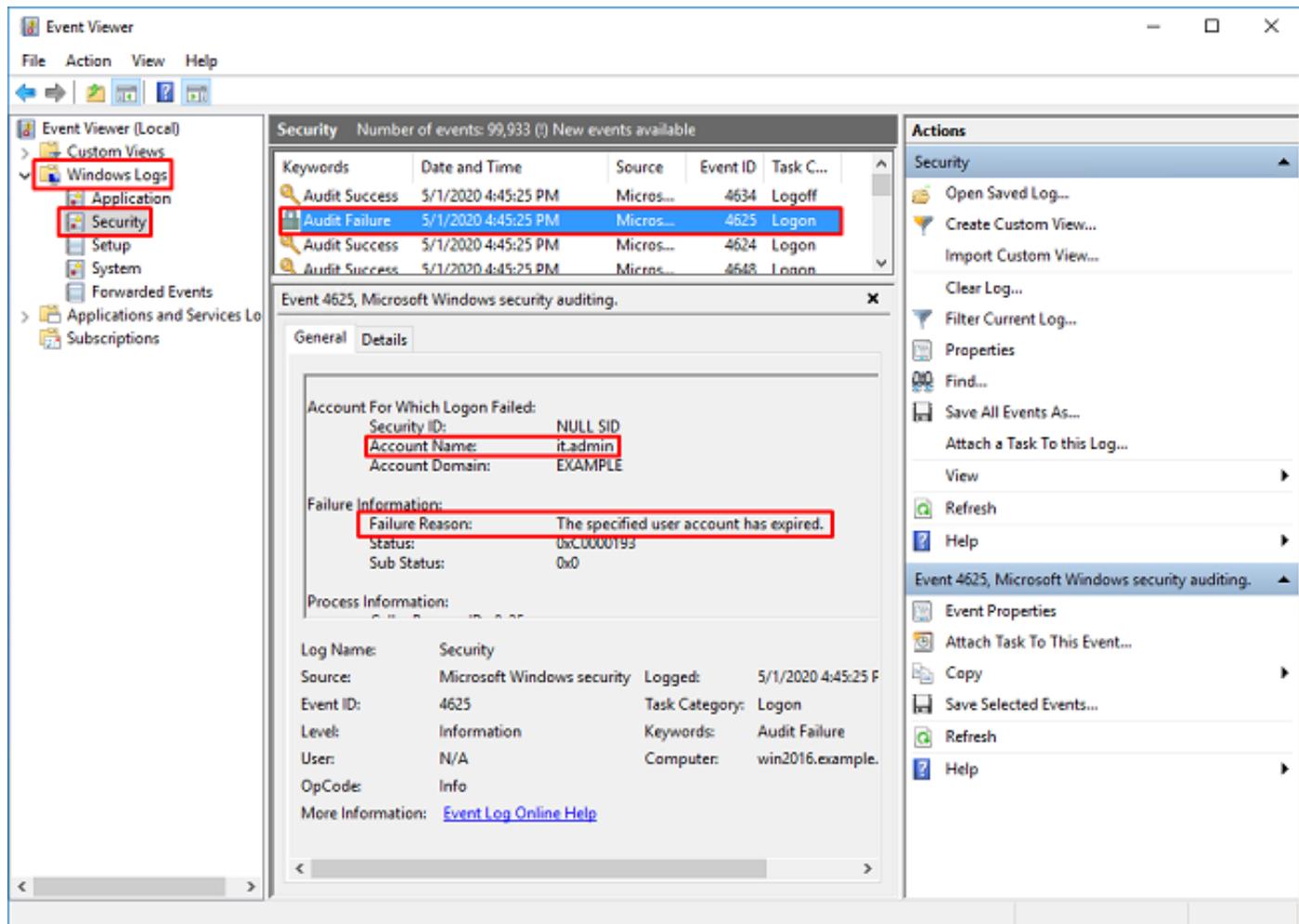
ثادحأ ضراع تالجس Windows Server

الىصفت رثكأ تامولعم ريفوتب "AD" مداخ "دوجوملا" ثادحألا ضراع" تالجس موقف لطع ثودج ببس لوح.

1. حاتف او ثادحألا ضراع نع ثحبلا.



مسا مادختساب قيقدتلا لشف نع ثحبا. ناما قوف رقناو Windows تالجس عيسوب مق.
ةروصلایف حضوم وه امک لشفلا تامولعم عجارو مدخلتسملاباسح



An account failed to log on.

Subject:
Security ID:SYSTEM
Account Name:WIN2016\$
Account 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

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).