AnyConnect ءالمعل AD ةقداصم نيوكت

تايوتحملا

<u>ةمدق مل ا</u>
<u>قي س اس أل ا ت ابل طت مل ا</u>
<u>تابلطتملا</u>
<u>قمدختس مل اتان وكمل ا</u>
مەر باس أ تامول عم
ان ي وكت ا
معيد المقاد من المقاد من المقاد من المعاد المعاد المعاد الم
<u>ت جوم مردن ۲۰۱۰ و ي شاهران ۲۰۱۰ و ي شاهران ۲۰۱</u>
<u> </u>
STARTTLS وأ LDAP ل طقرف بول طم) LDAP ب ص إخل SSL قدامش رذج خس ن
<u>FMC تانېوكت</u>
<u>مىخرىتانا ئىم قىقرىتانا</u>
<u>دادعال ا مل اع</u>
<u>AD ققداصمل AnyConnect ني،وكت</u>
مدختسمليا قيوما، نامأليا تاسايس نيوكتو قيومايا چەن نيكمت
<u>NAT ءان، تسا نيوكت NAT</u>
يشينانا
<u>قحصلاً نم ققحتاً،</u>
يريعناهناليا بجيتارتيليا
<u>AAA ني،وكت</u>
<u>AnyConnect نويوكت</u>
<u>اەنم قىقىچىلىاۋ AnyConnect نىم لىوصوليا يىف مەچىليا قسىلېس دغاۋقىپ لىاص،تىليا</u>
<u>FMC ل.اص.تا. ثادحاً مادختس.اب ق.ق.حتاا</u>
<u>امحالص او ءاطخأل ا فاشكتس ا</u>
<u> الطخال الحجيج صت</u>
<u>قل ماعل ا LDAP عاطخاً حيحصت</u>
<u>LDAP مداخب ل.اص.تا عاش.نا رذعت</u>
<u>قحيحص ريغ رورمليا قملك وأ/و DN يف طبرل التجس</u>
<u>مدختسما ا مسا یا عروثعا ا LDAP مداخ یا ع ردعت</u>
<u>مِدِخَتِسِمِلِ،ا مِسِال قَحِيحِص رِيغَ رورمِلِ،ا قَمِلِك</u>
٨٨٨ رابتخا
مزجل اطاق تل ا تا علمع
<u>Windows Server ثادحاً ضراع تالجس</u>

ةمدقملا

مقداصم نيوكت ةيفيك دنتسملا اذه حضوي Active Directory (AD) ءالمعل AnyConnect ديدهت يعافدب ةلصتملا FirePOWER (FTD).

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ترادإ زكرم ىلع (VPN) قرادا زكرم ىلع (VPN) قيرهاظلا قصاخلا RA قكبش نيوكت
- FMC ىلع (LDAP) ليلدلل لوصولل فيفخلا لوكوتوربلا مداخ نيوكت •
- مردخ Active Directory (AD)
- الماكلاب لەؤملا لاجملا مسا
- تامدخ Intersight Infrastructure (IIS)
- (RDP) ديعبلا بتكملا حطس لوكوتورب •

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Microsoft 2016 مداخ
- FMCv 6.5.0 ليغشت
- FTDv 6.5.0 ليغْشت

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

مت من يوكت ةيفيك دنتسملا اذه حضوي Active Directory (AD) عالمعل AnyConnect مال اذه حضوي قرادإ زكرم ةطساوب اهترادإ متت يتلاو ،FirePOWER (FTD) ديدهت تاعافدب قلصتملا FirePOWER (FMC).

يمدختسم دييقتل لوصولا تاسايس يف مدختسملا ةيوه مادختسإ متي AnyConnect ةنيعم ذفانمو IP نيوانعب.

نيوكتلا

ويرانيسلاو ةكبشلل يطيطختلا مسرلا



ليلد يف .مدختسملا ةيوه رابتخال RDP و IIS مادختساب اقبسم Windows مداخ نيوكت مت

نيتعومجمو نيمدختسم تاباسح ةثالث ءاشنإ متي ،اذه نيوكتلا.

:نيمدختسملا تاباسح

- مداخب طابترالاب FTD ل حامسلل ليلد باسحك باسحلا اذه مادختسإ متي FTD لوؤسم Active Directory.
- مدختسملا ةيوه راهظإل رابتخالا لوؤسم باسح مدختسي :تامولعملا ةينقت لوؤسم.
- .مدختسملا ةيوه راهظإل مدختسي رابتخا مدختسم باسح :رابتخالا مدختسم.

:تاعومجملا

- AnyConnect Admins: راەظإل اەيلإ تامولعملا ةينقت لوؤسم ةفاضإ متت رابتخإ ةعومجم Windows Server. ىلإ طقف RDP لوصو اەيدل ةعومجملا ەذە .مدختسملا قيوە
- مدختسملا ةيوه ضرعل مدختسمل رابتخإ ةعومجم ةفاضاً متت AnyConnect ومُدختسم. طقف Windows Server يلإ HTTP لوصو اهيدل ةعومجملاً هذه.

Active Directory تانيوكت

ليلق ددع رفوت مزلي ،FTD ىلع بسانم لكشب مدختسملا ةيوهو AD ةقداصم نيوكت لجأ نم ميقلا نم.

ىلع نيوكتلا ءارجإ لبق Microsoft Server ىلع اهعيمجت وأ ليصافتلا هذه عيمج ءاشنإ بجي FMC. يه ةيسيئرلا ميقلا:

• الاجملامسا:

لاجملا مسا وه example.com نوكي ،اذه نيوكتلا ليلد يف .مداخلا لاجم مسا وه اذه.

• مداخلل IP/FQDN ناونع:

بجيف ،FQDN مادختسإ مت اذإ .Microsoft مداخ ىلإ لوصولل مدختسملا FQDN وأ IP ناونع و FTD لخاد DNS مداخ نيوكت FQDN.

ىلإ لحلا متي يذلا) win2016.example.com يه ةميقلا هذه ،اذه نيوكتلا ليلد يف 192.168.1.1).

• مداخلا ذفنم:

ذفنم STARTTLS و LDAP مدختسي ،يضارتفا لكشب .ةمدخ LDAP لا ب لمعتسي ءانيملا TCP 636. ل و LDAP و LDAP ل SSL (LDAPs) ربع LDAP و LDAP ل

• :رذجلا قدصملا عجرملا

عيقوتل مدختسملا رذجلا قدصملا عجرملا نوكي ،STARTTLS وأ LDAP مادختسإ ةلاح يف ابولطم LDAPs ةطساوب ةمدختسملا SSL ةداهش.

• ارورملا ةملكو ليلدلا مدختسم مسا:

نيمدختسملا ةقداصمو LDAP مداخب طبرلل FTD و FMC لبق نم مدختسملا باسحلا وه اذه تاعومجملاو نيمدختسملا نع ثحبلاو. .ضرغلا اذهل "FTD لوؤسم" مساب باسح ءاشنإ مت

• (DN) ةعومجملاو ةدعاقلل زيمملا مسالا.

نع ثحبلا ءدبب Active Directory مالعإب FTD موقيو FMC ءدبلا ةطقن يه يساسألا DN مەتقداصمو نيمدختسملا.

ءدبلا ناكمب Active Directory ملعت يتلا FMC ءدبلا ةطقن يه ةعومجملل DN نإف ،لثملابو مدختسملا ةيوهل تاعومجم نع ثحبلا يف.

ال الجمل مادختسإ متي ،اذه نيوكتلا ليلد يف DN مادختس متي ،اذه نيوكتلا ليلد يف DN مادختس متي ،اذه نيوكتلا ليل DN م الم من اللا من المال المال

جردتلا لخاد رثكأ يساسألا DNو DN مادختسإ نوكي ،جاتنإلا ةئيبل ةبسنلاب ،كلذ عمو ل ضفألا وه LDAP ل يمرهلا.

LDAP: ل يمرەلا جردتلا اذە ،لاثملا ليبس ىلع



اضيأ لوخدلا ليجستب ةيلاملا ةيميظنتلا ةدحولا نمض User1 ل اضيأ اذه حمسي ،كلذ عمو قيوستلاو ةيلاملا نوؤشلا ىلإ لقتنيو رذجلا نم أدبي مدختسملا نع ثحبلا نأ ثيح ثحبلاو.

example.com ىلع ةيساسألا DN ةكبش نييعت مت



،ەلبق امو قيوستلا ةسسۇم ةدحو يف ديحولا مدختسملا ىلا لوخدلا ليجست دييقت لجأ نم. قيوستلا ىلع يساسألا DN نييعت كلذ نم الدب لوؤسملل نكمي. .قيوستلا يف أدبي ثحبلا نأل ةقداصملا طقف User3 و User2 ل نآلا نكمي

قيوستلا ىلع يساسألا DN نييعت



نيمدختسملل حمسي يذلاو FTD لخاد تايوتسملا ددعتم مكحتلا نم ديزمل هنأ ظحال مهب ةصاخلا AD تامس ىلإ ادانتسا نيمدختسملل فلتخم ضيوفت نييعت وأ ليصوتب، LDAP. ضيوفت ةطيرخ نيوكت مزلي

مي ديزم يلع روثعلا نكمي AnyConnect LDAP <u>طيطخت نيوكت</u> :انه رمألا اذه لوح تامولعملا نم ديزم يلع روثعلا نكمي <u>FirePOWER (FTD)</u>.

مادختسإ متيو اذه نيوكتلا ليلد يف طسبملا LDAP ل يمرهلا جردتلا اذه مادختسإ متي DN مادختس متي المتي متي DN مادختس رذجلل DN و يساسألا DN نم لكل example.com رذجل



ةعومجملل DN و يساسألI LDAP DN ديدحت

.رتويبمكلا ةزهجأو Active Directory يمدختسم حتف .1



تانايب قارتخأ مت اذإ ةكبشلا لخاد رخآ ناكم ىلإ هب حرصملا ريغ لوصولا عنم وه لصفنم طبرلل ةمدختسملا دامتعالا.

.ةعومجملاب صاخلا DN وأ يساسألا DN قاطن نمض باسحلا اذه نوكي نأ مزلي ال

ا قوف نميألاا سواملا رزب رقنا Active Directory User and Computers، ألا سواملا رزب رقنا اميل إ FTD باسح ةفاضإ تمت يتلا.

مدختسملا مسا لفسأ نومدختسملا ةيواح نمض FTD باسح ةفاضإ متت ،نيوكتلا اذه يف <u>ftd.admin@example.com.</u>

مدختسم < ديدج ىلإ لقتنا مث ،نيمدختسملا قوف نميألا سواملا رزب رقنا.

Active Directory Users and Com	puters			-	х
File Action View Help					
🗢 🔿 🙍 🚾 🖌 🖬 🗶 🛛	🗉 🖻 📑 🖬	n 🙎 🔌 🛍 🤊	7 🗕 🕱		
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co ntrol	Type User Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests		Ŷ
All Tasks View Refresh Export List Properties	ers	Security Group Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr	All domain users		
Help	WseAlertA WseAllow WseAllow	msImaging-PSP MSMQ Queue A Printer User Shared Folder	s lias		v

2. مدختسم - ديدج نئاك جلاعم ىلإ لقتنا.

New Object - User		х
Create in:	example.com/Users	
<u>First name:</u>	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	Х
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

ةينقت لوؤسم امەو ،نييفاضإ نيباسح ءاشنإ مت .FTD باسح ءاشنإ نم ققحت .3 رابتخالا مدختسمو تامولعملا.

Active Directory Users and Computers					,	×
File Action View Help						
🗢 🔿 🖄 🖂 🖌 🗎 🌾	i 🧟 🔒 🛛 🖬	1 🗏 🐮 🕅 🦷	7 🗵 🗽			
Active Directory Users and Com Saved Queries Example.com Builtin Computers Domain Controllers Managed Service Accour Users	Name DefaultAcco Denied ROD DonsAdmins DonsUpdateP Domain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domai	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group User User User User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests Designated administrato Members of this group Members of this group Built-in account for gue Members of this group Members of this group Designated administrato			^
	178 (17 11 - 1 - 1 - 1					

(يرايتخإ) تانالعإ تاعومجم ىلإ نيمدختسم ةفاضإو تانالعإ تاعومجم ءاشنإ

قيبطت ليەستل تاعومجملا مادختسإ نكمي ،ةقداصملا ىلا ةجاحلا مدع نم مغرلا ىلعو لوصولا تاسايس LDAP. ضيوفت ىلا ةفاضإلاب نيمدختسم ةدع ىلع لوصولا تاسايس

لوصولاب مكحتلا جەن تادادعإ قيبطتل تاعومجملا مادختسإ متي ،اذە نيوكتلا ليلد يف لخاد مدختسملا ةيوە لالخ نم اقحال FMC.

ا ةدحولا وأ ةيواحلا قوف نميألاا سواملا رزب رقنا Active Directory User and Computers، يف اهيلإ ةديدجلا ةعومجملا ةفاضإ تمت يتلا ةيميظنتلاا.

نومدختسم ةيواحلا نمض ةعومجملا يف AnyConnect يلوؤسم ةفاضإ متت ،لاثملا اذه يف. ةعومجم < ديدج ىلإ لقتنا مث ،نيمدختسملا قوف نميألا سواملا رزب رقنا.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🖄 📰 🔏 🖬 🗙 🛙	🗈 🙆 📑 🔽 🖬	1 🕺 🔌 🗈 🤋	7 🧕 🕱		
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DnsUpdateP DnsUpdateP Domain Ad Domain Co n e ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		^
All Tasks View Refresh	>	Computer Contact Group InetOrgPerson msDS-KeyCreder	, itial		
Export List Properties Help	Read-only	msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al	ropertyList incipalContainer i ias		
< >> Creates a new item in this container.	Schema A	User Shared Folder			v

.ةعومجم - ديدج نﺉاك جلاعم ىلإ لقتنا .2

New Object - Group	×
Create in: example.com/	Users
Group name:	
AnyConnect Admins	
Group name (pre-Windows 2000):	
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
 Global 	Obistribution
OUniversal	
	OK Cancel

AnyConnect. يمدختسم ةعومجم ءاشنإ اضيأ متي .ةعومجملا ءاشنإ نم ققحت .3

، نيوكتلا اذه يف .صئاصخ رتخأ مث (نيمدختسملا) ةعومجملا قوف نميألا سواملا رزب رقنا .4 متتو AnyConnect يلوؤسم ةعومجم ىل مدختسملل تامولعملا ةينقت لوؤسم ةفاضإ متت مدختسم ةعومجم ىل مدختسمل ا مدختسملا رابتخا مدختسم قاضا

Active Directory Users and Computers					×
File Action View Help					
🗢 🔿 🙍 📆 🐇 🗈 🗶 🖫] @ 🗟 🛛 🖬 🖏 !	k 🛙 🔻 🧕 k	Ł		
Active Directory Users and Com Saved Queries	Name	Туре	Description		^
 example.com Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Donied RODC Passw DnsAdmins DnsUpdateProxy Domain Admins Domain Computers Domain Computers	Security Group User Security Group Security Group User Security Group Security Group Security Group Security Group Security Group Security Group	Add to a group Buil Move Mer Send Mail Mer All Tasks A u: Cut DNS Delete DNS Rename Des All v Properties All v Help	>	
< >>	Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Security Group Security Group Security Group Security Group User Security Group User User User Security Group	All domain users All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		~
Renames the current selection.	178 S 111				

.ةفاضإ قوف رقنا ،ءاضعأ بيوبتلا ةمالع تحت .5

AnyConnect Admins	Properties			?	×
General Members	Member Of	Managed By			
Members:					
Name	Active Dir	ectory Domain	Services Folder		
Add	Remove				
		OK	Cancel	Ac	ply

ىلع روثعلا نم ققحتلل ءامسألاا نم ققحتلا قوف رقناو لقحلا يف مدختسملا لخدأ ما تقطقط ،ققحتلا مت نإ ام .مدختسملا

Select Users, Contacts, Computers, Service Accounts, or Groups	×
Select this object type:	Object Topos
From this location:	Zelece (Abea
Example.com	Locations
T Admin (t. admin@example.com)	Qheck Names
Advanced OK	Cancel

رابتخإ مدختسم ةفاضإ متت امك .قفاوم قوف رقنا مث حيحصلا مدختسملا ةفاضإ نم ققحت مدختسم ةعومجم ىلٍ مدختسملاً.

AnyConnect Admin	s Properties			?	х
General Members	Member Of	Managed B	У		
Members:					
Name LT Admin	Active Dir example o	ectory Domai com/Users	n Services Folde	r	
Add	Remove				
		OK	Cancel	Aç	ply

(STARTTLS وأ LDAPs ل طقف بولطم) LDAP ب صاخلاا SSL ةداهش رذج خسن

.OK قوف رقنا مث .mmc.exe لخدأو Win+R ىلع طغضا .1



.ةيفاضإلا ةادألا ةلازإ/ةفاضإ < فلم ىلإ لقتنا .2

Tonsole1 - [Console Root]		- 🗆 ×
File Action View Favorites Window	v Help	- 8 ×
New Ctrl+N		
Open Ctrl+O	Actions	
Save Ctrl+S	There are no items to show in this view. Console Root	-
Save As	More Actions	,
Add/Remove Snap-in Ctrl+M		
Options		
1 dnsmgmt		
2 014		
Edt		

ةفاضإ ىلع رقنا مث تاداهشلا ددح ،ةحاتملا ةيفاضإلا تاودألا تحت .3.

	Vendor /	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor			Demove
Active Directory Use	Mcrosoft Cor			
ActiveX Control	Microsoft Cor	_		Move Up
ADSI Edit	Microsoft Cor			Move Down
Authorization Manager	Mcrosoft Cor	<u>A</u> dd >		
Certificate Templates	Mcrosoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and	~		Advanced
Computer Managem Device Manager Disk Management ription: Certificates snap-in allo	Microsoft Cor Microsoft Cor Microsoft and	♥ the contents of the	e certificate stores for yourself, a	Ad <u>v</u> anced

.يلاتلا قوف رقنا مث رتويبمكلا باسح ددح .4

Certificates snap-in	×
This snap-in will always manage certificates for: 	
< Back <u>N</u> ext > Cancel	

.ءاەنإ قوف رقنا

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage:	
< Back Finish Cancel	

.OK قوف رقنا .5

Vendor	^		Console Root	Edit Extensions
Microsoft Cor			Certificates (Local Computer)	Remove
Microsoft Cor				
Microsoft Cor				Maria
Microsoft Cor				Move Up
Microsoft Cor				Move Down
Mcrosoft Cor		<u>A</u> dd >		
Microsoft Cor				
Microsoft and				Advanced
	Vendor Microsoft Cor Microsoft Cor	Vendor Microsoft Cor Microsoft Cor	Vendor Microsoft Cor Microsoft Cor	Vendor Image: Console Root Microsoft Cor Image: Console Root Microsoft Cor

ةمدختسملا ةداەشلا رادصإ متي .تاداەشلا قوف رقنا مث ،يصخشلا دلجملا عيسوتب مق .6 مداخب صاخلا (FQDN) لماكلاب لەؤملا لاجملا مسا ىلإ UDAPs لبق نم مداخلا اذه ىلع قجردم تاداەش.

- لائملاو ىل قرداص قرصم عجرم ةداەش WIN2016-CA.
- example-WIN2016-CA ةطساوب Win2016 ليغشتلا ماظنل ةرداص ةيوه ةداهش
- مطساوب win2016.example.com ىلإ ةرداص ةيوه ةداهش example-win2016-ca.

ىلوألاا تاداەشلا نإف يلاتلابو ،win2016.example.com وە FQDN نوكي ،اذە نيوكتلا ليلد يف ىلإ اەرادصإ مت يتلا ةيوەلا ةداەش .LDAP SSL ةداەشك مادختسالل ةحلاص ريغ ةيناثلاو ل قدصملا عجرملا ةمدخ ةطساوب ايئاقلت اەرادصإ مت ةداەش يە win2016.example.com لايصافتلا نم ققحتلل ةداەشلا ىلع اجودزم ارقن رقنا .Windows Server



:تابلطتملا هذه ةداهشلا يفوتست نأ بجي ،LDAPS ل SSL ةداهشك اهمادختسإ متي يكل .7

- مداخب صاخلا FQDN عوضومل ليدبلا مسالا وأ عئاشلا مسالا قباطتي Windows.
- .نسحمل حاتفمل مادختس لقح نمض مداخل قداصم ىلع قداهشل يوتحت

دجوي ،ليدبلا عوضوملا مساو عوضوملا ددح ،ةداەشلل ليصافت بيوبتلا ةمالع تحت FQDN دجوي ،ليدبلا عوضومل مساو عوضومل ددح ،ةداەشلل ليصافت بيوبتلا قمالع تحت

💀 Certificate	×
General Details Certification Path	1
Show: <ai></ai>	\sim
Field	Value ^
Subject	win2016.example.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Certificate Template Name	DomainController
Enhanced Key Usage	Client Authentication (1.3.6.1
SMIME Capabilities	[1]SMIME Capability: Object I
Subject Key Identifier	30 b7 2b 4e 48 0f 2f 17 17 e6
733 gumonity key inentitier	X49/112303F263776111144
CN = win2016.example.com	
I	
5	t Properties Conv. to File
	copy to mean
	ОК

مداخلا ةقداصم دجوت ،حيتافملل نسحملا مادختسالا تحت.

🙀 Certificate			×
General Details	Certification Pat	h	
Show: <ai></ai>		\sim	
Field		Value	^
Subject		win2016.example.com	
Public key		RSA (2048 Bits)	
Public key p	varameters	05 00	
Certificate	Template Name	DomainController	
Enhanced H	(ey Usage	Client Authentication (1.3.6.1	
SMIME Cap	abilities	[1]SMIME Capability: Object I	
Subject Ke	/ Identifier	30 b7 2b 4e 48 0f 2f 17 17 e6	
Authority K	ev Identifier	KevID=3d 9f 26 37 fb 11 1f 4	v
Client Authentic Server Authent	ation (1.3.6.1.5.5 ication (1.3.6.1.5.	5.7.3.1)	
	Ę	dit Properties Copy to File.	

يه يتلا ايلعلا ةداهشلا ددح ،ةداهشلا راسم بيوبتلا ةمالع تحت ،كلذ نم دكأتلا درجمب .8 ةداهشلا ضرع قوف رقنا مث ،رذجلا قدصملا عجرملا قداهش.

💼 Certificate	×
General Details Certification Path	
Certification path	_
win2016.example.com	
View Certificate	
Certificate status:	
This certificate is OK.	
	_
0	к

.رذجلا قدصملا عجرملا ةداەشل تاداەشلا ليصافت حتف ىلإ كلذ يدؤي .9

Certificate	×
General Details Certification Path	
Certificate Information This certificate is intended for the following purpose(s): • Al issuance policies • Al application policies	
Issued to: example-W/IN2016-CA	
Issued by: example-W/IN2016-CA	
Valid from 4/27/2020 to 4/19/2060	
Issuer Statement	I
OK	

.فلم ىلإ خسن قوف رقنا ،ليصافت بيوبتلا ةمالع تحت

💼 Certificate		×
General Details Certification Path	1	
Show: <al></al>	\sim	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from Subject	V3 13 86 46 e5 9d 70 4f a9 4e 35 sha256RSA sha256 example-WIN2016-CA Monday, April 27, 2020 10:50: Monday, April 19, 2060 10:50: example-WIN2016-CA	¥
E	dit Properties	
	OF	¢

اقيسنتب رذجلا قدصملا عجرملا جلاعملا ردصي .تاداەشلا ريدصت جلاعم ربع لقتنا .10 PEM.

🗧 ᡒ 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, dick Next.	
<u>N</u> ext Cancel	

ددح Base-64 زمرملا 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:	
	O 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	

ەريدصت متي نيأو فلملا مسا ددح.

		\times
÷	🍜 Certificate Export Wizard	
	File to Export Specify the same of the file you want to expect	
	specify the name of the net you want to export	
		_
	File name:	
	Browse	
	Next Cancel	

save As				×
← → ∽ ↑ 🔜 > This PC > Desktop		✓ ひ Search Des	ktop	Q,
Organize 🔻 New folder			800	• 🕜
Name Name	Date modified	Туре	Size	
Desktop	No items match your searc	h.		
🖶 Downloads 🛷				
🗄 Documents 🖈				
📰 Pictures 🛷				
System32				
💻 This PC				
i Network				
File name: root				~
Save as type: Base64 Encoded X.509 (*.cer)				~
∧ Hide Folders		Save		Cancel

		X
←	Sertificate Export Wizard	
	Specify the name of the file you want to export	
	Ele name:	
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cance	ł

.ءاەنإ قوف رقنا نآلا



اذه ضرعي .رخآ صوصن ررحم يأ وأ ةركفم مادختساب ةداهشلا حتفاو عقوملا ىلإ لقتنا .11 قيسنت ةداهش PEM. قيان تقاول اذه ظفحا.

----BEGIN CERTIFICATE-----

MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJ1eGFtcGx1LVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDAOMTkxNDUwNT1aMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV 00+k6dVVY/E5qVkEKSGoY+v940S23161zdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfA1LPuM aob4XE/0zxYQpPa18djsNnskfcFqD/HOTFQN4+Sr0hHw1RnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKq0L7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00 BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xp11IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscbubR1+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFfQV3DgZg+R96 9WLCR30big6xyo9Zu+1ixcWpdrbAD06zMhbEYEhkh00jBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33Pp1W6E -----END CERTIFICATE-----

لبق نم اهمادختسإ نكمي يتلا ةيوهلا تاداهش نم ديدعلا دوجو ةلاح يف (يرايتخإ) .12 نم ،LDAP مداخ ىلإ لوصو دوجو مدع وأ ،مدختسملا ةيهامب قلعتي اميف نيقي مدع كانه ناكو دعب FTD وأ Windows مداخ ىلع مت ةمزح طاقتلا نم يرذجلا عجرملا جارختسإ نكمملا

FMC تانيوكت

صيخرتلا نم ققحتلا

قيبطت بجيو ،يكذلا صيخرتلا مداخ عم FTD ليجست مزلي ،AnyConnect نيوكت رشنل ميخرت Apex وأ Apex ميخرت .

.يكذلا صيخرتلا < صيخارتلا < ماظنلا ىل لقتنا .



2. صيخرت مادختساب زاهجلا ليجست نم دكأت .حاجنب ةلجسمو ةقفاوتم ةزهجألاا نأ نم دكأت AnyConnect Apex، Plus، وأ VPN وأ

¢	verview	Analysis	Policies	Devices	Objects	AMP Int	elligence				Deplo	•	System Help +	admin 🔻
					Co	onfiguration	Users	Domains	Integration	Updates	Licenses + Smart Licenses	Health	 Monitoring • 	Tools *
	Smart L	icense St	atus					Cisco Sm	art Software Man	un 🔴 🦻				
	Usage Aut	horization:		Authori	zed (Last Syn	chronized On M	fay 03 2020)							

Product Registration:	0	Registered (Last Renewed On Mar 03 2020)
Assigned Virtual Account:		SEC TAC
Export-Controlled Features:		Enabled
Cisco Success Network:		Disabled 0
Cisco Support Diagnostics:		Disabled 🕕

		Filter Devices		× Edit License
License Status	Device Type		Domain	Group
0				
0				
٥				
0				
0				
0				
0	Cisco Firepower Threat Defen	se for VMWare	Global	N/A
	License Status	License Status Device Type		License Status Device Type Demain Columnation Colum

دادعإلا ملاع

.لماكتلا < ماظنلا ىلإ لقتنا .1

Overview	Analysis	Policies	Devices	Objects	АМР	Intelligence					Deploy	🦳 🔒 <mark>s</mark>	ystem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses *	Health 🔻	Monitoring •	Tools *

2. تحت Realms، قوف رقنا مث New Realm.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy Q System Help + adm												
		Configu	ration Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring	Tools 🔻		
Cloud Services Realms	Identity Sources eStr	treamer Host Inpu	t Client Sma	rt Software S	atellite							
								K Compa	are realms	🔇 New realm		
Name	Description 0	Domain	Туре	Base DN	Group	DN	Group Attri	bute	State			

مث .Microsoft مداخ نم اهعيمجت مت يتلا تامولعملا ىلٍ ادانتسا ةبسانملا لوقحلا ألما .3 قوف رقنا OK.

Add New Realm

Name *	LAB-AD	
Description		
Type *	AD 💙	
AD Primary Domain *	example.com	ex: domain.com
AD Join Username		ex: user@domain
AD Join Password		Test AD Join
Directory Username *	ftd.admin@example.com	ex: user@domain
Directory Password *	•••••	
Base DN *	DC-example,DC-com	ex: ou=user,dc=cisco,dc=com
Group DN *	DC=example,DC=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member 💙	
* Dequired Field		
- Keyairea Fiela		
		OK Cancel

4. ليلد ةفاضإ قوف رقنا ،لعفلاب هرايتخإ مت دق نكي مل اذإ ليلد ددح ،ديدجلا راطإلا يف.

Overview	Analysis	Policies	Devices	Objects AMP	Intellig	ence			Deploy	🖉 🍳 Sy	stem Help v	admin 🔻
				Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health •	Monitoring •	Tools •
LAB-AD Enter Descript	ion										Save	Cancel
Directory	Realm Con	figuration	User Down	nload								
											O A	dd directory

طبرلا FTD و FMC ل نكمي ال ،FQDN مادختسإ ةلاح يف هنأ ظحال .AD مداخ ليصافت ألما لحل DNS نيوكت متي مل ام حاجنب DNS لحل DNS تيوكت متي مل ام حاجنب

.ةرادإلا تاهجاو ددحو نيوكت < ماظن ىلإ لقتنا ، FMC ل SNS دادعإل

ةسايس ءاشنإب مق وأ ،يساسألا ماظنلا تادادعإ < ةزهجألا ىلإ لقتنا ،FTD ل DNS دادعإ لجأ نم علإ لقتنا مث ةيلاح قسايس ررح وأ ،ةديدج DNS.

Add directory	? ×
Hostname / IP Address	win2016.example.com
Port	389
Encryption	○ STARTTLS ○ LDAPS ④ None
SSL Certificate	▼ ②
	OK Test Cancel

امسا صيخرتلاا طعأو ،رضخألاا (دئاز) + زمر رقنا ،ةمدختسم STARTTLS وأ LDAPs تناك اذإ ظفح قوف رقنا مث .PEM قيسنتل رذجلا قدصملاً عجرملاً ةداهش خسناو.

Import Trusted Certificate Authority	? ×
Name: LDAPS_ROOT Certificate Data or, choose a file: Browse	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFKMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW10FmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR30big6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhO0jBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E FDD CEDTUFICATE	
	\sim
Encrypted, and the password is:	
Save	Cancel

ةداەشل ةرواجملا ةلدسنملا ةمئاقلا نم اثيدح ەتفاضإ تمت يذلا رذجلا قدصملا عجرملا ددح قوف رقناو STARTTLS وأ LDAPs.

Edit directory		?	×
Hostname / IP Address	win2016.example.com		
Port	636		
Encryption	○ STARTTLS		
SSL Certificate	LDAPS_ROOT 💙 🔕		
	OK Test Cance	el	

رورملا ةملكو ليلدلا مدختسم مساب حاجنب FMC طبر ةيناكمإ نم دكأتلل رابتخإ قوف رقنا ةقباسلا ةوطخلا يف نيرفوملا.

سيلو (FMC) ةيساسألاا ةحوللاا ةرادإ يف مكحتلاا ةدحو نم اهؤدب متي تارابتخالاا هذه نأل ارظنو ةيلخادلا تاهجاولا لثم) FTD ىلع اهنيوكت مت يتلا هيجوتلل قلباقلا تاهجاولا ىدحإ لالخ نم ةجيتنلا سفن نمضي ال (لشافلا وأ) حجانلا لاصتالا نإف ،(DMZ ةطقنلاو ةيجراخلاو TD تاهجاو ىدحإ نم اهؤدب متي AnyConnect LDAP ةقداصم تابلط نأل AnyConnect قلاول التا حاليا ال

ةقداصملا رابتخإ مسق عجار ،FTD نم LDAP تالاصتإ رابتخإ لوح تامولعملا نم ديزمل ءاطخألا فاشكتسأ ةقطنم يف مزحلا طاقتلا مسقو (AAA) ةبساحملاو ضيوفتلاو اهحالصإو.



مدختسملا ةيوەل اەمادختسإ متي يتلا تاعومجملا ليزنتب مق ،مدختسملا ليزنت تحت . ةقحاللا تاوطخلا يف.

ةحاتملا تاعومجملاب صاخلا دومعلاو تاعومجملاو نيمدختسملا ليزنتب صاخلا عبرملا ددح نمض اهنيوكت مت يتلا تاعومجملاب اهتئبعت متي يتلا

مت يتلاا تاعومجملا عيمج نيمضت متي كلذ عمو ،اهداعبتسإ وأ تاعومجملا نيمضت نكمي يضارتفا لكشب ةعومجملاب ةصاخلا DN نمض اهيلع روثعلا.

ةنمضم تاعومجم يأ رفوتت .كلذك مەداعبتسإ وأ نيددحم نيمدختسم نيمضت نكمي امك قحال تقو يف مدختسملا ةيوەل مەدىدحت متيل نيمدختسمو.

ظفح قوف رقنا ،ءاەتنالا دنع.

Overview Analysis Policies Devices Objects	s AMP I	ntelligence						Deplo	📃 🔍 Sy	stem Help 🔻	admin v
		Configuration	Users	Domains	Integration	Upd	lates	Licenses *	Health v	Monitoring •	Tools *
LAB-AD Enter Description								You have un	saved change	s 📑 Save	8 Cancel
Directory Realm Configuration User Download											
Download users and groups											
Begin automatic download at 8 V PM V America/New	York Repeat 6	tvery 24 ¥ Hour									
🛃 Download Now											
Available Groups 😋		Groups to Ir	nduđe (2)				Group	s to Exclude (0)		
Search by name		💰 AnyConn	ect Admina			8	None				
AnyConnect Admins		💣 AnyConn	ect Users			8					
DrisUpdateProxy	^										
A WseRemoteAccessUsers											
A WseInvisibleToDashboard											
Allowed RODC Password Replication Group	Add t										
🝰 Enterprise Key Admins	Includ	fe .									
🝰 Domain Admins	Add t										
A WseAlertAdministrators	Exclud	5a									
🝰 Event Log Readers											
A Replicator											
🝰 Domain Guests											
A Windows Authorization Access Group											
Account Operators											
Aministrators	~	Contraction of	a di sela a				-	Hara Parlacian			
System Managed Accounts Group		Enter User 1	ndusion			Add	Enter	User Exclusion			Add

. ديدجلا لاجملا نيكمت.

Overview Analysis Policie	es Devices Objec	ts AMP 1	Intelligence					Deploy	0, Sys	Atem Help	o ▼ admin ▼
			Configurat	ion Use	ers Domains	Integration	Updates	Licenses 🔻	Health *	Monitorin	ig ▼ Tools ▼
Cloud Services Realms	Identity Sources	eStreamer	Host Input	Client	Smart Software	Satellite					
									Comp	are realms	New realm
Name	Description	Domain	т	ype	Base DN	Grou	up DN	Group Attri	bute	State	
LAB-AD		Global	A	D	DC=example,D	C-com DC-	example,DC=com	member			ቷ 🥖 🔁 🖯

7. إمادختسإ مت اذا CA قرف وأ STARTTLS وأ LDAPs مادختس مت اذا . تاداهشلا < ةزهجألا يل لقتنا ،الوأ اذهب مايقلل.

Overview Analy	is P	Policies	Dev	ices	Objects	AMP In	ntelligence		Deploy	05	System	Help 🔻	admin 🔻
Device Management	N	IAT 1	VPN 🔻	QoS	Platform	Settings	FlexConfig	Certificates					

نيمي ىلعألا يف فيضي ةقطقط.

Overview Analysis	Policies	Device	s 0	bjects	AMP	Intelligence		Deploy	0,	System	Help 🔻	admin 🔻
Device Management	NAT N	/PN +	QoS	Platform	Setting	s FlexConfig	Certificates					
											0	Add

ددخاز) + زمر قوف رقنلا ىلإ LDAP نيوكت ةفاضإ متت ،FTD ددح

Add New Certificate		? >	×					
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.								
Device":	FTD-2	~						
Cert Enrollment*:	Select a certificate entrollment object	▼						
		Add Cancel						

ليجستلا عون ةلدسنملا ةمئاقلا نم يوديلا ليجستلا رتخأ مث لاصتالا ةطقنل مسا حنم. ظفح يلع رقنا مث ،انه PEM رذج قيدصت عجرم ةداهش قصلا.

Add Cert Enrollmer	nt	? ×
Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual	^
CA Certificate:*	 MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki G9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI 3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU tv0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N zSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf d++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo ficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN O7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU aLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuvtmsHBtCieyC062a8BKgOL7N86 	~
Allow Overrides		
	Save	Cancel

.ةفاضإ قوف رقنا مث هؤاشنإ مت يذلIrustPoint ديدحت نم ققحت

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:	FTD-2	~
Cert Enrollment*:	LDAPS_ROOT	~ ©
Cert Enrollment Details:		
Name:	LDAPS_ROOT	
Enrollment Type:	Manual	
SCEP URL:	NA	
		Add Cancel

ةيوەلا ةداەش داريتسإ نأ ركذي ەنأ نم مغرلا ىلع .FTD نمض ةديدجلا ةقثلا ةطقن رەظت ،كلذل .LDAP مداخ نم ةلسرملا SSL ةداەش ةقداصم FTD نم ابولطم سيل ەنأ الإ ،بولطم .قلاسرلا ەذە لەاجت نكمي

Overview Analysis	Policies Devices	Objects AMP Int	telligence	Deploy 🔍 System	Help 🔻 admin 🔻
Device Management	NAT VPN VQ05	6 Platform Settings	FlexConfig Certificates		
					O Add
Name	Domain	Enrollment Typ	e Status		
4 🗐 FTD-1					
FTD-1-PKCS12	Global	PKCS12 file	CA OLD		P 🗘 🗎
4 🗐 FTD-2					
FTD-2-PKCS12	Global	PKCS12 file	CA QID		P 🗘 🗟
FTD-2-Selfsigned	Global	Self-Signed	S CA LD		i? ¢ 🗎
LDAPS_ROOT	Global	Manual	🔍 CA 🛛 🔺 Ide	ntity certificate import required	P 🗘 🗎

AD ةقداصمل AnyConnect نيوكت

ا ءاشنإ مت اذإ .لعفلاب دعب نع لوصولل VPN جەن ءاشنإ متي مل ەنأ تاوطخلا ەذە ضرتفت .1 3. ةوطخلا يطختو جەنلا اذەل "ريرحت" رزلا قوف رقناف ،دحاو

دعب نع لوصولا < VPN < ةزەجألاا ىلإ لقتنا.

Overview Analysis P	olicies	Device	s Obje	ects AMP Intell	igence			Deploy	0	System	Help 🔻	admin v
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates						
		Site To S	ite									
		Remote /	Access									
		Troubles	hooting									

دعب نع لوصولل ديدج VPN جەن ءاشنإل ةفاضإ قوف رقنا

? X

Overview Analysis	Policies Devices Objects	AMP	Intelligence			Deploy	0	System	Help 🔻	admin v
Device Management	NAT VPN + Remote Access	Qo5	Platform Settings	FlexConfig	Certificates					
									0	Add
Name			Status		Last Modified					

No configuration available Add a new configuration

2. ةزەجألاو جەنلل امسا ددح ،جەنلا نييعت تحت .دعب نع لوصولل VPN جەن جلاعم لامكإب مق اەيلع جەنلا قيبطت متي يتلا.

Overview Analysis Policies D	evices Objects AMP I	ntelligence		Deploy 🔒 System	n Help v admin v
Device Management NAT VPN	Remote Access QoS	Platform Settings FlexConfig	Certificates		
Remote Access VPN Policy	Wizard				
1 Policy Assignment 2 0	Connection Profile >3 /	AnyConnect 🔰 🕢 Access &	Certificate $>$ 5 Summary _		
Targeted Devi	ces and Protocols				~
This wizard will gu	ide you through the required minim	al steps to configure the Remote Access	s VPN policy with () Before	You Start	
M THE P MARK "MATTERS			Before you configuration	start, ensure the following elements to be in place to	
Name:*	PTD-2-RA-Policy		complete Ren	note Access VPN Policy.	
Description:			Configure Be	ion Server alm or <u>RADIUS Server Group</u>	
VPN Protocols:	SSL IPsec-IKEv2		to authentica AnyConnect	te VPN clients.	
Targeted Devices:	Available Devices	Selected Device	Make sure y	ou have AnyConnect package	
	🔍 Search	🚍 PTD-2	the relevant it during the	Cisco credentials to download	
	🚌 FTD-1		Denice Tete	aface.	
	PTD-2		Interfaces sh	ould be already configured on	
			as a securit	ces so that they can be used y zone or interface group to	
			enable VPTs a	coma.	
		Add			
					Ť
				Back Next	Cancel

راعتسم مساك اضيأ مدختسي يذلا ليصوتلا فيصوت مسا ددح ،ليصوتلا فيصوت تحت مەليصوت دنع AnyConnect ومدختسم ەاري ةعومجملل.

ةقداصملا مداخ تحت اقبسم هؤاشنإ مت يذلا قاطنلا ددح.

AnyConnect. ءالمعل IP نيوانع نييعت اهب متي يتلا ةقيرطلا ددح

اذه لاصتالا فيرعت فلمل مدختسملا يضارتفالا ةعومجملا جهن ددح.

Overview Analysis Policies Devices Objects AMP	Intelligence	De	ploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT VPN • Remote Access QoS	Platform Settings FlexConfig Certific	ates		
Remote Access VPN Policy Wizard				
1 Policy Assignment 2 Connection Profile 3	AnyConnect > ④ Access & Certifica	te 🔰 🜀 Summary		
Connection Profile:				-
Connection Profiles specify the tunne accomplished and how addresses are	group policies for a VPN connection. These policies p assigned. They also include user attributes, which ar	ertain to creating the tunnel itself, how AAA e defined in group policies.	is	
Connection Profile Name:*	General			
	This name is configured as a connection alias, it can be	used to connect to the VIN gateway		
Authentication, Authorization & A	ccounting (AAA):	will be used for VPM exceptions		
specity the method of autoentocation	(www.cerencebes.or.boon), and the www.servers.cher	ten be used for ven connections.		
Authentication Hethod:	AAA Only			
Authentication Server:*	LAB-AD V G+ (Res	im or RADIUS)		
Authorization Server:	- C (RA)	nus)		
Accounting Server:	- (RA	nus)		
Client Address Assignment:				
Client IP address can be assigned fro assignment is tried in the order of A4	n AAA server, DHCP server and IP address pools. WI A server, DHCP server and IP address pool.	en multiple options are selected, 1P address		
Use AAA Server (RADIUS)	nly) 🕕			
Use DHCP Servers				
Use IP Address Pools				
IPv4 Address Pools:	AnyConnect-Pool 🧳			
IPv6 Address Pools:	1			
Group Policy:				
A group policy is a collection of user- or create a Group Policy object.	riented session attributes which are assigned to clie	it when a VPN connection is established. Sele	ect	
Group Policy:*	DfltGrpPolicy V			
	Edit Group Policy			~
			tack Next	Cancel
			Next Next	Cancel

.مزحلا هذه ديدحتو اهمادختسإ متي يتلا AnyConnect مزح ليمحتب مق ،AnyConnect نمض

Overview Analysis Polici	Bevices Objects AMP 1	ntelligence	Deploy 🔍 System Help 🔻 admin 🔻
Device Management NAT	VPN + Remote Access QoS	Platform Settings FlexConfig Certificates	
Remote Access VPN P	olicy Wizard		
(1) Policy Assignment $>$	 Connection Profile 3 / 	AnyConnect 🔰 🕢 Access & Certificate > 💲 Summar	ry
	AnyConnect Client Image he VPN gateway can automatically downlo	ad the latest AnyConnect package to the client device when the VPN conn	nection is
i	nitiated. Minimize connection setup time by	choosing the appropriate OS for the selected package.	
	Download AnyConnect Client packages from	Cisco Software Download Center. Show Re-order buttons	a
	AnyConnect File Object Name	AnyConnect Client Package Name Operating System	
	anyconnect-linux64-4.7.03052-we	anyconnect-linux64-4.7.03052-webdeploy-k9	v
	anyconnect-win-4.7.00136-webde	anyconnect-win-4.7.00136-webdeploy-k9.pkg Windows	× .
			Back Next Cancel

لجأ نم اهيلإ لوصولا AnyConnect يمدختسمل نكمي يتلا ةمجاولا ددح ،ةداهشلاو لوصولا تحت AnyConnect.

.SSL ةحفاصم ءانثأ FTD لبق نم اهمادختسإ متي يتلا ةداهشلا ديدحت وأ/و ءاشنإب مق

كف مت يتلا رورملا ةكرحل يفافتلالا لوصولاب مكحتلا ةسايسل رايتخالا ةناخ نأ نم دكأت اهؤاشنا مت يتلا مدختسملا ةيوه حبصت ثيحب ةددم ريغ (sysopt allowed-vpn) اهريفشت الاصتال لوعفملا ةذفان اقحال RAVPN.



ءاەنإ قوف رقنا نيوكتلا عجار ،صخلم تحت.

Overview Analysis Policies Devices Obje	ects AMP Intelligence	Deploy 🔒 System Help 🔻	admin v
Device Management NAT VPN • Remote Acc	ess QoS Platform Settings FlexConfig Certificates		
Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Pro	ofile $>$ (3) AnyConnect $>$ (4) Access & Certificate	S Summary	
Remote Access VPN Policy Cor	figuration	Additional Configuration Requirements	~
Firepower Management Center will	configure an RA VPN Policy with the following settings	After the wizard completes, the following	
Name:	PTD-2-RA-Policy	configuration needs to be completed for VPN to work on all device targets.	
Device Targets:	🚍 FTD-2	() Access Control Policy Update	
Connection Profile:	General	An Access Control rule must be defined to allow VPN traffic on all targeted devices.	
Connection Alias:	General	NAT Exemption	
AA4:		If NAT is enabled on the targeted devices, you must define a <u>NAT_Policy</u> to exempt VPN	
Authentication Method:	AAA Only	trathc.	
Authentication Server:	LAB-AD	To resolve hostname specified in AAA Servers	
Authorization Server:	-	or CA Servers, configure DNS using <u>FlexConfig</u> Billion on the targeted devices	
Accounting Server:	-	Port Configuration	
Address Assignment:		SSL will be enabled on port 443.	
Address from AAA:	-	IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect	
DHCP Servers:	-	image download.NAT-Traversal will be enabled by default and will use port 4500.	
Address Pools (IPv4):	🔜 AnyConnect-Pool	Please ensure that these ports are not used in NAT Policy or other services before deploying	
Address Pools (IPv6):		the configuration.	
Group Policy:	E OffcGrpPolicy	A Network Interface Configuration	
AnyConnect Images:	anyconnect-linux54-4.7.03052-webdeploy-k9.pkg	Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'	
Tabadan Objector	anyconnect-win-4.7.00136-webdeploy-k9.pkp		
Interface Objects:	6 outside-zone		
Device Certificates:	FTD-2-Selfsigned		
Device Identity Certificate Enr	ollment		
Certificate enrollment object 'FTD- installation will be initiated on the check the status of the installation	2-Selfsigned' is not installed on one or more targeted devices. Certificate argeted devices on finishing the wizard. Go to the <u>Certificates</u> page to		~
		Back Finish Ca	incel

ة تا قوف رقنا ،دعب نع لوصولا ةسايس < (VPN) ةيرهاظلا ةصاخلا ةكبشلا نمض. بسانملا لاصتالا فيرعت فلم يلع لوصحلل (صاصر ملق) ريرحت.

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🧕 System Help 🔻 admin 🔻
Device Management NAT VPN • Remote Access	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy Enter Description		Save Cancel
Connection Profile Access Interfaces Advanced	1	Policy Assignments (1)
		G
Name	AAA Group Policy	
DefaultWEBVPNGroup	Authentication: None 📑 OftGrpPolicy Authorization: None Accounting: None	/ 0
General	Authentication: LAB-AD (AD) Et Dft:GrpPolicy Authorization: Imm Accounting: Acros	200

اقبسم ەۋاشنإ مت يذلا قاطنلا ىلع ةقداصملا مداخ نييعت نم دكأت.

اوريغي نأ نيمدختسملل حامسلل رورملا ةملك ةرادإ ةحاتإ قيقدت نكمي ،ةمدقتم تادادعإ تحت اهتيحالص يەتنت نأ لبق وأ امدنع مەرورم ةملك.

قوف رقنا ،تارييغت يأ ءارجإ مت اذإ .LDAPs قاطنلا مدختسي نأ بلطتي دادعإلاا اذه نأ ريغ ظفح.

Edit Connection Pr	ofile		? ×
Connection Profile:* Group Policy:*	General DfltGrpPolicy Edit Group Po	y V S	
Client Address Assign	ment AA	Aliases	
Authentication Authentication Meth Authentication Serve	od: er:	AAA Only ¥ LAB-AD (AD)	
L Use secondary an Authorization Authorization Server	r:	Allow connection only if user exists in authorization database	
Accounting Accounting Server:	gs	▼	
Strip Realm from	username username		
Enable Password Notify User Notify user on the second secon	Management days prio	t or to password expiration word expiration	
		Save Cance	el 👘

ظفح قوف رقنا ،ءاەتنالا دنع.

Overview Analys	is Po	olicies	Devices	Objects	AMP	Intelligence				Deploy	e ,	System	Help 🔻	admin •
Device Management	NA	T V	PN • Remo	te Access	QoS	Platform Settings	FlexConfig	Certificates						
FTD-2-RA-Po	licy								You ha	ave unsaved	l chang	e 📔	Save	🔀 Cancel

مدختسملا ةيوەل نامألا تاسايس نيوكتو ةيوەلا جەن نيكمت

.ةيوەلا < لوصولا يف مكحتلا < تاسايسلا ىلإ لقتنا .1



ديدج ةيوه جەن ءاشنإ.

Overview Analysis Policies Devices O	jects AMP Intelligence		eploy 🔍 System Help 🔻 admin 🔻
Access Control > Identity Network Discovery	Application Detectors Correlation	Actions •	
			Object Management Access Control
Identity Policy	Domain	Status	Last Modified
	The	re are no policies created. Add a new policy	

ديدجلا ةيوەلا جەنل امسا ددح.



.ةدعاق ةفاضإ قوف رقنا .2

0	verview Analysis Poli	cies Device	s Objects	AMP Intellig	gence				De	ploy 🔒 Sy	stem Help v	admin 🔻
A	cess Control > Identity	Network Disc	overy Appli	cation Detectors	Correlation	Actions *						
F	TD-2 Identity Poli ter Description	cy									E Save	😢 Cancel
Ru	les Active Authentication											
								Add Category	/ 🖸 Add Ruk	Search Rules		20
	Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Pro	tocol

ةلماخلا ةقداصملا ىلع ءارجإلا نييعت متو اەنيكمت نم دكأت .ةديدجلا ةدعاقلل امسا ددح .3.

هؤاشنإ مت يذلا قاطنلا ددحو (تادادعإلاو قاطنلا) Realm & Settings بيوبتلا ةمالع قوف رقنا ءاهتنالا دنع ةفاضإ قوف رقنا .اقبسم.

Add Ru	le									
Name	RAVPN			🖌 Enable	ed	Insert	into Category	~	Standard Rules	¥
Action	Passive Authentic	cation	*	Realm: LAB-AD (AD)	Authentication Pro	tocol:	HTTP Basic Exclude HT	TTP User-	Agents: None	
	Remote access VP	W sessions are a	ctively authentic	ated by VPN. Other sessio	ins use the rule Action.					
Zone	s Networks	VLAN Tags	Ports						Realm &	Settings
Realm	•	LAB-AD (AI	0)		V					
🗌 Use	active authentica	tion if passive o	r VPN identity ca	nnot be established						
* Requ	ired Field									
								I	Add	Cancel

.ظفح قوف رقنا .4

0	verview Analysis Poli	cies Device	s Objects	AMP Intellig	jence				Dep	play 🧛 Sys	stem Help v av	dmin v	
A	cess Control > Identity	Network Disc	overy Applic	ation Detectors	Correlation	Actions *							
F	FTD-2 Identity Policy You have unsaved changes Save Cancel												
Ru	kes Active Authentication												
								Add Categoria	y 🕓 Add Rule	Search Rules		×	
	Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protoco	al	
Adr	ninistrator Rules												
Thi	s category is empty												
Sta	ndard Rules												
1	RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authentic	ation none	/ 8	
Roo	it Rules												
Thi	s category is empty												

Displaying 1 - 1 of 1 rules |< < Page 1 of 1 > >| C

5. لوصولا يف مكحتاا < لوصولا يف مكحتال < تاسايساا ىل لقتانا.

.اەب صاخلا FTD نيوكت مت يتلا لوصولا يف مكحتلا ةسايس ريرحت .6

Overview Analysis Policies	Devices Objects	AMP Intelligence			Deploy	🛛 🔒 System Help	p v admin v
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions *			
					Object Management Intrusion Netv	ork Analysis Policy DNS	Import/Export
Access Control Policy		Status			Last Modified		
Default-Policy		Targeting 1 de Up-to-date on	evices all targeted devic	es	2020-05-04 09:15:56 Modified by "admin"	9	8 🖉 8

7. ةيوەلا جەنل ةرواجملا ةميقلا قوف رقنا.

Overview Analysis Policies	Devices Objects	AMP Intelligence			Deploy 🧕 System Help 🔻 admin 🔻
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions *	
Default-Policy Enter Description					Analyze Hit Counts 🛛 🔛 Save 🛛 🕄 Cancel
Prefilter Policy: Default Prefilter Policy		55	L Policy: None		Identity Policy: None
					🍞 Inheritance Settings 📉 Policy Assignments (1)

قفاوم قوف رقنا مث اقبسم ەؤاشنإ مت يذلا ةيوەلا جەن ددح.

Identity Policy	
FTD-2 Identity Policy	▼
Revert to Defaults	OK Cancel

ةدعاق ءاشنإ ىلع تاوطخلا هذه لمعت .ةديدج ACP ةدعاق ءاشنإل ةدعاق ةفاضإ قوف رقنا .8 ةكبشلا لخاد ةزهجأب لاصتالاب AnyConnect يلوؤسم ةعومجم نمض مدختسملل حامسلل مادختساب

Overview Analy	sis Polici	es Devi	ces Obje	ects AM	P Intellig	gence						Dep	oloy (0 ₂ System	Help 🔻	admin v
Access Control > /	Access Cont	rol Net	work Disco	very Ap	plication De	tectors	Correlation	n Action	ns ▼							
Default-Policy You have unsaved changes Analyze Hit Counts 🔛 Save 🔞 Cance Enter Description												Cancel				
Prefilter Policy: Defa	Prefilter Policy: Default Prefilter Policy: ETD-2 Identity Policy: ETD-2 Identity Policy															
												Ta Ini	heritance	Settings 🛐	Policy Assi	priments (1)
Rules Security	Intelligence	HTTP Res	ponses	Logging	Advanced											
曲 Fiber by Device							🗆 st	ow Rule Cor	flicts 😣	🔘 Add Cat	iegory [🤇) Add Rule	÷	Search Rules		×
a Name	Sourc	Dest Z	Sourc	Dest N	VLAN	Users	Applic	Sourc	Dest P	URLs	Sourc	Dest S	Action	0 8 4	• • •	•
👻 Mandatory - Del	ault-Policy (•)														
There are no rules in	this section. A	dd Rule or A	dd Category													
👻 Default - Defaul	t-Policy (-)															
There are no rules in	this section. A	dd Rule or A	dd Category													
Default Action										Acces	s Control: Bi	ock All Traffic				× 🔳

Displaying 0 - 0 of 0 rules $|\langle \langle Page | 1 \rangle$ of 1 $\rangle >| C |$ Rules per page: 100 -

بسانملا ءارجإلا رفوت نمو ةدعاقلا نيكمت نم دكأت .ةدعاقلل امسا ددح.

ةديفملا رورملا ةكرحل ةبسانملا قطانملا ددح ،قطانم بيوبتلا ةمالع تحت.

ةيجراخلا ةقطنملا ةهجاو نم اهردصملا FTD ىلإ نومدختسملا اهأدب يتلا RDP رورم ةكرح يتأت ةيلخادلا ةقطنملا نم جرختو.

Name AC RDP Access Action Action Allow Zones Networks VLAN Tags Users Available Zones C	Applications Po	Enabled	Insert T/ISE Attributes	into Mandatory Y	pection Logging	Comments
Zones Networks VLAN Tags Users	Applications Po	orts URLs SG	T/ISE Attributes	Ins	pection Logging	Comments
Available Zones C		Courses Trease (4)				
A state		Source Zones (1)		Destination 2	Zones (1)	
- side	×	outside-zone		🗐 🚠 inside-zon	e .	6
슈 inside-zone 슈 outside-zone	Add to Source Add to Destination					

ةەجولاو ردصملا تاكبش فيرعتب مق ،تاكبشلا تحت.

AnyConnect. ءالمعل اەنييعت متي يتلا IP نيوانع AnyConnect_POOL نئاكلا نمضتي

ةيلخادلا ةيعرفلا ةكبشلا inside_net نئاكلا نمضتي.

Add Rule

Name	AC RDP Access				🖌 Er	abled		Insert	into Manda	tory			*
Action	Allow			V 0 0.8	1								
Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE	Attributes			Inspection	Logging	Comments
Availabl	e Networks C		0		Sourc	e Netwo	rks (1)			Destinat	tion Networks	(1)	
🔍 Sear	ch by name or value					Source		Original C	Client	📰 Insid	ie_Net		6
	Networks	Geolocat	ion		A 🚍	nyConned	_Pool		6				
Insid IPv4 IPv4	de_Net I-Benchmark-Tests I-Link-Local I-Multicast I-Private-10.0.0.0-8 I-Private-172.16.0.0- I-Private-192.168.0.0 I-Private-192.168.0.0	12)-16	^	Add To Source Networks Add to Destination									
IPv6	-IPv4-Mapped	-	~		Enter	an IP add	fress		Add	Enter an	IP address		Add
												Add	Cancel

قوف رقنا مث ،ةحاتملا RealMs نمض اقبسم ەؤاشنا مت يذلا قاطنلا قوف رقنا Users تحت ةدعاقلا ىل قفاضا قوف رقنا مث ،Available Users نمض بسانملا مدختسملا/ةعومجملا.

مايق نم دكأتف ،نيحاتملا نيمدختسملا مسق نمض تاعومجم وأ نيمدختسم يأ رفوتي مل اذا نمض تاعومجملاو نيمدختسملا ليزنتب (FMC) ةيساسألاا ةحوللا ةرادا يف مكحتلا ةدحو بسانملا مدختسملا/تاعومجملا نيمضت نمو قاطنلا مسق.

ردصملا روظنم نم انه ةددحملا ةعومجملا/نيمدختسملا نم ققحتلا متي.

ةكرح نأ FTD ميقي ،نآلاا ىتح ةدعاقلاا هذه يف هفيرعت مت ام مادختساب ،لااثملا ليبس ىلع متيو ،ةيلخادلا ةقطنملا ىل اههيجوت متيو ةيجراخلا ةقطنملا نم اهيلع لوصحلا متي رورملا يف ةكبشلا ىل اههيجوت متيو AnyConnect_Pool نئاك يف ةكبشلا نم اهيلع لوصحلا يف ميكومجم يف مدختسم نم رورملا ةكرح ىلع لوصحلا متيو ،Inside_Net نئاك Admins.

Add Rule		?
Name AC RDP Access	Enabled	Insert into Mandatory
Action 🖋 Allow	 O.B & U 	
Zones Networks VLAN Tags Users	Applications Ports URLs SGT/ISE	Attributes Inspection Logging Comments
Available Realms 😋	Available Users 😋	Selected Users (1)
Search by name or value	Search by name or value	🛃 LAB-AD/AnyConnect Admins 📋
Special Identities	IAB-AD/*	
🜐 LAB-AD	AnyConnect Admins	
	AnyConnect Users	
	at it.admin	Add to Rule
	atest.user	
		Add Cancel

هنأ ظحال .3389 ءانيم UDP و TCP حمسي نأ تفضأو نﺉاك RDP صصخم تنيع ،ءانيم تحت نم ققحتلا متي ،ةطاسبلا لجأ نم نكلو تاقيبطتلا مسق نمض RDP ةفاضإ نكمي

.طقف ذفانملا

dd Ru	le											?
Name	AC RDP Access				🖌 Er	abled	In	isert	into Mandatory	~		
Action	Allow			V 00,	8 th D							
Zones	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attribu	ites		Inspection	Logging	Comments
Availabl	e Ports 🖸		C)	Select	ted Sour	rce Ports (0)		Selecte	Destination I	Ports (2)	
🔍 Sear	ch by name or va	slue]	any				🤌 RDP	TCP		ũ
الله AOL الله Bitto الله Bitto INS INS INS INS INS INS INS INS	rrent _over_TCP _over_UDP -HTTPS -SSH 3-FDM 3-SSH			Add to Source Add to Destinatio					ADP	UDP		
🥜 нтті	P		~						Add Protocol	TCP (6)	Y Port	Enter a Add
											Add	Cancel

ققحتلل لاصتالا ةياهن يف لجسلا نم ققحتلا متي ،ليجستلا تحت هنأ نم دكأت ،اريخاً .ءاەتنالا دنع ةفاضإ قوف رقنا .قحال تقو يف يفاضإلا

Add Ru	le											? 3
Name	AC RDP Access					Enabled	1	nsert	into Mendetory	•		
Action	Allow			• • • • •	3 🖄 📕							
Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attribu	tes		Inspection	Logging	Comments
Log	at Beginning of C	onnection										
Log.	at End of Connect	tion										
file Ever	nts:	_										
Log	Files											
Send Co	nnection Events t	01										
Svel	nt Viewer	dela di custan co	alia vatia	in Anness Conto	11000000	Show (boarridae					
SNM	P Trap Select an	SNMP Alert Con	figuration.		a coyyery	,	0					
										_		
											Add	Cancel

ةعومجملا نمض نيمدختسملل حامسلل HTTP لوصول ةيفاضإ ةدعاق ءاشنإ متي .9 AnyConnect عقوم يلإ مدختسما لوصوب Windows Server IIS ظفح قوف رقنا .بيولا يلع كالم

Overview Analysis Policies Devices	Objects AMP Intelligence	Deploy 🍳 System Help 🔻 admin
Access Control > Access Control Network	iscovery Application Detectors Correlation Actions •	
Default-Policy Enter Description		You have unsaved changes 🛛 Analyze Hit Counts 📄 🔚 Save 🛛 🕲 Cance
Prefilter Policy: Default Prefilter Policy	SSL Policy: <u>None</u>	Identity Policy: FID-2 Identity Policy
		Ta Inheritance Settings 📃 Policy Assignments (1
Rules Security Intelligence HTTP Response	Logging Advanced	
# Filter by Device	Show Rule Co	anflicta 😣 😋 Add Category 😋 Add Rule 📫 Search Rules
a Name Source Zo Dest Zon	s Source Networks Dest Netwo V., Users	A S Dest Ports U S D Action
 Mandatory - Default-Policy (1-2) 		
1 AC RDP Access 🗠 outside-zone 📥 inside-	ne 👼 AnyConnect_Pool 👼 Inside_Net 🗛 🏕 LAB-AD/AnyConnect Admins	Any Any 🏂 ROP-TOP Any Any Any Any Vilow 🗍 🗋 🔗 📩 🗐 0 🥒
2 AC HTTP Access db outside-zone db inside-	ne 🚔 AnyConnect_Pool 🚔 Inside_Net 🗛 🏕 LAB-AD/AnyConnect Users	- Any Any PHTTP - Any Any Any VAllow 🛈 🖸 🗟 🖄 🗐 O 🥔
▼ Default - Default-Policy (-)		
There are no rules in this section. Add Rule or Add Cat	901Y	
Default Action		Access Control: Block All Traffic 🌱 📃

Displaying 1 - 2 of 2 rules $|\langle \cdot \rangle$ Page 1 of 1 > >| C | Rules per page: 100 *

NAT ءانثتسإ نيوكت

نأ مەم وە ،ةدعاق برض تنرتنإ لثم ،رورم ةكرح AnyConnect ىلع رثۇي نأ ةدعاق nat كانە نإ رثأتي nat ال رورم ةكرح so that AnyConnect ةدعاق ءانثتسإ nat لكشي.

1. ةزەجألا ىلإ لقتنا NAT.



.FTD ىلع قبطملا NAT جەن ددح

Overview Analysis	Policies	Devices	Objects	AMP I	ntelligence		Deploy) Q	System	Help 🔻	admin 🔻
Device Management	NAT	VPN V Q	oS Platfo	orm Settings	FlexConfig	Certificates					
										🔾 Nev	Policy
NAT Policy				De	evice Type		Status				
FTD-2-NAT-Policy				Th	reat Defense		Targeting 1 devices Up-to-date on all targeted devices			% 5	/ 6

امب) رورم ةكرح لك رثؤي برض يأ ةياهنلاا يف يكيمانيد برض كانه ،هذه NAT ةسايس يف .2 يجراخ نراقلا علاٍ يجراخ نراقلا كلوذ يف.

.ةدعاق ةفاضإ قوف رقنا ،NAT ىلع AnyConnect رورم ةكرح ريثأت عنمل

0	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence				Deploy	🔒 System	Help 🔻	admin 🔻
0	Device Mar	agement	NAT VP	N V Qo	S Platform	m Setting	s FlexConfig	Certificates						
F	TD-2-	NAT-Pol	icy								🛕 Show V	/arnings 📄 🔚	Save	😫 Cancel
R	ules											B	Policy A	ssignments (1)
đà	Filter by De	vice											0	Add Rule
							Original Pack	et	\sim	Translated Pac	ket			
#.	. Directio	n Type	Source Interface	Obje Inte	tination rface Object	Original Sources	Original Destinatio	Orig. ns Servi	. Translate ces Sources	d Translated Destinations	Tra Ser	ns Option	15	
٠	NAT Rules	Before												
•	Auto NAT P	tules												
2	+	Dynamic	🍕 any	🚓 o	utside-zone	🚔 obj-ar	iy		🥵 Interfa	0e		🔩 Dn	stfalse	N 🗎
٠	NAT Rules	After												

Displaying 1-1 of 1 rows |< < Page 1 of 1 > >| C | Rows per page: 100 -

عونلا عم ةيودي NAT ةدعاق يه ةدعاقلا نأ نم دكأتو ،NAT ءانثتسإ ةدعاق نيوكتب مق .3 مرورم ةكرح ىلع قبطنت هاجتإلا ةيئانث NAT ةدعاق اذه .يكيتاتسإ نكاس AnyConnect.

ناونع ىلا قەجومو Inside_Net نم قردصم رورم قكرح FTD فشتكي امدنع ،تادادعإلا ەذە عم قارى مەن ىل مەن يا ردصمل قامجرت متت ،AnyConnect_IP (قارى مەري مال مەن يا مەن يا مەن يا مەن يا مەن يا مەن يا مەن (Inside_Net) قامجرت متتو (AnyConnect_POOL) مەن يا قەجول قامجرت متتو متي امدنع NAT يساسأ لكشب اذە زواجتي .zone_جراخ ليجستو Inside_zone تانايبلا متي امدن مەرش مەن يا مەن يا مەن يا مەن يا مەن يا مەرى يا مەرى يا مەرى يا مەرى يا تابايبل

Add NAT Rule								? ×
NAT Rule:	Manual NAT Ru	e 👻	Insert	:	In Category	▼ NAT Rule	s Before 💙	
Type:	Static	×	Enable					
Description:								0
Interface Objects	Translation	PAT Pool	Advanced					
Available Interface O	bjects C		Sou	rce Interface Obje	cts (1)	Destination Inte	erface Objects (1)	
🔍 zone		×		inside-zone	ü	💼 outside-zone		6
inside-zone		A	id to					
ana outside-zone			ource					
		A Des	dd to tination					
							OK Ca	ancel

T Rule: Ma	nual NAT Rule 💙	Insert:	In Category	✓ NAT Rules Before ✓	
pe: Sta	tic 💌	🗹 Enable			
scription:					
terface Objects Tra	nslation PAT Pool	Advanced			
riginal Packet			Translated Packet		
riginal Source:*	Inside_Net	~ ◎	Translated Source:	Address	~
riginal Destination:	Address	×		Inside_Net	~
	AnyConnect_Pool	~ 0	Translated Destination:	AnyConnect_Pool	~ (
riginal Source Port:		¥ 0	Translated Source Port:		v (
riginal Destination Port:		× 0	Translated Destination Port:		~ (

سيلو هذه رورملا ةكرح راسم نع ثحب ءارجإل FTD نييعت متي ،كلذ ىلإ ةفاضإلابو ARP سيلو هذه رورملا ةكرح راسم نع ثحب ءارجإل ARP . مت امدنع ok ققطقط .ليكولل.

Add NAT Rule					? ×
NAT Rule:	Manual NAT Rule 💙	Insert:	In Category	✓ NAT Rules Before ✓	
Type:	Static 👻	Enable			
Description:					0
Interface Objects	Translation PAT Pool	Advanced			
Translate DNS repli	ies that match this rule				
Fallthrough to Inter	face PAT(Destination Interface)				
IPv6					
Net to Net Mapping	1				
🗹 Do not proxy ARP o	on Destination Interface				
Perform Route Look	kup for Destination Interface				
Unidirectional					
				ОК	Cancel

.ظفح قوف رقنا .4

	Overview /	nalysis	Policies [Devices	Objects	AMP	Intellige	ence				Deploy	0,	System	Help v	admin 🔻
	Device Manage	ement	NAT VP	v Qo	S Platform	n Setting	s Flex	xConfig Certifi	cates							
	FTD-2-N/	AT-Poli	cy							You have a	insaved changes	A Show	/ Warning	ps 🔡	Save	😫 Cancel
	Rules													5	Policy As	signments (1)
đ	B Filter by Device														0	Add Rule
							Ori	iginal Packet			Translated Pac	ket				
1	P Direction	Туре	Source Interface	Obje: Inte	tination rface Object	Original Sources		Original Destinations	Orig Services	Translated Sources	Translated Destinations	1 5	rans iervices	Options	•	
•	NAT Rules Bef	are														
1	42	Static	å inside-z	ione 🚠 d	outside-zone	👼 Inside	_Net	AnyConnect_Po:	N	👼 Inside_Net	📻 AnyConne	ct_Pool		용 Dris: 용 rout 용 no-p	false e-lookup proxy-arp	/ 6
•	Auto NAT Rule	s														
-	• •	Dynamic	🧠 any		outside-zone	📄 obj-ar	ny -			🍓 Interface				🍓 Dns	false	/8
•	NAT Rules Afte	r														
									Displaying	1-2 of 2 rows	IK K Page 1	of 1	> >	Ć R	ows per pa	sge: 100 •

رشنلا

.رشن قوف رقنا ،نيوكتلا ءاەتنا دنع .1



قوف رقنا مث اهيلع نيوكتلا قيبطت متي ثيح FTD ل ةرواجملا رايتخالا ةناخ قوف رقنا .2 رشن

Dep	loy Policies Version:2020-05-04 09:40 AM					×
V	Device	Inspect Interruption	Туре	Group	Current Version	۲
₹ 3	=/FTD-2	No	FTD		2020-05-04 09:16 AM	
Selec	ted devices: 1					
					Deploy Can	cel

ةحصلا نم ققحتلا

يئاەنلا بيترتلا

AAA نيوكت

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
max-failed-attempts 4
realm-id 5
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-group-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type microsoft
```

AnyConnect نيوكت

```
> show running-config webvpn
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
anyconnect profiles Lab disk0:/csm/lab.xml
 anyconnect enable
 tunnel-group-list enable
cache
 no 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-simultaneous-logins 10
vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Lab
 user-authentication-idle-timeout none
webvpn
 anyconnect keep-installer none
 anyconnect modules value dart
 anyconnect ask none default anyconnect
 http-comp none
 activex-relay disable
 file-entry disable
 file-browsing disable
 url-entry disable
 deny-message none
 anyconnect ssl df-bit-ignore enable
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

اەنم ققحتلاو AnyConnect نم لوصولا يف مكحتلا ةسايس دعاوقب لاصتالا

Sisco AnyConnect Secure Mobility Client − □ ×
VPN: Contacting ftd2.example.com. ftd2.example.com Connect
Cisco AnyConnect ftd2.example.com ×
Username: it.admin Password: ******
OK Cancel
🕙 Cisco AnyConnect Secure Mobility Client — 🗌 🛛 🗙
VPN: Connected to ftd2.example.com. ftd2.example.com Disconnect
00:00:12 IPv4
¢ ()

مداخ ىلا RDP لوصو اەيدل يټلا AnyConnect Admins ةعومجملا يف دوجوم Windows. مداخ ىل ال ميدل سيل ،كلذ عمو Windows.

ىلإ لوصولا ەنكمي مدختسملا اذه نأ نم ققحتي مداخلا اذەل Firefox و RDP لمع ةسلج حتف نإ طقف RDP ربع مداخلا



ةعومجم يف دوجوملا "مدختسملا رابتخإ مدختسم" مادختساب لوخدلا ليجست ةلاح يف ققحتلا كنكمي ،RDP ىلإ سيلو HTTP ىلإ لوصولا مەنكمي نيذلا AnyConnect يمدختسم لوعفملا ةيراس تحبصأ لوصولا يف مكحتلا جەن دعاوق نأ نم.



FMC لاصتا ثادحأ مادختساب ققحتلا

ثادحاً نم ققحتلا نكمي ،لوصولاب مكحتلا ةسايس دعاوق يف ليجستلا نيكمتل ارظنو دعاوقلا هذه قباطت رورم ةكرح يأل لاصتالا.

ليل حتال Analysis (ليل حتال) > Connections > Events.



لوؤسمل لاصتالا ثادحاً ضرعل تالجسلا ةيفصت متت ،لاصتالا ثادحاًل لودجلا ضرع تحت طقف تامولعملا ةينقت.

رسيأ ،امەم ،(UDP 3389 و TCP) مداخلا ىلإ RDP رورم ةكرح حمسي نأ تققد عيطتسي تنأ ،انە تعنم نوكي رورم ةكرح 80.

C	verv	lew	Analysi	s Policies I	Devices Obj	jects AM	P Inte	lligence		Depl	oy 🔒 System	Help 🔻 admin 🔻
C	ontex	t Exp	lorer C	onnections + E	vents Intr	rusions •	Files 🔻	Hosts • Us	sers Correlatio	n • Advanced •	Search	
									Bookmark Thi	s Page Report Designe	r Dashboard View B	ookmarks Search •
¢	Connection Events (switch workflow)											
c	Connections with Application Details > Table View of Connection Events Expanding											
٠	Search Constraints (Edit Search Save Search) Disabled Columns											
	Jump	o to	•									
	Jump	to	• Action ×	Initiator × IP	Initiator User	<u>r</u> ×		Responder × IP	Ingress X Security Zone	Egress × Security Zone	Source Port / × ICMP Type	Destination Port / × ICMP Code
	Jump	to	Action ×	Initiator × IP 10.10.10.1	Initiator User	g X AB-AD\it.admin	1, LDAP)	Responder × IP 192.1681.1	Ingress × Security Zone	Earess × Security Zone	Source Port / × ICMP Type	Destination Port / × ICMP Code 3389 / tcp
	Jump C J L L L	to	Action ×	Initiator × IP 10.10.10.1 10.10.10.1	Initiator User	g × AB-AD\it.admin AB-AD\it.admin	1, LDAP)	Responder × IP 192.168.1.1 192.168.1.1	Ingress Security Zone × outside-zone outside-zone	Egress × Security Zone inside-zone inside-zone	Source Port / × ICMP Type 62473 / tcp 62474 / tcp	Destination Port / × ICMP Code 3389 / tcp 80 (http) / tcp
	Jump 0 4 (0 4 (0 4 (0)		Action × Allow Slock Slock	Initiator × IP 10.10.10.1 10.10.10.1 10.10.10.1	Initiator User	g × AB-AD\it.admin AB-AD\it.admin AB-AD\it.admin	n, LDAP) n, LDAP) n, LDAP)	Responder × IP 192.168.1.1 192.168.1.1 192.168.1.1	Ingress X Security Zone X outside-zone outside-zone	Egress X Security Zone inside-zone inside-zone inside-zone	Source Port / × ICMP Type 62473 / tcp 62474 / tcp 62475 / tcp	Destination Port / × ICMP Code 3389 / tcp 80 (http) / tcp 80 (http) / tcp

مداخلا ىلٍ RDP رورم ةكرح رظح نم ققحتلا كنكمي ،مدختسملا رابتخإ مدختسمل ةبسنلاب 80. ذفنملا رورم ةكرحب حامسلاو

C	verviev	Analysi	s Policies I	Devices Object	i Ami	P Inte	lligence				Deplo	y 🔒	System	Help 🔻	admin 🔻
C	ontext E	xplorer C	onnections + E	vents Intrusio	ns 🔻 🛛	Files 🔻	Hosts ¥	Users *	Correl	lation 🔻	Advanced •	Search			
<u>c</u>	Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events • Search Constraints (Edit Search Save Search) Disabled Columns											Search • <u>16:26:39</u> Expanding led Columns			
	Action X Initiator X Initiator User X Responder X Ingress X Source Port / X Destination Port ICMP Code									ation Port / >					
	1	Block	<u>iii 10.10.10.1</u>	📇 test user (LAB-)	D\test.use	r, LDAP)	192.168	1.1 out	ide-zone	ins	ide-zone	<u>62493 / t</u>	50	3389 / t	92
	4 🗆	Allow	<u>10.10.10.1</u>	📇 <u>test user (LAB-/</u>	D\test.use	r, LDAP)	192.168	1.1 out	ide-zone	ins	ide-zone	<u>62494 / t</u>	œ	80 (http) / tcp

اهحالصإو ءاطخألا فاشكتسا

ءاطخألا حيحصت

لام المعاطخة فاشكتسال يصيخشت CLI يف اذه ءاطخألا حيحصت ليغشت نكمي LDAP ققداصم ءاطخأ فاشكتسال يصيخشت نكمي LDAP ق امحالصإو debug Idap 255.

ليغشت نكمي ،امحالصإو مدختسملا ةيومل لوصولا يف مكحتلا ةسايس ءاطخأ فاشكتسال رورملا ةكرحب حامسلا ببس ديدحتل مكحتلا ةمئاق يف ماظنلا معد ةيامح رادج ءاطخأ حيحصت عقوتم ريغ لكشب امعنم وأ.

ةلماعلا LDAP ءاطخأ حيحصت

```
[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]
                = [SUBTREE]
        Scope
[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:
        objectClass: value = top
[53]
[53]
        objectClass: value = person
[53]
        objectClass: value = organizationalPerson
[53]
        objectClass: value = user
[53]
        cn: value = IT Admin
        sn: value = Admin
[53]
[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
        whenChanged: value = 20200421204622.0Z
[53]
[53]
        displayName: value = IT Admin
        uSNCreated: value = 25896
[53]
[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
        objectSid: value = .....{I...;....j...
[53]
        accountExpires: value = 9223372036854775807
[53]
[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
        dSCorePropagationData: value = 16010101000000.0Z
[53]
[53]
        lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

LDAP مداخب لاصتا ءاشنإ رذعت

<#root>

[-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 لولحلا

- . LDAP مداخ نم ةباجتسإ ىقلتي FTD نأ نم دكأتو هيجوتلا نم ققحت •
- اهب قوثوم ةحيحصلا رذجلا CA ةداهش نأ نم دكأت ،STARTTLS وأ LDAP مادختسإ ةلااح يف حاجنب SSL تحفاصم ل|مك| نكمي ثيحب.
- نم ققحتف ،فيضملا مسا مادختسا مت اذا .حيحص ءانيمو ناونعلا لمعتسي نأ تققد مردق IP ناونع يل المح يلع DNS قردق.

ةحيحص ريغ رورملا ةملك وأ/و DN يف طبرلا لجس

<#root>

```
[-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
```

لكشب لوخدلا ليجستو DN ىلإ لوخدلا ليجست رورم ةملك نيوكت نم ققحت :لمتحملا لحلا مادختساب AD مداخ ىلع ءارجالا اذه نم ققحتلا نكمي .حيحص قيناكمإ نم ققحتلل .LDP مادختساب تاوطخلا عبتا .LDP مادختساب حاجنب باسح طبر

AD مداخ یلع Idp.exe نع ثحبلاو Win+R یلع طغضا .1



2. ددح ،لاصتالا تحت Connect.

🚰 Ldp	- 🗆 ×	, 1
Connection Browse View Options Utilities Help		_
Connect		
Disconnect		
New Ctrl+N		
Save As		
Exit		
	NUM	

Connect		×
Server:	localhost	
Port:	389	Connectionless
<u>O</u> K		<u>C</u> ancel

.طبر < لاصتا ىلإ لقتنا .ججان لاصتا ىلإ ريشي اصن نميألا دومعلا رەظي

🔝 Idap://w	_		Х							
Connection	Browse	View	Optio	ns Utilities	Help					
Connection Connect Bind Disconr New Save Save Save As Exit	Browse t	View Ctrl+B Ctrl+N	Optio	ns Utilities Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configur CN= current Tim defaultM dnsHos domainf domainf dsServi	Help en("localho connection ase DSA in atries: SE) rationNamin =Configurati Time: 5/1/20 e; VamingCont atName: win ControllerFu ControllerFu Functionality iceName: Cl	est", 389); to localhost. formation gContext: ion,DC=examp 2014:16:55 PN ext: DC=examp 2016.example inctionality: 7 = y: 7 = (WIN201 N=NTDS	le,DC=co 1 Easterr ple,DC=c .com; = (WIN20 16);	om; n Daylight com; 016);		
				Set Firs Nan con forestFi highest isGlobal isSynch IdanSer	tings,CN=W st-Site- me,CN=Sites n; unctionality: CommittedU ICatalogRea pronized: TF tyiceName:	(IN2016,CN=Se s,CN=Configur : 7 = (WIN2010 SN: 13410; ady: TRUE; RUE; example.com;	ervers,Cl ation,DC 6); win2016	N=Default- =example,[DC=	

OK. قوف رقناو .رورملا ةملكو ليلدلا باسح مدختسم ددح مث طيسب طبر ددح .5

Bind									
<u>U</u> ser: <u>P</u> assword:	ftd.admin@example.com								
Domain: Bind type Bind as cur Bind with c Bind with c Dimple bind Advanced Advanced	rrently logged on user redentials (DIGEST) affic after bind Cancel OK								

DOMAIN\username :ك قدصم LDP رەظي ،حجان طبر مادختساب

Idap://win2016.example.com/DC=example,DC=com -												
Connection	Browse	View	Options	Utilities	Help							
				 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; MaxResultSetSize; MinResultSets; MaxResultSetSize; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 								
				es = Idap_s unavailable .uthenticate	simple_bind e>); // v.3 ed as: 'EXA	_s(ld, 'ftd.adı MPLE\ftd.adı	min@exan nin'.	mple.com',]			
Ready												

لثم لشف ةحيحص ريغ رورم ةملك وأ حلاص ريغ مدختسم مساب طبرلا ةلواحم نع جتني انه امهارن نيذللاا نينثالاا.

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; 	<pre>MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5; </pre>									
Error <49>: ldap_simple_bind_s() failed: Invalid Credentials Server error: 80090308: LdapErr: DSID-0C09042A, comment: AccentSecurityContext error_data 52e_v3839										
Comment: AcceptSecurityContext error, data 52e, v3839 Error 0x80090308 The token supplied to the function is invalid										
Ready	۷.									

مدختسملا مسا یلع روثعلا LDAP مداخ یلع رذعت

<#root>

```
[-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

ةطساوب مت يذلا ثحبلا عم مدختسملا ىلع روثعلا ەنكمي AD نأ نم ققحت :لمتحملا لحلا FTD. اضيأ ldp.exe عم اذه متي نأ نكمملا نمو.

ةرجش < ضرع ىلإ لقتنا ،هالعأ حضوم وه امك حاجنب طبرلا دعب .1.

🔝 Idap://w	in2016.exa		—		\times	<				
Connection	Browse	View	/ Option	s Utilities	Help					
			Tree Enterprise Status Ba Set Font	e Configurati r Max Max Max Max Max Thre supporte supporte SPN res = Idap_s <unavailable Authenticate</unavailable 	Ctrl+T ion DirSyncDuration; I ResultSetSize; Mir ResultSetSPerCon ValRange; MaxVa adMemoryLimit; S adLDAPVersion (2 edSASLMechanism EGO; EXTERNAL; imple_bind_s(Id, 'ff >); // v.3 d as: 'EXAMPLE\ft	Maxin Ress n; M IRar yste): 3; ms (- DIGI td.ac	MaxPooIThr sts; MaxDo cvTimeout; nldleTime; s; MaxQue TempTable sultSets; laxNotifica ngeTransiti emMemoryl ; 2; 4): GSSAP EST-MD5; dmin@exa dmin	reads; atagramR MaxPage ryDuratio Size; tionPerCo ve; LimitPerce	ecv; Size; n; onn; ent;	~

قفاوم قوف رقنا مث FTD ىلع ەنيوكت مت يذلا يساسألI DN ددح .2

Tree View	×
BaseDN: DC=example,DC=com	~
Cancel	ОК

.ثحب قوف رقنا مث يساسألا DN قوف نميألا سواملا رزب رقنا .3
Idap://win2016.example.com/DC=example,DC=com						– 🗆 X	<
Connection	Browse	View	Options	Utilities	Help		
DC=exam C S C S C S C S	nple,DC=co	om	Search Virtual List View Delete Modify Modify DN Add child Compare Advanced		Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ole,DC=com; 11D1AA4B00C04FD7D83A:O 3,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 311D1ADED00C04FD8D5CD:C	^
			Copy Select al Clear ou	I Itput	Ctrl+C Ctrl+N	e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~
Create a new document							

.ءاطخألا حيحصت يف رەظت امك Scopeو ،Filter، ةيساسألI DN ميق سفن ددح .4

ەذە ،لاثملا اذە يف:

- تەكبش DN تەكبش: dc=example،dc=com
- تَعَيَّفَصتل الماع: samaccountName=it.admi
- ۃيعرفلا ۃرجشل:قاطنلا •

🔝 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×						
Connection	Browse View Options Utilities Help							
Search	×	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^					
Base DN:	DC=example,DC=com ~	38811D1ADED00C04FD8D5CD:C ample,DC=com; 5D211D1AA4B00C04FD7D83A:O						
Filter:	sAMAccountName=it.admi ~							
Scope Base	One Level Subtree	lers,DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C example,DC=com;						
Attributes:	objectClass;name;description;canonicalName <	68811D1ADED00C04FD8D5CD:C mple,DC=com;						
Options	Run Close	020 3:43:59 PM Eastern Daylight						
***Searching dap_search_s(ld, "DC=example,DC=com", 2, "sAMAccountName=it.admi", attrList, 0, &msg) Getting 0 entries:								
Ready								

لفسأ sAMAccountname it.admi عم مدختسم باسح دوجو مدعل ارظن تالاخدا 0 نع LDP ثحبي DN ايساسألا example،dc=com.

لاخدا نع LDP ثحبي .ةفلتخم ةجيتن حيحصلا SAMAccountname it.admin عم ىرخأ ةلواحم رهظت مدختسملل DN=example، dc=com عبطيو يساسألا.

🔝 Idap://win2	2016.example.c	om/DC=ex	ample,DC:	=com		- 🗆	×	
Connection B	Browse View	Options	Utilities	Help				
Search					\times	58811D1ADED00C04FD8D5C DC=example,DC=com;	D:C	
Base DN: D)C=example,DC	=com			\sim	88811D1ADED00C04FD8D5C ample,DC=com;	D:C	
<u>F</u> ilter: s	AMAccountName	e=it.admin	$\overline{}$	D211D1AA4B00C04FD7D83A:O lers,DC=example,DC=com;				
Scope	◯ <u>O</u> ne Level	● <u>S</u> ubtree	2			58811D1ADED00C04FD8D5Cl example,DC=com; 68811D1ADED00C04FD8D5C mple_DC=com;	D:C :D:C	
<u>A</u> ttributes: o	bjectClass;name	description;	;canonicalN	lame	\sim	020 3:43:59 PM Eastern Dayl	ight	
Options		<u>R</u> un		<u>C</u> lose)20 2:41:57 PM Eastern Daylig	pht	
***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;								
Ready								

مدختسملا مسال ةحيحص ريغ رورملا ةملك

<#root>

```
[-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 erro

Invalid password for it.admin

[-2147483613]

[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End

ءاەتنا مدع نمو حيحص لكشب مدختسملا رورم ةملك نيوكت نم ققحت :لمتحملا لحلا مادختساب AD طبرب FTD موقي ،لوخدلا ليجستب صاخلا DN عم لاحلا وہ امكو .اەتيحالص مدختسملا دامتعا تانايب.

سفن ىلع فرعتلا ىلع رداق AD نأ نم ققحتلل ldp يف طبرلا اذهب مايقلا نكمي امك يف LDP يف ةدوجوملا تاوطخلا ضرع متي .رورملا ةملكو مدختسملا مسا دامتعا تانايب ةحيحص ريغ رورملا ةملك وأ/و مسقلا طبر لوخد ليجست.

.لمتحم لشف ببسل Microsoft مداخ ثادحاً ضراع تالجس ةعجارم نكمي ،كلذ ىلإ ةفاضإلاب

AAA رابتخإ

مألاا مادختسإ نكمي test aaa-server مدختسم مسا مادختساب تكمي FTD نم ققداصم قلواحم قاكاحمل test aaa-server رمألا وه رمألا. ةقداصملا وأ لـاصتالا لـشف تالـاح رابتخال اذه مادختسإ نكمي .نيددحم رورم قملكو مداخ ققداصم رابتخإ aaa [AAA-server] فيضملاا [AD IP/hostname].

<#root>

> 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
```

مزحلا طاقتلا تايلمع

ل حرداغ اذإ .AD مداخ ىلإ لوصولا ةيناكمإ نم ققحتلل مزحلا تاعومجم مادختسإ نكمي LDAP مزح ترداغ اذا .AD مداخ ىل لوصول المي دول الماح LDAP مزح ترداغ اذا . FTD ، ويجوتلا يف ةلكشم ىلإ كلذ ريشي دقف ،ةباجتسإ دجوت ال نكلو .

.هاجتإلا يئانث LDAP رورم ةكرح طاقتلالا رهظي

> 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

```
192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768
  1: 23:02:16.770712
                            192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128
  2: 23:02:16.772009
  3: 23:02:16.772039
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti
                            192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915
  4: 23:02:16.772482
  5: 23:02:16.772924
                            192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti
  6: 23:02:16.772955
  7: 23:02:16.773428
                            192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
                            192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
  8: 23:02:16.775030
  9: 23:02:16.775075
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti
Γ...1
```

54 packets shown

Windows Server ثادحأ ضراع تالجس

ثودح ببس لوح اليصفت رثكأ تامولعم AD مداخ ىلع ثادحألا ضراع تالجس رفوت نأ نكمي لشف.

.ەحاتتفاو ثادحألا ضراع نع ثحبلا 1.



ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما