LDAP مادختساب FTD و FMC نيوكت ةيجراخلا ةقداصملل

تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسماا تانوكماا</u> <u>قېساسأ تامولعم</u> <u>ةكېشلل ىطىطختلا مسرلا</u> <u>نىوكتلا</u> <u>FMC ةېموس رل امدختس مل اقەچاۋېف ېس اس أل ا LDAP نېوكت</u> <u>نېيچراخلا نېمدختسمل Shell Access</u> <u>FTD ل قېجراخلا ققداصملا</u> <u>مدختسماا راوداً</u> SSL 19 TLS <u>قحصالا نم ققحتاا</u> رابتخالا ثحب ةدعاق <u>LDAP لماكت رابتخا</u> <u>امحال ص او ءاطخأل ا ف اش ك ت س ا</u> <u>نېمدختسمالا لېېزنټل LDAP و FMC/FTD لعافتي فېك</u> <u>مدختسمالا لوخد ليجست بالط ةقداصمل LDAP و FMC/FTD لعافتي فيك</u> <u>عقوتم وه امك TLS وأ SSL لمعي ال</u> <u>ةلص تاذ تامولعم</u>

ةمدقملا

ليلدلا ىلإ لوصولا لوكوتوربل ةيجراخلا ةقداصملا نيكمت ةيفيك دنتسملا اذه حضوي FTD. و Cisco FMC و CDAP) لا مادختساب

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- isco نم FirePOWER (FTD) ديدهت دض عافدلا
- مرادإ زكرم FireSIGHT (FMC) نم (Cisco
- LDAP تفوسوركيام •

ةمدختسملا تانوكملا

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

- FTD 6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012 ليغشتلا ماظن

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ 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

ةفاضإ كنكمي .ةرادإلا ىلإ لوصولل يضارتفا لوؤسم باسح ةرادملا ةزهجألاو FMC نمضتت ىلعو (FMC) ةيساسألا ةحوللا ةرادإ يف مكحتلا ةدحو ىلع ةصصخم نيمدختسم تاباسح لا المداخ ىلع نييجراخ نيمدختسمك وأ نييلخاد نيمدختسمك امإ ،ةرادملا ةزهجألا RADIUS، و FTD و FTD. لا يجراخلا مدختسملا ةقداصم معد متي .اموعدم جذومنلا اذه ناك اذإ

· مدختسملا ةقداصمل قيلحم تانايب ةدعاق نم FMC/FTD زاهج ق ${
m c}$ حتي - يلخاد مدختسم.

تامولعم موقت ،ةيلحملا تانايبلا ةدعاق يف ادوجوم مدختسملا نكي مل اذإ - يجراخ مدختسم · .هب ةصاخلا مدختسملا تانايب ةدعاق ءلمب يجراخ RADIUS وأ LDAP ةقداصم مداخ نم ماظنلا

ةكبشلل يطيطختلا مسرلا



نيوكتلا

FMC ةيموسرلا مدختسملا ةهجاو يف يساسألا LDAP نيوكت

System > Users > External Authentication: کل لقتنا 1. قوطخلا

← → C ▲ No	secure 192.0.2.5/ddd/#ExternalAuthentication	1 *	Θ:
Overview Analysis	Policies Devices Objects AMP Intelligence	Deploy Q, System Help +	admin v
2		Configuration Users Domains Integration Updates Licenses Health • Monitoring •	Tools •
Users User Roles	External Authentication	2.	
		🖂 Save 😫 Caneel 📝 Sa	ive and Apply
Default User Role: None	Shell Authentication Disabled *	Add External Authentic	ication Object
Name		Hethod Enabled	



E	Save	😢 Car	ncel	🖌 Sa	ive and Apply			
Add External Authentication Object								
	Meth	nod	Ena	bled				

ةبولطملا لوقحلا لمكأ .3 ةوطخلا:

External Authentication Object	t										
Authentication Method	LDAP T										
CAC	Use for CAC authentication and authorization	Use for CAC authentication and authorization									
Name *	C-LDAP Name the External Authentication Object										
Description											
Server Type	MS Active Directory Set Defaults Choose MS Active Direct	MS Active Directory Set Defaults Choose MS Active Directory and click 'Set Defaults'									
Primary Server											
Host Name/IP Address *	192.0.2.10	ex. IP or hostname									
Port *	Default port is 389 or 636 for SSL										
Backup Server (Optional)											
Host Name/IP Address		ex. IP or hostname									
Port	389										
LDAD Coosific Decomptore											
LDAP-Specific Parameters	*Base DN specifies where users will be found										
Base DN *	DC=SEC-LA8 Fetch DNs	ex. dc=sourcefire,dc=com									
Base Filter		ex. (cn=jsmith), (Icn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))									
User Name *	Administrator@SEC-LAB0	ex. cn=jsmith,dc=sourcefire,dc=com									
Password *	Username of LDAP Serve	r admin									
Confirm Password *											
Show Advanced Options	•										
Attribute Mapping	*Default when 'Set Defaults' optio	n is clicked									
UI Access Attribute *	Eatch Alter										
Shall Assess Attribute											
Shell Access Attribute *	sAMAccountName										

Group Controlled Access Role	s (Optional) •
Access Admin	
Administrator	
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	
View-Only-User (Read Only)	
Default User Role	Access Admin Administrator Discovery Admin External Database User
Group Member Attribute	member
Group Member URL Attribute	
Shell Access Filter	Same as Base Filter
(Mandatory for FTD devices)	
Additional Test Parameters	
User Name	
Password	
*Required Field	
	Save Test Cancel

ظفحلاو نئاكلExternal Authentication نيكمتب مق .4 ةوطخلا

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	0 Sys	tem Help •	admin v
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring	Tools •
Users User Roles External Authentication								2.	
							🗟 Save	Cancel 🗹 S	ave and Apply
Default User Role: None Shell Authentication Disabled *							O Add	External Authen	tication Object
Name							Hethod	Enabled	
1. SEC-LDAP New External Authentication Object							LDAP		/ 60
								1.	3

نييجراخلا نيمدختسملل Shell Access

لوصوب رخآلاو ،بيولا ةەجاول دحاو :ةڧلتخملا ةيلخادلا ةرادالا يمدختسم نم نينثا FMC معدت ةەجاو ىلا لوصولا ەنكمي نم نيب حضاو زييمت دجوي ەنأ ينعي اذە .رماوألا رطس ةەجاو متت ،تيبثتلا تقو يف .رماوألا رطس ةەجاو ىلإ لوصولا ەنكمي نمو ةيموسرلا مدختسملا لك ىلع اەسفن يە نوكت يكل يضارتڧالا لوؤسملا مدختسمب قصاخلا رورملا ةملك ةنمازم قطساوب اەعبتت متي ،كلذ عمو ،(CLI) رماوألا رطس ةەجاوو (GUI) قيموسرلا مدختسمل ا مەزل او ن يول او نام

.shell ىلإ لوصولا قح نييجراخلا LDAP يمدختسم حنم اضيأ بجي

امك ةقطقطو لدسنملا System > Users > External Authentication عبرمل System > Users > External Authentication امك ةقطقطو لدسنملا يف رمظي

Overview Analysis	Policies Devices Objects AMP Intelligence						Deploy	🔍 Sy	stem Help •	adn	nin v
		Configuration	Users	Domains	Integration	Updates	Licenses •	Health +	Monitoring	• Ti	ools •
Users User Roles	External Authentication								2.		
								🗟 Save 🛛 🕻	Cancel 📝 t	Save and	d Apply
Default User Role: None	1. Shell Authentication Disabled Disabled							O Add	External Auther	tication	Object
Name	Insbled (SEC-LDAP)							Hethod	Enabled		
1. SEC-LDAP								LDAP		1	6 @

.FMC يف تارييغتلا رشن .2 ةوطخلا

ربع لوخدلا ليجست نيكمت متي ،نييجراخلا نيمدختسملل ةقبط لوصو نيوكت درجمب لوكوتورب SSH يف حضوم وه امك SH لوكوتورب



FTD ل ةيجراخلا ةقداصملا

.FTD ىلع ةيجراخلا ةقداصملا نيكمت نكمي

ظفحيوDevices > Platform Settings > External Authentication. خطفحيوEnabled القتارية على القريات المعادي ال

مدختسملا راودأ

مدختسم راودأ ءاشنإ اضيأ كنكمي .نيعملا مدختسملا رود ىلإ مدختسملا تازايتما دنتست وأ كتسسؤم تاجايتحإ ةيبلتل اهصيصخت مت يتلا لوصولا تازايتما مادختساب ةصصخم "فاشتكالا لوؤسم"و "نامألا للحم" لثم اقبسم ةددحم راودأ مادختسإ كنكمي".

مدختسملا راودأ نم ناعون كانه:

بيولا ةەجاو مدختسم راودأ .1

CLI يمدختسم راودأ .2

<mark>راودا</mark>ُ عجار ،تامولعملا نم ديزملاو اقبسم ةددحملا راوداُلا نم ةلماك ةمئاق ىلع لوصحلل <u>مدختسملا</u>.

لقتنا ،ةيجراخلا ةقداصملا تانئاك عيمجل يضارتفا مدختسم رود نيوكتل System > Users > External Authentication > Default User Role. رقناو ەنييعت يف بغرت يذلا يضارتفالا مدختسملا رود رتخأ Save.

Overview Analysis Policies Devices Objects AMP Intelligence								Deploy	0 System	m Help +	admin +
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health + I	Monitoring •	Tools •
Users User Roles External Authentication											
								8	Save 🙆 Ca	ncel 🖌 Sa	ive and Apply
Default User Role: None Shell Authentication Enabled (SEC-LDAP)									Q Add Ext	ernal Authent	ication Object
Name									Hethod	Enabled	
1. SEC-LDAP									LDAP		182
										_	
	Default User Pole Configuration		_								
	Cerual oser kole comgaratori										
	Default User Roles	Administrator External Database User (Read Only) Security Analyst Security Analyst Security Analyst Intrusion Admin									
		Access Admin Network Admin Maintenance User Discovery Admin Threat Intelligence Director (TID) Us									
	Custom User Roles	View-Only-User (Read Only) (Global)									
		Sau	e Cancel								

ةعومجم يف نينيعم نيمدختسمل ةنيعم راودأ نييعت وأ يضارتفا مدختسم رود رايتخال يف حضوم وه امكGroup Controlled Access Rolesهيلإ حفصتلاو نﺉاكلا رايتخإ كنكمي ،ةنيعم تانﺉاك اةروصلا:

Group Controlled Access Roles (Optional) •								
Access Admin								
Administrator	h.potter@SEC-LAB							
Discovery Admin								
External Database User	s.rogers@SEC-LAB							
Intrusion Admin								
Maintenance User								
Network Admin	h.simpson@SEC-LAB							
Security Analyst	r.weasley@SEC-LAB							
Security Analyst (Read Only)								
Security Approver								
Threat Intelligence Director (TID) User								
View-Only-User (Read Only)	ma.simpson@SEC-LAB							
Default User Role	Access Admin Administrator Discovery Admin External Database User							

TLS وأ SSL

يف DNS يف FMC نيوكت بجي Authentication عم قباطتت نأ بجي ةداهشلل عوضوملا ةميق نأل كلذو . Object Primary Server Hostname. ضرعت مزحلا طاقتلا تايلمع دعت مل ،نمآلا حضاو صن طبر تابلط.

.389 ةئيه ىلع ەب TLS ظفتحيو ،636 ىلإ يضارتڧالا ذڧنملا رييغتب SSL موقي

ال قبسنلاب .قيساسألا قمظنألاا لك ىلع قداەش TLS ريفشت بلطتي :قظحالم SSL، ل قبسنلاب .قيساسألا قمظنال الك ىلع قداەش الى SSL بلطتي ال ،ىرخألا قيساسألا قمظنألل قبسنلاب .قداەش اضيأ FTD بلطتي ل قداەش ليمحتب ىصوي ،كلذ عمو .قداەش.

تامولعمDevices > Platform Settings > External Authentication > External Authentication Object تامولعمSSL/TLS ةمدقتملا تارايخلا

LDAP-Specific Parameters			
Base DN *	DC=SEC-LAB	Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter			ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB		ex. cn=jsmith,dc=sourcefire,dc=com
Password *			
Confirm Password *			
Show Advanced Options	•		
Encryption	SSL O TLS None		
SSL Certificate Upload Path	Choose File No file chosen		ex. PEM Format (base64 encoded version of DER)
User Name Template	%s		ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30		

ةداەشلا نوكت نأ بجي .مداخلا ةداەش عقو يذلا قدصملا عجرملا ةداەش ليمحت .2 ةوطخلا قيسنتب PEM.

LDAP-Specific Parameters		
Base DN *	DC=SEC-LAB Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB	ex. cn=jsmith,dc=sourcefire,dc=com
Password *		
Confirm Password *		
Show Advanced Options	•	
Encryption	SSL TLS None	
SSL Certificate Upload Path	Choose File CA-Cert-base64.cer	ex. PEM Format (base64 encoded version of DER)
User Name Template	%eS	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

نيوكتلا ظفحا .3 ةوطخلا.

ةحصلا نم ققحتلا

رابتخالا ثحب ةدعاق

dsquery user -name:رمألا بتكاو LDAP نيوكت مت ثيح PowerShell وأ Windows رماوأ مجوم حتفا

:لاثملال ليبس ىلع

PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *

Σ	Administrator: Windows PowerShell 📃 🗖	x	
PS "CN PS "CN "CN "CN "CN "CN "CN "CN "CN "CN "CN	C:\Users\Administrator> dsquery user -name harry* =Harry Potter,CN=Users,DC=SEC-LAB C:\Users\Administrator> C:\Users\Administrator> dsquery user -name * =Administrator,CN=Users,DC=SEC-LAB =Guest,CN=Users,DC=SEC-LAB =krbtgt,CN=Users,DC=SEC-LAB =anthony E. Stark,CN=Users,DC=SEC-LAB =Dr. Robert B. Banner,CN=Users,DC=SEC-LAB =Dr. Robert B. Banner,CN=Users,DC=SEC-LAB =Harry Potter,CN=Users,DC=SEC-LAB =Harry Potter,CN=Users,DC=SEC-LAB =Harry Potter,CN=Users,DC=SEC-LAB =Hermione Granger,CN=Users,DC=SEC-LAB =Lisa Simpson,CN=Users,DC=SEC-LAB =Lisa Simpson,CN=Users,DC=SEC-LAB =Maggie Simpson,CN=Users,DC=SEC-LAB =Maggie Simpson,CN=Users,DC=SEC-LAB =Neville Longbottom,CN=Users,DC=SEC-LAB =Neville Longbottom,CN=Users,DC=SEC-LAB =Neville Longbottom,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB :\Users\Administrator> C:\Users\Administrator> C:\Users\Administrator>		
<		> .	н

LDAP لماكت رابتخإ

،ةحفصلا لفسأ يف .System > Users > External Authentication > External Authentication Object. ، ةروصلا يف ىري امك مسق Additional Test Parameters كانه

Additional Test Parameters User Name Password	h.potter
*Required Field	Save Test Cancel

.ةجيتنلا تيأر in order to رابتخإ ترتخأ

Overview Analysis Policies Devices Objects	AMP Intelligence							Deploy	0
			Configuration	Users	Domains	Integration	Updates	Licenses •	Hea
Users User Roles External Authentication									
		Success Test Complete.	×						
	External Authentication Object								
	Authentication Method								
	CAC Use for CA	authentication and authorization							
	Description								
	Server Type MS Active Direc	y * Set Defaults							
	01								

4	Capturing from Ethernet1											
File	Edit View Gr	Capture Analyze St	tatistics Telephony Wirele	ess Tools	Help							
st.	d 🛛 🗎	380 9 ***	ST 🛓 🖬 🔳 🔍 G									
	tsp.port399 88 (p.add192.0.2.5											
No.	Time	Source	Destination	Protocol	al Lengh Info	^						
	1799 55.131546	192.0.2.5	192.0.2.10	TCP	66 39784 + 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3077124549 TSecr=25708266							
	1800 55.131547	192.0.2.5	192.0.2.10	LDAP	127 [bindRequest(1) "CN+Marry Potter,CN+Users,DC+SEC-LA8 simple							
+	1801 55.132124	192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success							
	1802 55.132184	192.0.2.5	192.0.2.10	TCP	66 39784 → 389 [ACK] Seq=62 Ack=23 Hin=29312 Len=0 TSval=3077124549 TSecr=25708266							
	1803 55.132213	192.0.2.5	192.0.2.10	LDAP	73 unbindRequest(2)							
	1804 55.132213	192.0.2.5	192.0.2.10	TCP	66 19784 * 389 [FIN, ACK] Seq+69 Ack+23 Nin+29312 Len+0 TSval=3077124550 TSecr=25702266							
	1805 55.132227	192.0.2.10	192.0.2.5	TOP	00 389 * 38/84 [ACK] Sed#13 ACK#10 HITH80200 Femma 12A91*52408100 126CL+301/174248	Ľ						
P	rame 1800: 127	bytes on wire (1016	bits), 127 bytes captu	red (1016	/ bits) on interface \Device\NPF_(77DC31F6-8250-4F19-8412-E4596F960108}, id 0							
P 1	thernet II, Sr	c: VNware_29:cf:2d (0	N0:0c:29:29:cf:2d), Dst	: V?bare_e	_eb:1d:f7 (00:0c:29:eb:1d:f7)							
2	Internet Protoc	ol Version 4, Src: 19	2.0.2.5, Dst: 192.0.2.	10								
1.1	Fahseission Co	stroi Protocol, Src P	ort: 39764, Ust Port:	209, Sed:	A, ACKI A, LENI DA							
1.1	d LDAPMessage	indRequest(1) "Climits	ray Potter Challers DC	-SEC-LAB	" stanle							
	messageID	1		-966 696	a magan							
	4 protocol0	: bindRequest (0)										
	4 bindRec	uest										
	vers	ion: 3										
	name: CN+Marry Potter, CN+Users, DC+SEC-LAB											
	# authentication: simple (0)											
	5	imple: cisco										
	[Response	In: 1801]										

اهحالصإو ءاطخألا فاشكتسا

نيمدختسملا ليزنتل LDAP و FMC/FTD لعافتي فيك

بلط لاسرا FMC ىلع بجي ،Microsoft LDAP مداخ نم نيمدختسملا بحس نم FMC نكمتت يكل نأ درجمب .LDAP لوؤسم دامتعا تانايب مادختساب (SSL) 636 وأ 389 ذفنملا ىلع الوأ طبر عيطتست ،اريخأ .حاجن ةلااسرب بيجتسي هنإف ،FMC ةقداصم ىلع ارداق LDAP مداخ نوكي FMC يعيطتس عيطيطختلا مسرلا يف حضوم وه امك ثحبلا بلط ةلاسر عم بلط ميدقت

<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << --- FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

يضارتفا لكشب حسملا يف رورم تاملك لسرت ةقداصملا نأ ظحال:

83	4.751887 192.0	2.5	192.0.2.10	TCP	74 38002 + 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3073529344 TSecr=0 WS=128							
84	4.751920 192.0	2.10	192.0.2.5	TCP	74 389 + 38002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=25348746 TSecr=3073529344							
85	4.751966 192.0	2.5	192.0.2.10	TCP	_66 38002 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3073529344 TSecr=25348746							
86	4.751997 192.0	2.5	192.0.2.10	LDAP	110 bindRequest(1) "Administrator@SEC-LAB0" simple							
• 87	4.752536 192.0	2.10	192.0.2.5	LDAP	88 bindResponse(1) success							
88	4.752583 192.0	2.5	192.0.2.10	TCP	66 38002 → 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSyal=3073529345 TSecr=25348746							
89	4.752634 192.0	2.5	192.0.2.10	LDAP	122 searchRequest(2) "DC=SEC-LAB ' wholeSubtree							
 Frame Ethern Intern Transm Lightw LDA 	b Frame 86: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_[77DC31F6-8250-4F19-8412-E4596F960108}, id 0 b Ethernet II, Src: Whware_29:cf:2d (00:0c:29:29:cf:2d), Dst: Whware_eb:1d:f7 (00:0c:29:eb:1d:f7) b Internet Protocol Version 4, Src: 192.0c.25, Dst: 192.0c.26 b Transmission Control Protocol, Src Port: 38002, Dst Port: 389, Seq: 1, Ack: 1, Len: 44 a Lightweight Directory Access Protocol 4 LDAPMessage binAfequest(1) "Administrator@SEC-LA80" simple											
4	rotocolOp: bindReau	est (0)										
	✓ bindRequest	(-)										
	version: 3											
	name: Administ	rator@SEC-LAB0										
	4 authentication	simple (0)										
	simple: Cls	ot@c										
	Personne To: 971											

مدختسملا لوخد ليجست بلط ةقداصمل LDAP و FMC/FTD لعافتي فيك

، LDAP ةقداصم نيكمت ءانثأ FTD وأ FMC ىلإ لوخدلا ليجست نم مدختسملا نكمتي يكل

مسا هيجوت ةداعإ متت ،كلذ عمو ،FirePOWER ىلإ يلوألا لوخدلا ليجست بلط لاسرا متي و FMC نأ ينعي اذهو .ضفر/حاجن ةباجتسإ ىلع لوصحلل LDAP ىلإ رورملا ةملكو مدختسملا FTD نورظتني كلذ نم الدبو تانايبلا ةدعاق يف ايلحم رورملا ةملك تامولعمب ناظفتحي ال .قعباتملا ةيفيك لوح LDAP نم ديكأت



4							*Ethernet1			
File Edit	View Go Capt	ture Analyze Statistics	Telephony Wireless To	ools Help	р					
🛋 🔳 🖉 🐵 👪 🖾 🍳 ⇔ 🗢 🗟 🐺 🎍 🚍 📃 Q. Q. Q. X										
tcp.port	==389 && ip.addr==1	92.0.2.5 && ldap.messageID =	-= 1							
No.	Time	Source	Destination	Protocol	Length	Info				
58	13:11:59.695671	192.0.2.5	192.0.2.10	LDAP	110	<pre>bindRequest(1)</pre>	"Administrator@SEC-LAB0" simple			
• 59	13:11:59.697473	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success			
67	13:11:59.697773	192.0.2.5	192.0.2.10	LDAP	110	<pre>bindRequest(1)</pre>	"Administrator@SEC-LAB0" simple			
69	13:11:59.699474	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success			
97	13:11:59.729988	192.0.2.5	192.0.2.10	LDAP	127	<pre>bindRequest(1)</pre>	"CN=Harry Potter, CN=Users, DC=SEC-LAB	" simple		
98	13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success			

ةيموسرلا مدختسملا ةهجاو يف لاخدإ ةفاضإ متت ،رورملا ةملكو مدختسملا مسا لوبق مت اذإ (GUI) :ةروصلا يف حضوم وه امك بيولل:

Overview Analysis Policies Devices Objects AMP Intelligence Diploy 9, System Help + Reports											
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health +	Monitoring +	Tools •
Users User Roles External Authent	Users User Roles External Authentication										
										O Cri	eate User
Username	Authentication Method	Password Lifetime									
admin	Administrator	Internal	Unimited								1
h.potter	Administrator	External									0
h.eotter	Administrator	External									0

رمألا ليغشتب مق show user رمادختسملا تامولعم نم ققحتلل FMC رماوأ رطس ةمجاو يف show user مألا ليغشتب مق show user

ضرع متي .ددحملا (نيمدختسملا) مدختسملل ةيليصفتلا نيوكتلا تامولعم رمألا ضرعي ميقلا هذه:

```
لوخدلا ليجست مسا — لوخدلا ليجست
```

عقوتم وه امك TLS وأ SSL لمعي ال

تانايبلا طويخ لجس يف ءاطخأ ةدهاشم كنكميف ،FTDs ىلع DNS نيكمتب مقت مل اذإ علام لوصولا رذعتي هنأ علام ريشت LDAP: MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2. MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15 MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61

```
ةردق نم دكأت Firepower مداوخب صاخلا (FQDN) لماكلاب لەؤملا لاجملا مسا لح ىلع Firepower ةردق نم دكأت
قفاضإب مقف ،ةحاسم كانە نكت مل.
```

configure network dns servers : رمألا ليغشتو FTD CLISH ىلإ لوصولا : FTD جمانرب



:ةروصلا يف حضوم وه امك ةرادإلا تاهجاو رتخأ مث ،System > Configuration مكحتلا ةدحو

Access List	Tinto	Ancor					
Access Control Preferences	* ince	naces					
udit Log	Link	Name	Channels	MAC Addres	5	IP	
udit Log Certificate						Address	
Change Reconciliation	0	eth0	Management Traffi	c 00:0C:29:29:	CF:2D	192.0.2.5	
DNS Cache			Event tramic				
Dashboard	• Rout	tes					
Database							
mail Notification	IPv4	Routes					
External Database Access	Dest	tination	Netmask	Interface	Gate	way	
ITTPS Certificate					192.0	0.2.1	
nformation							
ntrusion Policy Preferences	IPv6	Routes			_		1
anguage	Dest	tination	Prefix Length	Interface	Gat	teway	
.ogin Banner							
Management Interfaces	• Shar	red Sett	ings				
Vetwork Analysis Policy Preferences	s Hostr	ame	E	SEC-FMC			
Process	Doma	ins					
EST API Preferences							
lemote Storage Device	Prima	ry DNS Se	rver 1	192.0.2.10			
SNMP	Secon	idary DNS	Server				
Shell Timeout	Tertia	ry DNS Ser	rver				
íme	Remo	te Manager	ment Port a	3305			
ime Synchronization							
JCAPL/CC Compliance	• ICM	Pv6					
Iser Configuration	Allow	Sending E	cho Reply /				
Mware Tools	Packe	ts		0			
ulnerability Mapping	Allow	Allow Sending Destination					
Neb Analytics	Unrea	chable Pac	kets	0			
	• Prox	nu l					
	Enabl	ed	6				

ىلع عقو يذلا قدصملا عجرملا ةداەش يە FMC ىلإ اەليمحت مت يتلا ةداەشلا نأ نم دكأت ةروصلا يف حضوم وه امك ،LDAP ب ةصاخلا مداخلا ةداەش:



:ةحيحصلا تامولعملا LDAP مداخ لاسرا ديكأتل مزحلا طاقتلا مدختسأ

							*Ethernet0	
Fi	le Edit View Go	Capture Analyze	Statistics Telephony Wireles	s Tools H	elp			
1	🔳 🖉 💿 💄 📇	X C 9 0 0	🕾 T 🕴 📜 🗨 Q Q	Q II				
	Idap tis && ip.addr==1	92.0.2.5		•				
No	. Time	Source	Destination	Protocol	Length Info			
	3 0.143722	192.0.2.5	192.0.2.15	TLSv1.2	107 Application Data			
	4 0.143905	192.0.2.15	192.0.2.5	TLSv1.2	123 Application Data			
	22 2.720710	192.0.2.15	192.0.2.5	TLSv1.2	1211 Application Data			
	29 3.056497	192.0.2.5	192.0.2.15	LDAP	97 extendedReq(1) LDAP_START_TLS_0I	D		
	30 3.056605	192.0.2.15	192.0.2.5	LDAP	<pre>112 extendedResp(1) LDAP_START_TLS_0</pre>	ID		
4	32 3.056921	192.0.2.5	192.0.2.15	TLSv1.2	313 Client Hello			
	33 3.057324	192.0.2.15	192.0.2.5	TLSv1.2	1515 Server Hello, Certificate, Serve	r Key	Exchange, Certificate Rec	quest, Server Hello Done
	35 3.060532	192.0.2.5	192.0.2.15	TLSv1.2	260 Certificate, Client Key Exchange	, Chan	ge Cipher Spec, Encrypted	d Handshake Message
ш	36 3.061678	192.0.2.15	192.0.2.5	TLSv1.2	173 Change Cipher Spec, Encrypted Ha	ndshak	e Message	
Þ	Frame 33: 1515 by	tes on wire (12120	bits), 1515 bytes captu	red (12120	bits) on interface \Device\NPF_{3EAD5E	9F-B6C	3-4EB4-A462-217C1A10A8FE}	, id 0
Þ	Ethernet II, Src:	VMware_69:c8:c6 ((00:0c:29:69:c8:c6), Dst:	VMware_29:	cf:2d (00:0c:29:29:cf:2d)			
Þ	Internet Protocol	Version 4, Src: 1	192.0.2.15, Dst: 192.0.2.	5			disco Firepower Managem	ent Co 🗙 🕂
Þ	Transmission Contr	rol Protocol, Src	Port: 389, Dst Port: 523	84, Seq: 47	, Ack: 279, Len: 1449			
4	Transport Layer Se	ecurity					← → C â fmc/pla	atinum/authconfig.cgi?id=72837432-51c1-11ea-
	⊿ TLSv1.2 Record	Layer: Handshake	Protocol: Multiple Hands	hake Messag	es			
	Content Type	: Handshake (22)					Overview Analysis Po	licies Devices Objects AMP Intellig
	Version: TLS	1.2 (0x0303)					Confi	guration Users Domains Integration
	Length: 1444	etosol, Comune Ha	11.				Com	guration Users Domains Integration
	v Handshake Pr	otocol: Server ne	110				Users User Dalas	External Authorities
	Handebaka	Tuna: Cartificat	e (11)				Users User Koles	External Authentication
	Length: 1	124						
	Certifica	tes Length: 1121					External Authenticati	on Object
	₄ Certifica	tes (1121 bytes)						
	Certif	icate Length: 111	8				Authentication Method	LDAP 🔻
	4 Certif	icate: 3082045a30	820342a00302010202133200	00000456c38	0c8 id-at-commonName=WIN.SEC-LAB	id-	CAC	Use for CAC authentication and authorization
	▷ sig	nedCertificate					Name -	2501040
	▷ alg	orithmIdentifier	(sha256WithRSAEncryption))			Name	SEC-LDAP
	Pad	ding: 0					Description	
	enc	rypted: 3645eb112	8788982e7a5178t36022ta30	e77bad1043t	obdd		Server Turne	MS Active Directory V Cat Defaulte
	P Handshake Pr	otocol: Server Ke	y Exchange				Server Type	MS Adave Directory *
	4 Handshake Pr	otocol: Certifica	llo Done					
	- Handshake Pr	Type: Server Hel	lo Done (14)				Primary Server	
	Length: 0	type. Server nex	10 00110 (14)				, and y our ter	
	congent o						Host Name/IP Address *	WIN.SEC-LAB
							Port *	389
						-		

ةلص تاذ تامولعم

<u>قرادال ایل لوصول نیمدختسملا تاباسح</u>

- <u>الي المان الي المان الم</u>
- FireSIGHT ماظن <u>ىلع LDAP ةقداصم نىئاك نيوكت</u>
- <u>Cisco Systems</u> <u>تادنتسمل او ينقتل امعدل</u>ا

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