외부 인증을 위해 LDAP를 사용하여 Firepower Management Center 및 FTD 구성

목	차
---	---

<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
사용되는 구성 요소
<u>배경 정보</u>
<u>네트워크 다이어그램</u>
<u>구성</u>
FMC GUI의 기본 LDAP 컨피그레이션
<u>외부 사용자에 대한 셸 액세스</u>
<u>FTD에 대한 외부 인증</u>
사용자 역할
<u>SSL 또는 TLS</u>
<u>다음을 확인합니다.</u>
테스트 검색 기준
<u>LDAP 통합 테스트</u>
<u>문제 해결</u>
FMC/FTD와 LDAP는 사용자를 다운로드하기 위해 어떻게 상호 작용합니까?
FMC/FTD와 LDAP는 사용자 로그인 요청을 인증하기 위해 어떻게 상호 작용합니까?
<u>SSL 또는 TLS가 예상대로 작동하지 않음</u>
<u>관련 정보</u>

소개

이 문서에서는 Cisco FMC(Lightweight Directory Access Protocol) 및 FTD(Firepower Firepower Threat Defense)를 사용하여 Microsoft LDAP(Lightweight Directory Access Protocol) 외부 인증을 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD
- Cisco FMC
- Microsoft LDAP

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FMC 및 관리되는 디바이스에는 관리 액세스를 위한 기본 관리자 계정이 포함되어 있습니다. FMC 및 관리되는 디바이스에서 사용자 지정 사용자 계정을 내부 사용자로 추가하거나, 모델에서 지원되는 경우 LDAP 또는 RADIUS 서버의 외부 사용자로 추가할 수 있습니다. 외부 사용자 인증은 FMC 및 FTD에서 지원됩니다.

·내부 사용자 - FMC/FTD 디바이스가 사용자 인증을 위해 로컬 데이터베이스를 확인합니다.

· 외부 사용자 - 사용자가 로컬 데이터베이스에 없는 경우 외부 LDAP 또는 RADIUS 인증 서버의 시 스템 정보가 사용자 데이터베이스를 채웁니다.

네트워크 다이어그램



구성

FMC GUI의 기본 LDAP 컨피그레이션

1단계. 탐색 System > Users > External Authentication:

← → C ▲ Not:	secure 192.0.2.5/ddd/#ExternalAuthentication							1.	Ŕ	Θ:
Overview Analysis	Policies Devices Objects AMP Intelligence						Deploy	🛛 🔍 🔊	stem Help v	admin v
2		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	

2단계. 선택 Add External Authentication Object:

Save	😢 Car	ncel	🗹 Sa	ave and Apply
	Add Exte	ernal A	Authent	ication Object
Method		Ena	bled	

3단계. 필수 필드를 완료합니다.

External Authentication Object	ect	
Authentication Method	LDAP T	
CAC	Use for CAC authentication and authorization	
Name *	SEC-LDAP Name the External Authentication Object	
Description		
Server Type	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 *	beault port is 389 or 636 for SSL	
Backup Server (Optional)		
Host Name/IP Address	ex. IP or hostname	
Port	389	
I DAD-Specific Darameters		
EDAP-Specific Parameters	*Base DN specifies where users will be found	
Base DN *	DC=SEC-LAB Fetch DNs ex. dc=sourcefire,dc=com	
Base Filter	ex. (cn=jsmith), (lcn=jsmith), (&(cn=jsmith)((cn=bsmith)	cn=csmith*)))
User Name *	Administrator@SEC-LABO ex. cn=jsmith,dc=sourcefire,dc=com	
Password *	Username of LDAP Server admin	
Confirm Password *		
Show Advanced Options	•	
Attribute Mapping	*Default when 'Set Defaults' option is clicked	
UI Access Attribute *	sAMAccountName Fetch Attrs	
Shell Access Attribute *	sAMAccountName	

Group Controlled Access Roles	(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-Ophy-Liner (Read Ophy)		
view-only-oact (waar only)	Access Admin	
Default User Role	Administrator	To specify the default user role if user is not found in any group
	External Database User 🔻	-
Group Mamber Attribute	member	
Group Member 1101 Attribute	member	
Group Hender OKC Attribute		
Shell Access Filter		
Shall Account Eilter	Same as Base Filter	
(Mandatory for FTD devices)		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csm
(
Additional Test Parameters		
User Name		
Password		
*Required Field		
	Save Test Cancel	

4단계. Enable(활성화) External Authentication 개체 및 저장:

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	0 S	ystem Help +	admin +
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring	 Tools •
Users User Roles External Authentication								2.	
						ł	Save 🕻	Cancel 🗹 S	ave and Apply
Default User Role: None Shell Authentication Disabled *							O Add	d External Auther	tication Object
Name							Hethod	Enabled	
1. SEC-LDAP New External Authentication Object							LDAP		080
								1.	2

외부 사용자에 대한 셸 액세스

FMC는 서로 다른 두 내부 관리자 사용자, 즉 웹 인터페이스용 사용자와 CLI 액세스용 사용자를 지 원합니다. 즉, GUI에 액세스할 수 있는 사용자와 CLI에 액세스할 수 있는 사용자의 구분이 명확합니 다. 설치 시 기본 관리자 사용자의 비밀번호는 GUI 및 CLI에서 동일하기 위해 동기화되지만, 서로 다른 내부 메커니즘에 의해 추적되므로 결국 다를 수 있습니다.

LDAP 외부 사용자에게도 셸 액세스 권한을 부여해야 합니다.

1단계. 탐색 System > Users > External Authentication 을 클릭하고 Shell Authentication 드롭다운 상자(이미지 및 저장 참조):

Overview Analysis	Policies Devices Objects AMP Intelligence						Deploy	0 Sy	Help +	admin v
		Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
Users User Roles	External Authentication								2.	
								🗟 Save 🛛 🖸	Cancel 🗹 Sa	ave and Apply
Default User Role: None	1. Shell Authentication Disabled Disabled							O Add	External Authent	ication Object
Name	Enabled (SEC-LDAP)							Hethod	Enabled	
1. SEC-LDAP								LDAP		/ 6 @

2단계. FMC에서 변경 사항 구축

외부 사용자에 대한 셸 액세스가 구성되면 이미지에 표시된 대로 SSH를 통한 로그인이 활성화됩니다.



FTD에 대한 외부 인증

외부 인증은 FTD에서 활성화할 수 있습니다.

1단계. 탐색 Devices > Platform Settings > External Authentication. 클릭 Enabled 및 저장:

AAP Inspection Banner DNS 3. Inspection External Authentication External Auth	Overview Analysis Policie Device Management NAT 1 Platform-Policy Enter Description	Devices Objects AMP Intellige LVPN • QoS Platform Settings Fit 2.	nce xConfig Certificates		
Bander Optig Amme Description Hethod Server/Bot Enabled 1 Schranl Auftentication SC-LDAP LDAP 192.0.2.10:39 no Fragment Settings HTTP 10rd Seture Shell Strip Shell Strip Shell Strip Shell Strip Shell	ARP Inspection			Manage External Author	tication Server 🛛 🔊
• Contrast Authentication SRC-LDAP 192.0.2.10.389 no Prayment Settings 4. HTTP 104P 58.0 Secure Shell 4. SNPP 55.1 SNP 104P Time Syndronization UCAPUCC Compliance	Banner DNS 3.	Name Description	Method	Server:Port Encryp	tion Enabled
Pragment Settings 4. MTTP ICMP Secure Shell Settings SMIP Settings SNIP Settings SNIP Settings Time Syndronization UCAPUCC Compliance	External Authentication	SEC-LDAP	LDAP	192.0.2.10:389 no	
	HTTP ICMP Secure Shell SMP Server SSUP SSUP SSUP SSUP Timevols Timevols Timevols				4.

사용자 역할

사용자 권한은 할당된 사용자 역할을 기반으로 합니다. 또한 조직의 요구 사항에 맞게 조정된 액세 스 권한으로 사용자 지정 사용자 역할을 생성하거나 보안 분석가 및 검색 관리자와 같은 사전 정의 된 역할을 사용할 수 있습니다.

사용자 역할에는 두 가지 유형이 있습니다.

1. 웹 인터페이스 사용자 역할

2. CLI 사용자 역할

사전 정의된 역할의 전체 목록 및 자세한 내용은 <u>사용자</u> 역할을 <u>참조하십시오</u>.

모든 외부 인증 객체에 대한 기본 사용자 역할을 구성하려면 System > Users > External Authentication > Default User Role. 할당할 기본 사용자 역할을 선택하고 Save.

Overview Analysis Policies Devices Objects AMP Intelligence								Deploy	0 Syst	em Help +	admin +
			Configuration	Users	Domains	Integration	Updates	Licenses *	Health •	Monitoring •	Tools •
Users User Roles External Authentication											
									🗟 Save 🛛 🕄 🕻	iancel 🗹 Si	ive and Apply
Default User Role: None Shell Authentication [Enabled (SEC-LDAP) *									Q Add D	ternal Authent	cation Object
Name									Hethod	Enabled	
1. SEC-LDAP									LDAP		182
	Default User Role Configuration		_								
	Default User Role Configuration	Administratur Betaral Dabbase User (Bead Only) Security Ankyst Security Ankyst (Bead Only) Security Ankyst (Bead Only) Security Ankyst (Bead Only) Keesen Admin Materica Admin Materica Admin Threat Intelligence Director (TID) Us Vees-Only-User (Read Only) (Sidea)	er 1								

기본 사용자 역할을 선택하거나 특정 객체 그룹의 특정 사용자에게 특정 역할을 할당하려면 객체를 선택하고 Group Controlled Access Roles 그림에서 볼 수 있듯이:

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
	Access Admin
Default User Role	Administrator Discovery Admin
	External Database User 🔻

SSL 또는 TLS

DNS는 FMC에서 구성해야 합니다. 이는 인증서의 Subject 값이 Authentication Object Primary Server Hostname. 보안 LDAP가 구성되면 패킷 캡처에 더 이상 일반 텍스트 바인딩 요청이 표시되지 않습니다.

SSL은 기본 포트를 636으로 변경하고 TLS는 이를 389로 유지합니다.

✤ 참고: TLS 암호화에는 모든 플랫폼에 인증서가 필요합니다. SSL의 경우 FTD에도 인증서가 필요합니다. 다른 플랫폼의 경우 SSL에는 인증서가 필요하지 않습니다. 그러나 중간자 공격 (man-in-the-middle attack)을 방지하려면 항상 SSL용 인증서를 업로드하는 것이 좋습니다.

1단계. 탐색 Devices > Platform Settings > External Authentication > External Authentication Object 고급 옵션 SSL/TLS 정보 를 입력합니다.

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 O 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		

2단계. 서버의 인증서에 서명한 CA의 인증서를 업로드합니다. 인증서는 PEM 형식이어야 합니다.

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	%s	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

3단계. 설정 저장.

다음을 확인합니다.

테스트 검색 기준

.

LDAP가 구성된 Windows 명령 프롬프트 또는 PowerShell을 열고 명령을 입력합니다. dsquery user - name

예를 들면 다음과 같습니다.

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

Σ	Administrator: Windows PowerShell – 🗖	x	
	C:\Users\Administrator> dsquery user -name harry* Harry Potter,CN=Users,DC=SEC-LAB C:\Users\Administrator> C:\Users\Administrator> dsquery user -name * Hadministrator,CN=Users,DC=SEC-LAB Heduest,CN=Users,DC=SEC-LAB Herbtgt,CN=Users,DC=SEC-LAB Herbtgt,CN=Users,DC=SEC-LAB Henry Robert B. Banner,CN=Users,DC=SEC-LAB Herry Potter,CN=Users,DC=SEC-LAB Herry Potter,CN=Users,DC=SEC-LAB Herminoe Granger,CN=Users,DC=SEC-LAB Herminoe Granger,CN=U		
<	III	>	н

LDAP 통합 테스트

탐색 System > Users > External Authentication > External Authentication Object. 페이지 하단에 Additional Test Parameters 섹션 (이미지 참조):

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

결과를 보려면 테스트를 선택합니다.

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 CAC authent	tication and authorization							
	Name * SEC-LDAP Description Server Type MS Adive Directory *	Set Defaults							

					Capturing from Ethernet1	- 0 X					
Fi	e Edit View	w Go Capture Analyze	Statistics Telephony Wirele	ess Tools	Help						
4	ی کے 🔳		🕾 T 🛓 🗐 🗨 G								
	Tap.port399 84 (p.adv192.0.2.5										
No	Time	Source	Destination	Protocol	al Length Info	~					
T	1799 55.13	31546 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 55.13	31547 192.0.2.5	192.0.2.10	LDAP	127 bindRequest(1) "CN+Marry Potter,CN+Users,DC+SEC-LAB simple						
÷	1801 55.13	32124 192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success						
	1802 55.13	32184 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 55.13	32213 192.0.2.5	192.0.2.10	LDAP	73 unbindRequest(2)						
	1804 55.13	32213 192.0.2.5	192.0.2.10	TCP	66 39784 = 389 [FIN, ACK] Seq+69 Ack=23 Win=29312 Len+0 TSval=3077124550 TSecr=25705266						
	1805 55.13	32227 192.0.2.10	192.0.2.5	TCP	66 389 + 39784 [4CK] Seq=23 Ack=70 Win=66560 Len=0 TSval=25708266 TSecr=3077124549	×					
Þ	Frame 1800:	: 127 bytes on wire (101	6 bits), 127 bytes captu	red (1016	bits) on interface \Device\NPF_{77DC31F6-8250-4F19-8412-E4596F960100}, id 0						
Þ	Ethernet II	I, Src: VMware_29:cf:2d	(00:0c:29:29:cf:2d), Dst	: Vhware_e	eb:1d:f7 (00:0c:29:eb:1d:f7)						
Þ	Internet Pr	notocol Version 4, Src:	192.0.2.5, Dst: 192.0.2.	10							
Þ	Transmissio	on Control Protocol, Src	Port: 39784, Dst Port:	389, Seq:	1, Ack: 1, Len: 61						
4	Lightweight	t Directory Access Proto	col								
	# LDAPMessi	tage bindRequest(1) "CN+	Harry Potter, CN=Users, DC	*SEC-LAB	" simple						
	messar	meelD: 1		_							
	a proto	colop: bindkequest (0)									
	- 01/	version: 3									
		name: Chultarry Potter.(Nullsers DCuSEC-LAB								
		authentication: simple	(0)								
		simple: cisco	(-)								
	[Resp	onse In: 18011									

문제 해결

FMC/FTD와 LDAP는 사용자를 다운로드하기 위해 어떻게 상호 작용합니까?

FMC가 Microsoft LDAP 서버에서 사용자를 가져올 수 있으려면 먼저 LDAP 관리자 자격 증명이 포 함된 포트 389 또는 636(SSL)에서 바인딩 요청을 보내야 합니다. LDAP 서버가 FMC를 인증할 수 있게 되면 성공 메시지로 응답합니다. 마지막으로, FMC는 다이어그램에 설명된 대로 검색 요청 메 시지를 사용하여 요청할 수 있습니다.

<< --- 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

인증은 기본적으로 암호화되지 않은 상태로 비밀번호를 전송합니다.

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 8 Etherne: Interne: Iransmi Lightwe: LOAP me pr 	5: 110 bytes t II, Src: V t Protocol V ssion Contro ight Directo lessage bind restored p: bindRequest version: name: Ac 4 authenti simpl	on wire (880 bits), Mware_29:cfi2d (00:04 ersion 4, Src: 192.0. l Protocol, Src Port: ry Access Protocol Request(1) "Administr indRequest (0) t : 3 ministrator@SEC-LAB0 (cation: simple (0) e: Ciscot@c	110 bytes captured (8 :29:29:cf:2d), Dst: V 2.5, Dst: 192.0.2.10 38002, Dst Port: 385 ator@SEC-LABO" simple	800 bits) o Mware_eb:1 0, Seq: 1, 4	n interface \Device\WPF_{77DC31F6-B250-4F19-8412-E4596F960108}, id 0 d:f7 (00:0c:29:eb:1d:f7) Ack: 1, Len: 44
	reappointed inte				

FMC/FTD와 LDAP는 사용자 로그인 요청을 인증하기 위해 어떻게 상호 작용합니까?

LDAP 인증이 활성화된 동안 사용자가 FMC 또는 FTD에 로그인할 수 있도록 초기 로그인 요청이

Firepower으로 전송되지만 성공/거부 응답을 위해 사용자 이름과 비밀번호가 LDAP로 전달됩니다. 즉, FMC 및 FTD는 데이터베이스에 로컬로 비밀번호 정보를 보관하지 않고 대신 LDAP에서 진행 방법에 대한 확인을 기다립니다.



Firepower Management Center	
Username h.potter Password rem Log In	

	(*Ethernet1
F	ile E	dit View Go C	apture Analyze Statistic	Telephony Wireless	Tools Hel	р	
4		2 🖲 퉬 🛅 🎽	रे 🖸 🭳 🗢 🗢 🕾 🖗	🕹 📃 📃 @, Q, Q	. 🖽		
	tcp.p	ort==389 && ip.addr=	=192.0.2.5 && ldap.messageII) == 1			
N	o.	Time	Source	Destination	Protocol	Length	th Info
	1	58 13:11:59.6956	71 192.0.2.5	192.0.2.10	LDAP	110	10 bindRequest(1) "Administrator@SEC-LABO" simple
+	1	59 13:11:59.6974	73 192.0.2.10	192.0.2.5	LDAP	88	88 bindResponse(1) success
	(67 13:11:59.6977	73 192.0.2.5	192.0.2.10	LDAP	110	10 bindRequest(1) "Administrator@SEC-LABO" simple
	(69 13:11:59.6994	74 192.0.2.10	192.0.2.5	LDAP	88	88 bindResponse(1) success
	9	97 13:11:59.7299	88 192.0.2.5	192.0.2.10	LDAP	127	27 bindRequest(1) "CN=Harry Potter,CN=Users,DC=SEC-LAB simple
	1	98 13:11:59.7306	98 192.0.2.10	192.0.2.5	LDAP	88	88 bindResponse(1) success

사용자 이름 및 비밀번호가 수락되면 이미지에 표시된 대로 웹 GUI에 항목이 추가됩니다.

Overview Analysis Policies Devices O	bjects AMP Intelligence							Deploy	Ø Syste	m Help v	h.potter +
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	 Tools •
Users User Roles External Authen	tication									-	
										00	Create User
Username	Roles	Authentication Method		Pass	word Lifetim	e					
admin	Administrator	Internal		Unlim	nited						1
h.potter	Administrator	External									0
admin h.eotter	Administrator Administrator	Internal External		Unite	nted						1

사용자 정보를 확인하려면 FMC CLISH에서 show user 명령을 실행합니다. > show user

이 명령은 지정된 사용자에 대한 자세한 컨피그레이션 정보를 표시합니다. 다음 값이 표시됩니다.

Login(로그인) - 로그인 이름

UID -- 숫자 사용자 ID

Auth (Local or Remote)(인증(로컬 또는 원격)) - 사용자 인증 방법

Access(Basic 또는 Config) - 사용자의 권한 레벨

Enabled(활성화됨 또는 비활성화됨) — 사용자의 활성 여부

Reset (Yes or No)(재설정(예 또는 아니요) - 사용자가 다음 로그인 시 비밀번호를 변경해야 하는지 여부

Exp(Never 또는 a number) - 사용자의 비밀번호를 변경해야 할 때까지의 일수

경고(N/A 또는 숫자) — 비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경할 수 있는 일 수입 니다

Str(Yes 또는 No) — 사용자의 비밀번호가 강도를 확인하기 위한 기준을 충족해야 하는지 여부 Lock (Yes or No)(잠금(예 또는 아니요) - 로그인 실패가 너무 많아 사용자 계정이 잠겼는지 여부 Max(N/A 또는 a number) — 사용자 계정이 잠기기 전 최대 실패 로그인 수

SSL 또는 TLS가 예상대로 작동하지 않음

FTD에서 DNS를 활성화하지 않으면 pigtail 로그에서 LDAP에 연결할 수 없음을 나타내는 오류를 확인할 수 있습니다.

root@SEC-FMC:/\$ sudo cd /var/common root@SEC-FMC:/var/common\$ sudo pigtail 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

firepower에서 LDAP 서버 FQDN을 확인할 수 있는지 확인합니다. 그렇지 않은 경우 이미지에 표시 된 대로 올바른 DNS를 추가합니다.

FTD: FTD CLISH에 액세스하여 다음 명령을 실행합니다. > configure network dns servers

₽ 192.0.2.	6 - PuTTY		x
root@SEC-FTD:/etc# ping WIN.SEC-LAB ping: unknown host WIN.SEC-LAB			^
root@SEC-FTD:/etc# exit			
exit			
admin@SEC-FTD:/etc\$ exit			
logout			
>			
> configure network dns servers 192.0.2.3	15		
<pre>> expert ************************************</pre>	in future releases arate expert mode CLI.		
admin@SEC-FTD:~\$ ping WIN.SEC-LAB			
PING WIN.SEC-LAB (192.0.2.15) 56(84)	bytes of data.		
64 bytes from win.sec-lab.net (192.0.2.1	5): icmp_seq=1 ttl=128 time=0.1	76 ms	
64 bytes from win.sec-lab.net (192.0.2.1)	5): icmp_seq=2 ttl=128 time=0.4	15 ms	
^C			
WIN.SEC-LAB ping statistics			
2 packets transmitted, 2 received, 0% packets	cket loss, time 1010ms		
rtt min/avg/max/mdev = $0.176/0.295/0.415$	0.120 ms		
admin@SEC-FTD:~\$			
			\sim

FMC: 선택 System > Configuration를 선택한 다음 이미지에 표시된 대로 Management Interfaces(관리 인 터페이스)를 선택합니다.

Access List	* Inter	faree					
Access Control Preferences	· incer	laces					_
ludit Log	Link	Name	Channels	MAC Address	s IP		
udit Log Certificate					Ad	iress	
hange Reconciliation	0	eth0	Management Traffic	00:0C:29:29:	CF:2D 192	2.0.2.5	6
NS Cache			Event france				
ashboard	• Route	25					
atabase							
nail Notification	IPv4 s	toutes					•
ternal Database Access	Desti	nation	Netmask	Interface	Gateway		
TPS Certificate	-				192.0.2.1		6
formation							
trusion Policy Preferences	IPv6 F	loutes					•
nguage	Desti	nation	Prefix Length	Interface	Gatewa	Y	
gin Banner							
anagement Interfaces	• Share	ed Sett	ings				
twork Analysis Policy Preferences	s Hostna	me	5	EC-FMC			
ocess	Domai					_	
ST API Preferences						-	
mote Storage Device	Primar	y DNS Se	rver 1	92.0.2.10			
IMP	Second	lary DNS	Server				
nell Timeout	Tertian	y DNS Ser	ver				
ne	Remot	e Managei	ment Port 8	105			
me Synchronization			<u></u>				
APL/CC Compliance	▼ICMP	v6					
er Configuration	Allow 5	lending Fi	the Realy				
ware Tools	Packet	s S	210 mpc) 2				
Inerability Mapping	Allow 5	lending D	estination				
b Analytics	Unread	hable Pac	kets 👻				
	• Proxy	/					
	Enable	d	6				

이미지에 표시된 대로 FMC에 업로드된 인증서가 LDAP의 서버 인증서에 서명한 CA의 인증서인지 확인합니다.



LDAP 서버가 올바른 정보를 전송하는지 확인하려면 패킷 캡처를 사용합니다.

	(*Ethernet0	
1	File Edit View Go	Capture Analyze S	Statistics Telephony Wireles	s Tools H	elp			
	🕻 🔳 🔬 💿] 🔒 🛅	🗙 🖸 🧣 👄 🔿	🕾 T 🛓 📃 🗨 Q	Q, II				
0	Idap tis && ip.addr==1	92.0.2.5						
N	o. 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_OID			
	30 3.056605	192.0.2.15	192.0.2.5	LDAP	<pre>112 extendedResp(1) LDAP_START_TLS_OID</pre>)		
-	32 3.056921	192.0.2.5	192.0.2.15	TLSv1.2	313 Client Hello			
н	33 3.057324	192.0.2.15	192.0.2.5	TLSv1.2	1515 Server Hello, Certificate, Server	Key E	xchange, Certificate Requ	Jest, Server Hello Done
	35 3.060532	192.0.2.5	192.0.2.15	TLSV1.2	260 Certificate, Client Key Exchange,	Chang	ge Cipher Spec, Encrypted	Handshake Message
	30 3.0010/8	192.0.2.15	192.0.2.5	11501.2	173 Change Cipner Spec, Encrypted Hand	ISNAK	e message	
	Frame 33: 1515 byt	tes on wire (12120	bits), 1515 bytes captu	red (12120	bits) on interface \Device\NPF_{3EAD5E9F	-B6CB	-4EB4-A462-217C1A10A8FE},	id 0
	Ethernet II, Src:	VMware_69:c8:c6 (00:0c:29:69:c8:c6), Dst:	Whware_29:	cf:2d (00:0c:29:29:cf:2d)			
	Internet Protocol	Version 4, Src: 1	92.0.2.15, Dst: 192.0.2.	5	4-1- 270 1 4440		Cisco Firepower Manageme	nt Ce × +
Ľ	Transmission Contr	rol Protocol, Src	Port: 389, Dst Port: 523	84, Seq: 4/	, ACK: 2/9, Len: 1449	Γ.		
1	4 TLSv1 2 Record	Lavers Mandchake	Protocol: Multiple Handr	hake Mercan	ar	11	← → G ■ fmc/pla	tinum/authconfig.cgi/id=/283/432-51c1-11ea-
L.	Content Type	Handshake (22)	Protocol. Huitiple hands	nake nessag				
L.	Version: TLS	1.2 (0x0303)					Overview Analysis Pol	icles Devices Objects AMP Intellig
L.	Length: 1444						Config	uration Users Domains Integration
L.	Handshake Pr	otocol: Server He	110					
L.	₄ Handshake Pr	otocol: Certifica	te				Users User Roles	External Authentication
	Handshake	Type: Certificate	e (11)					
L.	Length: 1	124						
	Certifica	tes Length: 1121					External Authentication	on Object
L.	4 Certifica	tes (1121 bytes)					Authoritization Mathed	1040
	Certif	icate Length: 1118	6				Authentication Method	LUAP
L.	4 Certif	icate: 3082045a308	820342a00302010202133200	00000456c380	<pre>dc8 id-at-commonName=WIN.SEC-LAB id</pre>	1	CAC	Use for CAC authentication and authorization
	P sig	nedCertificate	(Name *	SEC-LDAP
L.	v aig	dieg: 0	(Sna256withKSAEncryption)	,				
	Paul	cunted: 3645eb1128	788987e7a5178f36977fa30	e77had1043h	hdd		Description	
	Handshake Pr	otocol: Server Ke	v Exchange				Server Type	MS Active Directory V Set Defaults
	Handshake Pr	otocol: Certifica	te Request					
	4 Handshake Pr	otocol: Server He	llo Done					
	Handshake	Type: Server Hell	lo Done (14)				Primary Server	
	Length: 0)					Heat Name/ID Address 8	han and han
							HUSL Name/ IP Address *	WIN-SEC-LAB
							Port *	389

관련 정보

• 관리 액세스를 위한 사용자 계정

- <u>Cisco Firepower Management Center LDS(Lightweight Directory Access Protocol) 인증 우회</u> <u>취약성</u>
- FireSIGHT 시스템의 LDAP 인증 객체 컨피그레이션
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.