外部認証用のLDAPを使用したFirepower Management CenterおよびFTDの設定

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>ネットワーク図</u>
<u>設定</u>
<u>FMC GUIでの基本的なLDAP設定</u>
<u>外部ユーザのシェルアクセス</u>
<u>FTDへの外部認証</u>
<u>ユーザ ロール</u>
<u>SSLまたはTLS</u>
<u>テスト検索ベース</u>
<u>LDAP統合のテスト</u>
トラブルシュート
FMC/FTDとLDAPはどのように相互作用してユーザをダウンロードしますか <u>。</u>
<u>ユーザログイン要求を認証するためにFMC/FTDとLDAPはどのように相互作用しますか。</u>
<u>SSLまたはTLSが期待どおりに機能しない</u>
<u>関連情報</u>

はじめに

このドキュメントでは、Cisco Authentication Management Center(FMC)およびFirepower Threat Defense(FTD)でMicrosoft Lightweight Directory Access Protocol(LDAP)外部Firepowerを有効にする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・シスコFTD
- Cisco FMC
- Microsoft LDAP

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTD6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

FMCと管理対象デバイスには、管理アクセス用のデフォルトの管理者アカウントが含まれていま す。FMCおよび管理対象デバイス上に、内部ユーザとして、またはモデルでサポートされている 場合はLDAPまたはRADIUSサーバ上の外部ユーザとして、カスタムユーザアカウントを追加でき ます。外部ユーザ認証は、FMCとFTDでサポートされます。

・内部ユーザ:FMC/FTDデバイスは、ユーザ認証のためにローカルデータベースをチェックしま す。

・外部ユーザ:ユーザがローカルデータベースに存在しない場合、外部LDAPまたはRADIUS認証 サーバからのシステム情報がユーザデータベースに入力されます。



ネットワーク図

FMC GUIでの基本的なLDAP設定

ステップ1:移動先 System > Users > External Authentication:を入力します。

← → C ▲ No	secure 192.0.2.5/ddd/#ExternalAuthentication	1 ☆ Θ ÷
Overview Analysis	Policies Devices Objects AMP Intelligence	Deploy 🔩 System Help + admin +
3		Configuration Users Domains Integration Updates Licenses Health Monitoring Tools -
Users User Roles	External Authentication	2.
		🔚 Save 🖉 Cancel 😾 Save and Apply
Default User Role: None	Shell Authentication Disabled	Add External Authentication Object.
Name		Hethod Enabled

ステップ2: 選択 Add External Authentication Object:を入力します。

🔚 s	ave	😢 Car	ncel	🗹 Sa	ive and Apply		
	Add External Authentication Obje						
	Meth	nod	Ena	bled			

ステップ3:次の必須フィールドに入力します。

External Authentication Object	t	
Authentication Method	LDAP V	
CAC	Use for CAC authentication and authorization	
Name *	SEC-LDAP Name the External Auth	entication Object
Description		
Server Type	MS Active Directory Set Defaults Choose MS Active Direct	tory and click 'Set Defaults'
Primary Server		
Host Name/IP Address *	192.0.2.10	ex. IP or hostname
Port *	Default port is 389 or 630	5 for SSL
Backup Server (Optional)		
Host Name/IP Address		ex. IP or hostname
Port	389	
LDAD. Specific Darameters		
LDAF-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), (!cn=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=csmith*)))
User Name *	Administrator@SEC-LAB0	ex. cn=jsmith,dc=sourcefire,dc=com
Password *	Username of LDAP Serve	er admin
Confirm Password *		
Show Advanced Options	•	
	*Default when 'Set Defaults' optio	n is disked
Attribute Mapping	Default when Set Defaults optio	in is clicked
UI Access Attribute *	sAMAccountName Fetch Attrs	
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	
Shell Access Filter 🛈	🕑 Same as Base Filter
(Mandatory for FTD devices)	
Additional Test Parameters	
User Name	
Password	
*Required Field	Save Test Cancel

ステップ4:次を有効にします。 External Authentication オブジェクトと保存:

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	0 0 5	stem Help	v admin v	
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitorin	g 🔹 Tools	÷
Users User Roles External Authentication								2.		
						ł	🗟 Save 【	Cancel	Save and App	ły.
Default User Role: None Shell Authentication Disabled •							O Add	External Aut	entication Obje	rct
Name							Hethod	Enable	d	
1. SEC-LDAP New External Authentication Object							LDAP		/ 6	2
								1.	3	

外部ユーザのシェルアクセス

FMCでは、Webインターフェイス用とCLIアクセス用の2つの異なる内部管理者ユーザがサポート されています。つまり、誰がGUIにアクセスできるのか、誰がCLIにアクセスできるのかというこ とははっきりと区別されます。インストール時に、デフォルトの管理者ユーザのパスワードは、 GUIとCLIの両方で同じになるように同期されますが、これらは異なる内部メカニズムによって追 跡され、最終的には異なる場合があります。

LDAP外部ユーザにもシェルアクセスを許可する必要があります。

ステップ1:移動先 System > Users > External Authentication をクリックして Shell Authentication 図に示すドロップダウンボックスを使用して保存します。

Overview Analysis	Policies Devices Objects AMP Intelligence						Deploy	🔍 🔍 Syr	stem Help +	adm	in v
		Configuration	Users	Domains	Integration	Updates	Licenses •	Health +	Monitoring	• To	ols •
Users User Roles	External Authentication								2.		
								🗟 Save 🛛 🖸	Cancel 🖉 S	ave and	Apply
Default User Role: None	1. Shell Authentication Disabled Disabled							Q Add	External Autheri	tication (Object
Name	Enabled (SEC-LDAP)							Hethod	Enabled		
1. SEC-LDAP								LDAP		1	a e

ステップ2:FMCで変更を展開します。

外部ユーザのシェルアクセスが設定されると、次の図に示すように、SSH経由のログインが有効 になります。



FTDへの外部認証

外部認証はFTDでイネーブルにできます。

ステップ1:移動先 Devices > Platform Settings > External Authenticationを参照。クリック Enabled 保存します。

ユーザ ロール

ユーザ権限は、割り当てられたユーザロールに基づきます。また、組織のニーズに合わせてアク セス権限を持つカスタムユーザロールを作成したり、セキュリティアナリストやディスカバリ管 理者などの事前定義されたロールを使用することもできます。

ユーザロールには、次の2つのタイプがあります。

- 1. Webインターフェイスユーザロール
- 2. CLIユーザロール

事前定義されたロールの完全なリストと詳細については、「<u>ユーザロール</u>」を参照してください 。

すべての外部認証オブジェクトのデフォルトユーザロールを設定するには、 System > Users > External Authentication > Default User Roleを参照。 割り当てるデフォルトのユーザロールを選択し、 Saveを参照。

Overview Analysis Policies Devices Objects AMP Intelligence									0 Syste	em Help 👻	admin 🔻
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools *
Users User Roles External Authentication			_	_	_	_	_				
									Save 🖸 C	ancel 🗹 Sa	eve and Apply
Default User Role: None Shell Authentication Enabled (SEC-LDAP) *									O Add Ex	ternal Authent	ication Object
Name									Hethod	Enabled	
1. SEC-LOAP									LDAP		/ 8 2
			-								
	Default User Role Configuration										
	Default User Roles	Administratur Deternal Database User (Beed Only) Security Analyst (Beed Only) Security Analyst (Beed Only) Security Approver Intrusion Admin Access Admin Network Admin Mathemace User Discovery Admin Threes Lifelligence Director (TED) Us	er.								
	Custom User Roles	C view-Uniy-User (Read Only) (Global									
		Sav	e Cancel								

デフォルトのユーザロールを選択したり、特定のオブジェクトグループ内の特定のユーザに特定 のロールを割り当てたりするには、オブジェクトを選択し、 Group Controlled Access Roles 次の図に示す ように、

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
	External Database User

SSLまたはTLS

DNSはFMCで設定する必要があります。これは、証明書のサブジェクト値が Authentication Object Primary Server Hostnameを参照。セキュアLDAPが設定されると、パケットキャプチャでクリアテキスト のバインド要求が表示されなくなります。

SSLではデフォルトポートが636に変更され、TLSでは389のままになります。

◆ 注:TLS暗号化では、すべてのプラットフォームで証明書が必要です。SSLの場合、FTDにも 証明書が必要です。その他のプラットフォームでは、SSLに証明書は不要です。ただし、中 間者攻撃を防ぐために、常にSSL用の証明書をアップロードすることをお勧めします。

ステップ1:移動先 Devices > Platform Settings > External Authentication > External Authentication Object SSL/TLSの詳細 オプション情報を入力します。

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

ステップ2:サーバの証明書に署名したCAの証明書をアップロードします。証明書はPEM形式で ある必要があります。

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	
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	

ステップ3:設定を保存します。

確認

テスト検索ベース

LDAPが設定されているWindowsコマンドプロンプトまたはPowerShellを開き、次のコマンドを 入力します。 dsquery user -name

を参照。

例:

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

Σ	Administrator: Windows PowerShell 📃 🗖	x	
25 25 25 25 25 25 25 25 25 25 25 25 25 2	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 =Bart Simpson,CN=Users,DC=SEC-LAB =Dr. Robert B. Banner,CN=Users,DC=SEC-LAB =Dr. Robert B. Banner,CN=Users,DC=SEC-LAB =Ginny Weasley,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 =Hargie Simpson,CN=Users,DC=SEC-LAB =Maggie Simpson,CN=Users,DC=SEC-LAB =Matthew Murdock,CN=Users,DC=SEC-LAB =Neville Longbottom,CN=Users,DC=SEC-LAB =Ron Weasley,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB C:\Users\Administrator> C:\Users\Administrator> C:\Users\Administrator> C:\Users\Administrator>		
<		> .	

LDAP統合のテスト

移動先 System > Users > External Authentication > External Authentication Objectを参照。ページの下部に、 Additional Test Parameters 図に示すセクション:

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

結果を表示するには、Testを選択します。

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 LOAP • CAC Use for CAC auth Name * SEC-LDAP Description	ntication and authorization Set Defaults							

4						Capturing from Ethernet1	- 0 X
Fi	e Edit	View Go	Capture Analyze St	tatistics Telephony Wirele	rss Tools	Help	
1	• 4		80 9 ***	S T 🛓 🗐 🔍 Q	Q. 11		
	tcp.port+	=389 8& (p. ac	dr==192.0.2.5				
No	1	Time	Source	Destination	Protocol	A Length Info	~
T	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-LAB * simple	
÷	1801	55.132124	192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success	
	1802	\$5.132184	192.0.2.5	192.0.2.10	TCP	66 39784 → 389 [ACK] Seq=62 Ack=23 Win=29312 Len=0 TSval=3077124549 TSecr=25708266	
ш	1803	55.132213	192.0.2.5	192.0.2.10	LDAP	73 unbindRequest(2)	
	1504	55.132213	192.0.2.5	192.0.2.10	TCP	66 39784 + 389 [FIN, KK] Seq+09 Ack+23 kUn=20312 Len+0 TSval=3077124550 TSec=25708266	
	1805	55.132227	192.0.2.10	192.0.2.5	TCP	66 389 + 39784 [ACK] Seq=23 ACK=70 Win+66560 Len+0 TSval=25708266 TSec7=3077124549	¥.
Þ	Frame 7	800: 127	bytes on wire (1016	bits), 127 bytes captur	red (1016	bits) on interface \Device\MPF_(77DC31F6-8250-4F19-8412-E4596F960108}, id 0	
Þ	Etherne	rt II, Src	: VNware_29:cf:2d (0	N0:0c:29:29:cf:2d), Dst	: V?Ware_e	tb:1d:f7 (00:0c:29:eb:1d:f7)	
P	Interne	rt Protoco.	l Version 4, Src: 19	2.0.2.5, Dst: 192.0.2.	10		
P.	Transes	ssion Con	trol Protocol, Src P	Port: 39784, Dst Port: :	389, Seq:	1, Ack: 1, Len: 61	
1	Lightwe	ight Dire	ctory Access Protoco	1			
	*	message of	indikequest(1) UN+Ha	rry Potter, chiosers, oci	*SEC-LAD	sample	
	1 - 2 k	cotocol0o	hindRequest (8)				
		4 bindRegu	est				
		versi	001 3				
		name	CN+Harry Potter, CN	Users, DC=SEC-LAB			
		4 authe	ntication: simple (0)			
		51	mple: cisco				
	1	Response 1	(n: 1801]				

トラブルシュート

FMC/FTDとLDAPはどのように相互作用してユーザをダウンロードしますか。

FMCがMicrosoft LDAPサーバからユーザをプルできるようにするには、FMCは最初に、LDAP管 理者クレデンシャルを使用して、ポート389(SSL)または636(SSL)でバインド要求を送信する必要 があります。LDAPサーバがFMCを認証できるようになると、成功メッセージで応答します。最 後に、FMCは次の図に示すように、検索要求メッセージを使用して要求を行うことができます。

<< --- 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

デフォルトでは、認証はクリアテキストでパスワードを送信することに注意してください。

192.0.2.5 192.0.2.10 192.0.2.5 192.0.2.5 192.0.2.5 192.0.2.5 192.0.2.5 192.0.2.5 an wire (880 bits), ware_23:cf:2d (00:0c rsion 4, Src: 192.0.	192.0.2.10 192.0.2.10 192.0.2.10 192.0.2.10 192.0.2.10 192.0.2.10 192.0.2.10 110 bytes captured (8 :29:29:cf:20), Dst: V 2.5, Dst: 192.0.2.10	TCP TCP LDAP LDAP TCP LDAP LDAP LDAP Mware_eb:1d	74 38002 + 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3073529344 TSecr=0 MS=128 74 380 + 38002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=25346746 TSecr=3073529344 63 30002 + 380 [ACK] Seq=1 Ack=1 Win=2912 Len=0 TSval=3073529344 TSecr=25346746 TSecr=3073529344 100 bindRequest(1) "Administrator@SEC-LAB0" simple 88 bindResponse(1) success 66 38002 + 380 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746 122 searchRequest(2) "DC=SEC-LAB" 'wholeSubtree h interface \Device\WPF_{77DC31F6-B250-4F19-8412-E4596F960108}, id 0 if7 (00:0c:29:eb:1d:f7)				
192.0.2.10 192.0.2.5 192.0.2.5 192.0.2.10 192.0.2.5 on wire (880 bits), ware_29:cf:2d (00:0c rsion 4, src: 192.0.	192.0.2.5 192.0.2.10 192.0.2.10 192.0.2.5 192.0.2.10 192.0.2.10 192.0.2.10 192.0.2.10 110 bytes captured (8: 129:29:cf:20), Dst: V 2.5, Dst: 192.0.2.10	TCP TCP LDAP LDAP TCP LDAP (80 bits) on Mware_eb:1d	74 389 + 38082 [SVN, ACK] Seq=0 Ack=1 Win=29312 Len=0 PKS=1460 WS=256 SACK PERM=1 TSval=25348746 TSecr=3073529344 66 38002 + 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3073529344 TSecr=25348746 110 bindResponse(1) success 66 38002 + 389 [ACK] Seq=45 Ack=3 Win=29312 Len=0 TSval=3073529345 TSecr=25348746 122 searchRequest(2) "AdviceSec-LAB ' wholeSubtree h interface \Device\NPF_{77DC31F6-B250-4F19-B412-E4596F960108}, id 0 d:f7 (00:0c:29:eb:1d:f7)				
192.0.2.5 192.0.2.5 192.0.2.5 192.0.2.5 192.0.2.5 192.0.2.5 on wire (880 bits), ware_29:cf:2d (00:0c rsion 4, Src: 192.0.	192.0.2.10 192.0.2.10 192.0.2.5 192.0.2.10 192.0.2.10 110 bytes captured (8 :29:29:cf:2d), Dst: V 2.5, Dst: 192.0.2.10	TCP LDAP LDAP TCP LDAP (80 bits) on Mware_eb:1d	66 38002 + 380 [ACK] Seq1.Ack=1 Win=2912 Lene® TSval=3073529344 TSecr=25348746 110 bindRequest(1) "Administrator@SEC-LAB0" simple 88 bindResponse(1) success 66 38002 + 380 [ACK] Seq=45 Ack=23 Win=29312 Lene® TSval=3073529345 TSecr=25348746 122 searchRequest(2) "DC-SEC-LAB " wholeSubtree interface \Device\NPF_{77DC31F6-B250-4F19-B412-E4596F960108}, id 0 d:f7 (00:0c:29:eb:1d:f7)				
192.0.2.5 192.0.2.10 192.0.2.5 192.0.2.5 on wire (880 bits), ware_29:cf:2d (00:0c rsion 4, Src: 192.0.	192.0.2.10 192.0.2.5 192.0.2.10 192.0.2.10 110 bytes captured (8 :29:29:cf:2d), Dst: V 2.5, Dst: 192.0.2.10	LDAP LDAP TCP LDAP 180 bits) on Mware_eb:1d	110 bindRequest(1) "Administrator@SEC-LAB0" simple 88 bindResponse(1) success 63 30002 + 309 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746 122 searchRequest(2) "DC-SEC-LAB wholeSubtree ninterface \Device\NPF_{77DC31F6-B250-4F19-8412-E4596F960108}, id 0 iff (00:0c:29:eb:ld:f7)				
192.0.2.10 192.0.2.5 192.0.2.5 on wire (880 bits), ware_29:cf:2d (00:0c rsion 4, Src: 192.0.	192.0.2.5 192.0.2.10 192.0.2.10 110 bytes captured (8 :29:29:cf:2d), Dst: V 2.5, Dst: 192.0.2.10	LDAP TCP LDAP 80 bits) on Mware_eb:1d	88 blndResponse(1) success 66 38002 + 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746 122 searchRequest(2) "Oc-SEC-LAB ' wholeSubtree n interface \Device\NPF_{77DC31F6-B250-4F19-B412-E4596F960108}, id 0 diff (00:0c:29:eb:ld:f7)				
192.0.2.5 192.0.2.5 on wire (880 bits), ware_29:cf:2d (00:0c rsion 4, Src: 192.0.	192.0.2.10 192.0.2.10 110 bytes captured (8 :29:29:cf:2d), Dst: V 2.5, Dst: 192.0.2.10	TCP LDAP 80 bits) on Mware_eb:1d	66 38002 + 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746 122 searchRequest(2) "DC=SEC=LAB ' wholeSubtree n interface \Device\NPF_{77DC31F6-8250-4F19-8412-E4596F960108}, id 0 1:f7 (00:0c:29:eb:1d:f7)				
192.0.2.5 on wire (880 bits), ware_29:cf:2d (00:0c rsion 4, Src: 192.0.	192.0.2.10 110 bytes captured (8 :29:29:cf:2d), Dst: W 2.5, Dst: 192.0.2.10	LDAP 80 bits) on Mware_eb:1d	122 searchRequest(2) "DC-SEC-LAB 'wholeSubtree n interface \Device\NPF_{77DC31F6-B250-4F19-B412-E4596F960108}, id 0 if7 (00:0c:29:eb:1d:f7)				
on wire (880 bits), Ware_29:cf:2d (00:0c rsion 4, Src: 192.0.	110 bytes captured (8 :29:29:cf:2d), Dst: W 2.5, Dst: 192.0.2.10	80 bits) on Mware_eb:1d	ninterface \Device\NPF_{77DC31F6-B250-4F19-B412-E4596F960108}, id 0 dif7 (00:0c:29:eb:ld:f7)				
<pre>b Frame 86: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\WPF_(770C31F6-8250-4F19-8412-E4596F960108}, id 0 b Ethernet II, Src: VMware_29:cf:2d (00:0c:29:29:cf:2d), Dst: WMware_eb:1d:f7 (00:0c:29:eb:1d:f7) b Internet Protocol Version 4, Src: 192.0.2.5, Dst: 192.0.2.10 b Transmission Control Protocol, Src Port: 38002, Dst Port: 380, Seq: 1, Ack: 1, Len: 44 4 Lightweight Directory Access Protocol 4 DDAPMessage bindRequest(1) "Administrator@SEC-LA80" simple messageID: 1 4 protocolOp: bindRequest (0) 5 bindRequest 5 version: 3 5 name: Administrator@SEC-LA80 5 version: 4 5 v</pre>							
nd 3 ni	iRequest (0) inistrator@SEC-LAB0 ation: simple (0)	iRequest (0) in inistrator@SEC-LAB0 ition: simple (0)	Request (0) inistrator@SEC-LAB0 ition: simple (0)				

ユーザログイン要求を認証するためにFMC/FTDとLDAPはどのように相互作用しま すか。 LDAP認証が有効な状態でユーザがFMCまたはFTDにログインできるように、最初のログイン要 求がFirepowerに送信されます。ただし、ユーザ名とパスワードはLDAPに転送され、成功/拒否応 答が返されます。つまり、FMCとFTDはパスワード情報をデータベース内にローカルに保持せず 、代わりに続行する方法に関するLDAPからの確認を待ちます。



L	4							*Ethernet1	
	File Edi	t View Go Capt	ture Analyze Statistics	Telephony Wireless Te	ools Hel	р			
		1 💿 🌗 🔚 🗙	🖸 🍳 🗢 🗢 🗟 🖗 .	୬ 📃 📃 ୧ ୧ ୧					
	tcp.por	t==389 && ip.addr==1	92.0.2.5 && Idap.messageID =	-= 1					
	No.	Time	Source	Destination	Protocol	Length	Info		
	5	3 13:11:59.695671	192.0.2.5	192.0.2.10	LDAP	110	<pre>bindRequest(1)</pre>	"Administrator@SEC-LAB0" simple	
	• 5	3 13:11:59.697473	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	
	6	7 13:11:59.697773	192.0.2.5	192.0.2.10	LDAP	110	<pre>bindRequest(1)</pre>	"Administrator@SEC-LAB0" simple	
	6	3:11:59.699474	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	
	9	7 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
	9	3 13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	

ユーザ名とパスワードが受け入れられると、次の図に示すようにWeb GUIにエントリが追加され ます。

Overview Analysis Policies Devices O	bjects AMP Intelligence							Deploy	0 Syste	m Help v I	h.potter v
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
Users User Roles External Authent	ication									00	reate User
Username	Roles	Authentication Hethod		Par	ssword Lifetim	ю					
admin	Administrator	Internal		Uni	mited						0
h.cotter	Administrator	External									1

ユーザ情報を確認するには、FMC CLISHでshow userコマンドを実行します。 > show user

コマンドは、指定したユーザの詳細な設定情報を表示します。次の値が表示されます。

Login: ログイン名

UID: 数値のユーザID

Auth(ローカルまたはリモート):ユーザの認証方法

Access(BasicまたはConfig):ユーザの特権レベル

有効(有効または無効):ユーザがアクティブかどうか

Reset(YesまたはNo):ユーザが次回ログイン時にパスワードを変更する必要があるかどうか Exp(NeverまたはNumber):ユーザのパスワードを変更するまでの日数

Warn(N/Aまたは数値):パスワードの有効期限が切れるまでにパスワードを変更するためにユ ーザに与えられる日数

Str(YesまたはNo):ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか ロック(YesまたはNo):ログインの失敗回数が多すぎるためにユーザーのアカウントがロック されているかどうか

Max(N/Aまたは数値):ログインに失敗した回数の上限。この回数を超えると、ユーザのアカウントがロックされます。

SSLまたはTLSが期待どおりに機能しない

FTDでDNSを有効にしないと、ピグテールログにLDAPが到達不能であることを示すエラーが表示される場合があります。

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

firepowerがLDAPサーバのFQDNを解決できることを確認します。そうでない場合は、図に示すよ うに正しいDNSを追加します。

FTD:FTD CLISHにアクセスし、次のコマンドを実行します。 > configure network dns servers

P 192.0.2.6 - PuTTY –	D X
root@SEC-FTD:/etc# ping WIN.SEC-LAB ping: unknown host WIN.SEC-LAB	<u>^</u>
root@SEC-FTD:/etc# exit	
admin@SEC-FID:/etc\$ exit	
Logout	
> configure network dns servers 192.0.2.15	
> expert ************************************	
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 (192.0.2.15): icmp_seq=1 ttl=128 time=0.176 64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=2 ttl=128 time=0.415	ms ms
<pre>^C WIN.SEC-LAB ping statistics 2 packets transmitted, 2 received, 0% packet loss, time 1010ms rtt min/avg/max/mdev = 0.176/0.295/0.415/0.120 ms admin@SEC-FTD:~\$</pre>	

FMC:選択 System > Configurationを選択し、次の図に示すようにManagement Interfacesを選択します。

Access List Access Control Preferences	•Inte	rfaces					
Audit Log	Link	Name	Channels	MAC Addres	IS	IP Address	
Change Reconciliation DNS Cache	0	eth0	Management Traff Event Traffic	ic 00:0C:29:29	:CF:2D	192.0.2.5	ø
Dashboard	• Rout	tes					
Database	IPv4	Routes					0
Email Notification	Dest	tination	Netmask	Interface	Gates	UNU UNU	
External Database Access			TTCLIND IN	100000			
HTTPS Certificate	-				192.0.	.2.1	6
Information	IPv6	Routes					0
Incrusion Policy Preferences	Dest	tination	Prefix Lengt	h Interface	Gate	PANAN	
Logio Banner			r rena beinge		Test field for the		
Management Interfaces	• Sha	red Sett	ings				
Network Analysis Policy Preferences	Harte						
Process	Host	lame	8	SEC-FMC			
REST API Preferences	Doma	lins					
Remote Storage Device	Prima	ry DNS Se	rver	192.0.2.10			
SNMP	Secon	ndary DNS	Server				
Shell Timeout	Tertia	ry DNS Se	rver				
Time	Remo	te Manage	ment Port	8305			
Time Synchronization							
UCAPL/CC Compliance	• ICM	Pv6					
User Configuration	Allow	Sending E	cho Reply				
VMware Tools	Packe	ts		*			
Vulnerability Mapping	Allow	Sending D	estination (,			
Web Analytics	Unrea	schable Pac	skets				
	• Prox	¢γ					
	Enabl	ed	(
				Save Can	cel		

次の図に示すように、FMCにアップロードされた証明書が、LDAPのサーバ証明書に署名した CAの証明書であることを確認します。



パケットキャプチャを使用して、LDAPサーバが正しい情報を送信していることを確認します。

					*Ethernet0
File	Edit View Go	Capture Analyze St	atistics Telephony Wireles	ss Tools Help	
	II 🖉 💿 🔰 🛅	🄀 🖸 🍳 👄 🕾 🖻	s T 🞍 🗐 🔍 Q	. e. II	
	dap tis && ip.addr==1	192.0.2.5			
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	
I.	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 112 extendedResp(1) LDAP_START_TLS_OID	0
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, Server	Key Exchange, Certificate Request, Server Hello Done
	35 3.000532	192.0.2.5	192.0.2.15	TLSVI.2 200 Certificate, Client Key Exchange,	change Cipner Spec, Encrypted Handshake Message
	50 5.001070	192.0.2.15	192.0.2.5	resvi.2 175 change cipher spec, encrypted hand	asnake nessage
P	rame 33: 1515 by	tes on wire (12120	bits), 1515 bytes captu	ured (12120 bits) on interface \Device\NPF_{3EAD5E9F	-B6CB-4EB4-A462-217C1A10A8FE}, id 0
P	thernet II, Src:	VMware_69:c8:c6 (0	0:0c:29:69:c8:c6), Dst:	: VNware_29:cf:2d (00:0c:29:29:cf:2d)	All Continues Managements and
1.5	Internet Protocol	version 4, Src: 19	2.0.2.15, Dst: 192.0.2.	· 3	Cisco Firepower Management Co X +
154	Cansmission Cont	roi protocol, src p	ort: 389, USt Port: 523	564, Seq: 47, ACK: 279, Len: 1449	
1.7.9	4 TISV1 2 Record	Laver: Handshake P	cotocol: Multiple Hands	chake Messages	← → C ■ fmc/platinum/autriconfig.cgl/id=72637452-51c1-11e
	Content Type	e: Handshake (22)	ococor. narcipie nanas	since hessages	Quertieu Arrhuse Delision Devison Obieste AMD Intel
	Version: TL	S 1.2 (0x0303)			Overview Analysis Policies Devices Objects AMP Intel
	Length: 144	4			Configuration Users Domains Integration
	Handshake Pr	rotocol: Server Hell	lo		
		rotocol: Certificate	e		Users User Roles External Authentication
	Handshake	e Type: Certificate	(11)		
	Length: 1	1124			
	Certifica	ates Length: 1121			External Authentication Object
	4 Certifica	ates (1121 bytes)			Authoritation Maked
	Certif	ficate Length: 1118			
	4 Certif	ficate: 3082045a3082	20342a00302010202133200	00000456c380c8 id-at-commonName=WIN.SEC-LAB ic	d - CAC Use for CAC authentication and authorizati
	P S1g	gnedCertificate		、	Name * SEC-LDAP
	P alg	gorithmidentifier (s	ma256witnkSAEncryption)	
	Pad	01ng: 0	100002a7aE170f26022fa20	Ze77bad1042bbdd	Description
	b Handshake Pi	rotocol: Server Key	Fychange	5277080104500000	Server Type MS Active Directory V Set Defaults
	b Handshake Pi	rotocol: Certificate	e Request		
	4 Handshake P	rotocol: Server Hel	lo Done		
	Handshake	e Type: Server Hello	Done (14)		Primary Server
	Length: (9			Heat Name/10 Address 8
					WIN.SEC-LAB
					Port * 389

関連情報

<u>管理アクセスのユーザーアカウント</u>

- <u>Cisco Firepower Management Center Lightweight Directory Access Protocol</u> 認証バイパスの 脆弱性
- <u>FireSIGHT システムでの LDAP 認証オブジェクトの設定</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。