# 使用LDAP配置Firepower管理中心和FTD以進行 外部身份驗證

目錄
<u>必要條件</u>
採用元件
<u>背景資訊</u>
網路圖表
<u>設定</u>
<u>FMC GUI中的基本LDAP配置</u>
外部使用者的外殼訪問
FTD的外部驗證
使用者角色
<u>SSL或TLS</u>
測試搜尋庫
<u>測試LDAP整合</u>
<u>疑難排解</u>
FMC/FTD和LDAP如何進行互動以下載使用者?
FMC/FTD和LDAP如何互動以驗證使用者登入請求?
<u>SSL或TLS未按預期工作</u>
相關資訊

# 簡介

本檔案介紹如何使用Cisco Firepower管理中心(FMC)和Firepower威脅防禦(FTD)啟用Microsoft輕型 目錄訪問協定(LDAP)外部身份驗證。

# 必要條件

## 需求

思科建議您瞭解以下主題:

- Cisco FTD
- Cisco FMC
- Microsoft LDAP

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

# 背景資訊

FMC和受管裝置包括用於管理訪問的預設管理員帳戶。您可以在FMC和受管裝置上新增自定義使用 者帳戶,以內部使用者的身份新增,或者,如果您的模型支援,以LDAP或RADIUS伺服器上的外部 使用者的身份新增。FMC和FTD支援外部使用者驗證。

·內部使用者 — FMC/FTD裝置檢查本地資料庫的使用者身份驗證。

·外部使用者 — 如果本地資料庫中不存在該使用者,則來自外部LDAP或RADIUS身份驗證伺服器的 系統資訊將填充其使用者資料庫。

# 網路圖表



# 設定

FMC GUI中的基本LDAP配置

步驟 1. 導航至 System > Users > External Authentication:

← → C A Not secure   192.02.5/ddd/#ExternalAuthentication							1.	☆	Θ:
Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	0 Sys	tem Help 👻	admin v
3	Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
Users User Roles External Authentication	2								
						ŧ	🗄 Save 🛛 🚨	Cancel 🗹 Sa	we and Apply
Default User Role: None Shell Authentication Disabled *							O Add 8	oternal Authenti	cation Object
Name							Hethod	Enabled	

步驟 2.選擇 Add External Authentication Object:

Save	😢 Car	icel	🖌 Sa	ve and Apply
	Add Exte	rnal Au	uthenti	cation Object
Meth	nod	Enab	led	

I

### 步驟 3.填寫必填欄位:

External Authentication Objec	t	
Authentication Method	LDAP T	
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	ory and click 'Set Defaults'
Primary Server		
Host Name/IP Address *	100 0 0 10	av. IP or hostname
Post *	Default part is 200 or 620	
FUL	Default port is 589 or 650	DIOL 22
Backup Server (Optional)		
Host Name/IP Address		ex. IP or hostname
Port	389	
LDAP-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	r admin
Confirm Password *		
Show Advanced Options	•	
And the second se	*Default when 'Set Defaults' optio	n is clicked
Attribute Mapping	Default when set befaults optio	in is cheved
UI Access Attribute *	sAMAccountName Fetch Attrs	
Shell Access Attribute *	sAMAccountName	

Group Controlled Access Role	(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	To specify the default user role if user is not found in any group
Group Member Attribute	member	
Group Member URL Attribute		
Shell Access Filter Shell Access Filter () (Mandatory for FTD devices)	Same as Base Filter     Same as Base Filter	ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)( (cn=bsmith)(cn=
Additional Test Parameters		
User Name		
Password		

#### 步驟 4. 啟用 External Authentication 對象並儲存:

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	0 Sy	stem Help	r admin +
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring	<ul> <li>Tools •</li> </ul>
Users User Roles External Authentication								2.	
						ł	Save 🕻	Cancel 🗹	Save and Apply
Default User Role: None Shell Authentication Disabled *							O Add	External Auther	ntication Object
Name							Hethod	Enabled	
L.SECLDAP New External Authentication Object							LDAP		0 60
								1.	3

## 外部使用者的外殼訪問

FMC支援兩個不同的內部管理員使用者:一個用於Web介面,另一個具有CLI訪問許可權。這表示 哪些人可以訪問GUI,哪些人也可以訪問CLI,兩者之間有明顯的區別。安裝時,預設管理員使用者 的密碼會同步,以便在GUI和CLI上相同,但是,不同的內部機制會跟蹤這些密碼,而且最終可能會 不同。

還必須授予LDAP外部使用者外殼訪問許可權。

步驟 1.導航至 System > Users > External Authentication 然後按一下 Shell Authentication 下拉框並儲存:

Overview Analysis	Policies Devices Objects AMP Intelligence						Deploy	Syst	em Help +	admin +
		Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
Users User Roles	External Authentication								2.	
							E	🔒 Save 🛛 🕄	Cancel <table-cell> 🗹 Sa</table-cell>	ve and Apply
Default User Role: None	1. Shell Authentication Disabled  Disabled							O Add E	iternal Authent	cation Object
Name	Enabled (SEC-LDAP)							Hethod	Enabled	
1. SEC-LDAP								LDAP		/ 6 @

步驟 2.在FMC中部署更改。

為外部使用者配置外殼訪問後,將啟用通過SSH登入,如下圖所示:



FTD的外部驗證

可在FTD上啟用外部驗證。

步驟 1.導航至 Devices > Platform Settings > External Authentication.按一下 Enabled 並儲存:

Overview Analysis Policies Device Management NAT 1- Platform-Policy Enter Description	Devices Objects AMP VPN • QoS Platform Setti 2.	Intelligence Ings FlexConfig Cer	tificates			
ARP Inspection Banner DIS 3. • External Authentication Prognent Satings HTTP IOHP Secure Shall SattP Server ShafP Sign Sign Sign Sign Timeous Time Synchronization UCAPL/CC Compliance	Name SEC-LDAP	Description	Hethod LDAP	Manuar Exten ServersPart 192.0.2.10:389	nal Authentication Encryption No	Stron
	"Applicable on FTD v6.2.3 and above					

### 使用者角色

使用者許可權基於分配的使用者角色。您還可以建立自定義使用者角色,這些角色具有根據組織需

求定製的訪問許可權,或者您可以使用預定義的角色,如安全分析師和發現管理員。

有兩種型別的使用者角色:

- 1. Web介面使用者角色
- 2. CLI使用者角色

有關預定義角色的完整清單以及更多資訊,請參閱<u>使用者角色</u>。

若要為所有外部身份驗證對象配置預設使用者角色,請導航至 System > Users > External Authentication > Default User Role. 選擇要分配的預設使用者角色,然後按一下 Save.

Overview Analysis Policies Devices Objects AMP Intelligence									0 Syste	em Help v	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) *									Q Add E	ternal Authent	ication Object
Name									Hethod	Enabled	
1. SEC-LDAP									LDAP		/ 8 2
	Default User Role Configuration	_	_								
	Default User Roles	Administrator     External Database User (Read Only)     Security Analysis     Security Analysis     Security Analysis     Instrusion Admin     Access Admin     Network Admn     Maintenance User     Discovery Admin									
	Custom User Roles	Threat Intelligence Director (TID) Us View-Only-User (Read Only) (Global	e Cancel								

要選擇預設使用者角色或將特定角色分配給特定對象組中的特定使用者,您可以選擇對象並導航至 Group Controlled Access Roles 如下圖所示:

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

SSL或TLS

必須在FMC中配置DNS。這是因為證書的Subject值必須與 Authentication Object Primary Server Hostname.配置 Secure LDAP後,資料包捕獲不再顯示明文繫結請求。

SSL將預設埠更改為636,TLS將其保留為389。

注意:TLS加密需要所有平台上的證書。若是SSL,FTD也需要憑證。對於其他平台,SSL不需 要證書。但是,建議您始終上傳用於SSL的證書,以防止中間人攻擊。

步驟 1.導航至 Devices > Platform Settings > External Authentication > External Authentication Object 並輸入高級選項 SSL/TLS資訊:

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		

### 步驟 2.上傳簽署伺服器證書的CA的證書。證書必須是PEM格式。

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 Certificate has been loaded (select to clear loaded certificate)	ex. PEM Format (base64 encoded version of DER)
User Name Template	%5	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

#### 步驟 3.儲存組態。

# 驗證

### 測試搜尋庫

開啟已配置LDAP的Windows命令提示符或PowerShell,然後鍵入命令: dsquery user -name

舉例來說:

.

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

Administrator: Windows	PowerShell 🗕 🗖 🗙
Administrator: Windows  S C:\Users\Administrator> dsquery user -name harr "CN=Harry Potter,CN=Users,DC=SEC-LAB  S C:\Users\Administrator>  PS C:\Users\Administrator> dsquery user -name * "CN=Administrator,CN=Users,DC=SEC-LAB "CN=Guest,CN=Users,DC=SEC-LAB "CN=Bart Simpson,CN=Users,DC=SEC-LAB "CN=Bart Simpson,CN=Users,DC=SEC-LAB "CN=Harry Potter,CN=Users,DC=SEC-LAB "CN=Hermione Granger,CN=Users,DC=SEC-LAB "CN=Hermione Granger,CN=Users,DC=SEC-LAB "CN=Hermione Granger,CN=Users,DC=SEC-LAB "CN=Harry Potter,CN=Users,DC=SEC-LAB "CN=Hermione Granger,CN=Users,DC=SEC-LAB "CN=Hermione Granger,CN=Users,DC=SEC-LAB "CN=Harry Potter,CN=Users,DC=SEC-LAB "CN=Hermione Granger,CN=Users,DC=SEC-LAB "CN=Harry Simpson,CN=Users,DC=SEC-LAB "CN=Maggie Simpson,CN=Users,DC=SEC-LAB "CN=Matthew Murdock,CN=Users,DC=SEC-LAB "CN=Neville Longbottom,CN=Users,DC=SEC-LAB "CN=Peter B. Parker,CN=Users,DC=SEC-LAB	PowerShell
"CN=Ron Weasley,CN=Üsers,DC=SEC-LAB "CN=Steven Rogers,CN=Users,DC=SEC-LAB PS C:\Users\Administrator> PS C:\Users\Administrator> PS C:\Users\Administrator> PS C:\Users\Administrator>	
< 111	ی <b>۲</b>

# 測試LDAP整合

導航至 System > Users > External Authentication > External Authentication Object.頁面底部有一個 Additional Test Parameters 一節,如下圖所示:

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

## 選擇「測試」以檢視結果。

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 Nethod CAC Use for CAC authen Name * SEC-LDAP Description Server Type MIS Active Directory *	tication and authorization							

4	Capturing from Ethernet1	• 0 ×							
File Edit View Go Capture Analyze Statistics Telepho	ny Wireless Tools Help								
<b># #</b> @                  <b>0</b>      <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>   <b>0</b>	<u> </u>								
tcp.port==389 && ip.addr==192.0.2.5	xp port+-399 84b p.add+-192.0.2.5								
No. Time Source Destination	Protocol Length 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-LAB " simple								
1801 55.132124 192.0.2.10 192.0.2.	s LDAP BB 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 39784 + 309 [FIN, AKE] Seq+09 Ack+23 Win+29312 Lene TSys1-3077124550 TSecr-425708266								
1805 55.132227 192.0.2.10 192.0.2.	2 ICP 00 303 + 33/04 [ACK] Sed+13 ACK+/0 H1H40200 Fem4 12A9T+12/06500 156C+30/7174348	×.							
Frame 1800: 127 bytes on wire (1016 bits), 127 by	<pre>ces captured (1016 bits) on interface \Device\NPF_(77DC31F6-8250-4F19-8412-E4596F960103}, id 0</pre>								
Ethernet II, Src: VNware_29:cf:2d (00:0c:29:29:cf	(2d), Dst: VMware_eb:1d:f7 (00:0c:29:eb:1d:f7)								
P Internet Protocol Version 4, Src: 192.0.2.5, Dst: Transfer Protocol Version 4, Src: 192.0.2.5, Dst:	192.0.2.10								
F Transmission Control Protocol, Src Port: 39764, U. d Lightumight Directory Access Rostorol	r Porti 309, Seqi 1, ACRI 1, Leni 01								
<ul> <li>A LDARMassage biodRequest(1) "Challarry Potter Chi</li> </ul>	dises_DC+SEC+LAB * stanle								
messageID: 1	ani yar an ampa								
4 protocolOp: bindRequest (0)									
4 bindRequest									
version: 3	version: 3								
name: Chi-Harry Potter, Chi-Users, DC=SEC-LAB									
# authentication: simple (0)									
simple: cisco									
[Response In: 1801]									

# 疑難排解

### FMC/FTD和LDAP如何進行互動以下載使用者?

為了使FMC能夠從Microsoft LDAP伺服器拉入使用者,FMC必須首先使用LDAP管理員憑據在埠 389或636(SSL)上傳送繫結請求。一旦LDAP伺服器能夠對FMC進行身份驗證,它會以成功消息做 出響應。最後,FMC能夠使用搜尋請求消息發出請求,如下圖所示:

<< --- 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

請注意,驗證預設會以明文形式傳送密碼:

83 4.7518	87 192.0.2.5	192.0.2.10	TCP	74 38002 → 389 [SYN] Seq=0 Win=29200 Len=0 M55=1460 SACK_PERM=1 T5val=3073529344 TSecr=0 W5=128
84 4.7519	20 192.0.2.10	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 4.7519	66 192.0.2.5	192.0.2.10	TCP	66 38002 + 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3073529344 TSecr=25348746
86 4.7519	97 192.0.2.5	192.0.2.10	LDAP	110 bindRequest(1) "Administrator@SEC-LAB0" simple
<ul> <li>87 4.7525</li> </ul>	36 192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success
88 4.7525	83 192.0.2.5	192.0.2.10	TCP	66 38002 + 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSyal=3073529345 TSecr=25348746
89 4.7526	34 192.0.2.5	192.0.2.10	LDAP	122 searchRequest(2) "DC=SEC-LAB
<ul> <li>Prame 66: 11</li> <li>Ethernet II,</li> <li>Internet Pro</li> <li>Transmission</li> <li>Lightweight</li> </ul>	Src: WHware_29:cf:2d (00:0 tocol Version 4, Src: 192.0 Control Protocol, Src Port Directory Access Protocol	110 bytes captured ( ::29:29:cf:2d), Dst: .2.5, Dst: 192.0.2.10 : 38002, Dst Port: 38	9, Seq: 1,	n interface (Device/WFF_[//DC31F6-D230-4F19-0412-24596F960100}, 10 0 d:f7 (00:0c:29:eb:1d:f7) Ack: 1, Len: 44
⊿ LDAPMessa	ge bindRequest(1) "Administr	'ator@SEC-LAB0" simpl	e	
messag	eID: 1			
₄ protoc	olOp: bindRequest (0)	_		
⊿ bind	Request			
,	version: 3			
	ame: Administrator@SEC-LAB0	1		
4 8	uthentication: simple (0)			
	simple: Ciscot@c			
[ Decen				

### FMC/FTD和LDAP如何互動以驗證使用者登入請求?

為了使使用者在啟用LDAP身份驗證時能夠登入到FMC或FTD,初始登入請求將傳送到 Firepower,但使用者名稱和密碼將轉發到LDAP以獲得成功/拒絕響應。這意味著FMC和FTD不會將 密碼資訊儲存在本地資料庫中,而是等待LDAP確認如何繼續。





4	(								*Ethernet1	
F	ile E	dit	View Go Capt	ture Analyze Statistics	Telephony Wireless Te	ools Helj	р			
4		đ	Θ 퉬 🛅 🗙	😋 🍳 🗢 🗢 🗟 🖗	୬ 📃 📃 ବ୍ ବ୍ ବ୍					
	tcp.p	ort:	==389 && ip.addr==1	92.0.2.5 && ldap.messageID =	-= 1					
N	o.		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	
ł		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	
	1	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
	1	98	13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	

如果接受使用者名稱和密碼,則會在Web GUI中新增一個條目,如下圖所示:

Overview Analysis Policies Devices Objects   AMP Intelligence Depicy Q System Help + hepother											
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring +	Tools •
Users User Roles External Author	Users User Roles External Authentication										
										O Cre	eate User
Usemame	Roles	Authentication Method		Par	ssword Lifetin	ю					
admin	Administrator	Internal		Uni	imited						0
h.eotter	Administrator	External									0

在FMC CLISH中運行命令show user以驗證使用者資訊: > show user

命令顯示指定使用者的詳細配置資訊。將顯示以下值:

Login — 登入名

UID — 數字使用者ID
身份驗證(本地或遠端) — 如何對使用者進行身份驗證
訪問(基本或配置) — 使用者的許可權級別
已啟用(啟用或禁用) — 使用者是否處於活動狀態
重設(Yes或No) — 使用者是否必須在下次登入時更改密碼
Exp(Never或數字) — 必須更改使用者密碼之前的天數
Warn(N/A or a number) — 使用者被指定在密碼到期之前更改其密碼的天數
Str(Yes或No) — 使用者的密碼是否必須滿足條件才能檢查強度
Lock(Yes或No) — 使用者帳戶是否由於登入失敗過多而被鎖定
最大(N/A或數字) — 鎖定使用者帳戶之前失敗登入的最大次數

#### SSL或TLS未按預期工作

如果您沒有在FTD上啟用DNS,則可以在尾日誌中看到錯誤,指示LDAP無法訪問:

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

確保Firepower能夠解析LDAP伺服器FQDN。如果沒有,請新增正確的DNS,如圖所示。

FTD:存取FTD CLISH並執行命令: > configure network dns servers

P 192.0.2.6 - PuTTY	-		х
root@SEC-FTD:/etc# ping WIN.SEC-LAB ping: unknown host WIN.SEC-LAB			^
root@SEC-FTD:/etc# exit			
exit			
logout			
>			
> configure network dns servers 192.0.2.15			
<pre>&gt; expert ************************************</pre>			
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. 64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=2 ttl=128 time=0. ^C WIN.SEC-LAB ping statistics	176 415	ms ms	
2 packets transmitted, 2 received, 0% packet loss, time 1010ms			
rtt min/avg/max/mdev = 0.176/0.295/0.415/0.120 ms			_
admingSEC-FID:~\$			~

FMC:選擇 System > Configuration,然後選擇Management Interfaces,如下圖所示:

Access List	- 1	and sound	-						
Access Control Preferences		nten	aces						
Audit Log		Link	Name	Channels		MAC Address		IP	
Audit Log Certificate								Address	
Change Reconciliation		0	eth0	Management Traf	ffic	00:00:29:29:	CF:2D	192.0.2.5	0
DNS Cache				Event indiric					
Dashboard	÷ p	loute	HS .						
Database									
Email Notification	1	Pv4 B	outes		_				• •
External Database Access		Desti	nation	Netmask		Interface	Gate	way	
HTTPS Certificate		-					192.0	0.2.1	0
Information									
Intrusion Policy Preferences	1	Pv6 R	loutes						• •
Language		Desti	nation	Prefix Lengt	th	Interface	Gat	teway	
Login Banner		-1							
Management Interfaces	*5	share	ed Sett	ings					
Network Analysis Policy Preferences	н	lostna	me		SEC	FMC			
Process	D	omain	15						
REST API Preferences	P	viman		over	102	0.2.10		1	
Remote Storage Device						v.e.tv			
SNMP	3	econo	ary DNS	Server	_				
Shell Timeout	Т	ertiar)	DNS Se	rver	_				
Time	R	emote	Manage	ment Port	8305	1			
Time Synchronization									
UCAPL/CC Compliance	•1	CMP	VĐ						
User Configuration	A	llow S	ending E	cho Reply	7				
VMware Tools	P	ackets	1		æ				
Vulnerability Mapping	A	llow S	ending D	estination	2				
Web Analytics	U	nread	nable Pac	xets					
	• P	Proxy	r						
	E	nable	d						
					5	ave Cano			
					1000				

確保上傳到FMC的證書是簽署LDAP伺服器證書的CA的證書,如下圖所示:



使用資料包捕獲確認LDAP伺服器傳送正確的資訊:

<b>A</b>				*Ethernet0	
File Edit View	Go Capture Analyze St	atistics Telephony Wire	less Tools Help		
🛋 🔳 🖉 💿	🎉 📇 🗙 🖸 🔍 👄 😔 🕯	🖴 Ŧ 👲 🚍 📃 🔍 (	Q, Q, II		
Idap    tis && ip.	addr==192.0.2.5				
No. Time	Source	Destination	Protocol Length Info		
3 0.14	722 192.0.2.5	192.0.2.15	TLSv1.2 107 Application Data		
4 0.14	905 192.0.2.15	192.0.2.5	TLSv1.2 123 Application Data		
22 2.720	710 192.0.2.15	192.0.2.5	TLSv1.2 1211 Application Data		
29 3.050	497 192.0.2.5	192.0.2.15	LDAP 97 extendedReq(1) LDAP_START_TLS_OI	0	
30 3.056	605 192.0.2.15	192.0.2.5	LDAP 112 extendedResp(1) LDAP_START_TLS_0	ID	
32 3.050	921 192.0.2.5	192.0.2.15	TLSv1.2 313 Client Hello		
33 3.057	192.0.2.15	192.0.2.5	TLSv1.2 1515 Server Hello, Certificate, Server	r Key Exchange, Certificate Req	uest, Server Hello Done
35 3.060	192.0.2.5	192.0.2.15	TLSv1.2 260 Certificate, Client Key Exchange	, Change Cipher Spec, Encrypted	Handshake Message
30 3.001	192.0.2.15	192.0.2.5	ILSVI.2 1/3 Change Cipher Spec, Encrypted Ha	nosnake Message	
Frame 33: 1	515 bytes on wire (12120	bits), 1515 bytes cap	tured (12120 bits) on interface \Device\NPF_{3EAD5ES	F-B6CB-4EB4-A462-217C1A10A8FE}	, id 0
P Ethernet II	, Src: VMware_69:c8:c6 (0	0:0c:29:69:c8:c6), Ds	t: VNware_29:cf:2d (00:0c:29:29:cf:2d)		
P Internet Pr	otocol Version 4, Src: 19	2.0.2.15, Dst: 192.0.	2.5	Cisco Firepower Manageme	ent Co × +
P Transmissio	n Control Protocol, Src P	ort: 389, Dst Port: 5	2384, Seq: 47, ACK: 279, Len: 1449		
4 TISV1 2	Becord Laver: Handshake P	cotocol: Multiple Han	dehake Maccagec	← → G ■ fmc/pia	atinum/authconfig.cgi/id=/283/432-51c1-11ea
Conte	nt Type: Handshake (22)	rotocor. narcipie nan	usinke hessages	Ouerview Applusie De	licica Dovison Objects AMD Tatellic
Versi	on: TLS 1.2 (0x0303)			Overview Analysis Po	licies Devices Objects AMP Intellig
Lengt	h: 1444			Config	guration Users Domains Integration
Hands	hake Protocol: Server Hel	lo			
⊿ Hands	hake Protocol: Certificat	e		Users User Roles	External Authentication
Ha	ndshake Type: Certificate	(11)			
Le	ngth: 1124				
Ce	rtificates Length: 1121			External Authenticati	on Object
⊿ Ce	rtificates (1121 bytes)			Authentication Method	IDAD
	Certificate Length: 1118			Addrend Cadon Hechod	LOAP
4	Certificate: 3082045a308	20342a0030201020213320	0000000456c380c8 id-at-commonName=WIN.SEC-LAB	id- CAC	Use for CAC authentication and authorization
	<pre>P signedCertificate </pre>			Name *	SEC-LDAP
	Palgorithmidentifier (	sna256withKSAEncryptic	on)		
	encrypted: 3645eb1128	788982e7a5178f36922fa3	303e77had1043hhdd	Description	
▶ Hands	hake Protocol: Server Key	Exchange	***************************************	Server Type	MS Active Directory V Set Defaults
Hands	hake Protocol: Certificat	e Request			
4 Hands	hake Protocol: Server Hel	lo Done			
Ha	ndshake Type: Server Hell	o Done (14)		Primary Server	
Lei	ngth: 0			Heat Name (TD Address	
				nost Name/IP Address *	WIN.SEC-LAB
				Port *	389

# 相關資訊

• 用於管理訪問的使用者帳戶

- Cisco Firepower管理中心輕型目錄訪問協定身份驗證繞過漏洞
- 在FireSIGHT系統上配置LDAP身份驗證對象
- <u>技術支援與文件 Cisco Systems</u>

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。