Configurazione di Firepower Management Center e FTD con LDAP per l'autenticazione esterna

Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Premesse Esempio di rete Configurazione Configurazione LDAP di base nell'interfaccia utente di FMC Accesso shell per utenti esterni Autenticazione esterna per FTD Ruoli utente SSL o TLS Verifica Base di ricerca test Verifica integrazione LDAP Risoluzione dei problemi Come interagiscono FMC/FTD e LDAP per scaricare gli utenti? Come interagiscono FMC/FTD e LDAP per autenticare una richiesta di accesso utente? SSL o TLS non funziona come previsto Informazioni correlate

Introduzione

In questo documento viene descritto come abilitare l'autenticazione esterna LDAP (Lightweight Directory Access Protocol) di Microsoft con Cisco Firepower Management Center (FMC) e Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco FTD
- Cisco FMC
- LDAP Microsoft

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

FMC e dispositivi gestiti includono un account amministratore predefinito per l'accesso alla gestione. È possibile aggiungere account utente personalizzati nel FMC e nei dispositivi gestiti, come utenti interni o, se supportato per il modello, come utenti esterni su un server LDAP o RADIUS. L'autenticazione utente esterno è supportata per FMC e FTD.

· Utente interno - Il dispositivo FMC/FTD controlla un database locale per l'autenticazione dell'utente.

 \cdot Utente esterno - Se l'utente non è presente nel database locale, le informazioni di sistema provenienti da un server di autenticazione LDAP o RADIUS esterno popolano il relativo database utenti.

Esempio di rete



Configurazione

Configurazione LDAP di base nell'interfaccia utente di FMC

Passaggio 1. Passa a System > Users > External Authentication:



Passaggio 2. Scegli Add External Authentication Object:

8	Save	😢 Car	ncel	🗹 Sa	ive and Apply
		Add Exte	ernal Au	uthent	ication Object
	Met	nod	Enab	oled	

Passaggio 3. Completare i campi obbligatori:

External Authentication Object	t	
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 D	Pirectory and click 'Set Defaults'
Drimany Conver		
Phinary Server		
Host Name/IP Address	192.0.2.10	ex. IP or hostname
Port *	Default port is 389 o	r 636 for SSL
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), (1cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	Administrator@SEC-LAB0	ex. cn=jsmith,dc=sourcefire,dc=com
Password *	Username of LDAP S	erver admin
Confirm Password *		
Show Advanced Options	•	
	*Default when 'Set Defaulte'	untion is disked
Attribute Mapping	Derault when set belauits to	prior is clicked
UI Access Attribute *	sAMAccountName Fetch Attrs	
Shell Access Attribute *	sAMAccountName	

Group Controlled Access Roles	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	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 🛈	Same as Base Filter	an (an invite) (in invite) (0 (an invite) (1)
(Mandatory for FTD devices)		ex. (cn=jsmicn), (:cn=jsmicn), (o(cn=jsmicn)(((cn=csmicn)(cn=csmicn)))
Additional Test Parameters		
User Name		
Password		
*Required Field		
	Save Test Cancel	

Passaggio 4. Attivare External Authentication Oggetto e salvataggio:

Overview Analysis Policies Devices Objects AMP Intelligence				
	Configuration	Users	Domains	
Users User Roles External Authentication				
Default User Role: None Shell Authentication Disabled				
Name				
1. SEC-LDAP New External Authentication Object				

Accesso shell per utenti esterni

La FMC supporta due diversi utenti amministratori interni: uno per l'interfaccia Web e l'altro con accesso alla CLI. Ciò significa che esiste una chiara distinzione tra chi può accedere alla GUI e chi può accedere anche alla CLI. Al momento dell'installazione, la password dell'utente amministratore predefinito viene sincronizzata in modo da essere la stessa sia sulla GUI sia sulla CLI; tuttavia, viene tenuta traccia di tali password da meccanismi interni diversi e può anche essere diversa.

Agli utenti esterni LDAP deve inoltre essere concesso l'accesso alla shell.

Passaggio 1. Passa a System > Users > External Authentication e fare clic su Shell Authentication come nell'immagine e salvare:

Overview Analysis Policies Devices Objects AMP Intelligence				
	Configuration	Users	Domains	In
Users User Roles External Authentication				
Default User Role: None 1. Shell Authentication Disabled Disabled				
Name Enabled (SECLDAP)				
1. SEC-LDAP				

Passaggio 2. Distribuire le modifiche in FMC.

Una volta configurato l'accesso alla shell per gli utenti esterni, l'accesso tramite SSH è abilitato come mostrato nell'immagine:



Autenticazione esterna per FTD

L'autenticazione esterna può essere abilitata sull'FTD.

Passaggio 1. Passa a Devices > Platform Settings > External Authentication. Fare clic su Enabled e salvare:

Overview Analysis Policies	Devices	Objects AMP Inte	ligence					
Device Management NAT 1.	VPN VQoS	Platform Settings	FlexConfig Certificates					
Platform-Policy Enter Description	1							
ARP Inspection					Manage Exte	rnal Authentication	Server	2
Banner 3.	Name	Descri	ption	Method	Server:Port	Encryption	Enabled	
External Authentication	SEC-LDAP			LDAP	192.0.2.10:389	no		
Fragment Settings HTTP ICMP Secure Shell SMTP Server SNMP SSL Syslog Timeouts Time Synchronization UCAPL/CC Compliance	"Applicable on A	7D v6.2.3 and above					4.	

Ruoli utente

I privilegi utente sono basati sul ruolo utente assegnato. È inoltre possibile creare ruoli utente personalizzati con privilegi di accesso personalizzati in base alle esigenze dell'organizzazione oppure utilizzare ruoli predefiniti quali Security Analyst e Discovery Admin.

Esistono due tipi di ruoli utente:

- 1. Ruoli utente interfaccia Web
- 2. Ruoli utente CLI

Per un elenco completo dei ruoli predefiniti e per ulteriori informazioni, vedere; Ruoli utente.

Per configurare un ruolo utente predefinito per tutti gli oggetti di autenticazione esterna, passare a System > Users > External Authentication > Default User Role. Scegliere il ruolo utente predefinito da assegnare e fare clic su Save.

Overview Analysis Policies Devices Objects AMP Intelligence						
			Configuration	Users	Domains	
Users User Roles External Authentication						
Default User Role: None Shell Authentication [Enabled (SEC-LDAP) *						
Name						
1. SEC-LOAP	Default User Roles	Administrator External Database User (Read Only) Security Analyst Security Analyst (Read Only) Security Approver Intrusion Admin Access Admin Network Admin Network Admin Discovery Admin Threat Intelligence Director (TID) U View-Only-User (Read Only) (Global	Ler D			
		Sm	e Cancel			

Per scegliere un ruolo utente predefinito o assegnare ruoli specifici a utenti specifici in un particolare gruppo di oggetti, è possibile scegliere l'oggetto e passare a Group Controlled Access Roles come mostrato nell'immagine:

Group Controlled Access Roles	s (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 o TLS

Il DNS deve essere configurato nel CCP. Infatti il valore Subject del certificato deve corrispondere al Authentication Object Primary Server Hostname. Dopo aver configurato Secure LDAP, le acquisizioni dei pacchetti non mostrano più le richieste di associazione in testo non crittografato.

Il protocollo SSL cambia la porta predefinita a 636 e il protocollo TLS la mantiene a 389.

Nota: la crittografia TLS richiede un certificato su tutte le piattaforme. Per SSL, l'FTD richiede anche un certificato. Per le altre piattaforme, SSL non richiede un certificato. Tuttavia, è consigliabile caricare sempre un certificato per SSL per evitare attacchi man-in-the-middle.

Passaggio 1. Passa a Devices > Platform Settings > External Authentication > External Authentication Object e immettere le informazioni SSL/TLS di Opzioni avanzate:

LDAP-Specific Parameters			
Base DN *	DC=SEC-LAB	Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter			ex. (cn=jsmith), (!cn=jsmith
User Name *	h.potter@SEC-LAB		ex. cn=jsmith,dc=sourcefire,
Password *			
Confirm Password *			
Show Advanced Options	•		
Encryption	SSL TLS None		
SSL Certificate Upload Path	Choose File No file chosen		ex. PEM Format (base64 enc
User Name Template	%5		ex. cn=%s,dc=sourcefire,dc
Timeout (Seconds)	30		

Passaggio 2. Caricare il certificato della CA che ha firmato il certificato del server. Il certificato deve essere in formato PEM.

LDAP-Specific Parameters		
Base DN *	DC=SEC-LAB Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (!cn=jsmith
User Name *	h.potter@SEC-LAB	ex. cn=jsmith,dc=sourcefire
Password *		
Confirm Password *		
Show Advanced Options	•	
Encryption	SSL TLS None	
SSL Certificate Upload Path	Choose File CA-Cert-base64.cer	ex. PEM Format (base64 end
Lices Name Template		av an-9/a da-sourcefice de
oser warne remplate	765	ex. cn= %s,dc=sourcenre,dc
Timeout (Seconds)	30	

Passaggio 3. Salvare la configurazione.

Verifica

Base di ricerca test

Aprire un prompt dei comandi di Windows o PowerShell in cui è configurato LDAP e digitare il comando: dsquery user -name

Ad esempio:

.

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

Σ	Administrator: Windows PowerShell 🗕 🗖	x	
PS C PS C PS C "CN= "CN= "CN= "CN=	:\Users\Administrator> dsquery user -name harry* Harry Potter,CN=Users,DC=SEC-LAB :\Users\Administrator> :\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		
"CN= "CN= "CN= "CN= "CN= "CN= "CN= "CN=	Bart Simpson, 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 Hermione Granger, CN=Users, DC=SEC-LAB Lisa Simpson, CN=Users, DC=SEC-LAB Maggie Simpson, CN=Users, DC=SEC-LAB Marge Simpson, CN=Users, DC=SEC-LAB Marge Simpson, CN=Users, DC=SEC-LAB Matthew Murdock, CN=Users, DC=SEC-LAB Neville Longbottom, CN=Users, DC=SEC-LAB		
"CN= "CN= PS C PS C PS C PS C PS C	Peter B. Parker,CN=Users,DC=SEC-LAB Ron Weasley,CN=Users,DC=SEC-LAB Steven Rogers,CN=Users,DC=SEC-LAB :\Users\Administrator> :\Users\Administrator> :\Users\Administrator> :\Users\Administrator>		
<	III	> ,	.:

Verifica integrazione LDAP

Passa a System > Users > External Authentication > External Authentication Object. Nella parte inferiore della pagina è presente una Additional Test Parameters come nell'immagine:

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

Scegliere il Test per visualizzare i risultati.

Risoluzione dei problemi

Come interagiscono FMC/FTD e LDAP per scaricare gli utenti?

Affinché FMC possa prelevare utenti da un server LDAP Microsoft, deve prima inviare una richiesta di binding sulla porta 389 o 636 (SSL) con le credenziali di amministratore LDAP. Una volta che il server LDAP è in grado di autenticare FMC, risponde con un messaggio di operazione riuscita. Infine, FMC è in grado di effettuare una richiesta con il messaggio Search Request descritto nel diagramma:

<< --- 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

Si noti che l'autenticazione invia le password in chiaro per impostazione predefinita:

0	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
	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
Т	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
Т	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 TSval=3073529345 TSecr=2534874
	89 4.752634	192.0.2.5	192.0.2.10	LDAP	122 searchRequest(2) "DC=SEC-LAB ' wholeSubtree
	Frame 86: 110 huts	es on wire (888 bi	te), 110 bytes capture	4 (880 bits)	on interface \Device\NEE /77DC31E6_8350_4E10_8412_E4506E960108\ id 0
ь Б	Ethernet TT Sect	Wwwwww.20.cf.2d (anac:20:20:cf:2d) De	t: Wware eb:	1d:f7 (00:0c:20:ab:1d:f7)
1	Ethernet II, Srt:	visuale_29:c1:20 (00:00:29:29:01:20), DS	t: whware_eb:	(00:00:29:00:10:17)
P	Internet Protocol	Version 4, Src: 1	92.0.2.5, Dst: 192.0.2	. 10	
₽	Transmission Contr	rol Protocol, Src	Port: 38002, Dst Port:	389, Seq: 1,	Ack: 1, Len: 44
4	Lightweight Direct	tory Access Protoc	01		
	₄ LDAPMessage bir	ndRequest(1) "Admin	nistrator@SEC-LAB0" si	ple	
	messageID: 1	L			
	₄ protocol0p:	bindRequest (0)			
	4 bindReque	st			
	versio	n: 3			
	001310	Administrator9555	1 480		
	nane:	Administrator@set*	CADO		
	authen	tication: simple ((0)		
	sim	ple: Ciscot@c			
	[Response In	n: 87]			

Come interagiscono FMC/FTD e LDAP per autenticare una richiesta di accesso utente?

Affinché un utente possa accedere a FMC o FTD mentre l'autenticazione LDAP è abilitata, la richiesta di accesso iniziale viene inviata a Firepower, tuttavia, il nome utente e la password vengono inoltrati a LDAP per una risposta di esito positivo/negativo. Ciò significa che FMC e FTD non conservano le informazioni sulla password localmente nel database e attendono invece la conferma di LDAP su come procedere.





						*Etherne
File	Edit	View Go Capt	ture Analyze Statistics	Telephony Wireless To	ools Help	
	1	💿 🄰 🛅 🗙	🗳 🍳 🗢 🗢 🗟 🖗	୬ 📃 📃 ବ୍ ବ୍ ବ୍		
📕 tq	p.port	==389 && ip.addr==19	92.0.2.5 && ldap.messageID =	= 1		
No.		Time	Source	Destination	Protocol Leng	th Info
	58	13:11:59.695671	192.0.2.5	192.0.2.10	LDAP 1	<pre>10 bindRequest(1) "Administrator(</pre>
+	59	13:11:59.697473	192.0.2.10	192.0.2.5	LDAP	<pre>38 bindResponse(1) success</pre>
	67	13:11:59.697773	192.0.2.5	192.0.2.10	LDAP 1	<pre>10 bindRequest(1) "Administrator(</pre>
	69	13:11:59.699474	192.0.2.10	192.0.2.5	LDAP	38 bindResponse(1) success
	97	13:11:59.729988	192.0.2.5	192.0.2.10	LDAP 1	27 bindRequest(1) "CN=Harry Potte
	98	13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	<pre>38 bindResponse(1) success</pre>

Se il nome utente e la password vengono accettati, viene aggiunta una voce nell'interfaccia utente del Web come mostrato nell'immagine:

(Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence						
										Configuration	Users	Domains	ŀ
	Users	User Role	s Ext	ernal Auth	entication	<u> </u>							
	Username	name			Roles	Roles Administrator			thentication Hethod		Pa	ssword Lifetim	e
	admin				Adminis				ernal		Un	imited	
[h.potter				Adminis	trator		Ext	ernal				

Eseguire il comando show user in FMC CLISH per verificare le informazioni utente: > show user

Il comando visualizza informazioni di configurazione dettagliate per gli utenti specificati. Vengono

visualizzati i seguenti valori:

Login â€" il nome di login

UID â€" l'ID utente numerico Auth (locale o remota) - modalità di autenticazione dell'utente Access (Basic o Config): il livello di privilegi dell'utente Abilitato (abilitato o disabilitato) â€" indica se l'utente è attivo Reimposta (Sì o No) - Consente di specificare se l'utente deve modificare la password al successivo accesso Exp (Never o number) - Numero di giorni trascorsi i quali è necessario modificare la password dell'utente. Avviso (N/D o numero): il numero di giorni concessi a un utente per modificare la password prima della scadenza Str (Sì o No) â€" indica se la password dell'utente deve soddisfare i criteri per verificare il livello Lock (Yes o No) - se l'account dell'utente è stato bloccato a causa di troppi errori di accesso Max (N/D o un numero): il numero massimo di accessi non riusciti prima che l'account dell'utente venga bloccato

SSL o TLS non funziona come previsto

Se non si abilita il DNS sugli FTD, nel log pigtail verranno visualizzati errori che indicano che LDAP non è raggiungibile:

```
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 ex 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 192.0.2.15 p MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15 p MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter f MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 614

Accertarsi che Firepower sia in grado di risolvere l'FQDN dei server LDAP. In caso contrario, aggiungere il DNS corretto come visualizzato nell'immagine.

FTD: accedere al CLISH FTD ed eseguire il comando: > configure network dns servers



FMC: Scegli System > Configuratione quindi scegliere Interfacce di gestione come illustrato nell'immagine:

ess Control i preferences fit Log fit Log Certificate inge Reconciliation S Cache ihboard abase ail Notification ernal Database Access reading Preferences guage guage guage time thereferences sets T API Preferences sets T API Preference sets T API Preferen	cess List	• Inter	faces					
Log Certificate Log Certificate ge Reconciliation Cache board base I Notification mail Database Access IS Certificate mation Securiticate mation Securiticate mation Securiticate mation Number of the security Securiticate mation Securiticate mation Securiticate mation Netmask Interface Gateway Securiticate mation Netmask Interface Gateway Securiticate mation Netmask Interface Gateway Securiticate Timeout Primary DNS Server Secondary	Log	Link	Name	Channels	MAC Addres	15	IP	1
apper Reconciliation Cache board base Notification nal Database Access S Certificate mation iion Policy Preferences gage Baner synchronization API Preferences te Storage Device Synchronization L/CC Compliance Configuration IVC Compliance Configuration IVC Compliance Configuration Ive Rability Mapping Analytics	Log Certificate						Address	
ache cord Event Traffic Cordens Provide Software	e Reconciliation	0	eth0	Management Traffi	c 00:00:29:29	CE:2D	192.0.2.5	
board • Routes Notification IPv4 Routes IPv4 Routes Interface Gateway inal Database Access • S Certificate • ination IPv6 Routes ision Policy Preferences Destination ision Policy Preferences Destination ge Destination Banner Destination spenent Interfaces Destination preferences Prefix Length Interface Gateway sage SEC-FMC ss Domains API Preferences Primary DNS Server te Storage Device Secondary DNS Server Synchronization ICMPv6 AUCC Compliance Allow Sending Echo Reply Configuration Allow Sending Destination Analytics Allow Sending Destination Analytics Interface	Cache		euro	Event Traffic	00.00.27.27		192.0.2.0	
base I Notification Inal Database Access IS Certificate Ination Ision Policy Preferences Imation Ision Policy Preferences Image Interface Image	board	* Rout	05					
I Notification IPv4 Routes Imail Database Access Destination IS Certificate - mation 192.0.2.1 mation IPv6 Routes uage Destination Banner - agement Interfaces Destination Irk Analysis Policy Preferences Hostname sess Domains API Preferences Hostname p Timeout Timeout Tertiary DNS Server Synchronization FICMPv6 Configuration Allow Sending Echo Reply Packets Allow Sending Destination Analytics Allow Sending Destination	base	- Nour						
Interface Gateway Scertificate - mation sion Policy Preferences uage Destination Banner Destination agement Interfaces Destination ork Analysis Policy Preferences SEC-FMC ess Domains API Preferences Domains ots Storage Device Primary DNS Server p Timeout Synchronization Tertiary DNS Server Publicy Mapping Allow Sending Echo Reply Analytics Allow Sending Destination Unreachable Packets Interface	I Notification	IPv4	Routes					2
S Certificate - mation sion Policy Preferences uage agement Interfaces ork Analysis Policy Preferences ess Condary DNS Server primary DNS Server Domains Primary DNS Server Synchronization Pu/CC Compliance Configuration are Tools are Tools analytics Configuration Analytics	mal Database Access	Dest	ination	Netmask	Interface	Gatew	vay	
mation sion Policy Preferences uage h Banner agement Interfaces bork Analysis Policy Preferences ess r API Preferences ot Storage Device p Timeout Synchronization PL/CC Compliance Configuration are Tools erability Mapping Analytics Allow Sending Echo Reply Packets Allow Sending Destination Unreachable Packets Primary DNS Server Remote Management Port B305 Price Allow Sending Echo Reply Packets Allow Sending Destination Unreachable Packets Proxy Enabled	S Certificate	-				192.0.	2.1	Π
sion Policy Preferences uage Destination Prefix Length Interface Gateway	mation							
Destination Prefix Length Interface Gateway agement Interfaces • Shared Settings • Shared Settings iork Analysis Policy Preferences Hostname SEC-FMC ess Domains • • • • • • • • • • • • • • • • • • •	sion Policy Preferences	IPv6	Routes					2
agement Interfaces agement Interfaces vork Analysis Policy Preferences ess r API Preferences ote Storage Device p 1 Timeout ess r Synchronization PL/CC Compliance Configuration are Tools erability Mapping Analytics I Iomains Primary DNS Server 192.0.2.10 Secondary DNS Server 192.0.2.10 Secondary DNS Server I Tertiary DNS Server Remote Management Port 8305 • ICMPv6 Allow Sending Echo Reply Packets Allow Sending Destination Unreachable Packets	uage	Dest	ination	Prefix Lengt	h Interface	Gate	eway	
work Analysis Policy Preferences work Analysis Policy Preferences tess T API Preferences work Storage Device ip Il Timeout e e Synchronization PL/CC Compliance r Configuration ware Tools ware Tools ware Tools Analytics Hostname SEC-FMC Primary DNS Server 192.0.2.10 Secondary DNS Server Secondary DNS Server Remote Management Port \$305 • ICMPv6 Allow Sending Echo Reply Packets Allow Sending Destination Unreachable Packets • Proxy Enabled	n Banner	• Shar	ed Sett	ings				
ess T API Preferences ote Storage Device p T Timeout s Secondary DNS Server Secondary DNS Sec	vork Analysis Policy Preferences	Harter		-				
T API Preferences Domains ote Storage Device Primary DNS Server p Secondary DNS Server 1 Timeout Tertiary DNS Server e Synchronization Remote Management Port PL/CC Compliance ICMPv6 e configuration Allow Sending Echo Reply are Tools Allow Sending Destination erability Mapping Allow Sending Destination Analytics Proxy	ess	Hostna	ame	E	pec-rmc			
ote Storage Device Primary DNS Server 192.0.2.10 p Secondary DNS Server Image: Secondary DNS Server Timeout Tertiary DNS Server e: Synchronization Remote Management Port PL/CC Compliance • ICMPv6 * Configuration Allow Sending Echo Reply packets Allow Sending Destination unreachable Packets • Proxy Enabled Image: Server	T API Preferences	Domai	ains					
p Secondary DNS Server I Timeout Tertiary DNS Server e Remote Management Port e Synchronization *ICMPv6 PU/CC Compliance *ICMPv6 Configuration Allow Sending Echo Reply Packets erability Mapping Allow Sending Destination Unreachable Packets * Proxy Enabled	ote Storage Device	Primar	y DNS Ser	rver 1	192.0.2.10			L
I Timeout Tertiary DNS Server e Synchronization Remote Management Port PL/CC Compliance ▼ICMPv6 * Configuration Allow Sending Echo Reply are Tools Allow Sending Destination erability Mapping Allow Sending Destination Analytics ▼Proxy Enabled Server	P	Secon	dary DNS :	Server				L
Remote Management Port 8305 Synchronization ICMPv6 ICMPv6 Allow Sending Echo Reply Packets Allow Sending Destination Unreachable Packets Image: Proxy Enabled Image: Image: Imag	l Timeout	Tertian	y DNS Ser	ver (
e Synchronization PL/CC Compliance Configuration are Tools erability Mapping Analytics Allow Sending Destination Unreachable Packets ▼Proxy Enabled	1	Remot	e Manager	ment Port	3305			
PL/CC Compliance Configuration Allow Sending Echo Reply Packets Allow Sending Destination Unreachable Packets	Synchronization							
Configuration Allow Sending Echo Reply are Tools Packets erability Mapping Allow Sending Destination Analytics Unreachable Packets • Proxy Enabled	PL/CC Compliance	▼ICMP	V6					
are Tools Packets analytics Packets Pa	Configuration	Allow	Sending Er	cho Reply o				
Allow Sending Destination Unreachable Packets	are Tools	Packet	15		0			
Analytics Unreachable Packets	erability Mapping	Allow :	Sending D	estination (8			
▼Proxy Enabled	Analytics	Unread	shable Pac	kets				
Enabled		• Prox	y					
		Enable	b	(
				0	6 mm			

Verificare che il certificato caricato in FMC sia il certificato della CA che ha firmato il certificato server del server LDAP, come illustrato nell'immagine:

Certificate		x			Certificate
General Details Certification Path				G	eneral Details Certification Path
Certificate Information		-			Certificate Information
This certificate is intended for the folk • Ensures the identity of a remote comp	owing purpose(s): puter				This certificate is intended for the fo • All issuance policies • All application policies
Issued to: WIN.SEC-LAB					Issued to: WIN-H9R5R13M8P6-CA
Issued by: WIN-H9R5R13M8P6-CA]				Issued by: WIN-H9R5R13M8P6-CA
Valid from 2/26/2020 to 2/26/202	21				Valid from 2/25/2020 to 2/25/2
Install Certifica	te Issuer Statement		ed (Select to c		Install Certific
	OK				

Utilizzare le acquisizioni di pacchetti per confermare che il server LDAP invia le informazioni corrette:

	(*Ethe
F	File Edi	t View Go C	apture Analyze St	atistics Telephony Wirel	ess Tools H	elp		
1		🤊 🛞] 🙆	रे 🖸 🤇 🗢 🔿 🖞	i T 👲 🗐 🔍 🤅	a 🔍 🎹			
Γ	Idap	tls && ip.addr==192	.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	
	2	2 2.720710	192.0.2.15	192.0.2.5	TLSv1.2	1211	Application Data	
	2	9 3.056497	192.0.2.5	192.0.2.15	LDAP	97	extendedReq(1) LDAP_START_TLS_OID	
	3	0 3.056605	192.0.2.15	192.0.2.5	LDAP	112	extendedResp(1) LDAP_START_TLS_OI	D
4	3	2 3.056921	192.0.2.5	192.0.2.15	TLSv1.2	313	Client Hello	
Ц	3	3 3.057324	192.0.2.15	192.0.2.5	TLSv1.2	1515	Server Hello, Certificate, Server	Key Exchange, Certificat
	3	5 3.060532	192.0.2.5	192.0.2.15	TLSv1.2	260	Certificate, Client Key Exchange,	Change Cipher Spec, Encr
Ц	3	5 3.061678	192.0.2.15	192.0.2.5	TLSv1.2	173	Change Cipher Spec, Encrypted Han	dshake Message
1	Frame	33: 1515 byte	s on wire (12120	bits), 1515 bytes capt	tured (12120	bits)	on interface \Device\NPF_{3EAD5E9F	F-B6CB-4EB4-A462-217C1A10
	Ether	net II, Src: V	Mware_69:c8:c6 (0	0:0c:29:69:c8:c6), Dst	t: VMware_29:	cf:2d	(00:0c:29:29:cf:2d)	
	> Inter	net Protocol V	ersion 4, Src: 19	2.0.2.15, Dst: 192.0.2	2.5			Cisco Firepower Mar
1	Trans	mission Contro	l Protocol, Src P	ort: 389, Dst Port: 52	2384, Seq: 47	, Ack	: 279, Len: 1449	
1	4 Trans	port Layer Sec	urity					← → C = fr
	4 11	SV1.2 Record L	ayer: Handshake P	rotocol: Multiple Hand	ishake Messag	es		
		Content Type:	Handshake (22)					Overview Analysis
		Version: TLS .	1.2 (0x0505)					
	Þ	Handshake Pool	tocol: Server Hel					
	4	Handshake Pro	tocol: Certificat					LICORE LICOR DO
		Handshake 1	Type: Certificate	(11)				USEIS USEI KU
		Length: 112	24	()				
		Certificate	es Length: 1121					External Authent
		4 Certificate	es (1121 bytes)					
		Certific	cate Length: 1118					Authentication Method
		4 Certific	cate: 3082045a3082	0342a0030201020213320	000000456c38	ðc8	id-at-commonName=WIN.SEC-LAB i	d- CAC
		▷ signe	edCertificate					Name #
		> algor	rithmIdentifier (s	ha256WithRSAEncryptio	n)			Name -
		Paddi	ing: 0					Description
	Server Turne							
	Server type							
	Primary Server							
	rinnary octver							
	Host Name/IP Address							
								Port *

Informazioni correlate

- Account utente per l'accesso alla gestione
- <u>Cisco Firepower Management Center Lightweight Directory Access Protocol Authentication Bypass</u> <u>Vulnerability</u>
- <u>Configurazione dell'oggetto di autenticazione LDAP sul sistema FireSIGHT</u>
- Documentazione e supporto tecnico Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).