# Come esportare un certificato TLS da CUCM Packet Capture (PCAP)

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Esporta certificato TLS da CUCM PCAP Verifica Risoluzione dei problemi

### Introduzione

In questo documento viene descritta la procedura per esportare un certificato da un protocollo PCAP di Cisco Unified Communications Manager (CUCM).

Contributo di Adrian Esquillo, Cisco TAC Engineer.

### Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti: ·Handshake Transport Layer Security (TLS) ·Gestione certificati CUCM ·Server SFTP (Secure File Transport Protocol) ·Strumento di monitoraggio in tempo reale (RTMT)

·Applicazione Wireshark

#### Componenti usati

·CUCM release 9.X e successive

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

Èpossibile esportare un certificato server/catena di certificati per verificare che il certificato

server/catena di certificati forniti dal server corrisponda ai certificati da caricare o caricati in Gestione certificati CUCM.

Come parte dell'handshake TLS, il server fornisce a CUCM il proprio certificato/catena di certificati server.

### Esporta certificato TLS da CUCM PCAP

Passaggio 1. Avviare il comando packet capture su CUCM

Stabilire una connessione Secure Shell (SSH) al nodo CUCM ed eseguire il comando utilizza network capture (o capture-rotate) file <nomefile> count 1000000 size ALL, come mostrato nell'immagine:

10.201.218.163 - PuTTY



Passaggio 2. Avviare una connessione TLS tra Server e CUCM

In questo esempio, viene avviata una connessione TLS tra un server Secure Lightweight Directory Access Protocol (LDAPS) e CUCM stabilendo una connessione sulla porta TLS 636, come mostrato nell'immagine:

Gisco Unified CM Administration     For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration V Go admin Search Documentation About Logout
System 🔻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 💌	
LDAP Directory	Related Links: Back to LDAP Directory Find/List 🗸 Go
🔚 Save 💥 Delete 🗈 Copy 🁌 Perform Full Sync Now 🚽 Add New	
Access Control Groups Access Control Group Feature Group Template < None > Warning: If no template is selected, the new line features below will not be active. Apply mask to synced telephone numbers to create a new line for inserted users Mask Assign new line from the pool list if one was not created based on a synced LDAP telephone number Order DN Pool Start DN Pool End Add DN Pool	
-LDAP Server Information	
WIN-H2Q74S1U39P.network218.com	
Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

Passaggio 3. Arrestare CUCM PCAP dopo il completamento dell'handshake TLS

Premere Control-C per interrompere l'acquisizione del pacchetto, come mostrato nell'immagine



Passaggio 4. Scaricare il file di acquisizione del pacchetto utilizzando uno dei due metodi elencati

1. Avviare RTMT per il nodo CUCM e passare a **Sistema > Strumenti > Traccia > Centro traccia e log > Raccogli file** e selezionare la casella **Registri acquisizione pacchetti** (continuare il processo RTMT per scaricare il pcap), come mostrato nell'immagine:

Collect Files			8						
Select System Services/Applications									
Select all Services on all Servers									
Name	All Servers	s 🗌 cucmpub216.netv	vork 🗌 imp216.network2						
FIFS LUgs									
Host Resources Agent									
IPT Platform CLI Created Reports									
IPT Platform CLI Logs									
IPT Platform Cert Monitor Logs									
IPT Platform CertMgr Logs									
IPT Platform Cluster Manager Logs									
IPT Platform GUI Logs									
IPT Platform IPSecMgmt Logs									
IPT Platform RemoteSupport Logs									
Install File Signing									
Install and Upgrade Logs									
Kerneldump Logs									
MIB2 Agent									
Mail Logs									
Mgetty Logs									
NTP Logs									
Packet Capture Logs		<b>~</b>							
Prog Logs									
SAR Logs									
SELinux logs									
SNMP Master Agent									
Security Logs									
Service Manager									
Service Registration Logs									
Spooler Logs									
System Application Agent									
< Baci	k Next>	Finish Cancel							

2. Avviare un server SFTP (Secure File Transport Protocol) e nella sessione SSH CUCM eseguire il **file di** comando **get activelog /form/cli/<nomefile pac>.cap** (continuare attraverso le richieste per scaricare PCAP sul server SFTP), come mostrato nell'immagine:



Passaggio 5. Determinare il numero di certificati presentati a CUCM dal server

Utilizzare l'applicazione Wireshark per aprire il cappuccio e filtrare in base a **tls** per determinare il pacchetto con **Server Hello** contenente la catena di certificati/certificati del server presentata a CUCM. Questo è il fotogramma 122, come mostrato nell'immagine:

File	Edit View Go Capture	Analyze Statistics Telephony	Wireless Tools Help		
Æ.	🔳 🔬 💿 📙 🛅 🗙 🛅 🔍	(⇔ ⇔ ≅ T ± ]	0, 0, 0, II		
l	ls				X 📼
No.	Time	Source	Destination	Protocol	Length Info
	14 09:09:22.241271	10.201.218.170	10.201.218.163	TLSv1.2	390 Application Data
	18 09:09:22.250389	10.201.218.163	10.201.218.170	TLSv1.2	271 Application Data
	29 09:09:22.252337	10.201.218.163	10.201.218.170	TLSv1.2	421 Application Data, Application Data, Application Data, Application Data, Application Data, A
	56 09:09:22.691660	10.201.218.166	10.201.218.163	TLSv1.2	390 Application Data
	57 09:09:22.692748	10.201.218.163	10.201.218.166	TLSv1.2	271 Application Data
	59 09:09:22.692972	10.201.218.163	10.201.218.166	TLSv1.2	391 Application Data, Application Data, Application Data, Application Data, Application Data, A
	61 09:09:22.693131	10.201.218.163	10.201.218.166	TLSv1.2	96 Application Data
	65 09:09:23.789625	10.201.218.169	10.201.218.163	TLSv1.2	407 Application Data
	66 09:09:23.790753	10.201.218.163	10.201.218.169	TLSv1.2	271 Application Data
	68 09:09:23.791100	10.201.218.163	10.201.218.169	TLSv1.2	421 Application Data, Application Data, Application Data, Application Data, Application Data, A
	112 09:09:25.178520	10.99.100.100	10.201.218.163	TLSv1.2	1146 Application Data
	117 09:09:25.290246	10.201.218.163	10.201.218.164	TLSv1.2	313 Client Hello
+	122 09:09:25.304369	10.201.218.164	10.201.218.163	TLSv1.2	845 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
	124 09:09:25.329331	10.201.218.163	10.201.218.164	TLSv1.2	255 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
	125 09:09:25.331128	10.201.218.164	10.201.218.163	TLSv1.2	173 Change Cipher Spec, Encrypted Handshake Message
<					· · · · · · · · · · · · · · · · · · ·
>	rame 122: 845 bytes on wir	re (6760 bits), 845 bytes (	aptured (6760 bits)	)	
> 6	thernet II, Src: Vmware_as	5:74:2a (00:50:56:a5:74:2a)	), Dst: Vmware 07:23	3:17 (00:0c:2	9:07:23:17)
> 1	Internet Protocol Version 4	4, Src: 10.201.218.164, Dst	t: 10.201.218.163		
> 1	Transmission Control Protoc	col, Src Port: 636, Dst Por	rt: 34726, Seq: 2897	, Ack: 248,	Len: 779
>	3 Reassembled TCP Segments	s (3675 bytes): #118(1448)	#120(1448), #122(7	79)]	

> Transport Layer Security

•Espandere **Transport Layer Security >Certificate** information dal pacchetto Server Hello con certificato per determinare il numero di certificati presentati a CUCM. Il certificato principale è il certificato del server. In questo caso, viene visualizzato un solo certificato, il certificato server, come illustrato nell'immagine:

File	e Edit	View Go	Capture	Analyze	Statistics	Telephony	Wireles	s Tools	Help					
		•	🗙 🖸   9	⇔ ⇒	🗟 🚹	& 📃 🔳	€.0	۹ 🏢						
	tls											$\mathbf{X}$		
No.		Time			Source		Dest	tination		Protocol	Length	1 Info	/	
+	122	09:09:25.30	04369		10.201.	218.164	10.	201.218	.163	TLSv1.	2 84	5 Server Hello, Certificate, Server	k	
	124	09:09:25.32	29331		10.201.	218.163	10.	201.218	.164	TLSv1.	2 25	5 Certificate, Client Key Exchange,	¢	
	125	09:09:25.33	31128		10.201.	218.164	10.	201.218	.163	TLSv1.	2 17	3 Change Cipher Spec, Encrypted Han	ds	
	126	09:09:25.33	33417		10.201.	218.163	10.	201.218	.164	TLSv1.	2 199	9 Application Data		
	127	09:09:25.33	35730		10.201.	218.164	10.	201.218	.163	TLSv1.	2 167	7 Application Data		
	128	09:09:25.33	39000		10.201.	218.163	10.	201.218	.164	TLSv1.	2 327	7 Application Data		
	129	09:09:25.33	39649		10.201.	218.164	10.	201.218	.163	TLSv1.	2 167	7 Application Data		,
<													>	
>	Frame	122: 845 by	tes on wi	re (6760	0 bits),	845 bytes	captur	ed (676	0 bits)					-
>	Ethern	et II, Src:	Vmware a	5:74:2a	(00:50:	56:a5:74:2	a), Dst	: Vmware	e 07:23:1	7 (00:0c	:29:07:	:23:17)		
>	Intern	et Protocol	Version 4	4, Src:	10.201.	218.164, D	st: 10.	201.218	.163					
>	Transm	ission Cont	rol Proto	col, Sro	Port:	636, Dst P	ort: 34	726, Sec	q: 2897,	Ack: 248	, Len:	779		
>	[3 Rea	ssembled TC	P Segment:	s (3675	bytes):	#118(1448	), #120	(1448),	#122(779	)]				
~	Fransp	ort Layer S	Security											
	✓ TLS	v1.2 Record	Layer: Ha	andshake	Protoc	ol: Multipl	Le Hand	shake Me	essages					
	Content Type: Handshake (22)													
	Version: TLS 1.2 (0x0303)													
	1	Length: 367	0											
	>	Handshake Pi	rotocol: S	ierver H	ello									
	~	Handshake Pi	rotocol: C	ertific	ate									
		Handshake	e Type: Ce	rtifica	te (11)									
		Length: 1	1481											
		Certifica	ates Lengt	h: 1478										
		✓ Iertifica	ates (1478	bytes)										
		Certif	ficate Len	gth: 147	75								_	
		> Certif	ficate: 30	8205bf30	08204a7a	0030201020	2136200	0000026	295e487	(id-at-c	ommonNa	ame=WIN-H2074S1U39P.network218.com)		
	>	Handshake Pi	rotocol: S	erver K	ey Excha	ange								
	>	Handshake Pi	rotocol: C	ertific	ate Requ	uest								
	>	Handshake Pi	rotocol: 5	erver H	ello Dor	ne								

Passaggio 6. Esportare la catena di certificati/certificati del server dal protocollo PCAP CUCM

In questo esempio viene presentato solo il certificato del server, pertanto è necessario esaminarlo. Fare clic con il pulsante destro del mouse sul certificato del server e selezionare **Export Packet Bytes** (Esporta byte pacchetti) per salvare come certificato con estensione cer, come mostrato nell'immagine:

File Edit View Go Capture Analyz	e Statistics Telephony	Wireless Tools Help						
🔟 🔳 🖉 💿 📙 🛅 🔀 🖆 🔍 👄	-> 😫 🗿 🕹 📃 📃	0.0.0.1						
📕 tls						+		
No.         Time         Source         Destination         Protocol         Length         I           122 09:09:25.304369         10.201.218.164         10.201.218.163         TLSv1.2         845 5         Collapse Subtrees           124 09:09:25.329331         10.201.218.163         10.201.218.164         TLSv1.2         845 5         Collapse Subtrees           125 09:09:25.331128         10.201.218.164         10.201.218.163         TLSv1.2         173 6         Expand All           126 09:09:25.333417         10.201.218.163         10.201.218.163         TLSv1.2         167 A           128 09:09:25.33900         10.201.218.163         10.201.218.164         TLSv1.2         167 A           129 09:09:25.339649         10.201.218.164         10.201.218.164         TLSv1.2         167 A           Apply as Column         Ctrl+Shi           129 09:09:25.339649         10.201.218.164         10.201.218.163         TLSv1.2         167 A           Sethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23         Conversation Filter         Colorize with Filter           Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163         TLSv1.2         167 A         Follow								
> [3 Reassembled TCP Segments (36	75 bytes): #118(1448	), #120(1448), #122(77	79)]		Сору	•		
✓ Transport Layer Security     Copy       ✓ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages     Show Packet Bytes       Content Type: Handshake (22)     Export Packet Bytes       Ctrl+     Export Packet Bytes								
Version: ILS 1.2 (0x0303)         Length: 3670         > Handshake Protocol: Server Hello         > Handshake Protocol: Certificate         Protocol Preferences								
Length: 1481 Certificates Length: 1478 V Certificates (1478 bytes) Certificates (1478 bytes)								
<ul> <li>Certificate: 308205b</li> <li>Handshake Protocol: Server</li> <li>Handshake Protocol: Certif</li> <li>Handshake Protocol: Server</li> </ul>	f308204a7a0030201020 • Key Exchange ficate Request • Hello Done	21362000000026295e487.	. (id-at-com	nmonName=W	IN-H2Q7451U39P.network21	8.com)		

•Nella finestra successiva, fornire un nome file con estensione cer e fare clic su Salva. Il file salvato (in questo caso sul desktop) è stato denominato servercert.cer, come mostrato nell'immagine:

	120 00.00.25 222417	10.001.010.101	10, 201, 2	Organize 🔻 🛛 🕅	ew tolde	er			<b>•</b>	•
	120 09:09:25.333417	10.201.218.163	10.201.2	This DC	^					
	128 09:09:25.339000	10.201.218.163	10.201.2				No items match your	search.		
	129 09:09:25.339649	10.201.218.164	10.201.2	3D Objects	- 1					
				📃 Desktop						
	Frame 122: 845 bytes on wire	(6760 bits), 845 bytes (	aptured (6	🔮 Documents						
	Ethernet II, Src: Vmware_a5:	74:2a (00:50:56:a5:74:2a)	, Dst: Vmw	👆 Downloads						
	> Internet Protocol Version 4,	Src: 10.201.218.164, Dst	: 10.201.2	👌 Music						
	Transmission Control Protoco	<pre>L, Src Port: 636, Dst Por (2675 butos), #118(1448)</pre>	t: 34726,	Pictures						
	<ul> <li>Transport Laver Security</li> </ul>	(30/3 Dytes): #110(1440),	#120(1440	Videos						
L	✓ TLSv1.2 Record Layer: Hand	dshake Protocol: Multiple	Handshake	Windows (C	a 👘					
L	Content Type: Handshake	(22)		Windows (C.	.,					
L	Version: TLS 1.2 (0x030	3)		💣 Network	~					
L	Length: 3670			File name	server	rcert.cer				~
L	> Handshake Protocol: Ser >> Handshake Protocol: Cer	ver Hello				. /*I` * I · * \				
L	Handshake Type: Cert	ificate (11)		Save as type	: Raw d	lata (^.bin ^.dat ^.raw)				~
L	Length: 1481								-	_
L	Certificates Length:	1478		<ul> <li>Hide Folders</li> </ul>				Save	Cance	:
	✓ Certificates (1478 b	ytes)	L						_	
	Certificate Lengt	h: 1475	2600000000				D			
	> Certificate: 30820	050T308204a7a003020102023	136200000002	26295e487 (1d-at	c-commo	onwame=wiw-H2Q/4S1U39	P.network218.com)			

Passaggio 7. Aprire il file con estensione CER salvato per esaminarne il contenuto

Fare doppio clic sul file con estensione cer per esaminare le informazioni nelle schede **Generale**, **Dettagli** e **Percorso certificato**, come mostrato nell'immagine:



### Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.