# Exportieren der TLS-Zertifizierung aus CUCM Packet Capture (PCAP)

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen TLS-Zertifikat vom CUCM PCAP exportieren Überprüfen Fehlerbehebung

## Einführung

Dieses Dokument beschreibt das Verfahren zum Exportieren eines Zertifikats von einem Cisco Unified Communications Manager (CUCM) PCAP.

Mitarbeiter: Adrian Esquillo, Cisco TAC Engineer.

## Voraussetzungen

#### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen: ·Transport Layer Security (TLS)-Handshake ·CUCM-Zertifikatsverwaltung ·Secure File Transport Protocol (SFTP)-Server ·Realtime Monitoring Tool (RTMT)

Wireshark-Anwendung

#### Verwendete Komponenten

·CUCM Version 9.X oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Ein Serverzertifikat/eine Zertifikatkette kann exportiert werden, um zu bestätigen, dass das vom

Server bereitgestellte Serverzertifikat/die vom Server bereitgestellte Zertifikatkette mit den hochzuladenden Zertifikaten übereinstimmt oder in das CUCM-Zertifikatsmanagement hochgeladen wird.

Im Rahmen des TLS-Handshake stellt der Server seine Serverzertifikat-/Zertifikatkette für CUCM bereit.

## TLS-Zertifikat vom CUCM PCAP exportieren

Schritt 1: Starten des Befehls zur Paketerfassung auf CUCM

Stellen Sie eine Secure Shell (SSH)-Verbindung zum CUCM-Knoten her, und führen Sie den Befehl **utils network capture (or capture-rotation) file <Dateiname> count 100000 size ALL aus**, wie im Bild gezeigt:



Schritt 2: TLS-Verbindung zwischen Server und CUCM starten

In diesem Beispiel starten Sie eine TLS-Verbindung zwischen einem LDAPS-Server (Secure Lightweight Directory Access Protocol) und dem CUCM, indem Sie eine Verbindung auf dem TLS-Port 636 herstellen, wie im Bild gezeigt:

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 Access Control Group Mask Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Add to Access Control Group The selected of the new line for inserted users Mask Access Control Group Access Control Group The selected of the new line for inserted users Mask Access Control Group Access Control Group Access Control Group The selected of the new line for inserted users Mask Access Control Group	,
-LDAP Server Information	
WIN-H2Q74S1U39R.network218.com	
Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

Schritt 3: CUCM-PCAP stoppen, nachdem der TLS-Handshake abgeschlossen ist

Drücken Sie Control-C, um die Paketerfassung zu stoppen, wie im Bild gezeigt.



Schritt 4: Laden Sie die Paketerfassungsdatei mit einer der beiden aufgeführten Methoden herunter

1. Starten Sie RTMT für den CUCM-Knoten, navigieren Sie zu **System > Tools > Trace > Trace & Log Central > Collect Files** und aktivieren Sie das Feld **Packet Capture Logs** (fahren Sie mit dem RTMT-Prozess fort, um die pcap-Datei herunterzuladen), wie im Bild gezeigt:

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. Starten Sie einen SFTP-Server (Secure File Transport Protocol), und führen Sie in der CUCM SSH-Sitzung die **Befehlsdatei get activelog /patform/cli/<pcap filename>.cap aus** (fahren Sie mit den Aufforderungen fort, um den PCAP auf dem SFTP-Server herunterzuladen), wie im Bild gezeigt:



Schritt 5: Bestimmen Sie die Anzahl der Zertifikate, die der Server dem CUCM vorlegt.

Verwenden Sie die Anwendung Wireshark, um die pcap-Datei zu öffnen und auf tis zu filtern, um das Paket mit Server Hello zu ermitteln, das das dem CUCM präsentierte Serverzertifikat/Zertifikatskette enthält. Dies ist Frame 122, wie im Bild gezeigt:

File	Edit View Go Capture Ar	nalyze Statistics Telephony	Wireless Tools Help		
A.	۹ 🖸 🗙 🔚 🧧 🕥 🔳	⇔⇒≅₹₹₹	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 wire	(6760 bits), 845 bytes	captured (6760 bits)		
> 6	thernet II, Src: Vmware a5:	74:2a (00:50:56:a5:74:2a	), Dst: Vmware 07:23:	:17 (00:0c:2	9:07:23:17)
5 1	Internet Protocol Version 4.	Src: 10.201.218.164, Ds	t: 10.201.218.163		· · · · · · · · · · · · · · · · · · ·
> 1	Transmission Control Protoco	ol. Src Port: 636, Dst Po	rt: 34726, Seg: 2897,	, Ack: 248,	Len: 779
>	3 Reassembled TCP Segments	(3675 bytes): #118(1448)	, #120(1448), #122(77	79)]	
		, , , , , , , , , , , , , , , , , , , ,			

> Transport Layer Security

·erweitern Sie die Informationen Transport Layer Security > Certificate vom Server Hello-Paket mit dem Zertifikat, um die Anzahl der Zertifikate zu bestimmen, die dem CUCM vorgelegt werden. Das oberste Zertifikat ist das Serverzertifikat. In diesem Fall wird nur ein Zertifikat, das Serverzertifikat, wie im Bild gezeigt angezeigt:

File	Edit	View Go	Capture	Analyze	Statistics	Telephony	Wireless	s Tools	Help						
		O	🗙 🔂 🤇	<b>\</b> ⇔ ⇒	🕋 👔	& ☴   ☴	€.0	Q 🎹							
	ls												$\times$ $\rightarrow$		÷
No.		Time			Source		Dest	ination		Protoco	Leng	th Info			^
+	122	09:09:25.30	04369		10.201.	218.164	10.3	201.218.	163	TLSv1	2 8	45 Server Hello, Certi	ficate, Server H		
	124	09:09:25.3	29331		10.201.	218.163	10.3	201.218.	164	TLSv1	2 2	55 Certificate, Client	Key Exchange, (		
	125	09:09:25.3	31128		10.201.	218.164	10.3	201.218.	163	TLSv1	2 1	73 Change Cipher Spec,	Encrypted Hands		
	126	09:09:25.3	33417		10.201.	218.163	10.3	201.218.	164	TLSv1	2 1	99 Application Data			
	127	09:09:25.3	35730		10.201.	218.164	10.3	201.218.	163	TLSv1	2 1	67 Application Data			
	128	09:09:25.3	39000		10.201.	218.163	10.3	201.218.	164	TLSv1	2 3	27 Application Data			
	129	09:09:25.3	39649		10.201.	218.164	10.3	201.218.	163	TLSv1	2 1	67 Application Data			¥
<													>		
>	Frame	122: 845 by	/tes on wi	re (6760	) bits),	845 bytes	capture	ed (6760	) bits)						_
>	Ethern	et II, Src:	: Vmware_a	5:74:2a	(00:50:	56:a5:74:2	a), Dst	: Vmware	07:23:1	17 (00:00	:29:0	7:23:17)			
>	Intern	et Protocol	Version	4, Src:	10.201.	218.164, D	st: 10.3	201.218.	163						
>	Fransm	ission Cont	trol Proto	col, Sro	Port:	636, Dst P	ort: 34	726, Sec	: 2897,	Ack: 248	, Len	: 779			
>	3 Rea	ssembled TO	'P Segment	s (3675	bytes):	#118(1448	), #120	(1448),	#122(779	9)]					
~	Fransp	ort Layer S	Security												
	✓ TLS <sup>1</sup>	v1.2 Record	Layer: H	andshake	Protoc	ol: Multip	le Hands	shake Me	ssages						
	(	Content Typ	e: Handshi	ake (22)											
	١	Version: TL	S 1.2 (0x0	0303)											
	I	Length: 367	0												
	>	Handshake P	rotocol: 9	Server H	ello										
	× 1	Handshake P	rotocol: (	Certific	ate										
		Handshak	e Type: Ce	ertifica	te (11)										
		Length: 3	1481												
		Certific	ates Lengt	th: 1478	_										
		<ul> <li>Tertification</li> </ul>	ates (1478	3 bytes)											
		Certi	ficate Ler	ngth: 147	75										
		> Certif	ficate: 30	)8205bf30	08204a7a	0030201020	2136200	0000026	295e487	(id-at-	ommon	Name=WIN-H2074S1U39P.r	etwork218.com)		
	> I	Handshake P	rotocol: 9	Server K	ey Excha	ange									
	> I	Handshake P	rotocol: (	Certific	ate Requ	uest									
	> Handshake Protocol: Server Hello Done														

Schritt 6: Exportieren des Serverzertifikats/der Zertifikatkette aus dem CUCM PCAP

In diesem Beispiel wird nur das Serverzertifikat angezeigt, daher müssen Sie das Serverzertifikat überprüfen. Klicken Sie mit der rechten Maustaste auf das Serverzertifikat, und wählen Sie **Packet Bytes exportieren aus**, um als .cer-Zertifikat zu speichern, wie im Bild gezeigt:

File Edit View Go Capture Analyze	Statistics Telephony	Wireless Tools Help							
◢ ■ ∅ ◉   🔒 🖾 🕱 🖻   ९ ⇔ ⇔ 🕾 🖗 🕹 🚍 🔳 ९ ९ ९ ९ 🏛									
📕 tls					×				
No. Time 122 09:09:25.304369 124 09:09:25.329331	Source 10.201.218.164 10.201.218.163	Destination 10.201.218.163 10.201.218.164	Protocol TLSv1.2 TLSv1.2	Length I 845 5 255 0	Expand Subtrees Collapse Subtrees				
125 09:09:25.331128 126 09:09:25.333417 127 09:09:25.335730	10.201.218.164 10.201.218.163 10.201.218.164	10.201.218.163 10.201.218.164 10.201.218.163	TLSv1.2 TLSv1.2 TLSv1.2	173 C 199 A 167 A	Expand All Collapse All				
128 09:09:25.339000 129 09:09:25.339649	10.201.218.163 10.201.218.164	10.201.218.164 10.201.218.163	TLSv1.2 TLSv1.2	327 A 167 A	Apply as Column Apply as Filter	Ctrl+Shift+I			
Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)       Prepare as Filter         > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)       Conversation Filter         > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23       Colorize with Filter         > Internet Protocol Version 4, Src: 10:201.218.164, Dst: 10:201.218.163       Dst: 2807, Ack: 248, Len: 77         Follow       Follow									
<ul> <li>[3 Reassembled TCP Segments (3675</li> <li>Y Transport Layer Security</li> </ul>	bytes): #118(1448)	, #120(1448), #122(77	9)]		Сору	+			
<ul> <li>✓ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages</li> <li>✓ Content Type: Handshake (22)</li> <li>✓ Export Packet Bytes</li> <li>Ctrl+Shift+Z</li> </ul>									
Version: ILS 1.2 (0x0303) Length: 3670 > Handshake Protocol: Server Hello > Handshake Protocol: Certificate > Handshake Protocol: Certificate > Handshake Protocol: Certificate > Handshake Protocol: Certificate > Handshake Protocol: Certificate									
Length: 1481 Certificates Length: 1478 Certificates (1478 bytes) Certificates (1478 bytes) Certificates (1478 bytes)									
Certificate Length: 1475       Show Linked Packet in New Window         > Certificate: 308205bf308204a7a003020102021362000000026295e487 (id-at-commonName=WIN-H2Q74S1U39P.network218.com)         > Handshake Protocol: Server Key Exchange         > Handshake Protocol: Certificate Request         > Handshake Protocol: Server Hello Done									

·Geben Sie im nachfolgenden Fenster einen Namen für die Cer-Datei an, und klicken Sie dann auf Speichern. Die Datei, die (in diesem Fall auf dem Desktop) gespeichert wurde, wurde ServerCert.cer genannt, wie im Bild gezeigt:

	115 0510511515511110	10120112101101		Organize 🔻 🛛 i	INEW TO	ider				<b>V</b>
	126 09:09:25.333417	10.201.218.163	10.201.2							
	127 09:09:25.335730	10.201.218.164	10.201.2	💻 This PC		,	No items match your s	earch.		
	128 09:09:25.339000	10.201.218.163	10.201.2	2D Objects			,,			
	129 09:09:25.339649	10.201.218.164	10.201.2	J SD Objects	_					
<				📃 Desktop						
>	Frame 122: 845 bytes on wire	(6760 bits), 845 bytes (	aptured (6	Documents	s					
>	Ethernet II, Src: Vmware_a5:7	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 Protocol	l, Src Port: 636, Dst Por	rt: 34726,							
>	[3 Reassembled TCP Segments (	(3675 bytes): #118(1448);	#120(1448	Pictures						
٧	Transport Layer Security			📑 Videos						
	✓ TLSv1.2 Record Layer: Hand	lshake Protocol: Multiple	Handshake	Mindows (	<b>C</b> 1					
	Content Type: Handshake	(22)		- Windows (	C.)					
	Version: TLS 1.2 (0x030	3)		💣 Network	~	+				
	Length: 3670									
	> Handshake Protocol: Ser	ver Hello		File nam	e: serv	vercert.cer				~
	∨ Handshake Protocol: Cer	tificate		Save as typ	e: Raw	/ data (*.bin *.dat *.raw)				$\sim$
	Handshake Type: Cert:	ificate (11)		71						
	Length: 1481									
	Certificates Length:	1478		<ul> <li>Hide Folders</li> </ul>				Save	Cancel	
	✓ Certificates (1478 b)	ytes)	L							
	Certificate Lengt	h: 1475								
	> Certificate: 30820	75bf308204a7a00302010202	136200000000	6295e487 (id-a	at-com	monName=WTN-H2074S1U39	P.network218.com)			

Schritt 7: Öffnen Sie die gespeicherte CER-Datei, um Inhalte zu prüfen.

Doppelklicken Sie auf die Datei .cer, um die Informationen in den Registerkarten **Allgemein**, **Details** und **Zertifikatspfad** zu überprüfen, wie im Bild gezeigt:



## Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.