Hoe u TLS-certificering kunt exporteren vanuit CUCM Packet Capture (PCAP)

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie TLS-certificaat exporteren vanuit CUCM PCAP Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft de procedure om een certificaat uit een Cisco Unified Communications Manager (CUCM) PCAP te exporteren.

Bijgedragen door Adrian Esquillo, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- TelePresence (Transport Layer Security) handdruk
- · CUCM-certificaatbeheer
- · Secure File Transport Protocol (SFTP) server
- · Realtime Monitoring Tool (RTMT)
- · Toepassing voor draadloos haaien

Gebruikte componenten

· CUCM release 9.X en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Een server certificaat/certificeringsketen kan worden geëxporteerd om te bevestigen dat de server

certificaat/certificeringsketen die door de server wordt geleverd, overeenkomt met de te uploaden certificaten of die worden geüpload naar CUCM certificaatbeheer.

Als onderdeel van de TLS-handdruk biedt de server de keten van het servercertificaat aan CUCM.

TLS-certificaat exporteren vanuit CUCM PCAP

Stap 1. Start de pakketvastlegging opdracht op CUCM

Stel een Secure Shell (SSH)-verbinding in op het CUCM-knooppunt en voer het **bestand** <**filename>** opnamen **van het** commando**-netwerk** uit **(of regeren-roteren), alsmede de grootte** ALL, zoals in de afbeelding:

х

🗬 10.201.218.163 - PuTTY



Stap 2. Start een TLS-verbinding tussen Server en CUCM

In dit voorbeeld start u een TLS-verbinding tussen een Secure Lichtgewicht Directory Access Protocol (LDAPS) server en CUCM door een verbinding op TLS poort 636 in te stellen, zoals in de afbeelding wordt getoond:

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 None Template Template is not created based on a synced LDAP telephone number Order DN Pool Start DN Pool End Add DN Pool	
- LDAP Server Information	
WIN-H2Q7451U39Rnetwork218.com	
Save Delete Copy Perform Full Sync Now Add New	

Stap 3. Stop CUCM PCAP nadat de TLS-handdruk is voltooid

Druk op Control-C om de pakketvastlegging te stoppen, zoals in de afbeelding



Stap 4. Download het bestand van de pakketvastlegging volgens een van de twee genoemde methoden

1. Start RTMT voor CUCM-knooppunt en navigeer naar **systeem > Gereedschappen > Zoeken > Centraal overschakelen > Opnemen** en **controleer** de **Packet Capture Logs** (ga door het RTMTproces om het pad te downloaden), zoals in de afbeelding te zien is:

Collect Files			X							
Select System Services/Applications										
Select all Services on all Servers										
Name	All Servers	Cucmpub216 netwo	rk 🗌 imp216 network2							
FIFS LOgs										
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										
Prog Logs										
SAR Logs										
SELinux logs										
SNMP Master Agent										
Security Logs										
Service Manager										
Service Registration Logs										
Spooler Logs										
System Application Agent										
• -			F							
< Back	Next>	Finish Cancel								

2. Start een Secure File Transport Protocol (SFTP) server en voer in de CUCM SSH-sessie het **opdrachtbestand activeren/patform/cli/<pcap filename>.cap** (doorgaan met de aanwijzingen om het PCAP op SFTP-server te downloaden), zoals in de afbeelding wordt weergegeven:



Stap 5. Bepaal het aantal certificaten dat door de server aan CUCM wordt aangeboden

Gebruik de toepassing Wireless-shark om het deksel en het filter op **tls** te openen om het pakket met **server Hallo** te bepalen dat de aan CUCM aangeboden server certificaat/certificeringsketen bevat. Dit is frame 122, zoals in de afbeelding weergegeven:

File Ed	it View Go Capture Analyze	Statistics Telephony W	/ireless Tools Help		
	1 💿 📙 🛅 🗙 🛅 🍳 👄 🔿	· 🕾 T 🕹 📃 🔳 🍳	Q. Q. 👖		
tls					
No.	Time	Source	Destination	Protocol	Length Info
1	4 09:09:22.241271	10.201.218.170	10.201.218.163	TLSv1.2	390 Application Data
1	8 09:09:22.250389	10.201.218.163	10.201.218.170	TLSv1.2	271 Application Data
2	9 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
5	6 09:09:22.691660	10.201.218.166	10.201.218.163	TLSv1.2	390 Application Data
5	7 09:09:22.692748	10.201.218.163	10.201.218.166	TLSv1.2	271 Application Data
5	9 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
6	1 09:09:22.693131	10.201.218.163	10.201.218.166	TLSv1.2	96 Application Data
6	5 09:09:23.789625	10.201.218.169	10.201.218.163	TLSv1.2	407 Application Data
6	6 09:09:23.790753	10.201.218.163	10.201.218.169	TLSv1.2	271 Application Data
6	8 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
11	2 09:09:25.178520	10.99.100.100	10.201.218.163	TLSv1.2	1146 Application Data
11	7 09:09:25.290246	10.201.218.163	10.201.218.164	TLSv1.2	313 Client Hello
• 12	2 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
12	4 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
12	5 09:09:25.331128	10.201.218.164	10.201.218.163	TLSv1.2	173 Change Cipher Spec, Encrypted Handshake Message
<					· · · · · · · · · · · · · · · · · · ·
> Frame	2 122: 845 bytes on wire (676	0 bits), 845 bytes ca	ptured (6760 bits)		
> Ether	net II, Src: Vmware a5:74:2a	(00:50:56:a5:74:2a),	Dst: Vmware 07:23:13	7 (00:0c:2	9:07:23:17)
> Inter	net Protocol Version 4, Src:	10.201.218.164, Dst:	10.201.218.163		
> Trans	mission Control Protocol, Sr	c Port: 636, Dst Port	: 34726, Seq: 2897, A	Ack: 248,	Len: 779
> [3 Re	assembled TCP Segments (3675	bytes): #118(1448),	#120(1448), #122(779)]	

> Transport Layer Security

 Uitbreidt de Beveiliging van de transportlaag > certificaat informatie uit het pakket van de Server Hallo met certificaat om het aantal certificaten te bepalen dat aan CUCM wordt aangeboden. Het hoogste certificaat is het servercertificaat. In dit geval wordt slechts 1 certificaat, het servercertificaat, gepresenteerd zoals in de afbeelding:

File	Edit	View Go	Capture	Analyze	Statistics	Telephony	Wireless	s Tools	Help						
		O	🗙 🔂 🤇	\ ⇔ ⇒	🕋 👔	& ☴ ☴	Θ Θ	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 ¹	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	_										
		 Tertification 	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														

Stap 6. Exporteren van het servercertificaat/de certificeringsketen uit de CUCM PCAP

In dit voorbeeld wordt alleen het servercertificaat weergegeven. U dient het servercertificaat dus te onderzoeken. Klik met de rechtermuisknop op het servercertificaat en selecteer **Packet Bytes exporteren** om op te slaan als .cer-certificaat, zoals weergegeven in de afbeelding:

File Edit View Go Capture Analyze	Statistics Telephony	Wireless Tools Help						
🔟 🔳 🖉 💿 📴 🛅 🔀 🖻 🔍 👄 🖛	> 🕾 T 🕹 📃 🔳	ଇ୍ପ୍ର୍ 🎹						
📕 tis						+		
No. Time 122 09:09:25.304369 124 09:09:25.329331 125 09:09:25.331128 126 09:09:25.333417 127 09:09:25.335730	Source 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.164	Destination 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.164	Protocol I TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2	Length I 845 5 255 0 173 0 199 A 167 A	Expand Subtrees Collapse Subtrees Expand All Collapse All			
128 09:09:25.339000 129 09:09:25.339649 Frame 122: 845 bytes on wire (676 Ethernet II, Src: Vmware_a5:74:26 Internet Protocol Version 4, Src:	10.201.218.163 10.201.218.164 50 bits), 845 bytes a (00:50:56:a5:74:2 : 10.201.218.164, D	10.201.218.164 10.201.218.163 captured (6760 bits) a), Dst: Vmware_07:23: st: 10.201.218.163	TLSv1.2 TLSv1.2 17 (00:0c:29	327 A 167 A 9:07:23	Apply as Column Apply as Filter Prepare as Filter Conversation Filter Colorize with Filter			
<pre>> Transmission Control Protocol, Sr > [3 Reassembled TCP Segments (367)</pre>	rc Port: 636, Dst P 5 bytes): #118(1448	ort: 34726, Seq: 2897,), #120(1448), #122(77	Ack: 248, 1 9)]	Len: 77	Follow	· ·		
 Transport Layer Security TLSv1.2 Record Layer: Handshak Content Type: Handshake (22 Vaccion: TLS 1.2 (0x0202) 	Transport Layer Security TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages Content Type: Handshake (22) Export Packet Bytes Ctrl+Shift+X							
Version: TLS 1.2 (0x0303) Wiki Protocol Page Length: 3670 Wiki Protocol Page > Handshake Protocol: Server Hello Filter Field Reference Handshake Protocol: Certificate Protocol Preferences								
Length: 1481 Decode As Certificates Length: 1478 Go to Linked Packet Certificates (1478 bytes) 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								

• Typ in het volgende venster een .cer-bestandsnaam en klik vervolgens op Opslaan. Het bestand dat werd opgeslagen (in dit geval naar het bureaublad) werd server cert.cer genoemd, zoals in de afbeelding weergegeven:

	126 00.00.25 222417	10 201 210 162	10, 201, 2	Organize 🔻 ivev	w tolde	er			•	•
	127 09:09:25.335730 128 09:09:25.339000	10.201.218.163 10.201.218.164 10.201.218.163	10.201.2	This PC	^		No items match your se	earch.		
	129 09:09:25.339649	10.201.218.164	10.201.2	Desktop	1					
	Frame 122: 845 bytes on wire (67	60 bits), 845 bytes c	aptured (6	Documents						
>	Ethernet II, Src: Vmware_a5:74:2	a (00:50:56:a5:74:2a)	, Dst: Vmw	👆 Downloads	- 64					
>	Internet Protocol Version 4, Src Transmission Control Protocol, S	: 10.201.218.164, Dst rc Port: 636, Dst Por	: 10.201.2 t: 34726,	👌 Music						
>	[3 Reassembled TCP Segments (367	5 bytes): #118(1448),	#120(1448	Pictures						
ľ	Transport Layer Security			📑 Videos						
	 TLSv1.2 Record Layer: Handshal Content Type: Handshake (22) 	ke Protocol: Multiple 2)	Handshake	🎬 Windows (C:)						
	Version: TLS 1.2 (0x0303)	,		i Network	¥					
	> Handshake Protocol: Server	Hello		File name:	server	rcert.cer				~
	✓ Handshake Protocol: Certific Handshake Type: Certific	icate		Save as type:	Raw d	ata (*.bin *.dat *.raw)				~
	Length: 1481 Certificates Length: 147	78		∧ Hide Folders				Save	Cancel	1
	✓ Certificates (1478 bytes Certificate Length: 1	;) 475	l							
	> Certificate: 308205bf	308204a7a003020102021	3620000000	26295e487… (id-at-	-commo	onName=WIN-H2Q74S1U39P.r	etwork218.com)			

Stap 7. Open het opgeslagen CER-bestand om de inhoud te onderzoeken

Dubbelklik op het .cer-bestand om de informatie te onderzoeken in de tabbladen **Algemeen**, **Details** en **certificaatpad**, zoals in de afbeelding weergegeven:



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.