Cómo exportar certificados TLS de la captura de paquetes de CUCM (PCAP)

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Exportar certificado TLS de CUCM PCAP Verificación Troubleshoot

Introducción

Este documento describe el procedimiento para exportar un certificado desde un PCAP de Cisco Unified Communications Manager (CUCM).

Colaborado por Adrian Esquillo, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas: Apretón de manos · Transport Layer Security (TLS) Administración de certificados de CUCM · Servidor · Secure File Transport Protocol (SFTP) Herramienta de supervisión en tiempo real de · (RTMT)

Aplicación · Wireshark

Componentes Utilizados

·CUCM versión 9.X y posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se puede exportar un certificado de servidor/cadena de certificado para confirmar que la cadena de certificado del servidor proporcionada por el servidor coincide con los certificados que se van a

cargar o que se cargan en CUCM Certificate Management.

Como parte del intercambio de señales TLS, el servidor proporciona su cadena de certificado/certificado del servidor a CUCM.

Exportar certificado TLS de CUCM PCAP

Paso 1. Iniciar el comando de captura de paquetes en CUCM

Establezca una conexión Secure Shell (SSH) al nodo CUCM y ejecute el comando **utils network capture (o capture-rotate) file <filename> count 1000000 size ALL**, como se muestra en la imagen:

х

PuTTY 10.201.218.163 - PuTTY



Paso 2. Iniciar una conexión TLS entre el servidor y CUCM

En este ejemplo, se inicia una conexión TLS entre un servidor Secure Lightweight Directory Access Protocol (LDAPS) y CUCM mediante el establecimiento de una conexión en el puerto TLS 636, como se muestra en la imagen:

Infultion Cisco Unified CM Administration CISCO 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 Group Access Control Group Feature Group Template < None > Warning: If no template is selected, the new line features below will not be active. Add to Access Control Group Remove from Access Co	
Add DN Pool	
-LDAP Server Information	
Host Name or IP Address for Server* LDAP Port* Use TLS WIN-H2Q74S1U39P.network218.com 636 Image: Comparison of the server	
Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

Paso 3. Detener CUCM PCAP después de que se complete el intercambio de señales TLS

Presione Control-C para detener la captura de paquetes, como se muestra en la imagen



Paso 4. Descargue el archivo de captura del empaquetador por cualquiera de los dos métodos enumerados

1. Inicie el nodo RTMT para CUCM y navegue hasta **System > Tools > Trace > Trace & Log Central > Collect Files** y marque la casilla **Packet Capture Logs** (continúe con el proceso RTMT para descargar el pcap), como se muestra en la imagen:

Collect Files			23							
Select System Services/Applications										
Select all Services on all Servers										
Name	All Servers	cucmpub216.network	k 🗌 imp216.network2							
FIFSLOgs			E							
Host Resources Agent			<u> </u>							
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		Ľ								
Prog Logs										
SAR Logs										
SELinux logs										
SNMP Master Agent										
Security Logs										
Service Manager										
Service Registration Logs										
Spooler Logs			2000							
System Application Agent										
< Bac	k Next>	Finish Cancel								

2. Inicie un servidor de protocolo seguro de transporte de archivos (SFTP) y en la sesión de CUCM SSH ejecute el comando **file get activelog /patform/cli/<pcap filename>.cap** (siga con las indicaciones para descargar el PCAP en el servidor SFTP), como se muestra en la imagen:



Paso 5. Determinar el número de certificados presentados a CUCM por el servidor

Utilice la aplicación Wireshark para abrir el pcap y filtrar en **tls** para determinar el paquete con **Server Hello** que contiene la cadena de certificado/certificado del servidor presentado a CUCM. Esta es la trama 122, como se muestra en la imagen:

File	Edit View Go Capture	Analyze Statistics Telephony W	Vireless Tools Help								
A.	I 🖉 🛞 📙 🛅 🔀 ট I	९ ⇔ ⇒ ≅ ₹ ₺ 📮 🗏 €									
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						
<					····· >						
> F	rame 122: 845 bytes on w	vire (6760 bits), 845 bytes ca	ptured (6760 bits))							
> 6	thernet II, Src: Vmware	a5:74:2a (00:50:56:a5:74:2a),	Dst: Vmware 07:2	3:17 (00:0c:2	9:07:23:17)						
> 1	internet Protocol Version	4, Src: 10.201.218.164, Dst:	10.201.218.163								
> 1	ransmission Control Prot	tocol, Src Port: 636, Dst Port	: 34726, Seq: 2893	7, Ack: 248,	Len: 779						
>	[3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]										

> Transport Layer Security

•Expanda la información **Transport Layer Security > Certificate** del paquete Hello del servidor con el certificado para determinar el número de certificados presentados a CUCM. El certificado superior es el certificado del servidor. En este caso, sólo se presenta un certificado, el certificado del servidor, como se muestra en la imagen:

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												
	✓ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages														
	Content Type: Handshake (22)														
	Version: TLS 1.2 (0x0303)														
	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														

Paso 6. Exportar la cadena de certificado/certificado del servidor desde CUCM PCAP

En este ejemplo, sólo se presenta el certificado del servidor, por lo que debe examinar el certificado del servidor. Haga clic con el botón derecho del ratón en el certificado del servidor y seleccione **Exportar bytes de paquete** para guardar como un certificado .cer, como se muestra en la imagen:

File Edit View	Go Capture Analyze	Statistics Telephony	Wireless Tools Help					
	🛅 🔀 🔂 🍳 👄 🗉	> 🕾 🗿 🕹 📃 📃	0.0.0.1					
📕 tls						×	+	
No. Time 122 09:09:21 125 09:09:22 126 09:09:22 127 09:09:22 128 09:09:22 129 09:09:22	.304369 .329331 .331128 .333417 .335730 .339000 .339649 bytes on wire (67	Source 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.164 10.201.218.164 10.201.218.164 60 bits). 845 bytes	Destination 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.164 10.201.218.163 Captured (6760 bits)	Protocol TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2	Length I 845 5 255 C 173 C 199 A 167 A 327 A 167 A	Expand Subtrees Collapse Subtrees Expand All Collapse All Apply as Column Apply as Filter Prepare as Filter	Ctrl+Shift+I	
 > Ethernet II, S > Internet Proto > Transmission (> [3 Reassembled > Transport Laye 	> Frame 122: 645 bytes on wire (6766 bits), 645 bytes captured (6766 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 Conversation Filter > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163 Follow > Transmission Control Protocol, Src Port: 636, Dst Port: 34726, Seq: 2897, Ack: 248, Len: 77 Follow [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)] Copy							
Y TLSV1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages Show Packet Bytes Ctrl+Shift+O Content Type: Handshake (22) Export Packet Bytes Ctrl+Shift+X Version: TLS 1.2 (0x0303) Export Packet Bytes Ctrl+Shift+X Handshake Protocol: Server Hello Filter Field Reference Filter Field Reference								
Handshake Type: Certificate (11) Length: 1481 Certificates Length: 1478 V Certificates (1478 bytes) Certificate Length: 1475 > Certificate: 308205bf308204a7a00302010202136200000026295e487 (id-at-commonName=WIN-H2Q74S1U39P.network218.com)								
> Handshake Protocol: Certificate Request > Handshake Protocol: Server Hello Done								

•En la ventana siguiente, proporcione un nombre de archivo .cer y, a continuación, haga clic en guardar. El archivo que se guardó (en este caso, en el escritorio) se denominó servercert.cer, como se muestra en la imagen:

	126 00.00.25 222417	10 201 210 162	10 201 2	Organize 🔻 ive	w tolde	er			•	•
	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	20 Objects			No items match yours	carcii		
	129 09:09:25.339649	10.201.218.164	10.201.2	J SD Objects	_					
				📃 Desktop						
Ē	Frame 122: 845 bytes on wire	(6760 bits), 845 bytes o	aptured (6	🔮 Documents						
	Ethernet II, Src: Vmware_a5:7	4:2a (00:50:56:a5:74:2a)	, Dst: Vmw	👆 Downloads						
E	Internet Protocol Version 4, :	Src: 10.201.218.164, Dst	: 10.201.2	Music						
	3 Reassembled TCP Segments (3675 bytes): #118(1448).	#120(1448	Pictures						
	 Transport Layer Security 			Videos						
L	 TLSv1.2 Record Layer: Hand Content Type: Handshake 	shake Protocol: Multiple (22)	Handshake	🔛 Windows (C:)						
L	Version: TLS 1.2 (0x0303	3)		鹶 Network	~					
L	Length: 3670									_
L	> Handshake Protocol: Serv	ver Hello		File name:	server	rcert.cer				~
L	✓ Handshake Protocol: Cert	tificate		Save as type:	Raw d	ata (*.bin *.dat *.raw)				\sim
L	Handshake Type: Certi	ificate (11)								
L	Length: 1481	1470		A Hide Folders				Save	Cancel	
L	Certificates Length:	14/8		r filder ofders						
	✓ certificates (14/8 by Contificate Longth)	/tes)	L							
	Certificate Length	1; 1473 NShf308204=7=003020102021	3620000000	06205e487 (id.at.	- c ommo	onName-UTN_H2074S1U30D	atwork218 com)			
	/ certificate: 50620	501505204a7800502010202	13020000000	202556407 (10-at-	- comme	511Valle=W1V-1/2Q/451059P.1	(COM) (210.COM)			

Paso 7. Abrir el archivo .CER guardado para examinar el contenido

Haga doble clic en el archivo .cer para examinar la información en las fichas **General**, **Detalles** y **Ruta de certificado**, como se muestra en la imagen:



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.