Como exportar o certificado TLS da captura de pacote (PCAP) do CUCM

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Exportar certificado TLS do CUCM PCAP Verificar Troubleshoot

Introduction

Este documento descreve o procedimento para exportar um certificado de um PCAP do Cisco Unified Communications Manager (CUCM).

Contribuído por Adrian Esquillo, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos: Handshake de TLS (Transport Layer Security) CUCM Certificate Management Servidor Secure File Transport Protocol (SFTP) Real-time Monitoring Tool (RTMT)

Wireshark Application

Componentes Utilizados

CUCM versão 9.X e superior

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Uma cadeia de certificado/certificado do servidor pode ser exportada para confirmar se a cadeia de certificado/certificado do servidor fornecida pelo servidor corresponde ao(s) certificado(s) a ser

carregado(s) ou que é carregado(s) no CUCM Certificate Management.

Como parte do handshake TLS, o servidor fornece sua cadeia de certificado/certificado do servidor ao CUCM.

Exportar certificado TLS do CUCM PCAP

Etapa 1. Iniciar o comando de captura de pacote no CUCM

Estabeleça uma conexão Secure Shell (SSH) com o nó CUCM e execute o comando **utils network capture (ou capture-rotate) file <filename> count 100000 size ALL**, como mostrado na imagem:



Etapa 2. Iniciar uma conexão TLS entre o servidor e o CUCM

Neste exemplo, você inicia uma conexão TLS entre um servidor Secure Lightweight Diretory Access Protocol (LDAPS) e o CUCM estabelecendo uma conexão na porta TLS 636, como mostrado na imagem:

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 贅 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 in one was not created based on a synced LDAP telephone number Order DN Pool Start DN Pool End Add DN Pool	
Host Name or IP Address for Server* LDAP Port* Use TLS WIN-H2Q74S1U39R.network218.com 636 Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

Etapa 3. Parar a PCAP do CUCM após a conclusão do handshake TLS

Pressione Control-C para interromper a captura de pacotes, como mostrado na imagem



Etapa 4. Baixe o arquivo de captura do pacote por qualquer um dos dois métodos listados

1. Inicie RTMT para o nó CUCM e navegue até System > Tools > Trace > Trace & Log Central > Collect Files e marque a caixa Packet Capture Logs (continue pelo processo RTMT para fazer o download do pcap), como mostrado na imagem:

Collect Files					23						
Select System Services/Applications											
Select all Services on all Servers											
Name		All Serve	ers	cucmpub216.network	. 🗌 imp216.network2						
FIFS LOUS											
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				V							
Prog Logs											
SAR Logs											
SELinux logs					0000						
SNMP Master Agent					00000						
Security Logs					00000						
Service Manager					00000						
Service Registration Logs					00000						
Spooler Logs					00000						
System Application Agent											
< E	Back	Next >	Finish	Cancel							

2. Inicie um servidor Secure File Transport Protocol (SFTP) e, na sessão CUCM SSH, execute o **arquivo de** comando **get ativelog /patform/cli/<pcap filename>.cap** (continue através dos prompts para baixar o PCAP no servidor SFTP), como mostrado na imagem:



Etapa 5. Determine o número de certificados apresentados ao CUCM pelo servidor

Utilize o aplicativo Wireshark para abrir o pcap e filtrar em **tls** para determinar o pacote com **Servidor Hello** que contém o certificado/cadeia de certificado do servidor apresentado ao CUCM. Este é o quadro 122, como mostrado na imagem:

File	Edit View Go Capture A	nalyze Statistics Telephony	Wireless Tools Help									
Æ.	🔳 🔬 💿 📘 🛅 🗙 🛅 🔍	⇔⇒≊₹∮₫ 📃 🕻	e e e									
	tls											
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							
<					···· · · · · · · · · · · · · · · · · ·							
>	Frame 122: 845 bytes on wir	e (6760 bits), 845 bytes c	aptured (6760 bits))								
> 1	Ethernet II, Src: Vmware_a5	:74:2a (00:50:56:a5:74:2a)	, Dst: Vmware_07:23	3:17 (00:0c:2	9:07:23:17)							
> :	Internet Protocol Version 4	, Src: 10.201.218.164, Dst	: 10.201.218.163									
> '	Transmission Control Protoc	ol, Src Port: 636, Dst Por	t: 34726, Seq: 2893	7, Ack: 248,	Len: 779							
>	3 Reasembled TCP Segments (3575 bytes): #118(1448), #122(779)]											

> Transport Layer Security

•Expanda as informações **Transport Layer Security > Certificate** do pacote Server Hello com certificado para determinar o número de certificados apresentados ao CUCM. O certificado superior é o certificado do servidor. Nesse caso, apenas 1 certificado, o certificado do servidor, é apresentado como mostrado na imagem:

File	Edit	View Go	Captu	re A	nalyze	Stati	istics	Teleph	nony	Wireless	Tools	Help											
		•	🗙 🖸	9	÷ =	> 🖻	Ŷ	₺ 📃		କ୍କ୍	Q 🎹												
	tls																X		+				
No.		Time				Sour	ce			Desti	nation			Protocol	Length	Info			^				
+	122	09:09:25.3	04369			10.	201.	218.16	4	10.2	01.218	.163		TLSv1.2	845	Server Hello, Cert	ificate, Serve	n k					
	124	09:09:25.3	29331			10.	201.	218.16	3	10.2	01.218	.164		TLSv1.2	255	Certificate, Clien	t Key Exchange	, C					
	125	09:09:25.3	31128			10.	201.	218.16	4	10.2	01.218	.163		TLSv1.2	173	Change Cipher Spec	, Encrypted Ha	nds					
	126	09:09:25.3	33417			10.	201.	218.16	3	10.2	01.218	.164		TLSv1.2	199	Application Data							
	127	09:09:25.3	35730			10.	201.	218.16	4	10.2	01.218	.163		TLSv1.2	167	Application Data							
	128	09:09:25.3	39000			10.	201.	218.16	3	10.2	01.218	.164		TLSv1.2	327	Application Data							
	129	09:09:25.3	39649			10.	201.	218.16	4	10.2	01.218	.163		TLSv1.2	167	Application Data			~				
<																		>	1				
>	Frame	122: 845 b	ytes or	n wir	e (676	50 bi	ts),	845 b	ytes	capture	d (676	0 bits)											
>	Etherr	net II, Src	: Vmwar	re_a5	:74:2a	a (00	:50:	56:a5:	74:2a	a), Dst:	Vmwar	e_07:23	:17	(00:0c:	29:07:	23:17)							
>	Interr	net Protoco	l Versi	ion 4	, Src:	: 10.3	201.	218.16	4, Ds	t: 10.2	01.218	.163											
>	Transm	ission Con	trol Pr	rotoc	ol, Sr	nc Po	rt:	636, D	st Po	ort: 347	26, Se	q: 2897	, Ac	k: 248,	Len:	779							
>	[3 Rea	ssembled T	CP Seg	nents	(3675	5 byt	es):	#118(1448)	, #120(1448),	#122(7	79)]										
~	Fransp	ort Layer	Securit	ty																			
	✓ TLS	v1.2 Record	d Layer	: Har	ndshak	ce Pro	otoc	ol: Mul	ltipl	e Hands	hake Me	essages											
		Content Typ	be: Han	dshak	ke (22	.)																	
		Version: Tl	S 1.2	(0x03	303)																		
		Length: 367	70																				
	>	Handshake F	Protoco	1: Se	erver	Hello)																
	~	Handshake F	Protoco	1: Ce	ertifi	cate																	
		Handshak	се Туре	: Cer	tific	ate (11)																
		Length:	1481																				
		Certific	ates L	ength	147	8																	
		✓ Iertific	ates (1478	bytes)																	
		Certi	ficate	Leng	th: 14	475																	
		> Certi	ficate	: 308	205bf	30820	4a7a	003020	10202	2136200	000026	295e487	/… (i	d-at-co	mmonNa	me=WIN-H2074S1U39P.	network218.com	1)					
	>	Handshake F	Protoco	1: Se	erver	Key E	Excha	ange															
	>	Handshake F	Protoco	1: Ce	ertifi	cate	Requ	uest															
	>	Handshake F	rotoco	1: Se	erver	Hello	Dor	ne				Wition Protocol Length Info 1.218.163 TLSv1.2 845 Server Hello, Certificate, Server 1.218.163 TLSv1.2 255 Certificate, Client Key Exchange, (1.218.163 TLSv1.2 173 Change Cipher Spec, Encrypted Hands 1.218.163 TLSv1.2 199 Application Data 1.218.163 TLSv1.2 167 Application Data 1.218.163 6, Seq: 2897, Ack: 248, Len: 779 448), #122(779)] ake Messages Ake Messages Ake Messages											

Etapa 6. Exportar a cadeia de certificado/certificado do servidor do CUCM PCAP

Neste exemplo, somente o certificado do servidor é apresentado, portanto é necessário examinar o certificado do servidor. Clique com o botão direito do mouse no certificado do servidor e selecione **Exportar bytes de pacote** para salvar como um certificado .cer, como mostrado na imagem:

File Edit View Go Capture Analyze	Statistics Telephony	Wireless Tools Help								
🛋 🔳 🙋 🛞 📴 🛅 🔀 🖻 🔍 👄 🛋	> 😫 🗿 🕹 📃 📃	ର୍ ପ୍ 🛛 🎹								
📕 tis						×				
No. Time 122 09:09:25.304369 124 09:09:25.329331 125 09:09:25.331128 126 09:09:25.333417 127 00:09:25	Source 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.163	Destination 10.201.218.163 10.201.218.164 10.201.218.163 10.201.218.164 10.201.218.164	Protocol TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2 TLSv1.2	Length I 845 5 255 0 173 0 199 A 167 0	Expand Subtrees Collapse Subtrees 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	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 Colorize with Filter > Transmission Control Protocol, Src Port: 636, Dst Port: 34726, Seg: 2897, Ack: 248, Len: 77 Follow										
> [3 Reassembled TCP Segments (367)	5 bytes): #118(1448), #120(1448), #122(77	9)]		Сору	•				
 Transport Layer Security TLSv1.2 Record Layer: Handshak Content Type: Handshake (22 Varior: TLS 1.2 (4x8303) 	e Protocol: Multip)	Le Handshake Messages			Show Packet Bytes Export Packet Bytes	Ctrl+Shift+O Ctrl+Shift+X				
Version: ILS 1.2 (0x0303) Length: 3670 > Handshake Protocol: Server Hello > Handshake Protocol: Certificate Handshake Protocol: Certificate (11) Handshake Trotocol Preferences										
Length: 1481 Certificates Length: 1478 Certificates (1478 bytes) Certificate Length: 1475 Certificate Length: 1475 Certificate Length: 1475										
Certificate: 308205bf308204a7a003020102021362000000026295e487 (id-at-commonName=WIN-H2Q74S1U39P.network218.com) Handshake Protocol: Server Key Exchange Handshake Protocol: Certificate Request Handshake Protocol: Server Hello Done										

Na janela subsequente, forneça um nome de arquivo .cer e clique em salvar. O arquivo que foi salvo (neste caso, na área de trabalho) foi chamado servercert.cer, como mostrado na imagem:

	115 051051251551120	10120112101101	10120112	Organize 🔻	ivew toid	er			- ·	U
I	126 09:09:25.333417	10.201.218.163	10.201.2		^					
I	127 09:09:25.335730	10.201.218.164	10.201.2	💻 This PC			No items match y	our search.		
I	128 09:09:25.339000	10.201.218.163	10.201.2	3D Object						
I	129 09:09:25.339649	10.201.218.164	10.201.2		-					
	<			📃 Desktop						
ľ	> Frame 122: 845 bytes on wire	(6760 bits), 845 bytes (aptured (6	🔮 Document	ts					
I	> Ethernet II, Src: Vmware_a5:74	4:2a (00:50:56:a5:74:2a), Dst: Vmw	👆 Download	s					
I	> Internet Protocol Version 4,	Src: 10.201.218.164, Dst	t: 10.201.2	👌 Music						
I	> Transmission Control Protocol	, Src Port: 636, Dst Por	rt: 34726,	Pictures						
I	> [3 Reassembled TCP Segments (36/5 bytes): #118(1448),	, #120(1448							
L	 Transport Layer Security 			Videos						
I	✓ TLSv1.2 Record Layer: Hands	shake Protocol: Multiple	e Handshake	🎬 Windows	(C:)					
I	Content Type: Handshake	(22)								
L	Version: TLS 1.2 (0x0303	(1		💣 Network	\checkmark					
I	Length: 3670									
L	> Handshake Protocol: Serv	/er Hello		File nan	ne: serve	ercert.cer				~
l	Ƴ Handshake Protocol: Cert	ificate		Save as ty	e: Raw o	data (*.bin *.dat *.raw)				\sim
I	Handshake Type: Certi	ficate (11)								
I	Length: 1481								-	
I	Certificates Length:	1478		 Hide Folders 				Save	Cancel	
I	✓ Certificates (1478 by	tes)	L							
I	Certificate Length	: 1475								
	> Certificate: 30820	5bf308204a7a00302010202	13620000000	26295e487… (id-	at-comm	ionName=WIN-H2Q74S1U	<pre>J39P.network218.com)</pre>			

Passo 7. Abra o arquivo .CER salvo para examinar o conteúdo

Clique duas vezes no arquivo .cer para examinar as informações nas guias **Geral**, **Detalhes** e **Caminho do certificado**, como mostrado na imagem:



Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.