CUCMパケットキャプチャ(PCAP)からTLS証明 書をエクスポートする方法

内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>CUCM PCAPからのTLS証明書のエクスポート</u> <u>確認</u> トラブルシュート

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)PCAPから証明書をエク スポートする手順について説明します。

著者: Cisco TACエンジニア、Adrian Esquillo

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Transport Layer Security(TLS)ハンドシェイク
- CUCM証明書管理
- ・セキュアファイル転送プロトコル(SFTP)サーバ
- ・リアルタイム監視ツール(RTMT)

・ Wiresharkアプリケーション

使用するコンポーネント

・ CUCMリリース9.X以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

サーバ証明書/証明書チェーンは、サーバから提供されたサーバ証明書/証明書チェーンが、アップ

ロードする証明書またはCUCM証明書管理にアップロードされた証明書と一致することを確認す るためにエクスポートできます。

TLSハンドシェイクの一部として、サーバはサーバ証明書/証明書チェーンをCUCMに提供します。

CUCM PCAPからのTLS証明書のエクスポート

ステップ1:CUCMでpacket captureコマンドを開始します

CUCMノードへのセキュアシェル(SSH)接続を確立し、図に示すように、utils network capture (or capture-rotate) file <filename> count 1000000 size ALLコマンドを実行します。

 \times

10.201.218.163 - PuTTY



ステップ2:サーバとCUCM間のTLS接続を開始します

この例では、図に示すように、TLSポート636で接続を確立することで、Secure Lightweight Directory Access Protocol(LDAPS)サーバとCUCM間のTLS接続を開始します。

Juluin, Cisco Unified CM Administration	Navigation Cisco Unified CM Administration V Go
For Lisco Unitied Communications Solutions	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 Add to 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-	
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	

ステップ3:TLSハンドシェイク完了後にCUCM PCAPを停止する

図に示**すように、Control-C**を押してパケットキャプチャを停止します

Putty 10.201.218.163 - Putty	-	\times
2 login as: admin 2 admin@10.201.218.163's password: Command Line Interface is starting up, please wait		
Welcome to the Platform Command Line Interface		
<pre>VMware Installation: 2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz Disk 1: 80GB, Partitions aligned 4096 Mbytes RAM</pre>		
admin:utils network capture file servercert count 1000000 size A	LL	
size=ALL count=100000 interface=eth0 src= dest= port= ip=		
Control-C pressed		
admin:		

ステップ4:次の2つの方法のいずれかでパッカーキャプチャファイルをダウンロードします

1. CUCMノードのRTMTを起動し、[**System] > [Tools] > [Trace] > [Trace & Log Central] > [Collect Files]に移動し、[Packet Capture Logs]ボックスをオンにします**(pcapをダウンロードするには RTMTプロセスをします)。

Collect Files			23							
Select System Services/Applications										
Select all Services on all Servers										
Name	All Serve	rs Cucmpub2	16 network 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		Ľ								
Prog Logs										
SAR Logs										
SELinux logs										
SNMP Master Agent										
Security Logs										
Service Manager										
Service Registration Logs										
Spooler Logs										
System Application Agent										
•			99900099 ·							
< Bac	k Next>	Finish Cancel								

2. SFTP (Secure File Transport Protocol)サーバを起動し、CUCM SSHセッションで**file get activelog /patform/cli/<pcap filename>.capコマンドを実行します(プロンプトに従ってSFTPサーバ にPCAPをダウンロードしま**す)。



ステップ5:サーバがCUCMに提示する証明書の数を決定する

Wiresharkアプリケーションを使用してpcapを開き、**tlsでフィルタを実行**し、CUCMに提示されるサーバ証明書/証明書チェーンを含む**Server Hello**パケットを判別します。これは、図に示すように、フレーム122です。

a l					
<u> </u>			લ લ લ જ		
📕 tł	s				
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,
	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 wi	re (6760 bits), 845 bytes	captured (6760 bits)		
> E	thernet II, Src: Vmware a	5:74:2a (00:50:56:a5:74:2a), Dst: Vmware 07:23	:17 (00:0c:2	29:07:23:17)
> 1	nternet Protocol Version	4, Src: 10.201.218.164, Ds	t: 10.201.218.163		

> Transmission Control Protocol, Src Port: 636, Dst Port: 34726, Seq: 2897, Ack: 2
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]

> Transport Layer Security

・ CUCMに提示される証明書の数を確認するには、証明書を含むServer Helloパケットから [Transport Layer Security] > [Certificate]の情報を展開します。一番上の証明書はサーバ証明書で す。この場合、サーバ証明書である1つの証明書だけが図のように表示されます。

Fil	e Edit	View Go	Capture	Analyze	Statistics	Telephony	Wire	less Tools	; Help								
		O	🗙 🖸 🤇	۹ ⇔ ⇒	🕋 👔	& 📃 🔳	•	ຊ 🔍 🎹									
	tls														×→	-	+
No.		Time			Source		0	estination		1	Protocol	Length	Info				^
÷	122	09:09:25.30	04369		10.201.	218.164	1	0.201.218	3.163	1	TLSv1.2	845	Server Hello, Cert	ificate, S	Server k		
Г	124	09:09:25.32	29331		10.201.	218.163	1	0.201.218	3.164	1	TLSv1.2	255	Certificate, Clier	nt Key Exch	nange, (
	125	09:09:25.33	31128		10.201.	218.164	1	0.201.218	3.163	1	TLSv1.2	173	Change Cipher Spec	, Encrypte	ed Hands		
	126	09:09:25.33	33417		10.201.	218.163	1	0.201.218	3.164	1	TLSv1.2	199	Application Data				
	127	09:09:25.33	35730		10.201.	218.164	1	0.201.218	3.163	1	TLSv1.2	167	Application Data				
	128	09:09:25.33	39000		10.201.	218.163	1	0.201.218	3.164	1	TLSv1.2	327	Application Data				
	129	09:09:25.33	39649		10.201.	218.164	1	0.201.218	3.163	1	TLSv1.2	167	Application Data				¥
<															>		
>	Frame	122: 845 bv	tes on wi	ire (6760) bits).	845 bytes	capt	ured (676	0 bits)								
Ś	Ethern	et II. Src:	Vmware a	a5:74:2a	(00:50:	56:a5:74:2	a). D	st: Vmwar	e 07:23	:17	(00:0c:	29:07:	23:17)				
5	Intern	et Protocol	Version	4. Src:	10.201.	218.164. D	st: 1	0.201.218	3.163		(
5	Transm	ission Cont	rol Proto	ocol. Sro	Port:	636, Dst P	ort:	34726, Se	a: 2897	. Acl	k: 248.	Len:	779				
>	[3 Rea	ssembled TC	P Segment	ts (3675	bytes):	#118(1448), #1	20(1448),	#122(7	- 79)1	- 1						
~	Fransp	ort Layer S	ecurity							1							
	✓ TLS	v1.2 Record	Layer: H	landshake	Protoc	ol: Multipl	le Ha	ndshake M	essages								
		Content Type	e: Handsh	ake (22)					-								
		Version: TLS	5 1.2 (0x	:0303)													
	1	Length: 3670	0														
	> 1	Handshake Pr	rotocol:	Server H	ello												
	~ 1	Handshake Pi	rotocol:	Certific	ate												
		Handshake	e Type: C	ertifica	te (11)												
		Length: 1	1481														
		Certifica	ates Leng	th: 1478													
		✓ Iertifica	ates (147	8 bytes)													
		Certif	ficate Le	ngth: 14	75												
		> Certif	ficate: 3	08205bf3	08204a7a	0030201020	21362	000000020	5295e487	/… (i	d-at-co	mmonNa	me=WIN-H2074S1U39P	network218	3.com)		
	>	Handshake Pr	rotocol:	Server K	ey Exch	ange											
	>	Handshake Pr	rotocol:	Certific	ate Req	uest											
	>	Handshake Pr	rotocol:	Server H	ello Do	ne											

ステップ6:CUCM PCAPからサーバ証明書/証明書チェーンをエクスポートします

この例では、サーバ証明書だけが示されているため、サーバ証明書を調べる必要があります。図 に示すように、サーバ証明書を右クリックし、[Export Packet Bytes]を選択して.cer証明書として 保存します。

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
	▝▖᠅᠅≌ᆥᢧ▁▁							
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 10.201.218.163	Protocol Length TLSv1.2 845 TLSv1.2 255 TLSv1.2 173 TLSv1.2 199 TLSv1.2 167	Expand Subtrees Collapse Subtrees Expand All Collapse All				
128 09:09:25.339000 10.201.218.163 10.201.218.164 TLSv1.2 327 f 129 09:09:25.339649 10.201.218.164 10.201.218.163 TLSv1.2 167 f Apply as Filter Prepare as Filter > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits) Fease 10:201.218.164, Dst: 10.201.218.163 Prepare as 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								
<pre>> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)] > Transport Layer Security > TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 3670 > Handshake Protocol: Server Hello</pre>								
 Handshake Protocol: Certificate Handshake Type: Certificate (11) Length: 1481 Certificates Length: 1478 Certificates (1478 bytes) Certificate Length: 1475 								
<pre>> Certificate: : > Handshake Protocol: > Handshake Protocol: > Handshake Protocol: > Handshake Protocol:</pre>	308205bf308204a7a00302010202 Server Key Exchange Certificate Request Server Hello Done	21362000000026295e487	. (id-at-commonNam	e=WIN-H2Q74S1U39P.network2	18.com)			

・後続のウィンドウで、.cerファイル名を入力し、[保存]をクリックします。次の図に示すように 、デスクトップに保存されたファイルの名前はservercert.cerです(この場合はデスクトップに保 存されます)。

		10120112101101		Urganize 🔻 🛛 i	New TOIC	ber			•	U
	126 09:09:25.33341/	10.201.218.163	10.201.2	_	^					
	12/ 09:09:25.335/30	10.201.218.164	10.201.2	💻 This PC			No items match your se	arch.		
	128 09:09:25.339000	10.201.218.163	10.201.2	🗊 3D Objects						
	129 09:09:25.339649	10.201.218.164	10.201.2	Dealstern						
<				Desktop						
>	Frame 122: 845 bytes on wire ((6760 bits), 845 bytes o	aptured (6	Documents	5					
>	Ethernet II, Src: Vmware_a5:74	1:2a (00:50:56:a5:74:2a)	, Dst: Vmw	👆 Downloads						
>	Internet Protocol Version 4, S	örc: 10.201.218.164, Dst	: 10.201.2	Music						
>	Transmission Control Protocol,	Src Port: 636, Dst Por	t: 34726,	- Distance						
>	[3 Reassembled TCP Segments (3	8675 bytes): #118(1448),	#120(1448	Pictures						
۲	Transport Layer Security			😽 Videos						
	✓ TLSv1.2 Record Layer: Hands	hake Protocol: Multiple	Handshake	🕮 Windows (C:)					
	Content Type: Handshake	(22)								
	Version: TLS 1.2 (0x0303)		💣 Network	~					
1	Length: 3670									
	> Handshake Protocol: Serve	er Hello		File nam	e: serve	ercert.cer				~
	✓ Handshake Protocol: Cert	ificate		Save as typ	e: Raw	data (*.bin *.dat *.raw)				\sim
	Handshake Type: Certi	ficate (11)				,,				
	Length: 1481								-	
	Certificates Length: 1	1478		 Hide Folders 				Save	Cance	1
	✓ Certificates (1478 by	tes)	L						_	
	Certificate Length:	: 1475								
	> Certificate: 308205	5bf308204a7a003020102021	136200000002	6295e487 (id-a	at-comm	nonName=WIN-H2Q74S1U39P	.network218.com)			
						•	,			

ステップ7:保存した.CERファイルを開いて内容を確認する

.cerファイルをダブルクリックして、[General]、[Details]、および[Certificate Path]タブの情報を 確認します(図を参照)。



確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。