طلتخملا عضولا نم CUCM ةعومجم رييغت مت نمآلا ريغ عضولا نيوكت لاثم ىلإ

المحتويات

<u>المتطلبات الأساسية</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> معلومات أساسية <u>التكوين</u> <u>تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام عميل CTL تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام LLD (واجهة سطر الأوامر) <u>التحقق من الصحة</u> مجموعة CUCM إلى وضع الأمان - المجموع الاختباري لملف <u>CTL</u> مجموعة MDUD إلى الوضع غير الآمن - محتوى ملف <u>CTL</u> مجموعة MDUD إلى الوضع غير الآمن - محتوى ملف <u>CTL</u> مع أمان مجموعة MUDD من الوضع المختلط إلى الوضع غير الآمن عند فقد رموز USB المميزة إستكشاف الأخطاء واصلاح<u>ه</u>ا</u>

المقدمة

يصف المستند الخطوات المطلوبة لتغيير وضع أمان Cisco Unified Communications Manager (CUCM) من الوضع المختلط إلى الوضع غير الآمن. كما تظهر كيفية تغيير محتوى ملف قائمة الشهادات الموثوق بها (CTL) عند اكتمال عملية النقل هذه.

هناك ثلاثة أجزاء رئيسية لتغيير وضع أمان CUCM:

1 أ. قم بتشغيل عميل CTL وحدد المتغير المرغوب في وضع الأمان. 1 مليا. دخلت ال CLI أمر in order to حددت ال مرغوب مختلف من أمن أسلوب. 2. إعادة تشغيل خدمات Cisco CallManager و Cisco TFTP على جميع خوادم CUCM التي تشغل هذه الخدمات. 3. قم إعادة تشغيل كلفة هواتف IP حتي تتمكن من تنزيل الام دار المحدث من ماف CTT

3. قم بإعادة تشغيل كافة هواتف IP حتى تتمكن من تنزيل الإصدار المحدث من ملف CTL.

ملاحظة: إذا تم تغيير وضع أمان نظام المجموعة من الوضع المختلط إلى الوضع غير الآمن، يظل ملف CTL موجودا على الخادم (الخوادم) وعلى الهواتف، ولكن ملف CTL لا يحتوي على أية شهادات CCM+TFTP (الخادم). بما أن شهادات CCM+TFTP (الخادم) غير موجودة في ملف CTL، فإن هذا يفرض على الهاتف التسجيل على أنه غير آمن باستخدام CUCM.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من CUCM صيغة 10.0(1) أو فيما بعد. بالإضافة إلى ذلك، تأكد من:

- خدمة "موفر CTL" قيد التشغيل على كافة خوادم TFTP النشطة في نظام المجموعة. تعمل الخدمة بشكل افتراضي على منفذ TCP 2444، ولكن يمكن تعديل هذا في تكوين معلمة خدمة CUCM.
 - خدمات "وظيفة وكيل المرجع المصدق" (CAPF) قيد التشغيل على عقدة Publisher.
- يعمل النسخ المتماثل لقاعدة البيانات (DB) في نظام المجموعة بشكل صحيح، كما تقوم الخوادم بنسخ البيانات في الوقت الفعلي.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مجموعة الإصدار 10.0.1.11900-2 من عقدتين
- هاتف بروتوكول الإنترنت Cisco 7975 IP Phone (مسجل مع بروتوكول التحكم في المكالمات Skinny Call (SCCP (SCCP75.9-3-1SR3-1S)، إصدار البرنامج الثابت SCCP75.9-3-1SR3-1S)
 - يلزم وجود علامتي أمان من Cisco لتعيين نظام المجموعة على الوضع المختلط
 - من الضروري وجود إحدى رموز الأمان المدرجة سابقا لتعيين نظام المجموعة على الوضع غير الآمن

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

لتشغيل المكون الإضافي لعميل CTL، يلزم توفر وصول إلى رمز أمان واحد على الأقل تم إدخاله لإنشاء أحدث ملف CTL أو تحديثه على خادم CUCM Publisher. بمعنى آخر، يجب أن تكون شهادة واحدة على الأقل من شهادات eToken الموجودة في ملف CTL الحالي على CUCM على الرمز المميز للأمان الذي يتم إستخدامه لتغيير وضع الأمان.

التكوين

تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام عميل CTL

أكمل الخطوات التالية لتغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام عميل CTL:

- 1. احصل على رمز أمان واحد قمت بإدراجه لتكوين أحدث ملف CTL.
- 2. قم بتشغيل عميل CTL. قم بتوفير اسم/عنوان IP الخاص ب CUCM PUB وبيانات اعتماد مسؤول CCM. انقر فوق Next (التالي).

Cn (CTL Client v5.0			
	Cisco CTL Cl For IP Telephony Solution	ient	cisco	
	Cisco Unified Communicatio	ns Manager Server		
	Hostname or IP Address:	10.48.47.153	Port: 24	144
	Username:	admin		
	Password:	yolololololok		
	<u>H</u> elp		<u>C</u> ancel	Next

3. انقر على الزر **تعيين مجموعة Cisco Unified CallManager على** لاسلكي **وضع غير آمن**. انقر فوق Next (التالي).

CrL Client v5.0	
Cisco CTL Client	
Cluster Security Mode	
C Set Cisco Unified CallManager Cluster to Mixed Mode	
Set Cisco Unified CallManager Cluster to Non-Secure Mode	,
C Update CTL File	
Help	Next

4. قم بإدراج رمز مميز واحد للأمان تم إدراجه لتكوين أحدث ملف CTL وانقر فوق **موافق**. هذا أحد الرموز المميزة التي تم إستخدامها لملء قائمة الشهادات في



؛. يتم عرض تعاصيل الرمز المميز للاما (**التالي)**.

C _n (CTL Client v5.0	
	Cisco CTL Ch For IP Telephony Solutions	ent altalta cisco
	Security Token Information	
	Subject Name:	cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Sy:
	Issuer Name:	cn=Cisco Manufacturing CA;o=Cisco Systems
	Valid From:	06/09/2010
	Expires on:	06/09/2020
	Help	Cancel Next

6. يتم عرض محتوى ملف CTL. انقر فوق **إنهاء**. عندما يطلب منك كلمة المرور، دخلت **Cisco123**.

💪 CTL Client v5.0						
Cis For	ico CTL C IP Telephony Solutio	lient	1	haha Isco		
CTLEntries						
Type CAPF CCM+TFTP CCM+TFTP Security T Security T	Hostname/I 10.48.47.153 10.48.47.154 10.48.47.153 — No Hostna — No Hostna	Issuer Nam CN=CAPF-e — No Issue — No Issue cn=Cisco M cn=Cisco M	e 9037b69;OU r Name — anufacturing anufacturing	Subject N CN=CAPF — No Sub — No Sub cn="SAST cn="SAST	ame e9037b69;OU=T oject Name — oject Name — T-ADN008580ef T-ADN0054f509	
Help	Add	TFTP	Add Fire	wall		
Cancel	Add	Tokens	Delete Se	lected	Finish	

7. يتم عرض قائمة خوادم CUCM الموجودة عليها ملف CTL. طقطقة **تم**.

C_n	TL Client v5.0			×
	Cisco For IP Tele	CTL Chent ephony Solutions	cisco	
Г	Server	File Location	Status	
	10.48.47.153	/usr/local/cm/tftp/CTLFile.tlv	Passed	
	10.48.47.154	/usr/local/cm/tttp/CTLFile.tiv	Passed	
	You must resta Cluster.	rt all the Cisco Unified Communicati	ions Manager and Tf	-TP nodes in the
	Help			Done
وضع	لمجموعة على الو	Enterprise وتحقق من تعيين نظام اا	< CUCM > معلمات بر	أختر صفحة إدارة System غير الآمن ("0" يشير إلى غ
			-	آمن).

-Security Parameters	
Cluster Security Mode *	0
LBM Security Mode *	Insecure T
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True 🔻

- 9. قم بإعادة تشغيل خدمات TFTP و Cisco CallManager على جميع العقد في نظام المجموعة التي تقوم بتشغيل هذه الخدمات.
- 10. قم بإعادة تشغيل جميع هواتف IP حتى تتمكن من الحصول على الإصدار الجديد من ملف CTL من CUCM TFTP.

تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن باستخدام CLI (واجهة سطر الأوامر)

هذا التكوين خاص فقط ب CUCM الإصدار x.10 والإصدارات الأحدث. من أجل تعيين وضع أمان نظام المجموعة CUCM على غير آمن، أدخل الأمر utils set-cluster non-secure-mode على واجهة سطر الأوامر (CLI) الخاصة ب Publisher. بعد اكتمال هذا الإجراء، قم بإعادة تشغيل خدمات TFTP و Cisco CallManager على جميع العقد في نظام المجموعة التي تقوم بتشغيل هذه الخدمات.

وفيما يلي نموذج إخراج واجهة سطر الأوامر (CLI) الذي يظهر إستخدام الأمر.

admin:**utils ctl set-cluster non-secure-mode** :(This operation will set the cluster to non secure mode. Do you want to continue? (y/n Moving Cluster to Non Secure Mode Cluster set to Non Secure Mode Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that run these services

admin

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من CTLFIle.tlv، يمكنك إستخدام إحدى الطريقتين:

- للتحقق من المحتوى والجملة الاختبارية MD5 الخاصة ب CTLFIIe.tlv الموجودة على جانب CUCM TFTP، أدخل الأمر show ctl على واجهة سطر الأوامر (CLI) الخاصة ب CUCM. يجب أن يكون ملف CTLFIIe.tlv هو نفسه في جميع عقد CUCM.
- للتحقق من المجموع الاختباري MD5 على هاتف IP 7975، أختر **الإعدادات > تكوين الأمان > قائمة الثقة > ملف** CTL.

ملاحظة: عند التحقق من المجموع الاختباري عبر الهاتف، ستري MD5 أو SHA1، معتمدا على نوع الهاتف.

مجموعة CUCM إلى وضع الأمان - المجموع الاختباري لملف CTL

```
admin:show ct1
The checksum value of the CTL file:
98784f6f6bcd5019ea165b1d2bc1372e(MD5)
(SHA1) 9c0aa839e5a84b18a43caf9f9ff23d8ebce90419
(SHA1) [...]
على جانب هاتف IP، يمكنك أن ترى أنه يحتوي على نفس ملف CTL المثبت (يطابق المجموع الاختباري MD5 عند
مقارنته بمخرجات CUCM).
```



مجموعة CUCM إلى الوضع غير الآمن - محتوى ملف CTL

فيما يلي مثال على ملف CTL من مجموعة CUCM تم تعيينها إلى الوضع غير الآمن. يمكنك أن ترى أن شهادات CCM+TFTP فارغة ولا تحتوي على أي محتوى. لا يتم تغيير بقية الشهادات الموجودة في ملفات CTL وهي تماما نفسها كما هو الحال عندما تم تعيين CUCM إلى الوضع المختلط.

> admin:show ctl :The checksum value of the CTL file (7879e087513d0d6dfe7684388f86ee96(MD5 (be50e5f3e28e6a8f5b0a5fa90364c839fcc8a3a0(SHA1 Length of CTL file: 3746 The CTL File was last modified on Tue Feb 24 16:37:45 CET 2015 Parse CTL File _____ Version: 1.2 (HeaderLength: 304 (BYTES BYTEPOS TAG LENGTH VALUE _____ ____ SIGNERID 2 117 3 SIGNERNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems 4 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45 5 CANAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems 6 SIGNATUREINFO 2 15 7 DIGESTALGORTITHM 1 8 SIGNATUREALGOINFO 2 8 9 SIGNATUREALGORTITHM 1 10 SIGNATUREMODULUS 1 11 SIGNATURE 128 12 ec 5 c 9e 68 6d e6 45 5d 4b d3 91 c2 26 cf c1 ee 8c b9 6 95 46 67 9e aa b1 e9 65 af b4 67 19 7e e5 ee 60 10 b 1b 36 c1 6 64 40 cf e2 57 58

aa 86 73 14 ec 11 b a 3b 98 91 e2 e4 6e 4 50 ba ac 3e 53 33 1 3e a6 b7 30 0 18 ae 68 3 39 d1 41 d6 e3 af 97 55 e0 5b 90 f6 a5 79 3e 23 97 fb b8 b4 ad a8 b8 29 7c 1b 4f 61 6a 67 4d 56 d2 5f 7f 32 66 5c b2 d7 55 d9 ab 7a ba 6d b2 20 6 FILENAME 12 14 TIMESTAMP 4 15 CTL Record #:1 ____ BYTEPOS TAG LENGTH VALUE ----- ----- ----RECORDLENGTH 2 1186 1 DNSNAME 1 2 SUBJECTNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems 3 FUNCTION 2 System Administrator Security Token 4 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems 5 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45 6 PUBLICKEY 140 7 (CERTIFICATE 902 19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2 CC 6D 93 90 (SHA1 Hash HEX 9 IPADDRESS 4 10 .This etoken was used to sign the CTL file CTL Record #:2 BYTEPOS TAG LENGTH VALUE ----- ---- ---- -----RECORDLENGTH 2 1186 1 DNSNAME 1 2 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems 3 FUNCTION 2 System Administrator Security Token 4 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems 5 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31 6 PUBLICKEY 140 7 (CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93 3E 8B 3A 4F (SHA1 Hash HEX 9 IPADDRESS 4 10 .This etoken was not used to sign the CTL file CTL Record #:3 BYTEPOS TAG LENGTH VALUE ----- ---- ----RECORDLENGTH 2 33 1 DNSNAME 13 10.48.47.153 2 FUNCTION 2 CCM+TFTP 4 IPADDRESS 4 10 CTL Record #:4 ____ BYTEPOS TAG LENGTH VALUE _____ ____ RECORDLENGTH 2 1004 1 DNSNAME 13 10.48.47.153 2 SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL 3 FUNCTION 2 CAPF 4 ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL 5 SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31 6 PUBLICKEY 140 7 (CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX 9

IPADDRESS 4 10

```
CTL Record #:5
BYTEPOS TAG LENGTH VALUE
RECORDLENGTH 2 33 1
DNSNAME 13 10.48.47.154 2
FUNCTION 2 CCM+TFTP 4
IPADDRESS 4 10
```

.The CTL file was verified successfully

:admin

على جانب هاتف Pl، بعد إعادة تشغيله وتنزيله إصدار ملف CTL المحدث، يمكنك أن ترى أن المجموع الاختباري MD5 يتطابق عند مقارنته بخرج CUCM.



ضع أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن عند فقد رموز USB المميزة

قد تفقد رموز الأمان المميزة للمجموعات الآمنة. في تلك الحالة، عليك أن تفكر في هذين السيناريوهين:

يقوم نظام المجموعة بتشغيل الإصدار 10.0.1 أو إصدار أحدث

• يقوم نظام المجموعة بتشغيل إصدار أقدم من x.10

في السيناريو الأول، أكمل الإجراء الموضح في <u>تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع غير الآمن</u> <u>باستخدام</u> قسم <u>واجهة سطر الأوامر</u> (<u>CL</u>) من أجل التعافي من المشكلة. بما أن أمر واجهة سطر الأوامر (CLI) لا يتطلب رمز CTL المميز، فيمكن إستخدامه حتى إذا تم وضع نظام المجموعة في الوضع المختلط مع عميل CTL.

ويصبح الوضع أكثر تعقيدا عندما يكون إصدار أقدم من x.10 من CUCM قيد الاستخدام. إذا فقدت أو نسيت كلمة مرور أحد الرموز المميزة، لا يزال بإمكانك إستخدام الكلمة الأخرى لتشغيل عميل CTL مع ملفات CTL الحالية. يوصى بشدة بالحصول على رمز مميز آخر وإضافته إلى ملف CTL في أقرب وقت ممكن من أجل التكرار. إذا فقدت أو نسيت كلمات المرور الخاصة بجميع الرموز المميزة المدرجة في ملف CTL الخاص بك، فإنك بحاجة إلى الحصول على زوج جديد من الرموز الإلكترونية وتشغيل إجراء يدوي كما هو موضح هنا.

1. أدخل الأمر file delete tftp ctifile.tiv لحذف ملف CTL من جميع خوادم TFTP.

admin:file delete tftp CTLFile.tlv
?Delete the File CTLFile.tlv
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1
admin:show ctl
Length of CTL file: 0
$\ldots \mbox{CTL}$ File not found. Please run CTLClient plugin or run the CLI - utils ctl
.to generate the CTL file
.Error parsing the CTL File

2. قم بتشغيل عميل CTL. دخلت ال ip hostname/address من ال CUCM PUB وال CCM مسؤول ورقة اعتماد. انقر فوق **Next**

C _{en}	CTL Client v5.0			(التالي) ــــــــــــــــــــــــــــــــــــ
	Cisco CTL Cl For IP Telephony Solution	ient	ahaha cisco	
	Cisco Unified Communicatio	ns Manager Server		1
	Hostname or IP Address:	10.48.47.153	Port: 2444	
	Username:	admin		
	Password:	jolololololok		
	<u>H</u> elp		<u>C</u> ancel <u>N</u> ext	

3. بما أن نظام المجموعة في الوضع المختلط، إلا أنه لا يوجد ملف CTL على Publisher، يتم عرض هذا التحذير. طقطقة **ok** in order to تجاهلت هو ومضت قدما.

CTLClient	×
	No CTL File exists on the server but the Call Manager Cluster Security Mode is in Secure Mode. For the system to function, you must create the CTL File and set Call Manager Cluster to Secure Mode.
	OK

	٬ . ۱. انقر فوق الزر انتقاء تحديث ملف CTL . انقر فوق Next
CTL Client v5.0	
Cisco CTL Chier For IP Telephony Solutions	nt ahala cisco
Cluster Security Mode	
C Set Cisco Unified CallMan	nager Cluster to <u>M</u> ixed Mode
C Set Cisco Unified CallMan	nager Cluster to N <u>o</u> n-Secure Mode
Opdate CTL File	
<u>H</u> elp	<u>Cancel N</u> ext
	(التالي).

5. يطلب عميل CTL إضافة رمز مميز للأمان. طقطقة **يضيف** in order to

Chent	ahaha cisco
cn=''SAST-ADN0054f50a	";ou=IPCBU;o="Cisi
cn=Cisco Manufacturing CA	a;o=Cisco Systems
06/08/2010	
06/08/2020	
<u>C</u> a	ncel Add
	Chient Solutions

6. تعرض الشاشة كافة الإدخالات في CTL الجديد. انقر فوق **إضافة العلامات المميزة** لإضافة الرمز المميز الثاني من الزوج

💪 CTL Client v5.0				
Cis For	COCTLChe	ent	ahaha cisco	
CTL Entries				1
Type Hostname/ Issuer Name CAPF 10.48.47.153 CN=CAPF-e9037b69;0U= CCM+TFTP 10.48.47.154 CN=cucm-1001-a-sub1;0 CCM+TFTP 10.48.47.153 CN=cucm-1001-a-pub;0U Security To No Host cn=Cisco Manufacturing C			Subject Name CN=CAPF-e9037t CN=cucm-1001-a CN=cucm-1001-a cn=''SAST-ADN0	
<u>H</u> elp	Add TFTP	<u>A</u> dd Firewall		
<u>C</u> ancel	<u>A</u> dd Tokens	Delete Selected	<u> </u>	حديد

7. ستتم مطالبتك بإزالة الرمز المميز الحالي وإدخال رمز مميز جديد. طقطقة ok ما إن



8. يتم عرض شاشة تظهر تفاصيل الرمز المميز الجديد. طقطقة **يضيف** in order to أكدت هم وأضفت هذا الرمز

econy roken monitati	on
ubject Name:	cn="SAST-ADN008580ef";ou=IPCBU;o="Cisi
suer Name:	cn=Cisco Manufacturing CA;o=Cisco Systems
alid From:	05/17/2012
xpires on:	05/17/2022

9. سيتم تقديم قائمة جديدة بإدخالات CTL التي تظهر كلا الشارات المميزة المضافة. انقر فوق **إنهاء** لإنشاء ملفات CTL

CTL Client v5.0							
Cisco CTL For IP Telephony Sol	Client allalla utions cisco						
CTL Entries							
Type Hostname/I Is CAPF 10.48.47.153 C CCM+TFTP 10.48.47.154 C CCM+TFTP 10.48.47.153 C CCM+TFTP 10.48.47.153 C Security To No Hostn c Security To No Hostn c	Issuer NameSubject NameN=CAPF-e9037b69;0U=CN=CAPF-e9037N=cucm-1001-a-sub1;0UCN=cucm-1001-aN=cucm-1001-a-pub;0U=CN=cucm-1001-an=Cisco Manufacturing Ccn=''SAST-ADN0n=Cisco Manufacturing Ccn=''SAST-ADN0						
	D Add Firewall						
<u><u>A</u>dd TFT <u>C</u>ancel <u>A</u>dd Toke</u>	ns <u>D</u> elete Selected <u>F</u> inish						
جديدة. 10. في حقل كلمة مرور الرمز المميز، أدخل Cisco123. وانقر فوق OK.							
Token Logon SafeNet. SafeNet Authentication Client							
Enter the Token Password.							
Token Name:	eToken PRO						
Token Password:	••••••						
This is an unlicensed copy for ev	Current Language: EN valuation use only.						
	OK Cancel						

۔ 11. سُتری تأکیدا علی نجاح العملیة. انقر فوق **تم** لتأکید عمیل CTL والخروج

For IP 1	D CIL Chent Telephony Solutions	CISCO
Server 10.48.47.153	File Location /usr/local/cm/tftp/CTLFile.tlv	Status Passed
10.48.47.154	/usr/local/cm/tftp/CTLFile.tlv	Passed
4		•
		ager and TETP nodes in
You must restart the Cluster.	all the Cisco Unified Communications Mana	ager and in the nodes in

12. قم بإعادة تشغيل Cisco TFTP متبوعة بخدمة CallManager (الخدمة الموحدة من Cisco > أدوات > مركز التحكم - خدمات الميزات). يجب إنشاء ملف CTL الجديد. أدخل الأمر show ctl للتحقق. admin:show_ctl

:The	checksum	value	of	the	CTL	file
(68a954	4fba070bbc	cc3ff03	36e1	8716	5e351	.(MD5
(4f7a02b60bb5083	3baac46110)f0c61e	eac2	2dceb	o0f7(SHA1

Length of CTL file: 5728 The CTL File was last modified on Mon Mar 09 11:38:50 CET 2015

- 13. احذف ملف CTL من كل هاتف في المجموعة (قد يختلف هذا الإجراء بناء على نوع الهاتف يرجى مراجعة الوثائق للحصول على تفاصيل، مثل <u>هاتف بروتوكول الإنترنت الموحد طراز 8961 و 9971 و 9971 من</u> (<u>Cisco</u>).**ملاحظة**: قد تظل الهواتف قادرة على التسجيل (اعتمادا على إعدادات الأمان على الهاتف) والعمل دون متابعة الخطوة 13. ومع ذلك، سيتم تثبيت ملف CTL القديم. قد يتسبب ذلك في حدوث مشاكل في حالة إعادة إنشاء الشهادات أو في إضافة خادم آخر إلى نظام المجموعة أو في إستبدال أجهزة الخادم. لا يوصى بترك المجموعة في هذه الحالة.
 - 14. نقل نظام المجموعة إلى نظام غير آمن. راجع <u>تغيير أمان مجموعة CUCM من الوضع المختلط إلى الوضع</u> <u>غير الآمن باستخدام</u> قسم <u>عميل CTL</u> للحصول على تفاصيل.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما