

VCS بيو هجاولى لىع TLS ةحفاصم لشف

المحتويات

[المقدمة](#)

[المشكلة](#)

[الحل](#)

المقدمة

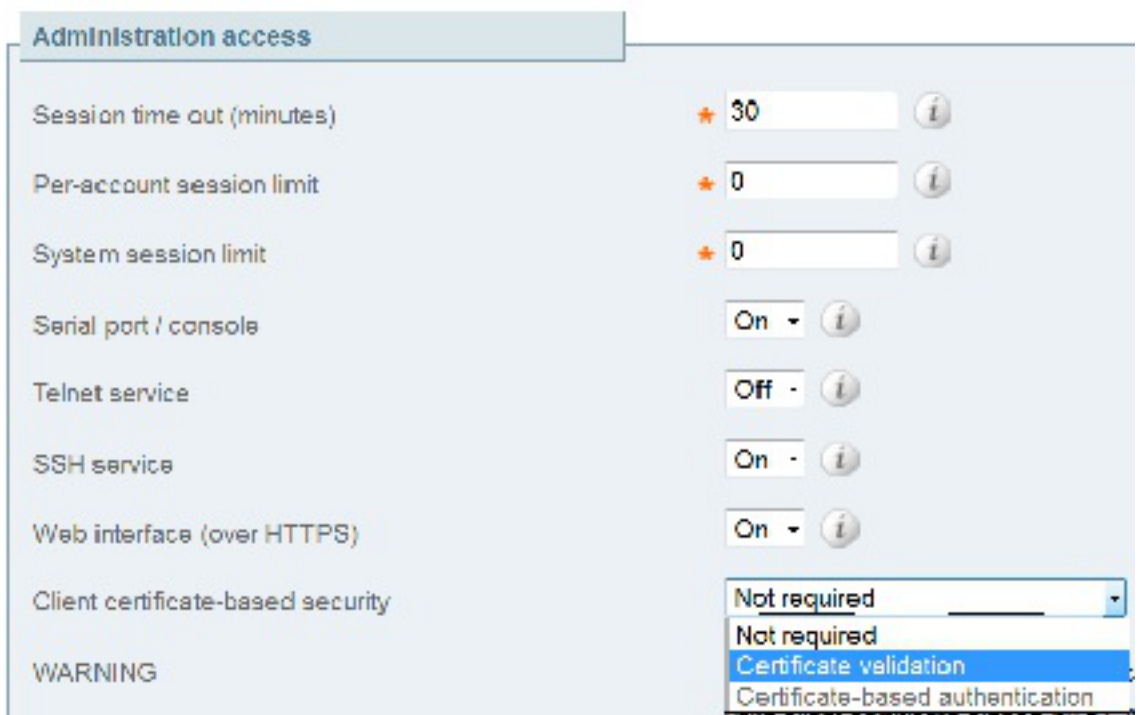
يستخدم Cisco Video Communication Server (VCS) شهادات العميل لعملية المصادقة والتحويل. هذه الميزة مفيدة للغاية لبعض البيئات، لأنها تتيح طبقة إضافية من الأمان ويمكن استخدامها لأغراض تسجيل الدخول الأحادي. ومع ذلك، في حالة تكوينه بشكل غير صحيح، فإنه يمكن قفل المسؤولين خارج واجهة ويب VCS.

يتم استخدام الخطوات الواردة في هذا المستند لتعطيل الأمان المستند إلى شهادة العميل على Cisco VCS.

المشكلة

إذا تم تمكين الأمان المستند إلى شهادة العميل على محول VCS وتم تكوينه بشكل غير صحيح، فقد لا يتمكن المستخدمون من الوصول إلى واجهة ويب VCS. تقابل محاولات الوصول إلى واجهة الويب بإخفاق مصافحة أمان طبقة النقل (TLS).

هذا التشكيل تغير أن يطلق الإصدار:



الحل

أكمل الخطوات التالية لتعطيل الأمان المستند إلى شهادة العميل وإعادة النظام إلى حالة يتمكن فيها المسؤولون من الوصول إلى واجهة الويب الخاصة بـ VCS:

1. اتصل بـ ال VCS كجذر عن طريق (SSH Secure Shell).

2. أدخل هذا الأمر كجذر حتى تتمكن من ترميز Apache لرمز ثابت لعدم استخدام الأمان المستند إلى شهادة العميل:

```
echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
```

ملاحظة: بعد إدخال هذا الأمر، ال VCS يستطيع لا يكون reconfiguration لـ Zon baser أمن إلى أن يحذف ال removecba.conf مبرد إلى أن أعدت ال VCS.

3. أنت ينبغي أعدت ال VCS in order to هذا تشكيل تغير أن يأخذ تأثير. عندما يكون أنت جاهز لإعادة تشغيل ال VCS، دخلت هذا الأمر:

```
tshell
```

```
xcommand restart
```

ملاحظة: يؤدي هذا إلى إعادة تشغيل VCS وإسقاط جميع المكالمات/التسجيلات.

بمجرد إعادة تحميل VCS، يتم تعطيل الأمان المستند إلى شهادة العميل. غير أنه ليس معطلا بطريقة مرغوبة. سجل الدخول إلى VCS باستخدام حساب مسؤول القراءة والكتابة. انتقل إلى النظام < صفحة النظام على VCS.



Cisco TelePresence Video (

Status	System	VCS configuration	Appli
Overview	System		
System info	Ethernet		
System name	IP		
Up time	Quality of Service		
Software version	DNS		
IPv4 addresses	Time		
Options	Login page		
Resource usage	SNMP		
Non-traversal	External manager		
	TMS Provisioning Extension services		
	Firewall rules		

في صفحة إدارة النظام الخاصة بـ VCS، تأكد من تعيين الأمان المستند إلى شهادة العميل على "غير مطلوب":

Administration access

Session time out (minutes)	★ 30	i
Per-account session limit	★ 0	i
System session limit	★ 0	i
Serial port / console	On -	i
Telnet service	Off -	i
SSH service	On -	i
Web interface (over HTTPS)	On -	i
Client certificate-based security	Certificate validation -	
Certificate revocation list (CRL) checking	Not required	
	Certificate validation	
	Certificate-based authentication	

بمجرد إجراء هذا التغيير، احفظ التغييرات.

5. ما إن يتم، دخلت هذا أمر كجذر في SSH in order to أعادت ضبط Apache إلى عادي:

```
rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
```

تحذير: إذا تخطت هذه الخطوة، فلن تتمكن أبدا من إعادة تمكين الأمان المستند إلى شهادة العميل.

6. قم بإعادة تشغيل VCS مرة أخرى للتحقق من عمل الإجراء. الآن بعد أن أصبح لديك الوصول إلى ويب، يمكنك

إعادة تشغيل VCS من واجهة الويب تحت الصيانة < إعادة التشغيل.

تهانينا! يتم الآن تشغيل VCS الخاص بك مع تعطيل الأمان المستند إلى شهادة العميل.