Webex Call Survivability Gateway Certificate Series Compatibility إصدار

المحتويات

مسألة

عند تكوين الاتصال المستمر عبر Webex وتمكين وضع الاختبار في Control Hub، تفشل السلوك show voice register session المأمور بالعرض. لا يعرض Webex Cloud. البوابة في المزامنة مع خوادم التسجيل الموقوف، كما يعرض Control Hub حالات فشل المزامنة.

تعرض سجلات تتبع الاستخدام هذه الخطأ أثناء محاولات المزامنة:

```
2026-08-12T19:22:58.745Z - ERROR - Thread-5 (handle_sgw_events) - wxcc_sgw_manager : TELEMETRYLOG : WxC
```

يفشل البوابة في إنشاء اتصال TLS آمن مع Webex Cloud للموقع الذي تم تكوينه، مما يمنع المزامنة والتسجيل السليم لعبارة البقاء.

البيئة

- Webex Call Survivability Gateway Configuration
- برنامج IOS XE، الإصدار 17.12.6
- شهادات GoDaddy TLS المثبتة على البوابة
- سلسلة الشهادات باستخدام GoDaddy TLS Intermediate CA DV - R1v1
- تكوين إستمرارية Control Hub مع تمكين وضع الاختبار

قرار

.تم حل هذه المشكلة باستبدال الشهادة بشهادة تستخدم سلسلة مرجع مصدق مدعومة
، كانت الشهادة التي تمثل مشكلة تستخدم سلسلة الشهادات GoDaddy R1v1 الأحدث
.والتي ال تدعمها الأنظمة الأساسية للاتصال عبر Webex

الخطوة 1: التحقق من سلسلة الشهادات الحالية

تحقق من الشهادات المثبتة حاليا على البوابة:

```
device# show crypto pki certificates
```

يعرض الإخراج سلسلة الشهادات الإشكالية:

```
<#root>

                                                    Certificate
                                                Status: Available
                                Certificate Serial Number (hex): 00923AC809A58436DD
                                                Certificate Usage: General Purpose
                                                                    Issuer:


                                                  cn=GoDaddy TLS Intermediate CA DV - R1v1


                                                                  o=GoDaddy.com
                                                                          c=US
                                                                     Subject:
                                                            Name: mhtlc-ls-r1.mhtlc.org


                                                               cn=mhtlc-ls-r1.mhtlc.org


                                                                 CRL Distribution Points:
                                                http://crl.godaddy.com/gdr1v1dv_s1-7.crl
                                                                      Validity Date:
                                                    start date: 13:43:39 CDT Jun 25 2026
                                                     end   date: 12:43:39 CST Jan 9 2027
                                                       Associated Trustpoints: webex-sgw
                                                    Storage: nvram:GoDaddyTLSIn#36DD.cer
```

الخطوة 2: تعريف مشكلة توافق سلسلة الشهادات

قبل GoDaddy TLS Intermediate CA DV - R1v1. الشهادة المتقاطعة (GoDaddy TLS Root CA - R1) والشهادة الجذر (Go Daddy Root Certificate Authority - G2) مفقودة من البوابة.

ال يدعم الاتصال عبر Webex سوى الشهادات التي تحتوي على المرجع الجذري لشهادة "GoDaddy" لكل وثائق رسمية.

- CN=Go Daddy Root Certificate Authority - G2

الخطوة 3: طلب شهادة جديدة مع سلسلة مدعومة

اتصل بموفر الشهادة (GoDaddy) لإعادة مفاتيح الشهادة والتأكد من أنها تستخدم سلسلة الشهادات المدعومة:

- طلب شهادة جديدة لنفس المجال FQDN (mhtlc-ls-r1.mhtlc.org).
- حدد الشهادة يجب أن تستخدم سلسلة الشهادات GoDaddy G2 (SHA-2).
- تأكد من تثبيت جميع الشهادات ذات الصلة لسلسلة ثقة كاملة على موجه SGW.

الخطوة 4: تثبيت الشهادة الجديدة

بمجرد الحصول على الشهادة الجديدة مع سلسلة G2 المدعومة، قم بتثبيتها على بوابة Webex. قم بتكوين نقطة الثقة المناسبة لاتصال إستمرارية النظام.

قم بإجراء هذه الخطوة إذا لم تكن شهادة جذر CA المعروفة بشكل عام متوفرة مع بوابة Cisco IOS XE الخاصة بك.

```
crypto pki trustpoint <CA name>
 enrollment terminal
 revocation-check crl
crypto pki authenticate <CA name>
```

الخطوة 5: التحقق من الدقة

بعد تثبيت الشهادة الجديدة، اختبر تسجيل بوابة القدرة على البقاء:

- مراقبة عملية المزامنة في Control Hub.
- تحقق من التسجيل الناجح من خلال تشغيل الأمر show voice register session.
- تأكد من أن سجلات تتبع الاستخدام لم تعد تعرض حالات فشل اتصال TLS.

السبب

كان السبب الجذري هو عدم توافق سلسلة الشهادات بين بوابة بقابلية البقاء وخدمات GoDaddy لمنطقة سحابة الاتصال عبر Webex. تم تكوين البوابة باستخدام شهادة موقعة من قبل GoDaddy R1 الأحدث. TLS Intermediate CA DV - R1v1، والتي تعد جزءا من سلسلة الشهادات

يدعم الاتصال عبر Webex فقط الشهادات التي تعمل بالتسلسل إلى مرجع شهادات Go Daddy Root - G2. لم يتم تضمين مرجع الشهادة الوسيطة الأحدث R1v1 الذي تم تقديمه من قبل GoDaddy في قائمة مرجع الشهادات الموثوق بها ل Webex Call، مما يتسبب في حدوث حالات فشل في تأكيد اتصال TLS أثناء عملية مزامنة بوابة إستمرارية الاتصال. وبالإضافة إلى ذلك، منعت الشهادة الجذر المفقودة على البوابة التحقق من صحة سلسلة الشهادات بشكل صحيح، مما ساهم في حالات فشل إنشاء الاتصال الآمن.

المحتوى ذي الصلة

- [ما هي السلطات المرجعية المدعومة للمكالمات إلى منصات Cisco WebEx للصوت والفيديو](#)
- [الدعم الفني والتنزيلات من Cisco](#)
- [إستمرارية الموقع للاتصال عبر Webex](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).