حل فشل مزامنة Webex Call Survivability Gateway بسبب سلسلة شهادات GoDaddy غير المدعومة R1

المحتويات

مسألة

تم تسجيل عبارتي Survivability (mcyitsrtr001.centralwire.com وprtitsrtr001.centralwire.com) في Control Hub ولكنهما فشلا في المزامنة؛ ركزت عملية أستكشاف الأخطاء وإصلاحها على رسالة الخطأ: mcyitsrtr001.centralwire.com. فشلت محاولات المزامنة بشكل متناسق مع

```
Sync failed due to internal server error (code - 31117)
```

تمت ملاحظته أول مرة أثناء محاولة مزامنة في 5 أغسطس/آب 2026. كشف تحليل سجلات تتبع بيانات Telemetry و Webex الخلفية (PYLON) أن البوابة كانت تقدم سلسلة شهادات GoDaddy R1v1 (GoDaddy TLS Root CA - R1)، والتي لا تدعمها خدمات Webex، مما تسبب في رفض سلسلة الشهادات وفشل المزامنة.

البيئة

- تم الإبلاغ عن بواباتين مداريتين: mcyitsrtr001.centralwire.com وprtitsrtr001.centralwire.com (يتم التركيز على أستكشاف الأخطاء وإصلاحها mcyitsrtr001.centralwire.com)
- إصدار IOS® XE: 17.12.6 (عقدة SGW)، 17.15.06 (MGW)
- تكوين عبارة البقاء (SGW) من Webex
- سلسلة شهادات GoDaddy TLS باستخدام R1v1 CA الوسيط
- سلسلة الشهادات: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

رارق

تم حل المشكلة عن طريق تنفيذ حل توقيع الشهادات التبادلي لإنشاء مسار شهادة Cross-signed عون من ةعقوملا GoDaddy R1-to-G2 ةدهاش تيبثت لحل نمضت .هب قوثوم لسلاسل التسلسل الهرمي GoDaddy R1 الجديد إلى هيئة شهادة Go Daddy Root الموثوق بها - G2.

✎ ةمدخ لطعتب crypto pki trustPool import clean رمألا ماق ،ةدهاش لا ريغت ءانثأ :ةظحالم NETCONF-YANG/DMI الخاصة بالبوابة، مما أدى إلى قطع اتصال الموصل لفترة وجيزة. تعذر فتح أخذ التوصيل إلى 192.168.217.55:830). تم إستردادا هذا الإجراء من خلال الخطوات من 6 إلى 7 وكان أحد الآثار الجانبية للصيانة، وليس فشل المزامنة الأصلي.

الخطوة 1: تثبيت حزمة TrustPool من Cisco

قم بتثبيت حزمة Cisco TrustPool التي تحتوي على مرجع شهادة Go Daddy Root - G2:

```
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_union.p7b
```

يعمل الاستيراد النظيف على إستبدال تجمع الثقة بالكامل — حيث يمكنه تعطيل الخدمات التي تعتمد عليه (راجع الملاحظة الخاصة ب connector-offline المدرجة سابقا). الاستخدام بعناية.

الخطوة 2: التحقق من شهادة جذر G2

تأكيد أن Go Daddy Root Certificate Authority - G2 موجود:

```
show crypto pki trustpool | include GoDaddy|Go Daddy
```

الخطوة 3: إزالة R1 TrustPoint الموقع ذاتيا

قم بإزالة R1 TrustPoint القديمة ذاتية التوقيع (نعم عند مطالبتك بإزالة الشهادات):

```
no crypto pki trustpoint GoDaddyRootR1
```

الخطوة 4: تثبيت شهادة R1 الموقعة

قم بإنشاء نقطة ثقة جديدة باستخدام شهادة R1 الموقعة من خلال قنوات متعددة (الموضوع: GoDaddy TLS Root CA - R1، المصدر: Go Daddy Root Certificate Authority - G2):

```
crypto pki trustpoint GoDaddyCrossR1
enrollment terminal
revocation-check none
exit
crypto pki authenticate GoDaddyCrossR1
<paste cross-signed R1 PEM – Subject: GoDaddy TLS Root CA - R1, Issuer: Go Daddy Root Certificate Autho
quit
yes
```

الخطوة 5: التحقق من سلسلة الشهادات

تحقق من أن السلسلة قد تم حلها الآن بشكل صحيح:

```
show crypto pki certificates webex-sgw
show crypto pki certificates GoDaddyCrossR1
```

الخطوة 6: إعادة تشغيل خدمات NETCONF

انتظر 60 ثانية تقريبا بين (NETCONF-YANG وخدمات (الترميز) HTTP (مداوخ) خادم التعطيل والتمكين):

```
conf t
no netconf-yang
no ip http secure-server
```

```
no ip http server
end
```

انتظر 60 ثانية، ثم أعد التمكين:

```
conf t
ip http server
ip http secure-server
netconf-yang
end
write memory
```

الخطوة 7: إعادة تحميل البوابة (إذا لزم الأمر)

إذا كان NETconf-YANG لا يزال لا يعمل بشكل صحيح بعد إعادة تشغيل الخدمة، فأعد تحميل الموجه لإعادة تهيئة DMI بالكامل:

```
reload
```

تحذير: ممكن. يبدو أن التفاصيل المذكورة هنا تحتوي على إجراءات أو أوامر قد تتسبب في تأثير كبير إذا تم تنفيذها. يرجى التأكد من أن الإجراءات أو الأوامر المذكورة أعلاه قد تم تقييمها من قبل المؤسسات الصغيرة والمتوسطة أو وحدة الأعمال قبل تنفيذها أو التوصية بها.

الخطوة 8: التحقق من الدقة

بعد عودة البوابة إلى الاتصال، قم بتشغيل إعادة مزامنة SGW من Control Hub وتحقق من إكمال المزامنة بنجاح دون ظهور رسالة رمز الخطأ 31117 أو رسائل "فشل التحقق الموثوق به ل Certificate Server". تم الحل المؤكد — قدمت البوابة سلسلة الأوراق الكاملة → R1v1 → R1 (المصدر G2) وأكملت المزامنة بنجاح بعد حل العلامات التبادلية.

السبب

تم تعريف السبب الجذري على أنه فشل في ثقة الشهادة. Survivability Gateway كانت تقدم سلسلة شهادات باستخدام GoDaddy TLS Root CA - R1 Hierarchy (وتحديدا GoDaddy TLS Intermediate CA DV - R1v1)، والتي لم يتم تضمينها في قائمة مرجع الشهادات الموثوق بها الخاصة ب Webex Call.

عندما قامت Webex Backend (PYLON) بإجراء فحص ثقة شهادة الخادم أثناء طلب معلومات مصادقة SIP، فإنها لم تتمكن من إنشاء مسار شهادة صالح لشهادة جذر موثوق بها. نتج عن ذلك إستثناء SunCertPathBuilderException مع حدوث الخطأ "تعذر العثور على مسار شهادة صالح للهدف المطلوب"، مما تسبب في إستجابة HTTP 400 وإجهاض المزامنة.

يعتمد الاتصال عبر Webex على جذور GoFather/Starfield القديمة فقط (مثل Go Daddy Root Certificate Authority - G2) ولكن ليس التسلسل الهرمي الجديد لـ "GoDaddy TLS" (R1/R1v1).

المحتوى ذي الصلة

- هيئات الترخيص المدعومة لخدمات Webex المختلطة
- مستودع شهادات GoDaddy
- الدعم الفني والتنزيلات من Cisco

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).