Beheben Sie den Synchronisierungsfehler des WebEx Calling Survivability Gateway aufgrund der nicht unterstützten GoDaddy R1-Zertifikatkette.

Inhalt

Problem

Zwei Survivability Gateways (mcyitsrtr001.centralwire.com und prtitsrtr001.centralwire.com) wurden im Control Hub registriert, konnten jedoch nicht synchronisiert werden. Fehlerbehebung mit Schwerpunkt auf mcyitsrtr001.centralwire.com. Synchronisierungsversuche sind konsistent fehlgeschlagen. Fehlermeldung:

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

Erstmals beobachtet während eines Synchronisierungsversuchs am 5. August 2026. Die Analyse von Telemetrie- und WebEx Backend-Protokollen (Pylon) ergab, dass das Gateway eine GoDaddy R1v1-Zertifikatkette (GoDaddy TLS Root CA - R1 Hierarchie) präsentierte, die von den WebEx Services nicht unterstützt wird, sodass die Zertifikatkette abgelehnt wurde und die Synchronisierung fehlschlug.

Umwelt

- Zwei verwaltete Gateways meldeten: mcyitsrtr001.centralwire.com und prtitsrtr001.centralwire.com (Problembehandlung mit Schwerpunkt auf mcyitsrtr001.centralwire.com)
- IOS® XE-Version 17.12.6 (SGW-Knoten), 17.15.06 (MGW)
- Konfiguration des WebEx Calling Survivability Gateway (SGW)

- GoDaddy TLS-Zertifikatskette mit R1v1 Zwischen-CA
- Zertifikatskette: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

Auflösung

Das Problem wurde behoben, indem ein Problemumgehung für die gegenseitige Signierung von Zertifikaten implementiert wurde, um einen vertrauenswürdigen Zertifikatpfad einzurichten. Die Lösung beinhaltete die Installation des GoDaddy R1-to-G2-Zertifikats mit Kreuzsignatur, um die neuere GoDaddy R1-Hierarchie mit der vertrauenswürdigen GoDaddy Root Certificate Authority - G2 - zu ketten.

Anmerkung: Während der Zertifikatänderungen unterbrach der Befehl crypto pki trustpool import clean den NETCONF-YANG/DMI-Dienst des Kabelmodems und nahm den Anschluss kurzzeitig offline. `Der Socket konnte nicht zu 192.168.217.55:830 geöffnet werden`). Dies wurde in den Schritten 6-7 wiederhergestellt und war ein Nebeneffekt der Wartung, nicht der ursprüngliche Synchronisierungsfehler.

Schritt 1: Cisco Trustpool-Paket installieren

Installieren Sie das Cisco TrustPool-Paket, das die Go Daddy Root Certificate Authority - G2 enthält:

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

`import clean` ersetzt den gesamten Trustpool - es kann Dienste stören, die von ihm abhängen (siehe den Connector-Offline-Hinweis weiter oben). Vorsicht bei der Anwendung.

Phase 2: G2-Stammzertifikat überprüfen

Bestätigen Sie, dass Go Daddy Root Certificate Authority - G2 vorhanden ist:

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

Schritt 3: Entfernen des selbstsignierten R1-Vertrauenspunkts

Entfernen Sie den alten selbstsignierten R1-Vertrauenspunkt (antworten Sie mit Ja, wenn Sie aufgefordert werden, Zertifikate zu entfernen):

```
no crypto pki trustpoint GoDaddyRootR1
```

Schritt 4: Quersigniertes R1-Zertifikat installieren

Erstellen Sie einen neuen Vertrauenspunkt mit dem kreuzsignierten R1-Zertifikat (Betreff: GoDaddy TLS Root CA - R1, Aussteller: 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
```

Schritt 5: Zertifikatkette überprüfen

Stellen Sie sicher, dass die Kette nun korrekt aufgelöst wird:

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

Schritt 6: NETCONF-Dienste neu starten

Bounce-HTTP(S)-Server und NETCONF-YANG-Dienste (zwischen Deaktivieren und Aktivieren ca. 60 Sekunden warten):

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

Warten Sie 60 Sekunden, und aktivieren Sie dann erneut:

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

Schritt 7: Gateway neu laden (falls erforderlich)

Wenn NETCONF-YANG auch nach dem Neustart des Services nicht ordnungsgemäß funktioniert, laden Sie den Router neu, um DMI vollständig neu zu initialisieren:

```
reload
```

Vorsicht: Möglich. Die hier genannten Details enthalten offenbar Prozeduren oder Befehle, die bei ihrer Ausführung erhebliche Auswirkungen haben könnten. Stellen Sie sicher, dass die oben genannten Verfahren oder Befehle von einem SME oder einem Geschäftsbereich evaluiert wurden, bevor Sie sie ausführen oder empfehlen.

Schritt 8: Auflösung überprüfen

Wenn das Gateway wieder online ist, lösen Sie eine SGW-Resynchronisierung vom Control Hub aus, und stellen Sie sicher, dass die Synchronisierung ohne Fehlercode 31117 oder die Meldung "Certificate Server Trusted check failed" (Prüfung des vertrauenswürdigen Zertifikatsservers fehlgeschlagen) erfolgreich abgeschlossen wurde. Behoben bestätigt: Das Gateway präsentierte die vollständige Leaf → R1v1 → R1-Kette (Aussteller G2) und die Synchronisierung wurde nach der Umgehung des Vorzeichens erfolgreich abgeschlossen.

Ursache

Die Ursache wurde als Zertifikatvertrauensfehler identifiziert. Das Survivability Gateway präsentierte eine Zertifikatskette unter Verwendung der GoDaddy TLS Root CA - R1 Hierarchie (speziell die GoDaddy TLS Intermediate CA DV - R1v1), die nicht in der Liste der vertrauenswürdigen Zertifizierungsstellen von Webex Calling enthalten ist.

Wenn das WebEx-Backend (pylon) während der SIP-Authentifizierungsinformationsanforderung eine Überprüfung der Server-Zertifikatvertrauensstellung durchgeführt hat, konnte kein gültiger Zertifizierungspfad zu einem vertrauenswürdigen Stammzertifikat erstellt werden. Dies führte zu einer SunCertPathBuilderException mit dem Fehler "cannot to find valid certification path to requested target", wodurch die HTTP 400-Antwort und der Synchronisierungsabbruch verursacht wurden.

WebEx Calling vertraut nur den älteren GoDaddy/Starfield-Wurzeln (z. B. GoDaddy Root Certificate Authority - G2), nicht aber der neueren "GoDaddy TLS"-Hierarchie (R1/R1v1).

Verwandte Inhalte

- Unterstützte Zertifizierungsstellen für WebEx Hybrid Services
- GoDaddy-Zertifikats-Repository
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.