Webex-oproep tot overlevingsgateway-synchronisatiefout oplossen als gevolg van niet-ondersteunde GoDaddy R1-certificaatketen

Inhoud

uitgifte

Twee Survivability Gateways (mcyitsrtr001.centralwire.com en prtitsrtr001.centralwire.com) werden geregistreerd in Control Hub, maar konden niet synchroniseren; probleemoplossing was gericht op mcyitsrtr001.centralwire.com. Synchronisatiepogingen zijn mislukt consistent met de foutmelding:

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

Voor het eerst waargenomen tijdens een synchronisatiepoging op 5 augustus 2026. Analyse van telemetrie en Webex backend (pyloon) logs onthulde dat de gateway een GoDaddy R1v1 certificaatketen (GoDaddy TLS Root CA - R1 hiërarchie) presenteerde, die niet wordt ondersteund door Webex-diensten, waardoor de certificaatketen werd afgewezen en synchronisatie mislukte.

milieu

- Er zijn twee beheerde gateways gemeld: mcyitsrtr001.centralwire.com en prtitsrtr001.centralwire.com (probleemoplossing gericht op mcyitsrtr001.centralwire.com)
- IOS® XE-versie: 17.12.6 (SGW-knooppunt), 17.15.06 (MGW)
- Configuratie van WebEx Calling Survivability Gateway (SGW)
- GoDaddy TLS-certificaatketen met behulp van R1v1 intermediaire CA
- Certificaatketen: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

resolutie

Het probleem is opgelost door een workaround voor cross-signing van certificaten te implementeren om een vertrouwd certificaatpad tot stand te brengen. De oplossing bestond uit het installeren van het GoDaddy R1-to-G2 cross-signed certificaat om de nieuwere GoDaddy R1-hiërarchie te koppelen aan de vertrouwde GoDaddy Root Certificate Authority - G2.

Opmerking: Tijdens de certificaatwijzigingen heeft de crypto pki trustpool import clean opdracht de NETCONF-YANG/DMI-service van de gateway verstoord, waardoor de connector kort offline is. `Kan socket niet openen naar 192.168.217.55:830`). Dit werd hersteld via stappen 6-7 en was een bijwerking van het onderhoud, niet de oorspronkelijke synchronisatiefout.

Stap 1: Cisco Trustpool-bundel installeren

Installeer de Cisco trustpool-bundel die de Go Daddy Root Certificate Authority - G2 bevat:

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

`Schoon importeren` vervangt de volledige vertrouwensgroep — deze kan services die ervan afhankelijk zijn verstoren (zie de eerder vermelde notitie voor connector-offline). Gebruik met zorg.

Stap 2: G2-basiscertificaat verifiëren

Bevestig dat Go Daddy Root Certificate Authority - G2 aanwezig is:

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

Stap 3: Verwijder zelfondertekend R1 Trustpoint

Verwijder het oude zelfondertekende R1-vertrouwenspunt (antwoord ja wanneer u wordt gevraagd om certificaten te verwijderen):

```
no crypto pki trustpoint GoDaddyRootR1
```

Stap 4: kruisondertekend R1-certificaat installeren

Maak een nieuw vertrouwenspunt met het kruisondertekende R1-certificaat (Onderwerp: GoDaddy TLS Root CA - R1, Uitgever: 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
```

Stap 5: Certificaatketen verifiëren

Controleer of de keten nu correct is opgelost:

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

Stap 6: Start NETCONF-services opnieuw op

Bounce HTTP(S)-server en NETCONF-YANG-services (wacht ongeveer 60 seconden tussen uitschakelen en inschakelen):

```
conf t
```

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

Wacht 60 seconden en schakel vervolgens opnieuw in:

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

Stap 7: Gateway opnieuw laden (indien nodig)

Als NETCONF-YANG na het opnieuw opstarten van de service nog steeds niet goed werkt, laadt u de router opnieuw om de DMI volledig te initialiseren:

```
reload
```

Let op: mogelijk. De hier genoemde details lijken procedures of opdrachten te bevatten die aanzienlijke gevolgen kunnen hebben als ze worden uitgevoerd. Controleer of de bovenstaande procedures of opdrachten door een kmo of bedrijfseenheid zijn geëvalueerd voordat u ze uitvoert of aanbeveelt.

Stap 8: Resolutie controleren

Nadat de gateway weer online is, activeert u een SGW-resync vanuit Control Hub en controleert u of de synchronisatie met succes is voltooid zonder foutcode 31117 of "Certificate Server Trusted check failed"-berichten. Bevestigd opgelost — de gateway presenteerde de volledige leaf → R1v1 → R1 (emittent G2)-keten en de synchronisatie is met succes voltooid na de cross-sign-workaround.

Oorzaak

De onderliggende oorzaak werd geïdentificeerd als een fout in de certificaatvertrouwensrelatie. De Survivability Gateway presenteerde een certificaatketen met behulp van de GoDaddy TLS Root CA - R1-hiërarchie (met name de GoDaddy TLS Intermediate CA DV - R1v1), die niet is opgenomen in de vertrouwde certificaatautoriteitslijst van Webex Calling.

Wanneer de Webex-backend (pyloon) tijdens het SIP-verificatieverzoek een vertrouwenscontrole van het servercertificaat uitvoerde, kon er geen geldig certificeringspad naar een vertrouwd basiscertificaat worden gemaakt. Dit resulteerde in een SunCertPathBuilderException met de fout "kan geen geldig certificeringspad naar het aangevraagde doel vinden", waardoor de HTTP 400-respons en synchronisatieabortus werden veroorzaakt.

Webex Calling vertrouwt alleen de oudere GoDaddy / Starfield-wortels (zoals Go Daddy Root Certificate Authority - G2), maar niet de nieuwere "GoDaddy TLS" (R1 / R1v1) hiërarchie.

Gerelateerde inhoud

- Ondersteunde certificeringsinstanties voor Webex Hybrid Services
- GoDaddy Certificate Repository
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.