WebEx roept Survivability Gateway-certificaatketen compatibiliteitsprobleem op

Inhoud

uitgifte

Bij het configureren van Webex Calling Survivability en het inschakelen van de testmodus in de Control Hub, synchroniseert de gateway niet met Webex Cloud-servers. De opdracht Spraakregistersessie tonen geeft niet het verwachte registratiegedrag weer en de Control Hub toont synchronisatiefouten.

De telemetrielogboeken geven deze fout weer tijdens synchronisatiepogingen:

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

De gateway slaagt er niet in om een veilige TLS-verbinding met Webex Cloud tot stand te brengen voor de geconfigureerde locatie, waardoor een goede synchronisatie en registratie van de overlevingsgateway wordt voorkomen.

milieu

- WebEx roept Survivability Gateway-configuratie aan
- IOS XE Software versie 17.12.6
- GoDaddy TLS-certificaten geïnstalleerd op de gateway
- Certificaatketen met GoDaddy TLS Intermediate CA DV - R1v1
- Configuratie van overlevingskansen van controlehub met testmodus ingeschakeld

resolutie

Dit probleem is opgelost door het certificaat te vervangen door een certificaat dat gebruikmaakt van een ondersteunde certificeringsinstantie. Het problematische certificaat maakte gebruik van de nieuwere GoDaddy R1v1-certificaatketen, die niet wordt ondersteund door Webex Calling-platforms.

Stap 1: Verifieer de huidige certificaatketen

Controleer de momenteel geïnstalleerde certificaten op de gateway:

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

De uitvoer geeft de problematische certificaatketen weer:

<#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
```

Stap 2: Probleem met compatibiliteit van certificaatketen identificeren

Uit de certificaatanalyse bleek dat de gateway een certificaat gebruikte dat was ondertekend door GoDaddy TLS Intermediate CA DV - R1v1. Het kruiscertificaat (GoDaddy TLS Root CA - R1) en het basiscertificaat (GoDaddy Root Certificate Authority - G2) ontbraken in de gateway.

Webex Calling ondersteunt alleen certificaten met de "GoDaddy" rootcertificaatautoriteit per officiële documentatie.

- CN=Go Daddy Root Certificaat Autoriteit - G2

Stap 3: Nieuw certificaat aanvragen met ondersteunde keten

Neem contact op met de certificaataanbieder (GoDaddy) om het certificaat opnieuw in te toetsen en ervoor te zorgen dat het de ondersteunde certificaatketen gebruikt:

- Vraag een nieuw certificaat aan voor hetzelfde domein FQDN (mhtlc-ls-r1.mhtlc.org).
- Geef op dat het certificaat de certificaatketen GoDaddy G2 (SHA-2) moet gebruiken.
- Zorg ervoor dat alle relevante certificaten voor een complete vertrouwensketen op de SGW-router zijn geïnstalleerd.

Stap 4: Het nieuwe certificaat installeren

Zodra het nieuwe certificaat met de ondersteunde G2-keten is verkregen, installeert u het op de overlevingsgateway en configureert u het juiste vertrouwenspunt voor Webex-connectiviteit.

Voer deze stap uit als een algemeen bekend CA-basiscertificaat niet beschikbaar is met uw Cisco IOS XE-gateway.

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

Stap 5: Resolutie controleren

Test na het installeren van het nieuwe certificaat de registratie van de overlevingsgateway:

- Controleer het synchronisatieproces in de Control Hub.
- Verifieer de succesvolle registratie door de opdracht Spraakregistersessie tonen uit te voeren.
- Zorg ervoor dat de telemetrielogboeken geen TLS-verbindingsfouten meer vertonen.

Oorzaak

De oorzaak was de incompatibiliteit van de certificaatketen tussen de overlevingsgateway en de cloudservices van Webex Calling. De gateway is geconfigureerd met een certificaat ondertekend door GoDaddy TLS Intermediate CA DV - R1v1, dat deel uitmaakt van de nieuwere GoDaddy R1 certificaatketen.

Webex Calling ondersteunt alleen certificaten die zijn gekoppeld aan de Go Daddy Root Certificate Authority - G2. De nieuwere R1v1 intermediaire certificeringsinstantie die door GoDaddy is geïntroduceerd, is niet opgenomen in de lijst van vertrouwde certificeringsinstanties van Webex Callings, waardoor TLS-handdruk mislukt tijdens het synchronisatieproces van de overlevingsgateway. Bovendien voorkwam het ontbrekende rootcertificaat op de gateway de juiste validatie van de certificaatketen, wat bijdroeg aan de mislukte beveiligde verbindingsinstelling.

Gerelateerde inhoud

- Welke Root Certificate Authorities worden ondersteund voor oproepen naar Cisco Webex Audio- en Videoplatforms
- Cisco Technical Support en downloads
- Overlevingskansen voor webexbellen

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.