Problema di compatibilità della catena di certificati di Webex Calling Survivability Gateway

Sommario

Problema

Quando si configura Webex Calling Survivability e si abilita la modalità test nell'hub di controllo, il gateway non riesce a eseguire la sincronizzazione con i server Webex Cloud. Il comando show voice register session non visualizza il comportamento di registrazione previsto e l'hub di controllo visualizza gli errori di sincronizzazione.

Nei log di telemetria viene visualizzato questo errore durante i tentativi di sincronizzazione:

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

Il gateway non riesce a stabilire una connessione TLS sicura con Webex Cloud per il percorso configurato, impedendo la corretta sincronizzazione e registrazione del gateway di sopravvivenza.

Ambiente

- Configurazione di Webex Calling Survivability Gateway
- Software IOS XE versione 17.12.6
- Certificati TLS GoDaddy installati sul gateway
- Catena di certificati con GoDaddy TLS Intermediate CA DV - R1v1
- Configurazione della sopravvivenza dell'hub di controllo con la modalità test abilitata

Risoluzione

Il problema è stato risolto sostituendo il certificato con uno che utilizza una catena di autorità di certificazione supportata. Il certificato con problemi utilizzava la catena di certificati GoDaddy R1v1 più recente, non supportata dalle piattaforme Webex Calling.

Passaggio 1: Verifica catena di certificati corrente

Verificare i certificati attualmente installati nel gateway:

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

Nell'output viene visualizzata la catena di certificati con problemi:

<#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
```

Passaggio 2: Identifica il problema di compatibilità della catena di certificati

L'analisi del certificato ha rilevato che il gateway utilizza un certificato firmato da GoDaddy TLS Intermediate CA DV - R1v1. Il certificato incrociato (GoDaddy TLS Root CA - R1) e il certificato radice (Go Daddy Root Certificate Authority - G2) non sono presenti nel gateway.

Webex Calling supporta solo i certificati con l'autorità di certificazione radice "GoDaddy" per la documentazione ufficiale.

- CN=Go Daddy Root Certificate Authority - G2

Passaggio 3: Richiedi nuovo certificato con catena supportata

Contattare il provider di certificati (GoDaddy) per reimpostare la chiave del certificato e verificare che utilizzi la catena di certificati supportata:

- Richiedere un nuovo certificato per lo stesso FQDN di dominio (mhtlc-ls-r1.mhtlc.org).
- Specificare che il certificato deve utilizzare la catena di certificati GoDaddy G2 (SHA-2).
- Verificare che tutti i certificati pertinenti per una catena di attendibilità completa siano installati sul router SGW.

Passaggio 4: Installa il nuovo certificato

Una volta ottenuto il nuovo certificato con la catena G2 supportata, installarlo sul gateway di sopravvivenza e configurare il trust point appropriato per la connettività Webex.

Eseguire questo passaggio se un certificato radice CA noto pubblicamente non è disponibile con il gateway Cisco IOS XE.

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

Passaggio 5: Verifica risoluzione

Dopo l'installazione del nuovo certificato, verificare la registrazione del gateway di sopravvivenza:

- Monitorare il processo di sincronizzazione in Control Hub.

- Verificare la riuscita della registrazione eseguendo il comando show voice register session.
- Verificare che nei registri di telemetria non vengano più visualizzati errori di connessione TLS.

Causa

La causa principale è stata l'incompatibilità della catena di certificati tra il gateway di sopravvivenza e i servizi cloud Webex Calling. Il gateway è stato configurato con un certificato firmato da GoDaddy TLS Intermediate CA DV - R1v1, che fa parte della catena di certificati GoDaddy R1 più recente.

Webex Calling supporta solo certificati concatenati fino all'autorità di certificazione radice Go Daddy - G2. L'autorità di certificazione intermedia R1v1 più recente introdotta da GoDaddy non è inclusa nell'elenco delle autorità di certificazione attendibili di Webex Callings, causando errori di handshake TLS durante il processo di sincronizzazione del gateway di sopravvivenza. Inoltre, il certificato radice mancante nel gateway ha impedito la corretta convalida della catena di certificati, contribuendo agli errori di connessione sicura.

Contenuto correlato

- Quali autorità di certificazione radice sono supportate per le chiamate alle piattaforme audio e video Cisco Webex?
- Supporto tecnico Cisco e download
- Sopravvivenza del sito per Webex Calling

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).