Problème de compatibilité de la chaîne de certificats de la passerelle de survie des appels Webex

Table des matières

Problème

Lors de la configuration de la survie des appels Webex et de l'activation du mode test dans le Control Hub, la passerelle ne parvient pas à se synchroniser avec les serveurs cloud Webex. La commande show voice register session n'affiche pas le comportement d'enregistrement attendu et le Control Hub affiche les échecs de synchronisation.

Les journaux de télémétrie affichent cette erreur lors des tentatives de synchronisation :

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

La passerelle ne parvient pas à établir une connexion TLS sécurisée avec le cloud Webex pour l'emplacement configuré, ce qui empêche la synchronisation et l'enregistrement corrects de la passerelle de survie.

Environnement

- Configuration de la passerelle de survie des appels Webex
- Logiciel IOS XE version 17.12.6
- Certificats GoDaddy TLS installés sur le modem routeur
- Chaîne de certificats utilisant GoDaddy TLS Intermediate CA DV - R1v1
- Configuration de la survie du concentrateur de contrôle avec mode de test activé

Résolution

Ce problème a été résolu en remplaçant le certificat par un certificat utilisant une chaîne d'autorité de certification prise en charge. Le certificat problématique utilisait la nouvelle chaîne de certificats GoDaddy R1v1, qui n'est pas prise en charge par les plates-formes d'appel Webex.

Étape 1: Vérifier la chaîne de certificats actuelle

Vérifiez les certificats actuellement installés sur la passerelle :

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

Le résultat affiche la chaîne de certificats problématique :

<#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
```

Étape 2: Identifier le problème de compatibilité de la chaîne de certificats

L'analyse du certificat a révélé que la passerelle utilisait un certificat signé par GoDaddy TLS Intermediate CA DV - R1v1. Le certificat croisé (GoDaddy TLS Root CA - R1) et le certificat racine (GoDaddy Root Certificate Authority - G2) étaient manquants dans la passerelle.

Webex Calling ne prend en charge que les certificats avec l'autorité de certification racine « GoDaddy » selon la documentation officielle.

- CN=Autorité de certification racine Go Daddy - G2

Étape 3: Demander un nouveau certificat avec la chaîne prise en charge

Contactez le fournisseur de certificats (GoDaddy) pour ressaisir le certificat et vous assurer qu'il utilise la chaîne de certificats prise en charge :

- Demandez un nouveau certificat pour le même nom de domaine complet (FQDN) (mhtlc-ls-r1.mhtlc.org).
- Spécifiez que le certificat doit utiliser la chaîne de certificats GoDaddy G2 (SHA-2).
- Assurez-vous que tous les certificats nécessaires à une chaîne de confiance complète sont installés sur le routeur SGW.

Étape 4: Installer le nouveau certificat

Une fois le nouveau certificat avec la chaîne G2 prise en charge obtenu, installez-le sur la passerelle de survie et configurez le point de confiance approprié pour la connectivité Webex.

Effectuez cette étape si un certificat racine CA connu publiquement n'est pas disponible avec votre passerelle Cisco IOS XE.

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

Étape 5: Vérifier la résolution

Après avoir installé le nouveau certificat, testez l'enregistrement de la passerelle de survie :

- Surveillez le processus de synchronisation dans Control Hub.
- Vérifiez que l'enregistrement a réussi en exécutant la commande show voice register session.
- Assurez-vous que les journaux de télémétrie n'affichent plus les échecs de connexion TLS.

Motif

La cause principale était l'incompatibilité de la chaîne de certificats entre la passerelle de survie et les services cloud Webex Calling. La passerelle a été configurée avec un certificat signé par GoDaddy TLS Intermediate CA DV - R1v1, qui fait partie de la nouvelle chaîne de certificats GoDaddy R1 croisée.

Webex Calling ne prend en charge que les certificats qui sont reliés en chaîne à l'autorité de certification racine Go Daddy - G2. La nouvelle autorité de certification intermédiaire R1v1 introduite par GoDaddy n'est pas incluse dans la liste d'autorités de certification approuvées Webex Callings, ce qui entraîne des échecs de connexion TLS lors du processus de synchronisation de la passerelle de survie. En outre, le certificat racine manquant sur la passerelle a empêché une validation correcte de la chaîne de certificats, ce qui a contribué aux échecs d'établissement de connexion sécurisée.

Autres informations utiles

- Quelles sont les autorités de certification racine prises en charge pour les appels vers les plates-formes audio et vidéo Cisco Webex ?
- Assistance technique de Cisco et téléchargements
- Survie du site pour les appels Webex

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.