Résolution de l'échec de synchronisation de la passerelle de survie des appels Webex dû à une chaîne de certificats GoDaddy R1 non prise en charge

Table des matières

Problème

Deux passerelles de survie (mcyitsrtr001.centralwire.com et prtitsrtr001.centralwire.com) ont été enregistrées dans le Control Hub mais n'ont pas pu se synchroniser ; dépannage axé sur mcyitsrtr001.centralwire.com. Les tentatives de synchronisation ont échoué de manière cohérente avec le message d'erreur :

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

Première observation lors d'une tentative de synchronisation le 5 août 2026. L'analyse de la télémétrie et des journaux du serveur principal Webex (pylône) a révélé que la passerelle présentait une chaîne de certificats GoDaddy R1v1 (hiérarchie CA racine - R1 GoDaddy TLS), qui n'est pas prise en charge par les services Webex, ce qui a entraîné le rejet de la chaîne de certificats et l'échec de la synchronisation.

Environnement

- Deux passerelles gérées ont été signalées : mcyitsrtr001.centralwire.com et prtitsrtr001.centralwire.com (dépannage axé sur mcyitsrtr001.centralwire.com)
- Version d'IOS® XE : 17.12.6 (noeud SGW), 17.15.06 (MGW)
- Configuration de Webex Calling Survivability Gateway (SGW)
- Chaîne de certificats TLS GoDaddy utilisant l'autorité de certification intermédiaire R1v1

- Chaîne de certificats : CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

Résolution

Le problème a été résolu en implémentant une solution de contournement de signature croisée de certificat pour établir un chemin d'accès de certificat approuvé. La solution impliquait l'installation du certificat à signature croisée GoDaddy R1 vers G2 pour chaîner la nouvelle hiérarchie GoDaddy R1 à l'autorité de certification racine GoDaddy de confiance - G2.



Remarque : Pendant les modifications de certificat, la commande crypto pki trustpool import clean a interrompu le service NETCONF-YANG/DMI de la passerelle, mettant brièvement le connecteur hors ligne. `Impossible d'ouvrir le socket vers 192.168.217.55:830`). Cette erreur a été récupérée lors des étapes 6 à 7 et a été un effet secondaire de la maintenance, et non de la panne de synchronisation initiale.

Étape 1: Installer le bundle Cisco Trustpool

Installez le bundle Cisco trustpool qui contient l'autorité de certification racine Go Daddy - G2 :

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

`le nettoyage de l'importation` remplace l'intégralité du pool de confiance : il peut perturber les services qui en dépendent (voir la note relative à la connexion hors connexion répertoriée précédemment). À utiliser avec précaution.

Étape 2: Vérification du certificat racine G2

Vérifiez que Go Daddy Root Certificate Authority - G2 est présent :

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

Étape 3: Supprimer le point de confiance R1 auto-signé

Supprimez l'ancien point de confiance R1 auto-signé (répondez yes lorsque vous êtes invité à supprimer des certificats) :

```
no crypto pki trustpoint GoDaddyRootR1
```

Étape 4: Installer un certificat R1 contresigné

Créez un nouveau point de confiance avec le certificat R1 à signature croisée (Objet : Autorité de certification racine GoDaddy TLS - R1, émetteur : 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
```

Étape 5: Vérifier la chaîne de certificats

Vérifiez que la chaîne se résout correctement :

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

Étape 6: Redémarrer les services NETCONF

Rebondir le serveur HTTP(S) et les services NETCONF-YANG (patientez environ 60 secondes entre disable et enable) :

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

Patientez 60 secondes, puis réactivez :

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

Étape 7: Recharger la passerelle (si nécessaire)

Si NETCONF-YANG ne fonctionne toujours pas correctement après le redémarrage du service, rechargez le routeur pour réinitialiser complètement DMI :

```
reload
```

Mise en garde : Possible. Les détails mentionnés ici semblent contenir des procédures ou des commandes qui pourraient avoir un impact significatif si elles étaient exécutées. Veuillez vous assurer que les procédures ou commandes ci-dessus ont été évaluées par un expert ou une unité commerciale avant de les exécuter ou de les recommander.

Étape 8: Vérifier la résolution

Une fois que la passerelle est de nouveau en ligne, déclenchez une resynchronisation SGW à partir du Control Hub et vérifiez que la synchronisation s'effectue correctement sans le code d'erreur 31117 ou les messages « Certificate Server Trusted check failed ». Confirmé résolu - la

passerelle a présenté la chaîne complète leaf → R1v1 → R1 (émetteur G2) et la synchronisation s'est terminée correctement après la solution de contournement de la signalisation croisée.

Motif

La cause principale a été identifiée comme un échec d'approbation de certificat. Survivability Gateway présentait une chaîne de certificats utilisant la hiérarchie CA racine - R1 de GoDaddy TLS (en particulier la hiérarchie CA intermédiaire - R1v1 de GoDaddy TLS), qui n'est pas incluse dans la liste des autorités de certification de confiance de Webex Calling.

Lorsque le serveur principal Webex (pylône) a effectué un contrôle de confiance de certificat de serveur lors de la demande d'informations d'authentification SIP, il n'a pas pu créer un chemin de certification valide vers un certificat racine approuvé. Cela a entraîné une exception SunCertPathBuilderException avec l'erreur « Unable to find valid certification path to required target », provoquant la réponse HTTP 400 et l'interruption de la synchronisation.

Webex Calling ne fait confiance qu'aux racines GoDaddy/Starfield plus anciennes (telles que GoDaddy Root Certificate Authority - G2), mais pas à la nouvelle hiérarchie « GoDaddy TLS » (R1/R1v1).

Autres informations utiles

- Autorités de certification prises en charge pour les services hybrides Webex
- Référentiel de certificats GoDaddy
- Assistance technique de Cisco et téléchargements

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.