Risoluzione errore di sincronizzazione di Webex Calling Survivability Gateway a causa di una catena di certificati GoPapy R1 non supportata

Sommario

Problema

Due gateway di sopravvivenza (mcyitsrtr001.centralwire.com e prtitsrtr001.centralwire.com) sono stati registrati nell'hub di controllo, ma la sincronizzazione non è riuscita; risoluzione dei problemi incentrata su mcyitsrtr001.centralwire.com. Tentativi di sincronizzazione non riusciti con il messaggio di errore:

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

Osservato per la prima volta durante un tentativo di sincronizzazione il 5 agosto 2026. L'analisi dei log di telemetria e del back-end Webex (pilone) ha rivelato che il gateway presentava una catena di certificati GoDaddy R1v1 (gerarchia GoDaddy TLS Root CA - R1), non supportata dai servizi Webex, che ha causato il rifiuto della catena di certificati e il fallimento della sincronizzazione.

Ambiente

- Due gateway gestiti: mcyitsrtr001.centralwire.com e prtitsrtr001.centralwire.com (risoluzione dei problemi incentrata su mcyitsrtr001.centralwire.com)
- Versione IOS® XE: 17.12.6 (nodo SGW), 17.15.06 (MGW)
- Configurazione di Webex Calling Survivability Gateway (SGW)
- Catena di certificati TLS GoDaddy con CA intermedia R1v1
- Catena certificati: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

Risoluzione

Il problema è stato risolto implementando una soluzione per la firma incrociata dei certificati per stabilire un percorso di certificati attendibili. La soluzione prevedeva l'installazione del certificato con cross-signed GoDaddy R1-to-G2 per concatenare la nuova gerarchia GoDaddy R1 alla Go Daddy Root Certificate Authority - G2.



Nota: Durante le modifiche del certificato, il comando crypto pki trustpool import clean ha interrotto il servizio NETCONF-YANG/DMI del gateway, portando brevemente offline il connettore. `Impossibile aprire il socket su 192.168.217.55:830`). Questo è stato recuperato tramite i passaggi 6-7 ed è stato un effetto collaterale della manutenzione, non l'errore di sincronizzazione originale.

Passaggio 1: Installa Cisco Trustpool Bundle

Installare il bundle Cisco trustpool che contiene l'Autorità di certificazione radice Go Daddy - G2:

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

`import clean` sostituisce l'intero trustpool e può interrompere i servizi che dipendono da esso (vedere la nota relativa a connector-offline elencata in precedenza). Utilizzare con cautela.

Passaggio 2: Verifica certificato radice G2

Confermare la presenza di Go Daddy Root Certificate Authority - G2:

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

Passaggio 3: Rimuovi trust point R1 autofirmato

Rimuovere il trust point R1 autofirmato precedente (rispondere sì quando viene richiesto di rimuovere i certificati):

```
no crypto pki trustpoint GoDaddyRootR1
```

Passaggio 4: Installa certificato R1 con firma incrociata

Creare un nuovo trust point con il certificato R1 con firma incrociata (Oggetto: GoDaddy TLS Root CA - R1, Autorità emittente: 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
```

Passaggio 5: Verifica catena di certificati

Verificate che la catena sia ora risolta correttamente:

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

Passaggio 6: Riavvia servizi NETCONF

Rimbalzo del server HTTP(S) e dei servizi NETCONF-YANG (attendere circa 60 secondi tra la disabilitazione e l'abilitazione):

```
conf t
```

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

Attendere 60 secondi, quindi riattivare:

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

Passaggio 7: Ricarica Gateway (Se Necessario)

Se dopo il riavvio del servizio NETCONF-YANG non funziona ancora correttamente, ricaricare il router per reinizializzare completamente DMI:

```
reload
```

Attenzione: Possibile. I dettagli menzionati contengono procedure o comandi che potrebbero avere un impatto significativo se eseguiti. Prima di eseguire o consigliare le procedure o i comandi descritti in precedenza, accertarsi che siano stati valutati da uno SME o da una Business Unit.

Passaggio 8: Verifica risoluzione

Dopo il riavvio del gateway, avviare una risincronizzazione SGW dall'hub di controllo e verificare che la sincronizzazione sia stata completata senza messaggi di errore 31117 o "Controllo attendibile server certificati non riuscito". Confermato risolto — il gateway ha presentato la catena completa foglia → R1v1 → R1 (emittente G2) e la sincronizzazione è stata completata correttamente dopo la soluzione della segnaletica incrociata.

Causa

La causa principale è stata identificata come errore di attendibilità del certificato. Survivability Gateway stava presentando una catena di certificati usando la gerarchia GoDaddy TLS Root CA - R1 (nello specifico, GoDaddy TLS Intermediate CA DV - R1v1), che non è inclusa nell'elenco di autorità di certificazione attendibili di Webex Calling.

Quando il back-end Webex (pilone) ha eseguito un controllo dell'attendibilità del certificato del server durante la richiesta di informazioni per l'autenticazione SIP, non è stato possibile creare un percorso di certificazione valido per un certificato radice attendibile. In seguito a questa operazione SunCertPathBuilderException ha restituito l'errore "impossibile trovare un percorso di certificazione valido per la destinazione richiesta", causando la risposta HTTP 400 e l'interruzione della sincronizzazione.

Webex Calling considera attendibili solo le radici GoDaddy/Starfield meno recenti (ad esempio Go Daddy Root Certificate Authority - G2), ma non la nuova gerarchia "GoDaddy TLS" (R1/R1v1).

Contenuto correlato

- Autorità di certificazione supportate per i servizi ibridi Webex
- Archivio certificati GoDaddy
- Supporto tecnico Cisco e download

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).