Resuelva el error de sincronización de Webex Calling Survivability Gateway debido a una cadena de certificados GoDaddy R1 no compatible

Contenido

Problema

Dos gateways de supervivencia (mcyitsrtr001.centralwire.com y prtitsrtr001.centralwire.com) se registraron en el centro de control, pero no se pudieron sincronizar; la resolución de problemas se centró en mcyitsrtr001.centralwire.com. Los intentos de sincronización fallaron de forma consistente con el mensaje de error:

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

Observado por primera vez durante un intento de sincronización el 5 de agosto de 2026. El análisis de los registros de telemetría y backend de Webex (pilón) reveló que la puerta de enlace presentaba una cadena de certificados GoDaddy R1v1 (CA raíz de GoDaddy TLS - jerarquía R1), que no es compatible con los servicios Webex, lo que provocaba que se rechazara la cadena de certificados y que se produjera un error en la sincronización.

Entorno

- Se notificaron dos gateways administrados: mcyitsrtr001.centralwire.com y prtitsrtr001.centralwire.com (solución de problemas centrada en mcyitsrtr001.centralwire.com)
- Versión IOS® XE: 17.12.6 (nodo SGW), 17.15.06 (MGW)
- Configuración de Webex Calling Survivability Gateway (SGW)

- Cadena de certificados GoDaddy TLS mediante CA intermedia R1v1
- Cadena de certificados: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

Resolución

El problema se resolvió implementando una solución alternativa de firma cruzada de certificados para establecer una ruta de certificado de confianza. La solución implicaba la instalación del certificado firmado cruzado GoDaddy R1-to-G2 para encadenar la jerarquía más reciente de GoDaddy R1 a la autoridad de certificados raíz de confianza GoDaddy - G2.

Nota: Durante los cambios del certificado, el comando crypto pki trustpool import clean interrumpió el servicio NETCONF-YANG/DMI del gateway, desconectando brevemente el conector. `No se pudo abrir el socket a 192.168.217.55:830`). Esto se recuperó a través de los pasos 6-7 y fue un efecto secundario del mantenimiento, no el fallo de sincronización original.

Paso 1: Instalar Cisco Trustpool Bundle

Instale el paquete de trustpool de Cisco que contiene la autoridad de certificación raíz de Go Daddy - G2:

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

`import clean` reemplaza todo el conjunto de confianza: puede interrumpir los servicios que dependen de él (consulte la nota de conector sin conexión que se enumeró anteriormente). Utilícelo con cuidado.

Paso 2: Verificar certificado raíz G2

Confirme que Go Daddy Root Certificate Authority - G2 esté presente:

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

Paso 3: Quitar punto de confianza R1 autofirmado

Quite el antiguo punto de confianza R1 autofirmado (responda sí cuando se le pida que quite los certificados):

```
no crypto pki trustpoint GoDaddyRootR1
```

Paso 4: Instalar certificado R1 con firma cruzada

Cree un nuevo punto de confianza con el certificado R1 con firma cruzada (Asunto: CA raíz de TLS de GoDaddy - R1, emisor: Autoridad de certificados raíz de Go Daddy (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
```

Paso 5: Verificar cadena de certificados

Verifique que la cadena se resuelva ahora correctamente:

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

Paso 6: Reiniciar servicios NETCONF

Rebote del servidor HTTP(S) y los servicios NETCONF-YANG (espere aproximadamente 60 segundos entre deshabilitar y habilitar):

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

Espere 60 segundos y vuelva a activar:

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

Paso 7: Volver a cargar la puerta de enlace (si es necesario)

Si NETCONF-YANG sigue sin funcionar correctamente después del reinicio del servicio, recargue el router para reiniciar completamente DMI:

```
reload
```

Precaución: Posible. Los detalles mencionados aquí parecen contener procedimientos o comandos que podrían causar un impacto significativo si se ejecutan. Asegúrese de que una PYME o una unidad de negocio ha evaluado los procedimientos o comandos anteriores antes de ejecutarlos o recomendarlos.

Paso 8: Verificar resolución

Una vez que el gateway vuelva a estar en línea, active una sincronización SGW desde el concentrador de control y compruebe que la sincronización se completa correctamente sin los mensajes de código de error 31117 o "Error en la comprobación de confianza del servidor de certificados". Confirmada y resuelta: la puerta de enlace presentó la cadena de hoja completa → R1v1 → R1 (emisor G2) y la sincronización se completó correctamente después de la solución alternativa de firma cruzada.

Causa

La causa raíz se identificó como un error de confianza de certificado. El gateway de supervivencia presentaba una cadena de certificados mediante la jerarquía CA raíz de GoDaddy TLS - R1 (en concreto, la CA DV intermedia de GoDaddy TLS - R1v1), que no se incluye en la lista de autoridades de certificados de confianza de Webex Calling.

Cuando el servidor de Webex (pilón) realizó una comprobación de confianza del certificado de servidor durante la solicitud de información de autenticación SIP, no pudo crear una ruta de certificación válida para un certificado raíz de confianza. Esto produjo una excepción SunCertPathBuilderException con el error "no se pudo encontrar una ruta de certificación válida para el destino solicitado", lo que provocó la respuesta HTTP 400 y el aborto de sincronización.

Webex Calling confía solamente en las raíces antiguas de GoDaddy/Starfield (como Go Daddy Root Certificate Authority - G2) pero no en la jerarquía más reciente de "GoDaddy TLS" (R1/R1v1).

Contenido relacionado

- Autoridades de certificados compatibles con los servicios híbridos de Webex
- Repositorio de certificados de GoDaddy
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).