Problema De Compatibilidad De Cadena De Certificados De Gateway De Supervivencia De Llamadas Webex

Contenido

Problema

Al configurar Webex Calling Survivability y habilitar el modo de prueba en el concentrador de control, el gateway no se sincroniza con los servidores de Webex Cloud. El comando show voice register session no muestra el comportamiento de registro esperado y el concentrador de control muestra fallas de sincronización.

Los registros de telemetría muestran este error durante los intentos de sincronización:

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

El gateway no puede establecer una conexión TLS segura con Webex Cloud para la ubicación configurada, lo que impide la sincronización y el registro adecuados del gateway de supervivencia.

Entorno

- Configuración del gateway de supervivencia de llamadas Webex
- Versión 17.12.6 del software IOS XE
- Certificados GoDaddy TLS instalados en la puerta de enlace
- Cadena de certificados con GoDaddy TLS Intermediate CA DV - R1v1
- Configuración de supervivencia del centro de control con el modo de prueba habilitado

Resolución

Este problema se resolvió al reemplazar el certificado por uno que utilice una cadena de entidades emisoras de certificados admitida. El certificado problemático estaba usando la cadena de certificados GoDaddy R1v1 más reciente, que no es compatible con las plataformas de llamada Webex.

Paso 1: Verificar cadena de certificados actual

Compruebe los certificados instalados actualmente en el gateway:

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

El resultado muestra la cadena de certificados problemática:

<#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
```

Paso 2: Identificar problema de compatibilidad de cadena de certificados

El análisis del certificado reveló que la puerta de enlace estaba usando un certificado firmado por GoDaddy TLS Intermediate CA DV - R1v1. El certificado cruzado (GoDaddy TLS Root CA - R1) y el certificado raíz (Go Daddy Root Certificate Authority - G2) faltaban en la puerta de enlace.

Webex Calling sólo admite certificados con la autoridad de certificados raíz "GoDaddy" según la documentación oficial.

- CN=Autoridad de certificados raíz de Go Daddy: G2

Paso 3: Solicitar nuevo certificado con cadena admitida

Póngase en contacto con el proveedor de certificados (GoDaddy) para volver a introducir la clave del certificado y asegurarse de que utiliza la cadena de certificados admitida:

- Solicite un nuevo certificado para el mismo FQDN de dominio (mhtlc-ls-r1.mhtlc.org).
- Especifique que el certificado debe utilizar la cadena de certificados GoDaddy G2 (SHA-2).
- Asegúrese de que todos los certificados relevantes para una cadena completa de confianza estén instalados en el router SGW.

Paso 4: Instalar el nuevo certificado

Una vez obtenido el nuevo certificado con la cadena G2 admitida, instálelo en el gateway de supervivencia y configure el punto de confianza adecuado para la conectividad Webex.

Realice este paso si un certificado raíz de CA conocido públicamente no está disponible con su gateway de Cisco IOS XE.

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

Paso 5: Verificar resolución

Después de instalar el nuevo certificado, pruebe el registro del gateway de supervivencia:

- Supervise el proceso de sincronización en Control Hub.
- Verifique el registro exitoso ejecutando el comando show voice register session.
- Asegúrese de que los registros de telemetría ya no muestren los fallos de conexión TLS.

Causa

La causa raíz fue la incompatibilidad de la cadena de certificados entre el gateway de supervivencia y los servicios en la nube de Webex Calling. El gateway se configuró con un certificado firmado por GoDaddy TLS Intermediate CA DV - R1v1, que forma parte de la nueva cadena de certificados cruzada GoDaddy R1.

Webex Calling sólo admite certificados que se encadenan a Go Daddy Root Certificate Authority - G2. La autoridad de certificados intermedia R1v1 más reciente introducida por GoDaddy no se incluye en la lista de autoridades de certificados de confianza de Webex Callings, lo que provoca errores de intercambio de señales de TLS durante el proceso de sincronización del gateway de supervivencia. Además, el certificado raíz que falta en el gateway impidió la validación correcta de la cadena de certificados, lo que contribuyó a los errores del establecimiento de conexión segura.

Contenido relacionado

- Qué autoridades de certificados raíz son compatibles con las llamadas a las plataformas de audio y vídeo de Cisco Webex
- Soporte técnico y descargas de Cisco
- Supervivencia del sitio para llamadas Webex

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).