Problema De Compatibilidade De Cadeia De Certificados Do Webex Calling Survivability Gateway

Contents

Problema

Ao configurar o Webex Calling Survivability e ativar o modo de teste no Control Hub, o gateway não consegue sincronizar com os servidores Webex Cloud. O comando show voice register session não exibe o comportamento de registro esperado, e o Hub de Controle mostra falhas de sincronização.

Os logs de telemetria exibem este erro durante as tentativas de sincronização:

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

O gateway não consegue estabelecer uma conexão TLS segura com o Webex Cloud para o local configurado, impedindo a sincronização e o registro adequados do gateway de sobrevivência.

Ambiente

- Configuração Do Webex Calling Survivability Gateway
- Software IOS XE versão 17.12.6
- Certificados TLS GoDaddy instalados no gateway
- Cadeia de Certificados usando o DV de CA Intermediário GoDaddy TLS - R1v1
- Configuração de Persistência do Hub de Controle com Modo de Teste Ativado

Resolução

Esse problema foi resolvido com a substituição do certificado por um que usa uma cadeia de autoridade de certificação com suporte. O certificado problemático estava usando a cadeia de certificados GoDaddy R1v1 mais recente, que não é suportada pelas plataformas Webex Calling.

Passo 1: Verificar Cadeia de Certificados Atual

Verifique os certificados atualmente instalados no gateway:

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

A saída exibe a cadeia de certificados problemáticos:

<#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
```

Passo 2: Identificar Problema de Compatibilidade da Cadeia de Certificados

A análise de certificado revelou que o gateway estava usando um certificado assinado por GoDaddy TLS Intermediate CA DV - R1v1. O certificado cruzado (GoDaddy TLS Root CA - R1) e o certificado raiz (Go Daddy Root Certificate Authority - G2) estavam ausentes do gateway.

O Webex Calling suporta apenas certificados com a autoridade de certificação raiz "GoDaddy" por documentação oficial.

- CN=Go Daddy Root Certificate Authority - G2

Passo 3: Solicitar novo certificado com cadeia suportada

Entre em contato com o provedor de certificados (GoDaddy) para digitar novamente o certificado e garantir que ele use a cadeia de certificados suportada:

- Solicite um novo certificado para o mesmo FQDN de domínio (mhtlc-ls-r1.mhtlc.org).
- Especifique o certificado que deve usar a cadeia de certificados GoDaddy G2 (SHA-2).
- Verifique se todos os certificados relevantes para uma cadeia completa de confiança estão instalados no roteador SGW.

Passo 4: Instalar o novo certificado

Depois que o novo certificado com a cadeia G2 suportada for obtido, instale-o no gateway de sobrevivência e configure o ponto de confiança apropriado para a conectividade do Webex.

Execute esta etapa se um certificado raiz de CA publicamente conhecido não estiver disponível com seu gateway Cisco IOS XE.

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

Passo 5: Verificar resolução

Depois de instalar o novo certificado, teste o registro do gateway de sobrevivência:

- Monitore o processo de sincronização no Control Hub.

- Verifique o registro bem-sucedido executando o comando show voice register session.
- Certifique-se de que os registros de telemetria não mostrem mais falhas de conexão TLS.

Causa

A causa raiz foi a incompatibilidade da cadeia de certificados entre o gateway de sobrevivência e os serviços em nuvem do Webex Calling. O gateway foi configurado com um certificado assinado por GoDaddy TLS Intermediate CA DV - R1v1, que faz parte da cadeia de certificados GoDaddy R1 mais recente.

O Webex Calling só oferece suporte a certificados que se enquadram na Go Daddy Root Certificate Authority - G2. A mais recente autoridade de certificação intermediária R1v1 introduzida por GoDaddy não está incluída na lista de autoridades de certificação confiáveis do Webex Callings, causando falhas de handshake TLS durante o processo de sincronização do gateway de sobrevivência. Além disso, o certificado raiz ausente no gateway impediu a validação adequada da cadeia de certificados, contribuindo para o estabelecimento de falhas de conexão segura.

Conteúdo relacionado

- Quais autoridades de certificação raiz são suportadas em chamadas para plataformas de áudio e vídeo Cisco Webex
- Suporte técnico e downloads da Cisco
- Sobrevivência do site para Webex Calling

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.