Resolver falha de sincronização do Webex Calling Survivability Gateway devido à cadeia de certificados GoDaddy R1 sem suporte

Contents

Problema

Dois Gateways de Sobrevivência (mcyitsrtr001.centralwire.com e prtitsrtr001.centralwire.com) foram registrados no Control Hub, mas falharam ao sincronizar; Troubleshooting focado em mcyitsrtr001.centralwire.com. As tentativas de sincronização falharam consistentemente com a mensagem de erro:

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

Observado pela primeira vez durante uma tentativa de sincronização em 5 de agosto de 2026. A análise de telemetria e logs de back-end (pilone) do Webex revelou que o gateway estava apresentando uma cadeia de certificados GoDaddy R1v1 (CA raiz TLS GoDaddy - hierarquia R1), que não é suportada pelos serviços do Webex, fazendo com que a cadeia de certificados seja rejeitada e a sincronização falhe.

Ambiente

- Dois gateways gerenciados relatados: mcyitsrtr001.centralwire.com e prtitsrtr001.centralwire.com (solução de problemas concentrada em mcyitsrtr001.centralwire.com)
- Versão do IOS® XE: 17.12.6 (nó SGW), 17.15.06 (MGW)
- Configuração do Webex Calling Survivability Gateway (SGW)
- Cadeia de certificados TLS GoDaddy usando CA intermediária R1v1

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

Resolução

O problema foi resolvido com a implementação de uma solução alternativa de assinatura cruzada de certificado para estabelecer um caminho de certificado confiável. A solução envolvia a instalação do certificado assinado cruzado GoDaddy R1-to-G2 para encadear a hierarquia mais recente GoDaddy R1 à Autoridade de Certificação Raiz Go Daddy - G2 confiável.

Note: Durante as alterações de certificado, o comando crypto pki trustpool import clean interrompeu o serviço NETCONF-YANG/DMI do gateway, colocando brevemente o conector offline. `Não foi possível abrir o soquete para 192.168.217.55:830`). Isso foi recuperado através das Etapas 6-7 e foi um efeito colateral da manutenção, não a falha de sincronização original.

Passo 1: Instalar o pacote Cisco Trustpool

Instale o pacote Cisco trustpool que contém a Go Daddy Root Certificate Authority - G2:

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

`o import clean` substitui todo o pool confiável — ele pode interromper os serviços que dependem dele (consulte a nota conector-off-line listada anteriormente). Use com cuidado.

Passo 2: Verificar Certificado Raiz G2

Confirme se Go Daddy Root Certificate Authority - G2 está presente:

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

Passo 3: Remover Ponto de Confiança R1 Autoassinado

Remova o ponto confiável R1 autoassinado antigo (responda sim quando for solicitado a remover certificados):

```
no crypto pki trustpoint GoDaddyRootR1
```

Passo 4: Instalar Certificado R1 Assinado Cruzado

Crie um novo ponto confiável com o certificado R1 com assinatura cruzada (Assunto: CA raiz TLS GoDaddy - R1, Emissor: 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
```

Passo 5: Verificar Cadeia de Certificados

Verifique se a cadeia agora é resolvida corretamente:

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

Passo 6: Reiniciar os serviços NETCONF

Servidor HTTP(S) de devolução e serviços NETCONF-YANG (aguarde aproximadamente 60

segundos entre desabilitar e habilitar):

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

Aguarde 60 segundos e, em seguida, reative:

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

Passo 7: Recarregar Gateway (Se Necessário)

Se o NETCONF-YANG ainda não funcionar corretamente após a reinicialização do serviço, recarregue o roteador para reinicializar totalmente o DMI:

```
reload
```

Caution: Possível. Os detalhes mencionados aqui parecem conter procedimentos ou comandos que poderiam causar um impacto significativo se executados. Verifique se os procedimentos ou comandos acima foram avaliados por um SME ou Unidade de negócios antes de executar ou recomendar.

Passo 8: Verificar resolução

Depois que o gateway voltar a ficar online, acione uma ressincronização de SGW do Control Hub e verifique se a sincronização foi concluída com êxito sem o código de erro 31117 ou mensagens de "Falha na verificação confiável do servidor de certificado". Confirmado resolvido — o gateway apresentou a folha completa → R1v1 → R1 (emissor G2) e a sincronização foi concluída com êxito

após a solução de sinal cruzado.

Causa

A causa raiz foi identificada como uma falha de confiança de certificado. O Survivability Gateway estava apresentando uma cadeia de certificados usando a hierarquia CA raiz TLS GoDaddy - R1 (especificamente o DV CA intermediário TLS GoDaddy - R1v1), que não está incluído na lista de autoridades de certificação confiáveis do Webex Calling.

Quando o back-end do Webex (pilone) executou uma verificação de confiança de certificado do servidor durante a solicitação de informações de autenticação SIP, ele não pôde criar um caminho de certificação válido para um certificado raiz confiável. Isso resultou em uma SunCertPathBuilderException com o erro "não é possível encontrar um caminho de certificação válido para o destino solicitado", causando a resposta HTTP 400 e a interrupção da sincronização.

O Webex Calling confia somente nas raízes GoDaddy/Starfield mais antigas (como Go Daddy Root Certificate Authority - G2), mas não na hierarquia "GoDaddy TLS" (R1/R1v1) mais recente.

Conteúdo relacionado

- Autoridades de certificado com suporte para serviços híbridos do Webex
- Repositório de Certificados GoDaddy
- Suporte técnico e downloads da Cisco

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.