Webex Calling Survivability Gateway証明書チェーンの互換性問題

内容

問題

Control HubでWebex Calling Survivabilityを設定し、テストモードを有効にすると、ゲートウェイがWebex Cloudサーバとの同期に失敗します。show voice register sessionコマンドでは、期待される登録動作が表示されず、コントロールハブに同期障害が表示されます。

テレメトリログには、同期の試行中に次のエラーが表示されます。

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

ゲートウェイが、設定されたロケーションのWebex Cloudとのセキュアな TLS接続を確立できず、サバイバビリティゲートウェイの適切な同期と登録を妨げています。

環境

- Webexコール存続可能性ゲートウェイの設定
- IOS XEソフトウェアバージョン17.12.6
- ゲートウェイにインストールされたGoDaddy TLS証明書
- GoDaddy TLS中間CA DVを使用した証明書チェーン – R1v1
- テストモードを有効にしたコントロールハブ存続可能性設定

解決方法

この問題は、サポートされている認証局チェーンを使用する証明書に置き換えることで解決されました。問題のある証明書は、Webexコーリングプラットフォームでサポートされていない新しいGoDaddy R1v1証明書チェーンを使用していました。

ステップ1：現在の証明書チェーンの確認

ゲートウェイに現在インストールされている証明書を確認します。

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

出力には、問題のある証明書チェーンが表示されます。

<#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
```

ステップ2：証明書チェーンの互換性問題の特定

証明書の分析により、ゲートウェイでGoDaddy TLS Intermediate CA DV - R1v1によって署名された証明書が使用されていることがわかります。クロス証明書（GoDaddy TLSルートCA - R1）とルート証明書（Go Daddyルート認証局 – G2）がゲートウェイにありません。

Webex通話は、公式ドキュメントに記載されている「GoDaddy」ルート認証局による証明書のみをサポートしています。

- CN=Go Daddyルート認証局 – G2

ステップ3：サポートされているチェーンを使用して新しい証明書を要求する

証明書プロバイダー(GoDaddy)に問い合わせて証明書のキーを再生成し、サポートされている証明書チェーンが使用されていることを確認します。

- 同じドメインFQDN(mhtlc-ls-r1.mhtlc.org)の新しい証明書を要求します。
- 証明書がGoDaddy G2(SHA-2)証明書チェーンを使用する必要があることを指定します。
- 完全な信頼チェーンに関連するすべての証明書がSGWルータにインストールされていることを確認します。

ステップ4：新しい証明書をインストールする

サポートされているG2チェーンを持つ新しい証明書を取得したら、それをサバイバビリティゲートウェイにインストールし、Webex接続用の適切なトラストポイントを設定します。

Cisco IOS XEゲートウェイで公開されているCAルート証明書を使用できない場合は、この手順を実行します。

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

ステップ5：解決策の確認

新しい証明書をインストールした後、サバイバビリティゲートウェイの登録をテストします。

- Control Hubで同期処理を監視します。
- show voice register sessionコマンドを実行して、登録が正常に行われたことを確認します。
- テレメトリログにTLS接続障害が表示されていないことを確認します。

原因

根本原因は、耐障害性ゲートウェイとWebex Callingクラウドサービス間の証明書チェーンの非互換性です。ゲートウェイは、新しいクラスGoDaddy R1証明書チェーンの一部であるGoDaddy TLS Intermediate CA DV - R1v1によって署名された証明書を使用して設定されました。

Webex通話は、Go Daddyルート認証局(GCA)- G2にチェーン接続された証明書のみをサポートします。GoDaddyによって導入された新しいR1v1中間認証局はWebex Callsの信頼できる認証局リストに含まれないため、存続可能性ゲートウェイの同期プロセス中にTLSハンドシェイク障害が発生します。さらに、ゲートウェイ上にルート証明書が存在しないため、証明書チェーンの検証が適切に行われず、セキュアな接続の確立が失敗します。

関連コンテンツ

- Cisco Webex音声およびビデオプラットフォームへのコールでサポートされるルート認証局
- シスコのテクニカルサポートとダウンロード
- Webex通話のサイト存続可能性

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。