サポートされていないGoDaddy R1証明書チェーンが原因で発生したWebex Calling Survivability Gatewayの同期エラーの解決

内容

問題

2つのSurvivability Gateway（mcyitsrtr001.centralwire.comとprtitsrtr001.centralwire.com）がControl Hubに登録されましたが、同期に失敗しました。トラブルシューティングはmcyitsrtr001.centralwire.comに重点を置いています。同期の試行が次のエラーメッセージで一貫して失敗しました：

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

2026年8月5日の同期の試行中に初めて確認されました。テレメトリおよびWebexバックエンド(pylon)ログの分析により、ゲートウェイがGoDaddy R1v1証明書チェーン（GoDaddy TLSルートCA - R1階層）を提示していることが判明しました。これはWebexサービスでサポートされていないため、証明書チェーンが拒否され、同期が失敗する原因となります。

環境

- 2つの管理対象ゲートウェイ、mcyitsrtr001.centralwire.comおよびprtitsrtr001.centralwire.com（mcyitsrtr001.centralwire.comに焦点を当てたトラブルシューティング）が報告されました。
- IOS® XEバージョン：17.12.6（SGWノード）、17.15.06(MGW)
- Webex Calling Survivability Gateway(SGW)の設定
- R1v1中間CAを使用するGoDaddy TLS証明書チェーン
- 証明書チェーン：CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV -

R1v1 → GoDaddy TLS Root CA - R1

解決方法

この問題は、証明書の相互署名の回避策を実装して信頼できる証明書パスを確立することで解決されました。このソリューションでは、GoDaddy R1とG2の相互署名証明書をインストールして、新しいGoDaddy R1階層を信頼されたGo Daddyルート認証局(G2)にチェーンします。


注：証明書の変更中に、crypto pki trustpool import clean コマンドによってゲートウェイのNETCONF-YANG/DMIサービスが中断され、コネクタが一時的にオフラインになりました。Could not open socket to 192.168.217.55:830)で検出されました。 これは、ステップ6 ~ 7で復旧し、元の同期障害ではなく、メンテナンスの副作用でした。

ステップ1:Cisco Trustpoolバンドルのインストール

Go Daddyルート認証局(CA)- G2を含むCiscoトラストプールバンドルをインストールします。

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

`import clean`はtrustpool全体を置き換えます。これに依存するサービスを中断する可能性があります（前述のconnector-offlineの注を参照）。 注意して使用してください。

ステップ2:G2ルート証明書の確認

Go Daddyルート認証局 – G2が存在することを確認します。

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

ステップ3：自己署名R1トラストポイントを削除する

古い自己署名R1トラストポイントを削除します（証明書を削除するように求められたら、yesと応答します）。

```
no crypto pki trustpoint GoDaddyRootR1
```

ステップ4：クロス署名R1証明書をインストールする

クロス署名R1証明書（サブジェクト：GoDaddy TLSルートCA - R1、発行者：Go Daddyルート認証局 – G2）を使用して新しいトラストポイントを作成します。

```
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
```

ステップ5：証明書チェーンの確認

チェーンが正しく解決されることを確認します。

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

ステップ6:NETCONFサービスを再起動します。

HTTP(S)サーバとNETCONF-YANGサービスをバウンスします（disableとenableの間に約60秒間

待機します）。

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

60秒待ってから、再度イネーブルにします。

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

ステップ7：ゲートウェイをリロードします（必要な場合）。

サービスの再起動後もNETCONF-YANGが正常に動作しない場合は、ルータをリロードして DMIを完全に再初期化します。

```
reload
```

注意：可能です。ここで説明する詳細には、実行すると重大な影響を与える可能性のあるプロシージャまたはコマンドが含まれています。実行または推奨を行う前に、上記の手順またはコマンドがSMEまたは事業部門によって評価されていることを確認してください。

ステップ8：解決策の確認

ゲートウェイがオンラインに戻ったら、Control HubからSGWの再同期をトリガーし、エラーコード31117または「Certificate Server Trusted check failed」メッセージなしで同期が正常に完了することを確認します。確認済み解決済み：ゲートウェイはR1v1（発行者G2）チェーン→フルリーフを提示→、クロスサイン回避策の後で同期が正常に完了しました。

原因

根本原因は、証明書信頼の失敗として特定されました。Survivability Gatewayは、GoDaddy TLSルートCA - R1階層（具体的にはGoDaddy TLS中間CA DV - R1v1）を使用して証明書チェーンを提示していました。これは、Webex呼び出しの信頼された認証局リストには含まれていません。

Webexバックエンド(pylon)がSIP認証情報要求中にサーバ証明書信頼チェックを実行したとき、信頼できるルート証明書への有効な証明書パスを構築できませんでした。これにより、SunCertPathBuilderExceptionが発生し、「要求されたターゲットへの有効な証明書パスが見つかりません」というエラーが発生し、HTTP 400応答と同期が中断されました。

Webexコールは、古いGoDaddy/Starfieldルート（Go Daddyルート認証局 – G2など）のみを信頼し、新しい「GoDaddy TLS」(R1/R1v1)階層は信頼しません。

関連コンテンツ

- Webexハイブリッドサービスでサポートされる認証局
- GoDaddy証明書リポジトリ
- シスコのテクニカルサポートとダウンロード

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。