

Cisco Webex ハイブリッド コール サービス接続のトラブルシューティング ガイド

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コールのセットアップの問題](#)

[相互 TLS ハンドシェイクの失敗](#)

[相互 TLS のトラブルシューティングに役立つヒント](#)

[問題1: Expressway-EがCisco Webex証明書に署名した認証局\(CA\)を信頼しない](#)

[問題 2 : Expressway-E Cisco Webex ハイブリッド DNS ゾーンの TLS サブジェクト検証名の名前が正しくない](#)

[問題 3 : Expressway-E が Cisco Webex に完全な証明書チェーンを送信しない](#)

[問題 4 : ファイアウォールによって相互 TLS ハンドシェイクが終了する](#)

[問題 5 : Expressway-E がパブリック CA によって署名されているが、Cisco Webex Control Hub に代替証明書がロードされている](#)

[問題 6 : Expressway が着信コールを Cisco Webex ハイブリッド DNS ゾーンにマッピングしていない](#)

[問題 7 : Expressway-E でデフォルトの自己署名証明書が使用されている](#)

[インバウンド: Cisco Webex からオンプレミスへ](#)

[問題 1 : Cisco Webex が Expressway-E DNS SRV/ホスト名を解決できない](#)

[問題 2 : ソケット障害 : ポート 5062 で Expressway への着信がブロックされる](#)

[問題 3 : ソケット障害 : Expressway-E がポート 5062 をリッスンしていない](#)

[問題 4 : Expressway-E または C がプリロード済み SIP ルート ヘッダーをサポートしていない](#)

[問題 5 : Cisco Webex アプリで 2 つのコール通知 \(トースト \) を受信している](#)

[アウトバウンド: オンプレミスから Cisco Webex へ](#)

[問題1: Expresswayがcallservice.ciscospark.comアドレスを解決できない](#)

[問題 2 : ポート 5062 で Cisco Webex への発信がブロックされる](#)

[問題 3 : Expressway-E の検索ルールが正しく設定されていない](#)

[問題 4 : Expressway の CPL が正しく設定されていない](#)

[双方向 : Cisco Webex からオンプレミスへ、またはオンプレミスから Cisco Webex へ](#)

[問題 1 : IP フォン/コラボレーション エンドポイントで G.711、G.722、または AAC-LD 以外のオーディオコーデックを提供している](#)

[問題 2 : Unified CM の最大着信メッセージ サイズを超えている](#)

[付録](#)

[Expressway トラブルシューティング ツール](#)

[パターンの確認ユーティリティ](#)

[検索ユーティリティ](#)

[診断ログイン](#)

[関連情報](#)

概要

このドキュメントでは、既存の Cisco 呼制御インフラストラクチャから Cisco Collaboration Cloud に接続して相互の連携を可能にする Cisco Webex ハイブリッド コール サービス接続のソリューションについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Webex オファラーの知識
- Expressway ソリューション (B2B) の知識
- Cisco Unified Communications Manager (Unified CM) および Expressway との統合の知識
- Unified CM 10.5(2) SU5以降。
- Expressway (B2B) バージョン X8.7.1 以降 (X8.9.1 を推奨)
- Expressway (コネクタホスト) : 現在サポートされているバージョンについては、「[Expressway Connector Host Support for Cisco Webex Hybrid Services](#)」を参照してください

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Unified Communications Manager
- Expressway
- Webex for Windows
- Mac用WebEx
- Webexfor iOS
- Webex for Android
- シスコ コラボレーション エンドポイント
- コラボレーション デスク エンドポイント
- IP フォン
- ソフトウェア クライアント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このソリューションには、次の機能があります。

- Webexアプリを音声およびビデオ通話のモバイルソフトクライアントとして使用する
- アプリを使用してオフィスにいる場合とまったく同様に任意の場所から通話を発着信
- Webex、Cisco Jabber、またはそのデスクフォンを使用して通話を発信できます。使用する

オプションを心配する必要はありません

- オンプレミスの電話機で通話履歴をロック解除し、その履歴をWebexに統合

このガイドでは、ハイブリッド コール サービス接続に固有の問題について説明します。ハイブリッドコールサービス接続は、モバイルおよびリモートアクセスやBusiness to Business(B2B)コールなどの他のソリューションと同じExpressway E & Cペアで実行されるため、他のソリューションの問題がハイブリッドコールサービス接続に影響する可能性があります。コール サービス接続での使用を目的として Expressway ペアを導入しているお客様やパートナーは、ハイブリッド コール サービス接続の導入を試みる前に、必ず『[Cisco VCS Expressway および VCS Control 基本設定ガイド](#)』を参照してください。このトラブルシューティング ガイドでは、付録 3 と 4 の両方で、Expressway の設計とともにファイアウォール/NAT に関する考慮事項について説明します。このドキュメントに十分目を通してください。また、このドキュメントでは、Expressway コネクタ ホストとハイブリッド コール サービスのアクティベーションが完了していることを前提としています。

コールのセットアップの問題

相互 TLS ハンドシェイクの失敗

ハイブリッド コール サービス接続では、Cisco Webex と Expressway-E 間の認証に相互 Transport Layer Security (TLS) が使用されます。そのため、Expressway-E と Cisco Webex の両方が、互いに提示する証明書を確認し検査します。Expresswayサーバの新規導入時には相互 TLSの問題が非常に多く、Hybrid Call Service Connectなどのソリューションを有効にしているため、このセクションではExpresswayとCisco Webexの間の証明書ベースの問題をトラブルシューティングする際説明します。

Expressway-E は何を確認するか。

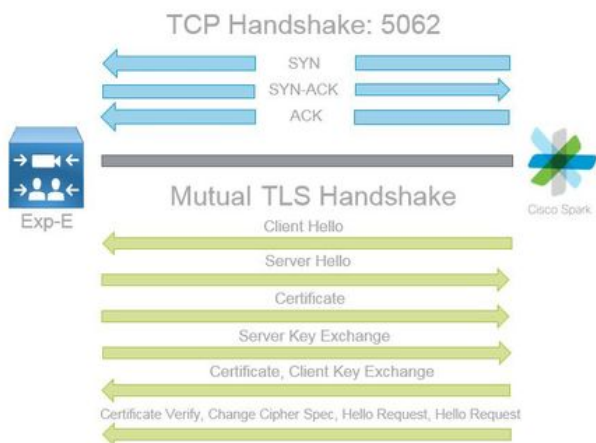
- Cisco Webex 証明書は、Expressway-E の信頼済み CA リストに記載されているパブリック CA によって署名されたか。
- `callservice.ciscospark.com`は、Cisco Webex証明書の[Subject Alternate Name]フィールドに存在しますか。

Cisco Webex は何を確認するか。

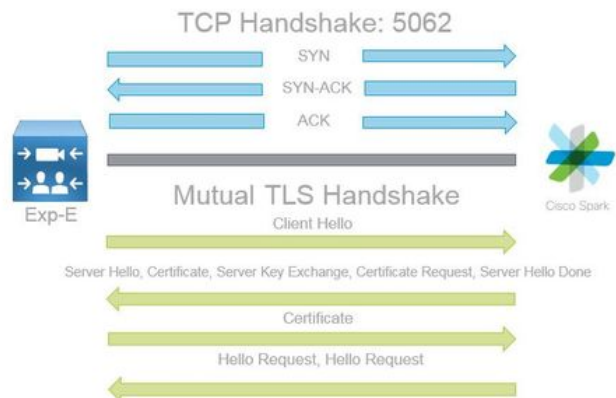
- Expressway-E証明書は、Webexが信頼するパブリックCAのいずれかによって署名されていますか。([Cisco Webex の信頼済み CA リスト](#))
- Expressway-Eが公開署名付き証明書を使用していない場合、Expressway証明書は、Cisco Webex Control Hub(<https://admin.ciscospark.com>)にアップロードされたルート証明書および中間証明書と一緒にありますか。

これは図のように説明されます。

Spark to On Premise



On Premise to Spark



相互 TLS のトラブルシューティングに役立つヒント

1.相互TLSハンドシェイクのデコード

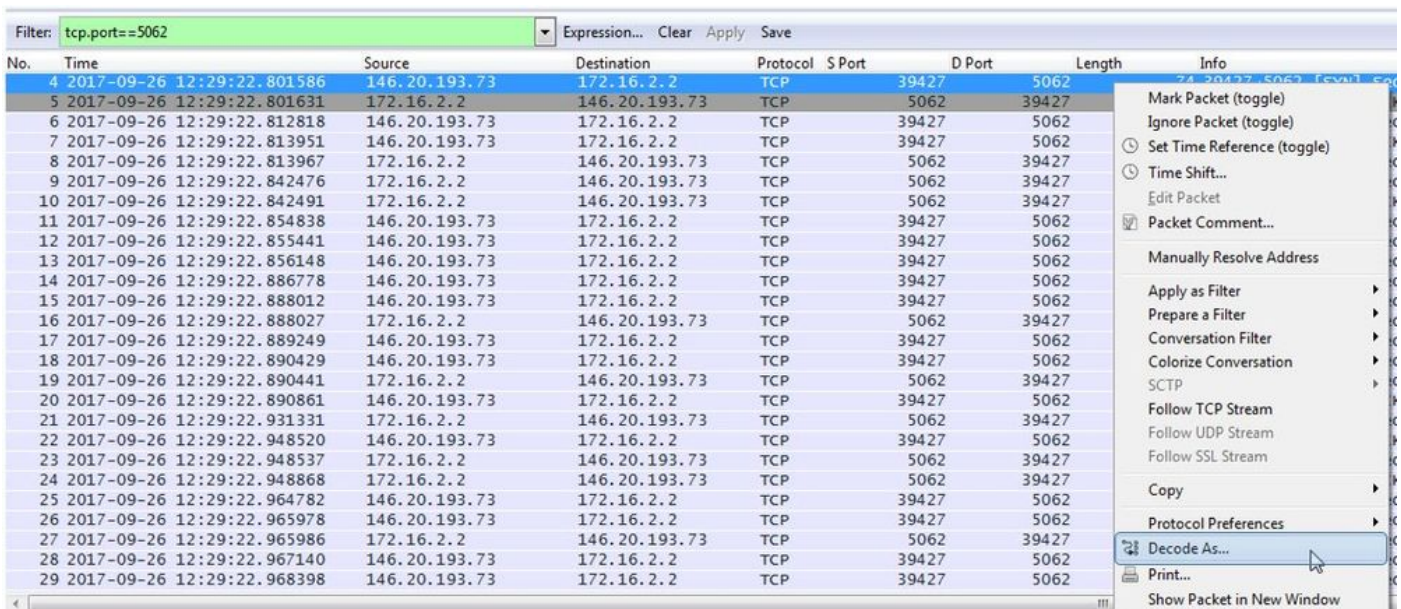
デフォルトでは、Wireshark は SIP TLS トラフィックをポート 5061 としてマークします。つまり、ポート5062で発生する（相互の）TLSハンドシェイクを分析する場合、Wiresharkはトラフィックを正しくデコードする方法を認識しません。ポート 5062 経由で発生している相互 TLS ハンドシェイクの例を次の図に示します。

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TCP	48520	5062	266	48520->5062 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=200 TSval=3875387349 TSecr=444315393
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TCP	5062	48520	2802	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=2736 TSval=444315436 TSecr=3875387349
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TCP	5062	48520	1426	5062->48520 [PSH, ACK] Seq=2737 Ack=201 Win=30080 Len=1360 TSval=444315436 TSecr=3875387349

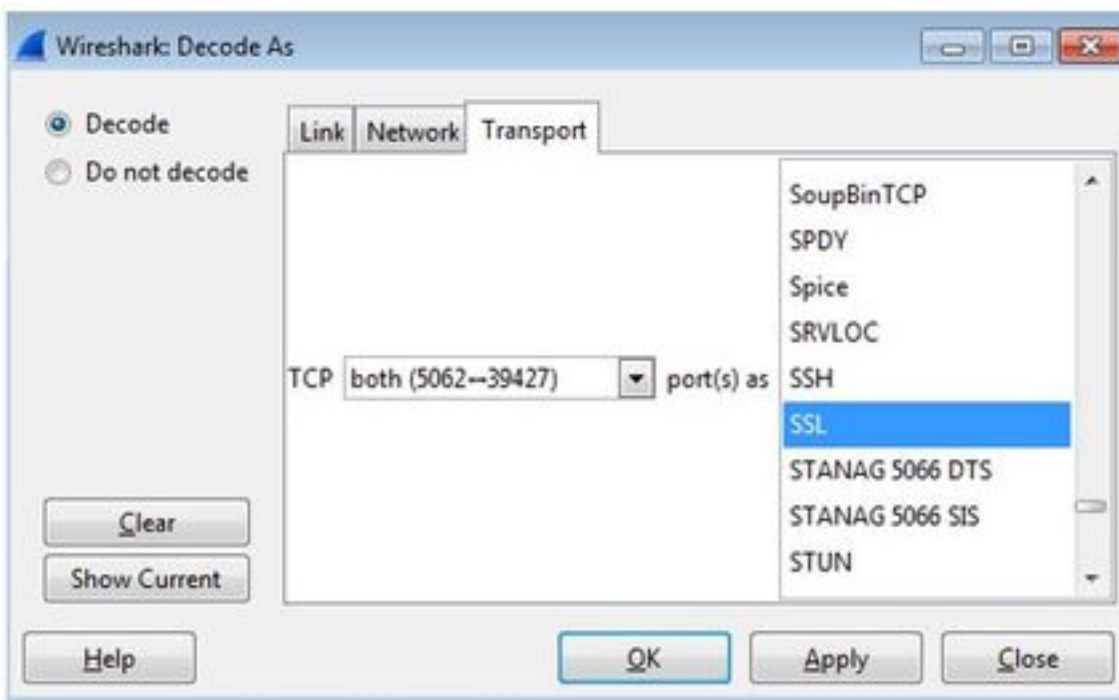
ご覧のように、Wireshark でのデフォルト設定ではハンドシェイクはこのようになります。パケット番号 175 は、Expressway から Cisco Webex に送信される証明書です。ただし、復号化しようとするトラフィックがなければそのことを判断できません。2つの方法を使用してこのトラフィックを復号化でき、証明書の情報や発生するエラーメッセージをもっと簡単に確認できます。

1a.ストリームを SSL として復号化します。

a.相互TLSハンドシェイクを分析すると、最初にキャプチャをtcp.port==5062でフィルタします。その後、ストリーム内の最初のパケットを右クリックし、**Decode As...**を選択します。図に示すように



b.[復号化 (Decode As...)] オプションを選択するとリストが表示され、選択したストリームの復号化方法を選択できます。リストから[SSL]を選択し、[Apply]をクリックしてウィンドウを閉じます。この時点では、図のようにストリーム全体で、ハンドシェイクの時点で交換される証明書とエラーメッセージを示しています。



1b.SIP TLS ポートを調整します。

Wireshark の設定で SIP TLS ポートを 5062 に調整するときは、ハンドシェイクに関連するすべての詳細を表示できます。これには証明書も含まれます。この変更を加えるには次の操作を行います。

- Wireshark を開きます。
- [編集 (Edit)] > [設定 (Preferences)] に移動します。
- プロトコルを展開し、[SIP] を選択します。
- SIP TLS ポートを 5062 に設定し、[適用 (Apply)] をクリックします。
- 図に示すように、解析が完了したら、値を5061に戻します。

SIP TCP ports:

SIP TLS Port:

Display raw text for SIP message:

ここで同じキャプチャを分析すると、パケット 169 ~ 175 が復号化されていることがわかります。パケット 175 は Expressway-E 証明書を示しており、パケットをドリルダウンすると、図のようにすべての証明書の詳細を表示できます。

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=3875387337 WS=128
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TLSv1.1	48520	5062	268	Client Hello
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TLSv1.1	5062	48520	2802	Server Hello
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TLSv1.1	5062	48520	1426	Certificate

2. Wiresharkフィルタリング

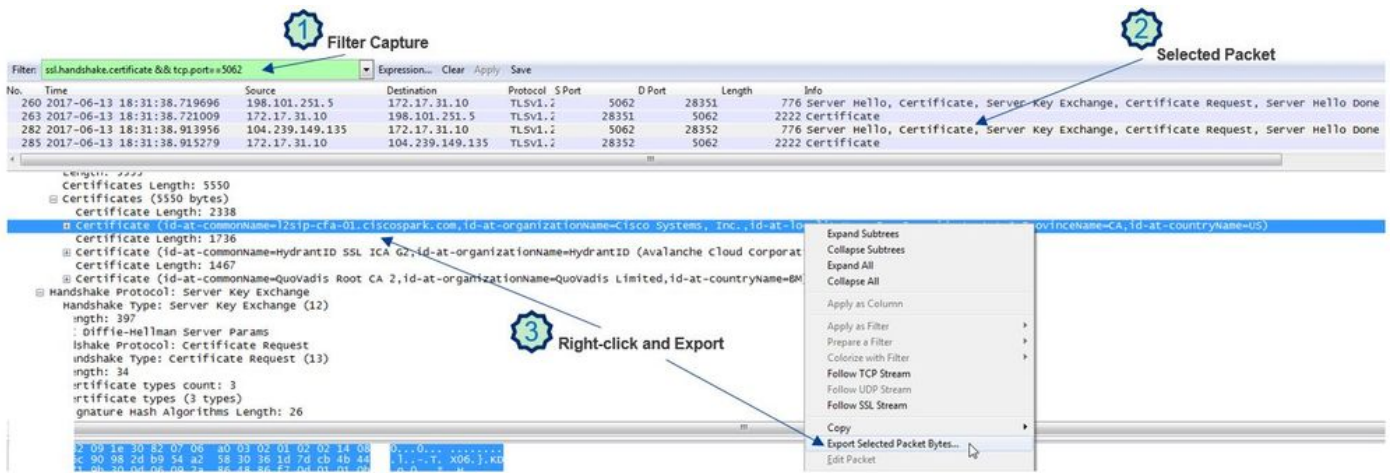
パケット キャプチャを分析するときは、特定のキャプチャで観察されるパケットの量が膨大になり、目標を見失いがちです。Wireshark でフィルタ処理を行って目的のトラフィックのみを表示できるように、どのようなトラフィック タイプが最も必要かを理解しておくことが重要です。相互 TLS ハンドシェイクに関する詳細情報を取得するためによく使用する Wireshark フィルタを次に示します。

- tcp.port == 5062
- ssl && tcp.port == 5062
- ssl.handshake.certificate && tcp.port == 5062

3. Pcapからの証明書の抽出

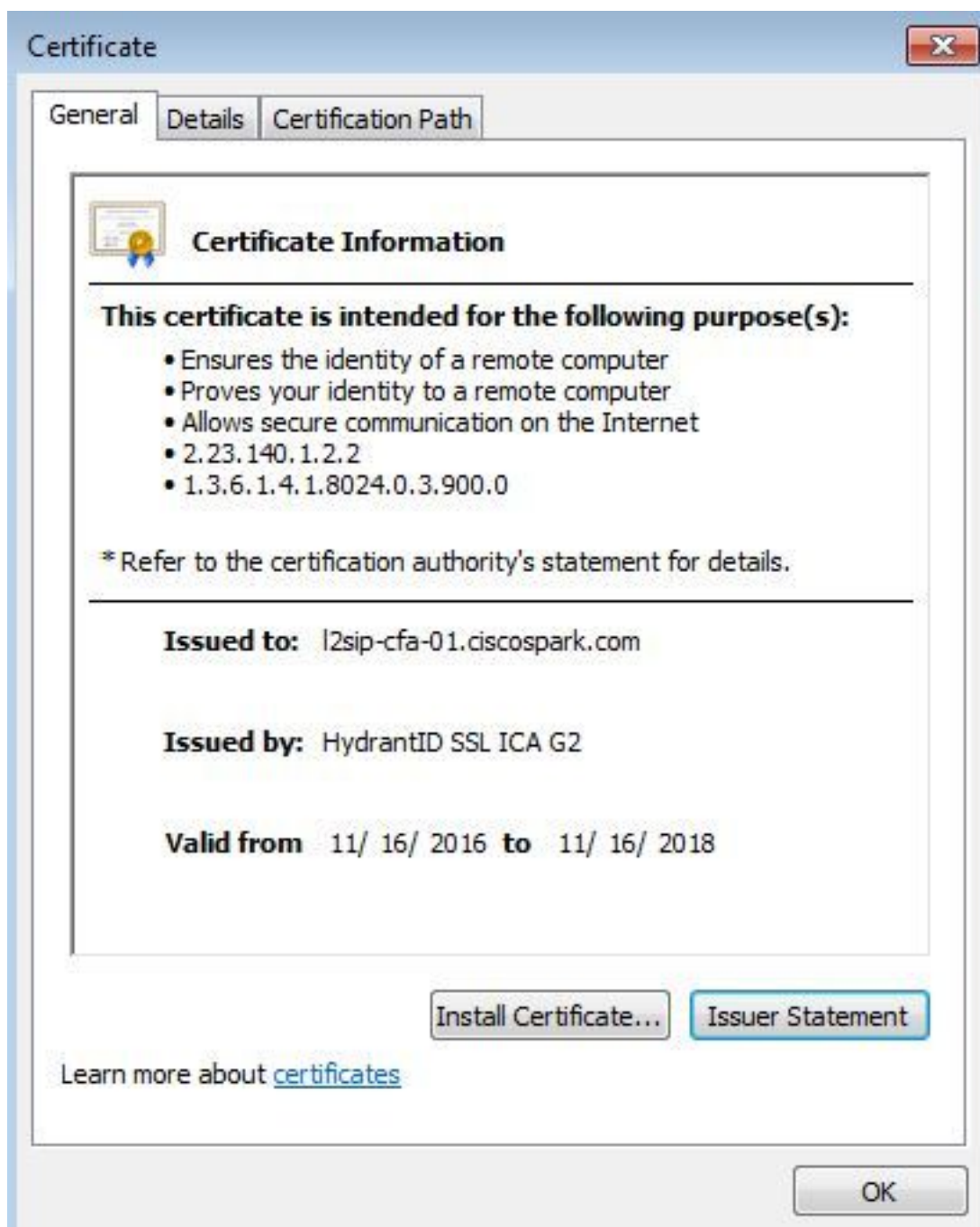
時々、証明書 (サーバ、ルート、または中間) のコピーを取得する必要がある場合があります。証明書をどこで検索すればよいか分からない場合は、パケット キャプチャから直接抽出できます。相互 TLS ハンドシェイクで提示される Cisco Webex 証明書を抽出する方法の手順を次に説明します。

1. `ssl.handshake.certificate && tcp.port == 5062` を使用してパケット キャプチャをフィルタ処理します。
2. Webex サーバ アドレスを送信元とし、証明書が [情報 (Info)] セクションに出力されているパケットを見つけます。
3. パケットの詳細で、[Secure Socket Layer] > [TLS Certificate] > [Handshake Protocol] > [Certificates]を展開します。注：チェーンの一番下/最後の証明書はルート CA です。
4. 目的の証明書を右クリックし、図のように [選択したパケット バイトをエクスポート (Export Selected Packet Bytes...)] を選択します。



5. ファイルを .cer として保存します。

6. 図に示すように、保存したファイルをダブルクリックして証明書を開きます。



4. Expresswayのログレベルを調整する

2つのロギングモジュールをExpresswayで使用できます。これらは、証明書を分析する際にExpresswayでどのようなロジックが実行されているのかについて理解を深めるのに役立ちます。

- developer.ssl
- developer.zone.zonemg

デフォルトでは、これらのロギングモジュールはINFOレベルに設定されています。DEBUGレベルに設定すると、実行される証明書のインスペクションについての情報や、どのゾーントラフィックがマッピングされるのかがわかるようになります。これらの機能はどちらもハイブリッドコールサービスに関連するものです。

Cisco Webexのサーバ証明書のSANインスペクションを実行するExpressway-Eの例です。

```
2017-09-22T11:11:19.485-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,485"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1960)"
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700": Detail="Handshake succeeded"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1629)"
Method="::TTSSL_retrieveCommonName" Thread="0x7f576cbee700": Detail="Found common name in peer
certificate" CommonName="l2sip-cfa-01.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01-web.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-web.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="callservice.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="callservice.call.ciscospark.com"
```

Expressway-EがMTLS接続をCisco WebexハイブリッドDNSゾーンにマッピングする例：

```
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1226)"
```



```
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" getDNSZoneByTLSVerifySubjectName classified subject name
callservice.ciscospark.com into DNS zone Hybrid Call Services DNS
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1183)"
Method="ZoneManager::getDNSZoneByTLSVerifySubjectNameList" Thread="0x7f577f0a0700":
this="0x56408ff81220" Detail="Searched for DNS Zones by Subject Name" Found="True"
Candidates="l2sip-cfa-01.ciscospark.coml2sip-cfa-01.ciscospark.coml2sip-cfa-01.wbx2.coml2sip-
cfa-01-web.wbx2.coml2sip-cfa-web.wbx2.comcallservice.ciscospark.com" MatchedZone="Hybrid Call
Services DNS" MatchedIdentity="callservice.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1054)"
Method="ZoneManager::getZoneByIdentities" Thread="0x7f577f0a0700": this="0x56408ff81220"
Detail="getZoneByIdentities, match complete" Identitites="{CN: l2sip-cfa-01.ciscospark.com, Alt-
DNS: l2sip-cfa-01.ciscospark.com, Alt-DNS: l2sip-cfa-01.wbx2.com, Alt-DNS: l2sip-cfa-01-
web.wbx2.com, Alt-DNS: l2sip-cfa-web.wbx2.com, Alt-DNS: callservice.ciscospark.com, Alt-DNS:
callservice.call.ciscospark.com, Alt-DNS: l2sip-a-Webexcall.ciscospark.com, Alt-DNS: l2sip-prod-
11-dfw-public.wbx2.com, Alt-DNS: l2sip-prod-12-dfw-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-
294-riad-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-817-riad-public.wbx2.com, Alt-DNS: l2sip-
l2sip-prod-wpsjc-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpsjc-web.wbx2.com, Alt-DNS:
l2sip-l2sip-prod-wpdfw-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpdfw-web.wbx2.com, Alt-
DNS: l2sip-cfa-02.wbx2.com, Alt-DNS: Webexcmr-wpa.ciscospark.com, Alt-DNS: Webexcmr-
wpb.ciscospark.com, Alt-DNS: Webexcmr-wpc.ciscospark.com, Alt-DNS: l2sip-wpa-01.wbx2.com, Alt-
DNS: l2sip-wpa-02.wbx2.com, Alt-DNS: l2sip-wpb-01.wbx2.com, Alt-DNS: l2sip-wpb-02.wbx2.com, Alt-
DNS: l2sip-wpc-01.wbx2.com, Alt-DNS: l2sip-wpc-02.wbx2.com}" MatchMechanism="DNSZoneMatch"
MatchedZone="Hybrid Call Services DNS"
```

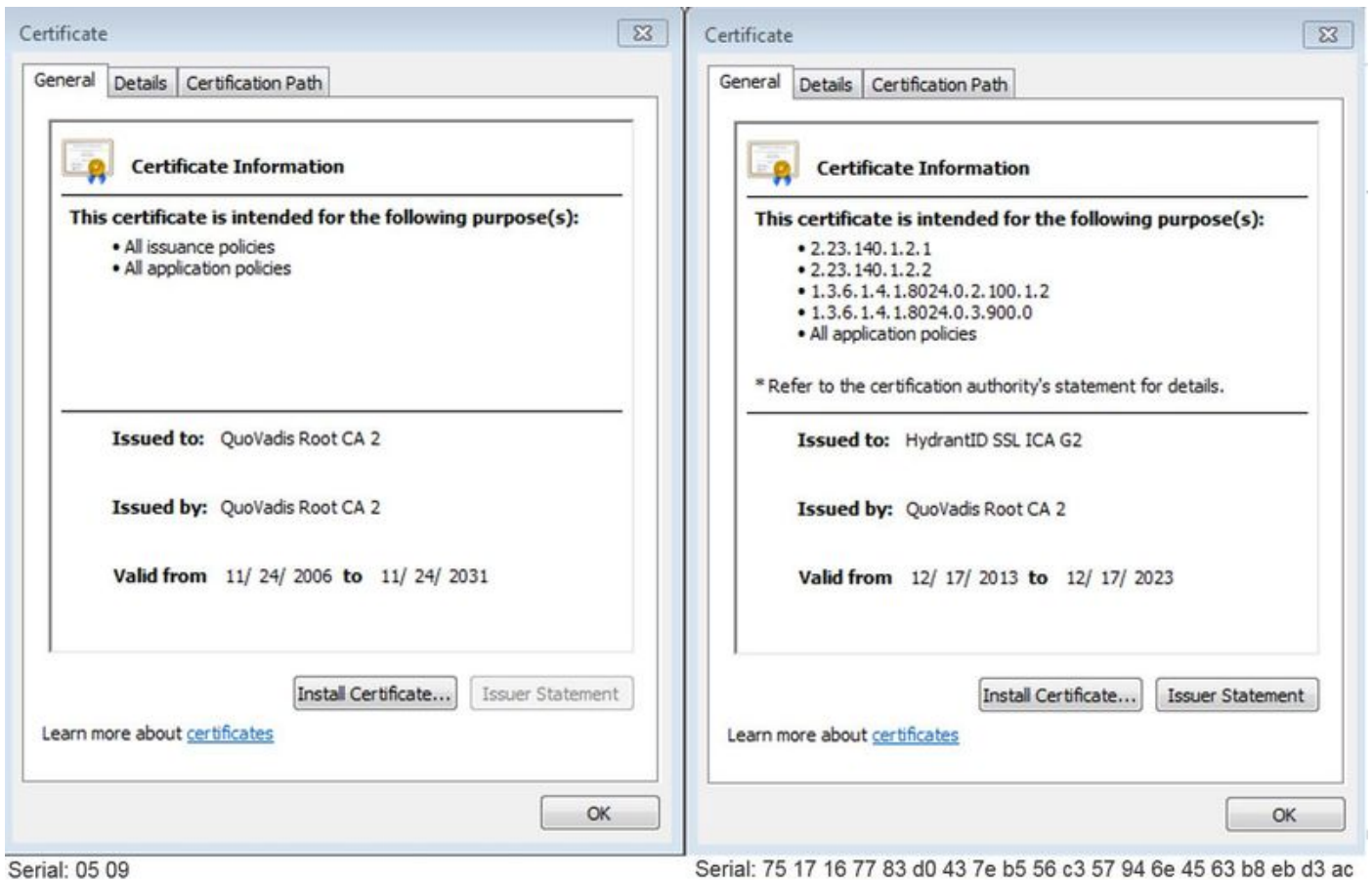
Expressway-E と Cisco Webex 間での相互 TLS の障害に関連してよく発生する問題を次のリストに示します。

問題1: Expressway-EがCisco Webex証明書に署名した認証局(CA)を信頼しない

Expressway-E と直接通信する Cisco Webex サーバのことを、L2SIP サーバと呼びます。この L2SIPサーバは、Hydant SSL ICA G2という共通名で中間サーバによって署名されます。図に示すように、中間サーバはQuoVadis Root CA 2という共通名のルート認証局によって署名されます。

。

注：この仕組みは変更される場合があります。



Expressway の診断の観点からこのトラフィックを分析するため、最初のステップとして TCP Connecting を検索します。TCP Connecting を検索したら、Dst-port=5062 という値を探します。ログ内で、この接続が試行され確立された領域を特定したら、TLS ハンドシェイクを探することができます。これは通常、進行中のハンドシェイクを示すログ エントリによって示されます。

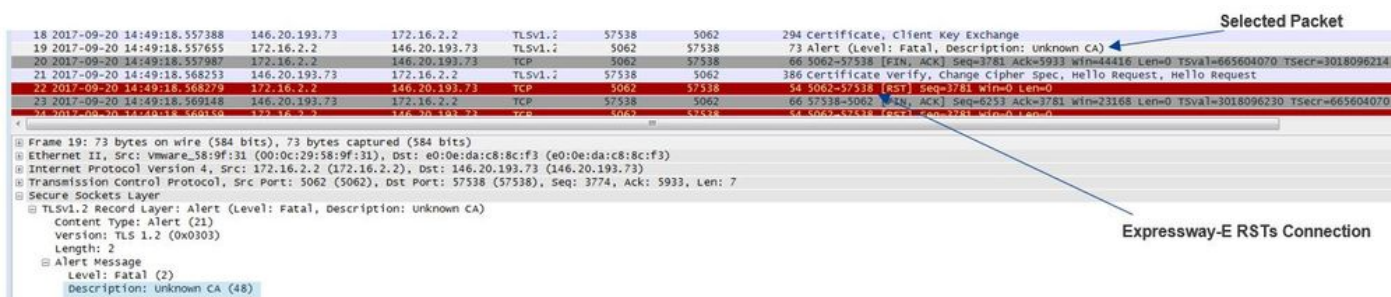
```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700": Detail="Handshake in progress"
Reason="want read/write"
```

Expressway-E が、Cisco Webex による署名の証明書を信頼していない場合は、ハンドシェイク完了直後に Expressway-E が証明書を拒否している可能性がありますと予想できます。このことは、Expressway-E ログにある次のログ エントリで特定できます。

```
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="self signed certificate in certificate chain" Protocol="TLS" Level="1" UTCTime="2017-09-20 14:49:18,724"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSL_ErrorOutput" Thread="0x7f29ddefa700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="-1" error="1" bServer="true"
localAddress="['IPv4' 'TCP' '172.16.2.2:5062']" remoteAddress="['IPv4' 'TCP' '146.20.193.73:58531']"
ssl_error_reason="error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify
failed"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="self signed certificate in certificate
chain"
```

Expresswayのエラーメッセージは、証明書チェーン内の自己署名証明書を参照しているため、やや誤った可能性があります。Wiresharkを使用すると、交換を詳しく見ることができます。

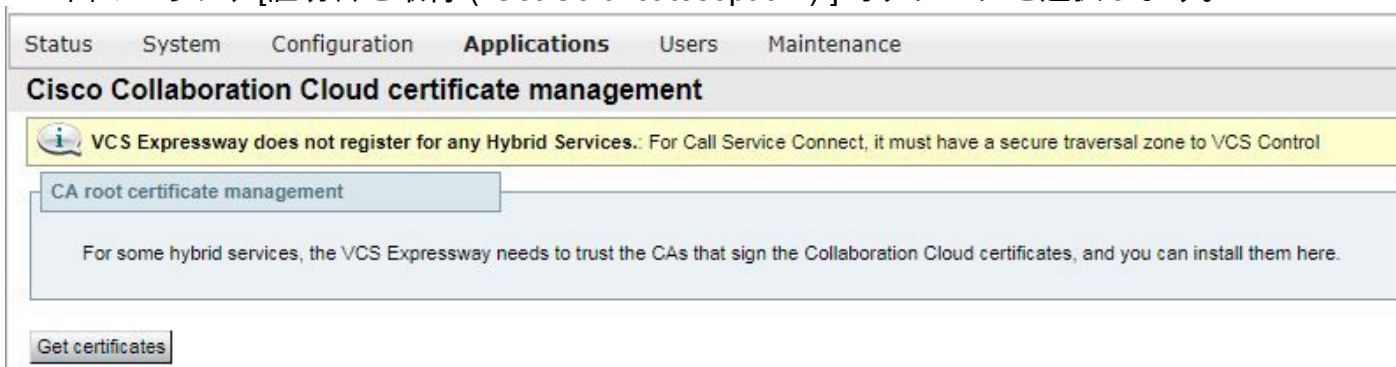
Wiresharkパケットキャプチャ分析の観点から見ると、Webex環境がその証明書を提示した後、Expresswayが振り返り、図に示すように不明なCAエラーを含む証明書で拒否されていることがわかります。



ソリューション :

この状況を解決するには、Expressway-E が Cisco Webex の認証局を信頼するようになる必要があります。これらの証明書を単純に Wireshark のトレースから抽出して、Expressway 上の信頼済み CA 証明書ストアにアップロードすることもできますが、Expressway ではもっと簡単な方法が提供されています。

- Expressway-E にログインします。
- [Applications] > [Cloud Certificate management]に移動します
- 図のように、[証明書を取得 (Get Certificatesoption)] オプションを選択します。



この時点で、Cisco Webex の証明書の認証局が Expressway-E の信頼済み CA ストアにアップロードされます ([メンテナンス (Maintenance)] > [セキュリティ (Security)] > [信頼済み CA 証明書 (Trusted CA certificate)]) 。

問題 2 : Expressway-E Cisco Webex ハイブリッド DNS ゾーンの TLS サブジェクト検証名の名前が正しくない

相互 TLS ハンドシェイクの一部として、ハイブリッド コール サービス接続で TLS 検証が使用されます。つまり、ExpresswayはCisco Webex CA証明書を信頼するだけでなく、提示された証明書のサブジェクト代替名(SAN)フィールドをチェックして証明書を検証し、**callservice.ciscopark.com**などの値が存在することを確認します。この値が存在しない場合、着信コールは失敗します。

この特定のシナリオでは、Cisco WebexサーバからExpressway-Eに証明書が提示されます。実際には、証明書には 25 の異なる SAN が存在します。Expressway-Eがcallservice.ciscopark.com SANの証明書をチェックするが、見つからない場合を検討します。この条件が満たされると、診断ログ内で次のようなエラーを見つけることができます。

```

2017-09-20T11:17:42.701-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
UTCtime="2017-09-20 15:17:42,700"
2017-09-20T11:17:42.701-04:00 amer-expressway01 tvcs: UTCtime="2017-09-20 15:17:42,700"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was
unacceptable"

```

Wireshark を使用してこの証明書ハンドシェイクを分析すると、図のように、Cisco Webex が自身の証明書を提示した後ですぐに、Expressway が接続を RST していることがわかります。

The image shows a Wireshark packet capture of a TLS handshake. Packet 76 is selected, showing a TCP segment with RST flag set. The extension list below shows the SAN value is callservice.ciscospark.com.

No.	Time	Source	Destination	Protocol	Length	Info
71	2017-09-20 15:17:42.646845	146.20.193.45	172.16.2.2	TLSv1.2	46049	5062 294 Certificate, Client Key Exchange
72	2017-09-20 15:17:42.687317	172.16.2.2	146.20.193.45	TCP	5062	46049 66 5062-46049 [ACK] Seq=4746 Ack=5933 win=4416 Len=0 TSval=447644787 TSecr=3878716684
73	2017-09-20 15:17:42.700250	146.20.193.45	172.16.2.2	TLSv1.2	46049	5062 386 Certificate verify, change cipher spec, Hello Request, Hello Request
74	2017-09-20 15:17:42.700260	172.16.2.2	146.20.193.45	TCP	5062	46049 66 5062-46049 [ACK] Seq=4746 Ack=6253 win=47104 Len=0 TSval=447644799 TSecr=3878716745
75	2017-09-20 15:17:42.700534	172.16.2.2	146.20.193.45	TLSv1.2	5062	46049 117 Change cipher spec, Encrypted Handshake Message
76	2017-09-20 15:17:42.700898	172.16.2.2	146.20.193.45	TCP	5062	46049 66 5062-46049 [FIN, ACK] Seq=4797 Ack=6253 win=47104 Len=0 TSval=447644800 TSecr=3878716745
77	2017-09-20 15:17:42.712865	146.20.193.45	172.16.2.2	TCP	46049	5062 1434 [TCP segment of a reassembled PDU]
78	2017-09-20 15:17:42.712869	172.16.2.2	146.20.193.45	TCP	5062	46049 54 5062-46049 [RST] Seq=4797 Win=0 Len=0

```

Extension (id-ce-subjectAltName)
  Extension Id: 2.5.29.17 (id-ce-subjectAltName)
  GeneralNames: 25 items
    dnsName: l2sip-cfa-01.ciscospark.com
    dnsName: l2sip-cfa-01.wbx2.com
    dnsName: l2sip-cfa-01.web.wbx2.com
    dnsName: l2sip-cfa-web.wbx2.com
    dnsName: callservice.ciscospark.com (SAN Value)
    dnsName: callservice.call.ciscospark.com

```

この値の設定を確認するには、ソリューション用に設定された Webex ハイブリッド DNS ゾーンに移動します。Expressway-E の xConfiguration が存在すれば、「ゾーン設定 (Zone configuration) 」セクションを探して TLS 検証サブジェクト名がどのように設定されたかを調べることができます。xConfiguration では、ゾーンが「ゾーン 1」を先頭に並んでいることに注意してください。前述のとおり分析した問題のある環境の xConfiguration を次に示します。

```

*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscospark.com"

```

この例で示すように、[TLS Verify Subject Name]は、callservice.ciscospark.comではなく callservice.ciscospark.comに設定されています。(追加の「l」に注意してください)。

ソリューション:

この問題を解決するには、TLS 検証サブジェクト名を変更する必要があります。

- Expressway-E にログインします。
- [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
- [Webex ハイブリッド サービス DNS ゾーン (Webex Hybrid Services DNS Zone)] を選択します。
- TLS検証サブジェクト名をcallservice.ciscospark.comに設定します
- [保存 (Save)] を選択します。

注: ロギングの基本的な動作については、を参照してください。この項では、Expressway による証明書の検証と Webex ハイブリッド DNS ゾーンへのマッピングを示しています。

注: Expresswayコードx12.5以降では、新しい「Webex」ゾーンがリリースされています。このWebexゾーンは、Webexへの通信に必要なゾーンの設定を事前に入力します。つまり、TLSサブジェクト検証モードとTLS検証サブジェクト名を設定する必要がなくなります。設定を簡素化するには、Expresswayコードのx12.5以降を実行している場合は、Webexゾーンを利用することをお勧めします。

問題 3 : Expressway-E が Cisco Webex に完全な証明書チェーンを送信しない

相互 TLS ハンドシェイクの一部として、Cisco Webex は Expressway-E 証明書を信頼する必要があります。Cisco Webex には、自身が信頼しているパブリック CA の全リストがあります。通常は、Expressway-E 証明書が、Cisco Webex がサポートしているパブリック CA によって署名されていれば、TLS ハンドシェイクは成功します。設計上、Expressway-E は、パブリック CA によって署名されているにもかかわらず、TLS ハンドシェイク中にのみ証明書を送信します。証明書の完全なチェーン (ルートおよび中間) を送信するには、これらの証明書を Expressway-E 自体の信頼できる CA 証明書ストアに追加する必要があります。

この条件が満たされていない場合、Cisco Webex は Expressway-E 証明書を拒否します。この問題に適合する状況をトラブルシューティングするときは、Expressway-E の診断ログと tcpdump を使用できます。Expressway-E の診断ログを分析すると、次のようなエラーが見つかります。

```
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-19
15:12:09,721"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSL_ErrorOutput" Thread="0x7fc67c6ec700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="[ 'IPv4' 'TCP' '172.16.2.2:5062' ]" remoteAddress="[ 'IPv4' 'TCP' '146.20.193.45:33441' ]"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

これを Wireshark の観点から分析すると、Expressway-E が自身の証明書を提示していることがわかります。パケットを展開すると、サーバ証明書しか送信されていないことがわかります。図に示すように、その後、Cisco Webex は不明な CA エラー メッセージでこの TLS ハンドシェイクを拒否します。

The image shows a Wireshark packet capture of a TLS handshake. The selected packet (40) is a Server Hello, certificate, server key exchange, certificate request, and server hello done. The packet details show the certificate chain, but the handshake fails with the error "Spark Rejects the Handshake 'Certificate Unknown' error".

ソリューション :

このシナリオの問題に対処するためには、Expressway-E 証明書の署名に参与している中間 CA とルート CA を信頼済み CA 証明書ストアにアップロードする必要があります。

ステップ 1 : Expressway-E にログインします。

ステップ 2 : [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [信頼済み CA 証明書 (Trusted CA certificate)] に移動します。

ステップ 3： UI の下部近くにある [アップロード (Upload)] メニューで、[ファイルを選択 (Choose File)] を選択します。

ステップ 4： Expressway-E の署名に参与した CA 証明書を選択します。

ステップ 5： [CA 証明書の追加 (Append CA certificate)] を選択します。

ステップ 6： Expressway-E 証明書の署名に参与したすべての CA 証明書 (中間、ルート) について手順を繰り返します。

ステップ 7： [CA 証明書の追加 (Append CA certificate)] を選択します。

この手順が完了すると、Expressway-E サーバ証明書の署名に参与した証明書の完全なチェーンがキー交換に含まれることがわかります。Wireshark でパケット キャプチャを分析した場合の表示の例を次に示します。

The image shows a Wireshark packet capture of a TLS handshake. The selected packet (1426) is a Certificate. The packet details show the TLSv1.2 Record Layer, Handshake Protocol, and Certificate. The certificate chain includes a Server certificate, an Intermediate certificate, and a Root certificate.

```
175 2017-09-20 14:22:13.336358 172.16.2.2 146.20.193.45 TLSv1.2 5062 48520 1426 Certificate
176 2017-09-20 14:22:13.354189 146.20.193.45 172.16.2.2 TCP 48520 5062 66 48520-5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=3875387398 TSecr=444315436
177 2017-09-20 14:22:13.354185 146.20.193.45 172.16.2.2 TCP 48520 5062 66 48520-5062 [ACK] Seq=201 Ack=2737 win=20480 Len=0 TSval=3875387399 TSecr=444315436
178 2017-09-20 14:22:13.355985 146.20.193.45 172.16.2.2 TCP 48520 5062 66 48520-5062 [ACK] Seq=201 Ack=4097 win=23296 Len=0 TSval=3875387400 TSecr=444315436
179 2017-09-20 14:22:13.355999 172.16.2.2 146.20.193.45 TLSv1.2 5062 48520 715 Server Key Exchange
180 2017-09-20 14:22:13.366930 146.20.193.45 172.16.2.2 TCP 48520 5062 66 48520-5062 [ACK] Seq=201 Ack=4746 win=26112 Len=0 TSval=3875387411 TSecr=444315455
197 2017-09-20 14:22:13.668592 146.20.193.45 172.16.2.2 TLSv1.2 48520 5062 73 Alert (Level: Fatal, Description: Certificate unknown)
198 2017-09-20 14:22:13.668604 146.20.193.45 172.16.2.2 TCP 48520 5062 66 48520-5062 [FIN, ACK] Seq=208 Ack=4746 win=26112 Len=0 TSval=3875387711 TSecr=444315459
199 2017-09-20 14:22:13.668611 172.16.2.2 146.20.193.45 TCP 5062 48520 66 5062-48520 [FIN, ACK] Seq=4746 Ack=209 win=20080 Len=0 TSval=444315768 TSecr=3875387711
200 2017-09-20 14:22:13.681586 146.20.193.45 172.16.2.2 TCP 48520 5062 66 48520-5062 [ACK] Seq=209 Ack=4747 win=26112 Len=0 TSval=3875387725 TSecr=444315768
```

Frame 175: 1426 bytes on wire (11408 bits), 1426 bytes captured (11408 bits) on interface 0

Ethernet II, Src: Vmware_58:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)

Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)

Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 48520 (48520), Seq: 2737, Ack: 201, Len: 1360

[2 Reassembled TCP Segments (3938 bytes): #174(2642), #175(1296)]

Secure Sockets Layer

- TLV1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3923
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 3929
 - Certificates Length: 3926
 - Certificates (3926 bytes)
 - Certificate Length: 1712
 - Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=Domain control validated)
 - Certificate Length: 1236
 - Certificate (id-at-commonName=Go Daddy Secure Certificate Authority - G2,id-at-organizationalUnitName=http://certs.godaddy.com/repositor,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)
 - Certificate Length: 969
 - Certificate (id-at-commonName=Go Daddy Root Certificate Authority - G2,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)

問題 4：ファイアウォールによって相互 TLS ハンドシェイクが終了する

Expressway ソリューションは通常、ファイアウォールとインターフェイスします。多くの場合、ソリューションのインライン ファイアウォールでは何らかのタイプのアプリケーション層インスペクションが実行されます。多くの場合、Expressway ソリューションでは、ファイアウォールでアプリケーション層インスペクションが実行されると、望ましくない結果が管理者に表示されます。この特定の問題は、どのような場合にファイアウォールのアプリケーション層インスペクションによって接続が突然終了するのかを明らかにするのに役立ちます。

Expressway の診断ログを使用して、試行された相互 TLS ハンドシェイクを探することができます。このハンドシェイクは、前述のように、ポート 5062 経由で TCP 接続が確立されたすぐ後に行われます。このシナリオでは、ファイアウォールによって接続が終了すると、次のエラーが診断ログ内に表示されます。

```
Thread="0x7f6496669700": TTSSL_continueHandshake: Failed to establish SSL connection iResult="-1" error="5" bServer="false" localAddress=["IPv4'TCP'172.17.31.10:28351']"]
2017-06-13T13:31:38.760-05:00 vcse tvcs: Event="Outbound TLS Negotiation Error" Service="SIP"
Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Common-name="callservice.ciscospark.com" Level="1" UTCTime="2017-06-13 18:31:38,758"
2017-06-13T13:31:38.760-05:00 vcse tvcs: UTCTime="2017-06-13 18:31:38,758" Module="network.tcp"
Level="DEBUG": Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062"
Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

パケット キャプチャの観点から見た場合、Expressway-E が自身の証明書を Cisco Webex に提示していることがわかります。図に示すように、TCP RST は Cisco Webex の方向から来ています。

Selected Packet

Unexpected RST with no error code

Server

Intermediate

Root

一見すると、Expressway-E 証明書に問題があるように見えます。この問題をトラブルシューティングするには、最初に次の問いへの答えを調べる必要があります。

- Expressway-E が、Cisco Webex が信頼するパブリック CA によって署名されているか。
- Expressway-E 証明書および Expressway-E 証明書の署名に関係する証明書は、Cisco Webex Control Hub (<https://admin.ciscospark.com>) に手動でアップロードされますか。

こうした特定の条件では、Cisco Webex Control Hub を使用して Expressway-E を管理することは解決策になりませんでした。つまり、Expressway-E 証明書を、Cisco Webex が信頼するパブリック CA によって署名する必要があります。Wireshark のキャプチャで証明書パケットを選択すると (前の図を参照)、証明書がパブリック CA によって署名され、完全なチェーンが Cisco Webex に送信されたことを確認できます。したがって、問題は Expressway-E 証明書には関連していません。

この時点でさらに分離を必要とする場合は、ファイアウォールの外部インターフェイスからパケット キャプチャを取り除くことができます。ただし、診断ログに SSL エラーが欠けていることは重要なデータポイントになります。前述の「問題 3」から、Cisco Webex が Expressway-E 証明書を信頼していない場合は、必ず何らかのタイプの SSL 切断理由が示されます。この状態では、使用できる SSL エラーはありませんでした。

注：仮にファイアウォールの外部インターフェイスからパケット キャプチャを取得した場合、Cisco Webex 環境から着信する TCP RST を確認できなくなります。

解決方法

この特定のソリューションについては、パートナーまたはお客様としてセキュリティ チームに頼ることが必要になります。チームでは、Expressway ソリューションで何らかの種類のアプリケーション層インスペクションを使用していないかを調べる必要があります。『VCS Control および Expressway 導入ガイド』の「[付録 4](#)」では、お客様がこの機能をオフにすることを勧める理由について説明しています。

問題 5：Expressway-E がパブリック CA によって署名されているが、Cisco Webex Control Hub に代替証明書がロードされている

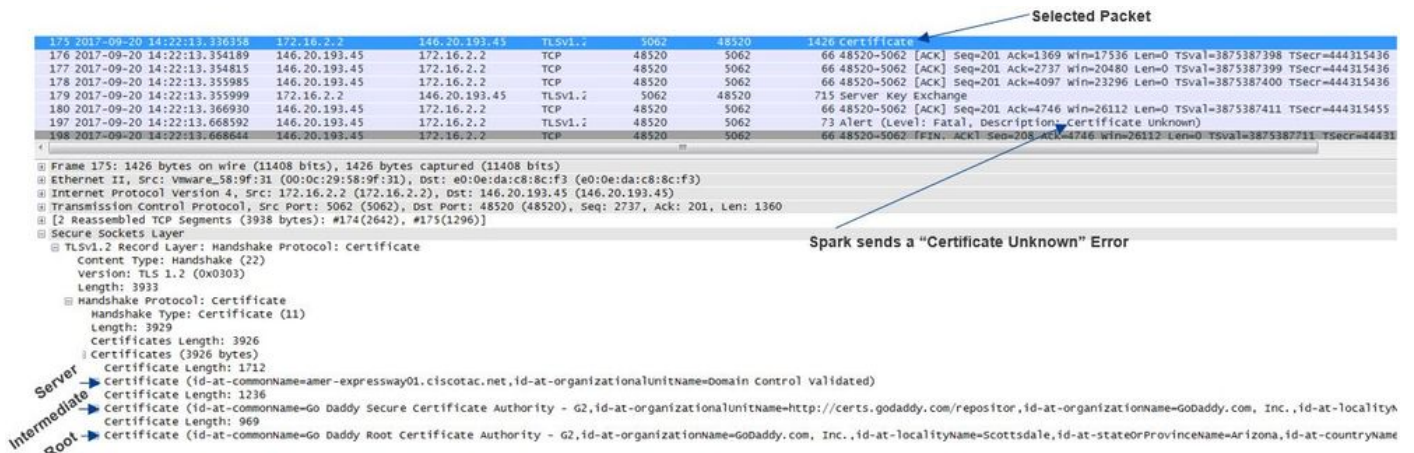
この特定の状況は、多くの場合 Expressway ソリューションを新規に導入して、最初に Expressway-E 証明書をパブリック CA によって署名していないときに生じます。このシナリオでは、相互 TLS のネゴシエーションを正常に完了できるように、Expressway-E サーバ証明書 (内部的に署名済み) を Cisco Webex Control Hub にアップロードします。その後、最終的に Expressway-E 証明書をパブリック CA によって署名しますが、Cisco Webex Control Hub からサ

一バ証明書を削除するのを忘れてしまいます。証明書が Cisco Webex Control Hub にアップロードされると、その証明書は、Expressway が TLS ハンドシイク中に提示する証明書およびチェーンよりも優先されるので注意してください。

Expressway-E診断ロギングの観点からは、この問題は、Cisco WebexがExpressway-E証明書を信頼しない場合に発生するログシグニチャに似ている可能性があります。たとえば、Expressway-Eがチェーン全体を送信していない場合です。TLS ハンドシイク中に Expressway-E ロギングで予期される内容の例を次に示します。

```
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-20
14:22:13,668"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSL_ErrorOutput" Thread="0x7f4a2c16f700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="[ 'IPv4' 'TCP' '172.16.2.2:5062' ]" remoteAddress="[ 'IPv4' 'TCP' '146.20.193.45:48520' ]"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Wiresharkの観点からこれを見ると、Expressway-Eが品目175でその証明書を提示していることがわかります。数行後の品目については、図に示すように、Cisco Webex環境が証明書不明エラーで証明書を拒否します。



Expressway-E が送信する証明書パケットを選択すると、証明書の情報を展開して次のことを調べることができます。

1. Expressway-E が、[Cisco Webex が信頼するパブリック CA](#) によって署名されているか。および、
2. Expressway-E が、署名に参与した自身の完全なチェーンを含めているか。

この状況では、これら両方の条件が満たされています。つまり、Expressway-E 証明書にはまったく問題がないことになります。

解決方法

ステップ 1 : [Cisco Webex Control Hub](#) にログインします。

ステップ 2 : 左側のペインで [サービス (Services)] を選択します。

ステップ 3 : [ハイブリッド コール (Hybrid Call)] カードで [設定 (Settings)] を選択します。

ステップ 4 : [コール サービス接続 (Call Service Connect)] セクションまでスクロールし、[暗号化された SIP コールの証明書 (Certificates for Encrypted SIP Calls)] の下で、望ましくない証明書がリストされているかどうかを調べます。望ましくない証明書がリストされている場合は、証明書の横にあるごみ箱アイコンをクリックします。

ステップ 5 : [削除 (Remove)] を選択します。

注 : 分析を行い、Webex Control Hub にアップロードされた証明書を使用していないことを確かめてから削除することが重要です。

Cisco Webex Control Hub での Expressway-E 証明書のアップロードの詳細については、[『ハイブリッド コール導入ガイド』のこの項](#)を参照してください。

問題 6 : Expressway が着信コールを Cisco Webex ハイブリッド DNS ゾーンにマッピングしていない

着信 TLS マッピングは TLS 検証サブジェクト名と連携して機能し、どちらもハイブリッド コール DNS ゾーンで設定されます。このシナリオでは、x12.5より前のExpresswayで観察された問題と課題について説明します。x12以降では、「Webex」ゾーンと呼ばれる新しいゾーンタイプが実装されました。このゾーンは、Webexとの統合に必要なすべての設定を事前に入力します。x12.5を実行し、Webexハイブリッドコールを展開する場合は、ハイブリッドコールサービスドメイン(callservice.webex.com)が自動的に設定されるように、Webexゾーンの種類を使用することをお勧めします。この値は、相互TLSハンドシェイク中に提示されるWebex証明書のサブジェクト代替名(SAN)と一致し、Expresswayへの接続と着信のマッピングが成功することを許可します。

x12.5より前のコードバージョンを使用している場合、またはWebexゾーンを使用していない場合は、次の説明に進みます。この説明は、Expresswayが着信コールをWebexハイブリッドDNSゾーンにマッピングしていない問題を識別し、修正する方法です。

この機能は 3 ステップのプロセスに分かれます。

1. Expressway-E は、Cisco Webex 証明書を受諾します。
2. Expressway-E は Cisco Webex 証明書を検査し、次の TLS 検証サブジェクト名に一致するサブジェクトの別名が存在するかどうかを確かめます。callservice.ciscospark.com
3. Expressway-E は、Cisco Webex ハイブリッド DNS ゾーンを経由して着信接続をマッピングします。

認証が成功しない場合は、証明書の検証が失敗したことを意味します。コールがデフォルト ゾーンに入り、Expressway-E で B2B を設定している場合は、B2B のシナリオで提供した検索ルールに従ってルーティングされます。

他のシナリオと同様に、診断ログとパケット キャプチャの両方を使用してこの障害の状況を調べ、パケット キャプチャを使用してどちら側が RST を送信しているかを調べる必要があります。試行後に確立されている TCP 接続の例を次に示します。

```
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

TCP 接続が確立されたので、続いて TLS ハンドシェイクを実行できます。ハンドシェイクが開始したすぐ後にエラーが発生していることがわかります。

```
2017-09-22T10:09:57.044-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,044"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method=":ttssl_continueHandshake" Thread="0x7f044e7cc700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
UTCTime="2017-09-22 14:09:57,123"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,123"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was unacceptable"
```

この状況を pcap の観点から見ると、次のことを詳しく把握できます。

- 誰が RST を送信しているか。
- 証明書が正しいかどうかを判断するためにどの証明書が渡されようとしているか。

この特定のキャプチャを分析すると、Expressway-E が RST を送信していることがわかります。渡される Cisco Webex 証明書を調べてみると、完全なチェーンを送信していることがわかります。さらに、診断ログのエラーメッセージから、結論として、Expressway-E が Cisco Webex のパブリック CA を信頼していないというシナリオを除外することができます。除外できないのであれば、「証明書チェーン内の自己署名証明書 (self signed certificate in certificate chain) 」のようなエラーが表示されます。図に示すように、パケットの詳細を調べることができます。

The screenshot shows a Wireshark capture of a network packet. The packet list pane shows a TCP segment at 70 seconds with a RST flag set. The packet details pane shows the structure of the RST packet, including the handshake protocol and certificate chain. The certificate chain includes a self-signed certificate for 'callservice.ciscospark.com'. A blue arrow points to the RST packet in the list pane, and a red arrow points to the self-signed certificate in the details pane. The text 'Expressway-E sends the RST' is written in red next to the RST packet. The text 'Server', 'Intermediate', and 'Root' are written in blue next to the certificate chain details.

Webexサーバ証明書をクリックして展開し、サブジェクト代替名(dnsName)を表示することで、callservice.ciscospark.comがリストされていることを確認できます。

[Wireshark :] [証明書 (Certificate)] > [拡張 (Extension)] > [一般名 (General Names)] > [GeneralName] > [dnsName :] callservice.ciscospark.com

これで、Webex 証明書には問題がないことが完全に確認されます。

今度は、TLS 検証サブジェクト名が正しいことを確認できます。すでに説明したように、xConfiguration があれば、「ゾーン設定 (Zone configuration) 」セクションを探して TLS 検証サブジェクト名がどのように設定されたかを調べることができます。xConfiguration では、ゾーンが「ゾーン 1」を先頭に並んでいることに注意してください。前述のとおり分析した問題のある環境の xConfiguration を次に示します。明らかに、TLS 検証サブジェクト名にもまったく問題はありせん。

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
```

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscospark.com"
```

次に調べる必要があるのは、**TLS 検証着信マッピング**です。ここでは、TLS 接続を Webex ハイブリッド DNS ゾーンに正しくマッピングしているかどうかを確認します。この分析には xConfiguration も利用できます。xConfiguration では、**TLS 検証着信マッピングは DNS ZIP TLS Verify InboundClassification** という名前になっています。この例でわかったように、値はオフに設定されています。

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "Off"
```

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
```

この値が Off に設定されている場合、VCS がこのゾーンへの着信 TLS 接続をマッピングしようとするのを防ぎます。コールはデフォルトゾーンに入り、Expressway-E で Business-to-Business が設定されている場合は、Business-to-Business のシナリオに検索ルールにに従ってチェックされます。

解決方法

これに対処するには、ハイブリッドコール DNS ゾーンの TLS 検証着信マッピングを [オン (On)] に設定する必要があります。これを完了する手順は次のとおりです。

1. Expressway-E にログインします。
2. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
3. [ハイブリッド コール DNS ゾーン (Hybrid Call DNS Zone)] を選択します。
4. [TLS 検証着信マッピング] で、[オン (On)] を選択します。
5. [保存 (Save)] を選択します。

注：ロギングのベースライン動作については、を参照してください。この項では、Expressway による証明書の検証と Webex ハイブリッド DNS ゾーンへのマッピングを示しています。

問題 7： Expressway-E でデフォルトの自己署名証明書が使用されている

ハイブリッド コール サービス接続の一部の新規導入では、Expressway-E 証明書の署名が見過ごされたり、デフォルト サーバ証明書を使用できるという認識があったりします。Cisco Webex Control Hub ではカスタムの証明書をポータルにロードできるので ([サービス (Services)] > [設定 (Settings)] ([ハイブリッド コール (Hybrid Call)] カードの下) > [アップロード (Upload)] ([暗号化されたコールの証明書 (Certificates for Encrypted Calls)] カードの下))、そうしたことが可能だと考えられています。

[暗号化された SIP コールの証明書 (Certificates for Encrypted SIP Calls)] という表現に注目してみると、次のように説明されています。「シスコ コラボレーションのデフォルト信頼リストから提供されている証明書を使用するか、または独自の証明書をアップロードします。独自の証明書を使用する場合は、ホスト名が検証済みのドメイン上にあることを確認してください。」ここ

で重要なのは「ホスト名が検証済みのドメイン上にあることを確認する」の部分です。

この条件に一致する問題をトラブルシューティングするときは、症状がコールの方向に依存していることに注意してください。コールがオンプレミス電話機から発信している場合は、Cisco Webex アプリの着信音が鳴らないと予想できます。また、Expressway の検索履歴からコールのトレースを試みれば、Expressway-E へのコールが成功してそこで停止することがわかります。コールが Cisco Webex アプリから発信していて、宛先がオンプレミスになっていた場合、オンプレミス電話機の着信音は鳴りません。そうした例では、Expressway-E と Expressway-C の検索履歴には何も示されません。

この特定のシナリオでは、コールはオンプレミス電話機から発信されています。Expressway-E の検索履歴を使用すると、サーバへのコールが成功したことを確認できます。この時点では、何が起きたかを判断するために診断ログを調べることができます。この分析を始めるには、最初に、TCP 接続が試行されてポート 5062 経由で確立されたかどうかを確認します。Expressway-E の診断ログで「TCP Connecting」を探し、「Dst-port=5062」というタグのある行項目を検索することで、接続が確立されているかどうかを判断できます。

```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

TCP 接続が確立されていることを確認したので、直後に行われる相互 TLS ハンドシェイクを分析できます。次のスニペットからわかるように、ハンドシェイクは失敗していて証明書は不明になっています (**Detail="ssl3 alert certificate unknown"**) 。

```
2017-09-26T08:18:08.441-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,441"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="ssl3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-26
12:18:08,455"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1997)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700": Detail="Handshake Failed"
Reason="want error ssl"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSL_ErrorOutput" Thread="0x7f930adab700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress=["IPv4'TCP'172.16.2.2:5062']" remoteAddress=["IPv4'TCP'146.20.193.45:59720']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:ssl3 alert certificate unknown"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Expressway-E で提供されたパケット キャプチャを詳しく調べてみると、図のように、証明書不明エラーが Cisco Webex の方向から発生していることがわかります。

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
3	2017-09-26 12:18:08.415918	146.20.193.45	172.16.2.2	TCP	59720	5062	74	59720->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=91375166 TSecr=0
4	2017-09-26 12:18:08.415941	172.16.2.2	146.20.193.45	TCP	5062	59720	74	5062->59720 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=95527059
5	2017-09-26 12:18:08.426317	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=1 Ack=1 win=14720 Len=0 TSval=91375177 TSecr=955270515
6	2017-09-26 12:18:08.427715	146.20.193.45	172.16.2.2	TLSv1.2	59720	5062	266	Client Hello
7	2017-09-26 12:18:08.427728	172.16.2.2	146.20.193.45	TCP	5062	59720	66	5062->59720 [ACK] Seq=1 Ack=201 win=30080 Len=0 TSval=955270527 TSecr=91375178
8	2017-09-26 12:18:08.440978	172.16.2.2	146.20.193.45	TLSv1.2	5062	59720	1780	Server Hello, Certificate, Certificate Request, Server Hello Do
9	2017-09-26 12:18:08.453269	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=91375204 TSecr=955270540
10	2017-09-26 12:18:08.453308	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1715 win=20352 Len=0 TSval=91375204 TSecr=955270540
11	2017-09-26 12:18:08.455958	146.20.193.45	172.16.2.2	TLSv1.2	59720	5062	73	Alert (Level: Fatal, Description: certificate unknown)

Certificate Unknown Sourced from Spark

Expressway-E からのデフォルト サーバ証明書を調べてみると、「共通名 (Common Name) 」と「サブジェクトの別名 (Subject Alternate Names) 」に「検証済みドメイン (Verified Domain) 」 (rtp.ciscotac.net) が含まれていないことがわかります。これで、図に示すように、何がこの問題の原因なのかについて証拠が得られます。

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
8	2017-09-26 12:18:08.440978	172.16.2.2	146.20.193.45	TLSv1.2	5062	59720	1780	Server Hello, Certificate, Server Key
9	2017-09-26 12:18:08.453269	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1369 win=

Secure Sockets Layer

- TLsv1.2 Record Layer: Handshake Protocol: Server Hello
- TLsv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - version: TLS 1.2 (0x0303)
 - Length: 1158
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1154
 - Certificates Length: 1151
 - Certificates (1151 bytes)
 - certificate Length: 1148
 - certificate (id-at-commonName=amer-expressway01.id-at-organizationalUnitName=Temporary Certificate b3821a0
 - signedCertificate
 - version: v2 (2)
 - serialNumber: 1
 - signature (sha256withRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items
 - Extension (id-ce-basicconstraints)
 - Extension Id: 2.5.29.19 (id-ce-basicconstraints)
 - basicConstraintsSyntax [0 length]
 - Extension (ns_cert_exts.comment)
 - Extension Id: 2.16.840.1.113730.1.13 (ns_cert_exts.comment)
 - Comment: Temporary Certificate
 - Extension (id-ce-subjectKeyIdentifier)
 - Extension Id: 2.5.29.14 (id-ce-subjectKeyIdentifier)
 - SubjectKeyIdentifier: f236e03c9b2caa6256cd7db07964e099c4510cc8
 - Extension (id-ce-authorityKeyIdentifier)
 - Extension Id: 2.5.29.35 (id-ce-authorityKeyIdentifier)
 - AuthorityKeyIdentifier
 - Extension (id-ce-keyusage)
 - Extension Id: 2.5.29.15 (id-ce-keyusage)
 - Padding: 5
 - Keyusage: e0 (digitalSignature, contentCommitment, keyEncipherment)
 - Extension (id-ce-extKeyusage)
 - Extension Id: 2.5.29.37 (id-ce-extKeyusage)
 - KeyPurposeIDs: 2 items
 - rithmIdentifier (sha256withRSAEncryption)
 - ing: 0
 - ypTcd: aa5acf123856ab22a57f0a8a512b37c54843cc55e60dc137...

No SAN

Common Name

Selected Packet

Call Service Aware
Users can share content from the Cisco Spark app during a call from their work phones and view their call history in the app.

Domain Verification
rtp.ciscotac.net
+ verified
Add Domain

Certificate Information
Windows does not have enough information to verify this certificate.

Issued to: amer-expressway01

Issued by: Temporary CA 01162d22-e216-470f-991b-802c49981ae7

Valid from 9/26/2017 to 9/26/2018

Install Certificate... Issuer Statement

Learn more about certificates

この時点で、Expressway-E サーバ証明書をパブリック CA または内部 CA によって署名する必要があると判断しました。

解決方法

この問題を解決するには、2 つのオプションを選択できます。

- Expressway-E 証明書が、[Cisco Webex が信頼するパブリック CA](#) によって署名されるようにします。
Expressway にログインします。[メンテナンス (Maintenance)] > [セキュリティ (Security)] > [サーバ証明書 (Server certificate)] に移動します。[CSR の作成 (Generate CSR)] を選択します。必要な証明書情報を入力し、[追加の別名 (Additional alternative names)] フィールドに、Webex Control Hub にリストされている [検証済みドメイン (Verified Domain)] が含まれていることを確認します。[Generate CSR] をクリックします。サードパーティのパブリック CA に署名用の CSR を提供します。証明書に戻り、[メンテナンス (Maintenance)] > [セキュリティ (Security)] > [サーバ証明書 (Server certificates)] に移動します。[サーバ証明書ファイルを選択 (Select the server certificate file)] の隣にある [新しい証明書のアップロード (Upload New Certificate)] セクションで、[ファイルを選択 (Choose File)] を選択し、**署名済みの証明書を選択します**。[サーバ証明

書データのアップロード (Upload server certificate data)] を選択します。 [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [信頼済み CA 証明書 (Trusted CA certificate)] に移動します。 [信頼済み CA 証明書が含まれているファイルを選択 (Select the file containing trusted CA certificates)] の隣にある [アップロード (Upload)] セクションで、 [ファイルを選択 (Choose File)] を選択します。パブリック CA によって提供されるすべてのルートおよび中間 CA 証明書を選択します。 [CA 証明書の追加 (Append CA certificate)] を選択します。 Expressway-E を再起動します。

2. Expressway-E 証明書が内部 CA によって署名されるようにし、内部 CA および Expressway-E 証明書を Cisco Webex Control Hub にアップロードします。 Expressway にログインします。 [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [サーバ証明書 (Server certificate)] に移動します。 [CSR の作成 (Generate CSR)] を選択します。必要な証明書情報を入力し、 [追加の別名 (Additional alternative names)] フィールドに、 Webex Control Hub にリストされている [検証済みドメイン (Verified Domain)] が含まれていることを確認します。 [CSR の生成 (Generate CSR)] をクリックします。サードパーティのパブリック CA に署名用の CSR を提供します。証明書に戻り、 [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [サーバ証明書 (Server certificates)] に移動します。 [サーバ証明書ファイルを選択 (Select the server certificate file)] の隣にある [新しい証明書のアップロード (Upload New Certificate)] セクションで、 [ファイルを選択 (Choose File)] を選択し、署名済みの証明書を選択します。 [サーバ証明書データのアップロード (Upload server certificate data)] を選択します。 [メンテナンス (Maintenance)] > [セキュリティ (Security)] > [信頼済み CA 証明書 (Trusted CA certificate)] に移動します。 [信頼済み CA 証明書が含まれているファイルを選択 (Select the file containing trusted CA certificates)] の隣にある [アップロード (Upload)] セクションで、 [ファイルを選択 (Choose File)] を選択します。パブリック CA によって提供されるすべてのルートおよび中間 CA 証明書を選択します。 [CA 証明書の追加 (Append CA certificate)] を選択します。 Expressway-E を再起動します。

- 2a. 内部 CA および Expressway-E 証明書を Cisco Webex Control Hub にアップロードします。
 1. 管理者として [Cisco Webex Control Hub にログインします。](#)
 2. [サービス] を選択します。
 3. [ハイブリッド コール サービス (Hybrid Call Service)] カードで [設定 (Settings)] を選択します。
 4. [Certificates for Encrypted SIP Calls] セクションで、 [Upload] を選択します。
 5. 内部 CA および Expressway-E 証明書を選択します。

インバウンド: Cisco Webex からオンプレミスへ

Cisco Webex からオンプレミスへの着信障害では、ほとんどすべての場合に同じ症状が報告されています。たとえば、「自分の Cisco Webex アプリから別の同僚のアプリに電話をかけると、同僚のアプリの着信音は鳴るがオンプレミス電話の着信音は鳴らない」などです。このシナリオをトラブルシューティングするためには、この種のコールで発生するコールのフローとロジックの両方について理解しておく必要があります。

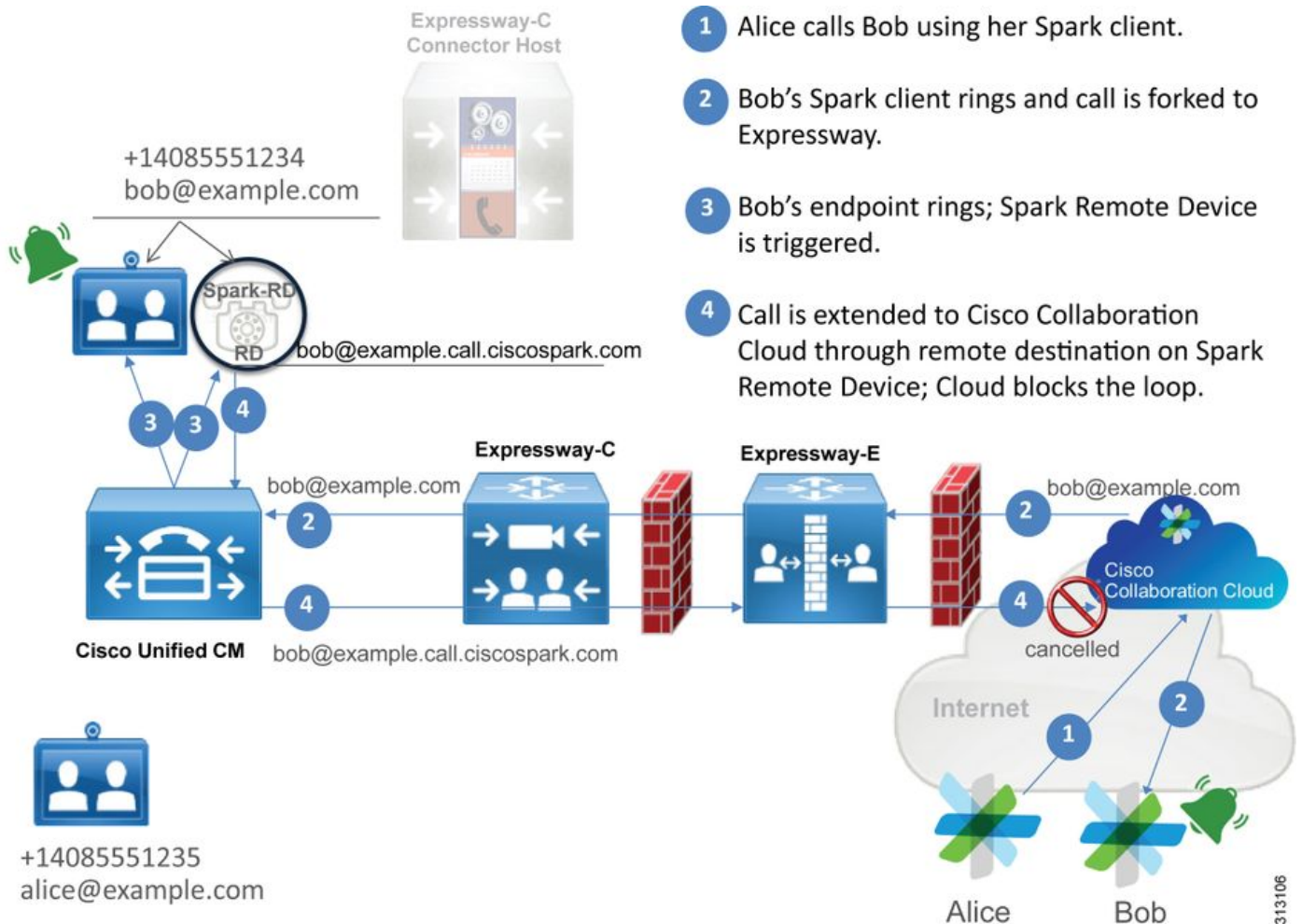
全体的なロジック フロー

1. Cisco Webex アプリの発信側がコールを開始します。
2. 着信側のアプリの着信音が鳴ります。
3. コールが Cisco Webex 環境にフォークされます。
4. Cisco Webex 環境では、顧客が Cisco Webex Control Hub で設定した SIP 宛先に基づいて DNS ルックアップを実行する必要があります。

5. Cisco Webex 環境が、ポート 5062 を介して Expressway への接続を試みます。
6. Cisco Webex 環境が、相互 TLS ハンドシェイクの実行を試みます。
7. Cisco Webex 環境が、SIP INVITE を Expressway に送信し、オンプレミス コラボレーション エンドポイント/IP フォンにまで渡されます。
8. Cisco Webex と会社が SIP ネゴシエーションを完了します。
9. Cisco Webex と会社がメディアの送受信を開始します。

コールフロー

図のように、[Cisco Webex アプリ (Cisco Webex app)] > [Cisco Webex 環境 (Cisco Webex environment)] > [Expressway-E] > [Expressway-C] > [オンプレミス コラボレーション エンドポイント/IP フォン (On-Premises Collaboration Endpoint/IP Phone)] に移動します。



Webex からオンプレミス インフラストラクチャへの着信コールでよく見られるいくつかの問題を次に示します。

問題 1 : Cisco Webex が Expressway-E DNS SRV/ホスト名を解決できない

Cisco Webex からオンプレミスへのコール フローについて考えるとき、Cisco Webex の最初の論理的なステップとなるのは、オンプレミスの Expressway へのコンタクト方法です。前述のように、Cisco Webex はオンプレミス Expressway への接続を試みるため、[Cisco Webex Control Hub の \[ハイブリッド コール サービスの設定 \(Hybrid Call Service Settings \) \]](#) ページにリストされている設定済みの [\[SIP 宛先 \(SIP Destination \) \]](#) に基づいて、SRV ルックアップを実行します。

Expressway-E 診断ログの観点からこの状況をトラブルシューティングしようとする、Cisco

Webex からのトラフィックがまったく確認できません。TCP 接続 (TCP Connecting) を検索しようとしても、Dst-port=5062 を確認できず、その後の MTLS ハンドシェイクも Cisco Webex からの SIP Invite も確認できません。

こうした状況では、Cisco Webex Control Hub で [SIP 宛先 (SIP Destination)] がどのように設定されていたかを調べる必要があります。また、**ハイブリッド接続テスト ツール**を利用して**トラブルシューティングに役立てることもできます**。ハイブリッド接続テスト ツールは、有効な DNS アドレスが存在するかどうか、Cisco Webex が SRV ルックアップで返されたポートに接続できるかどうか、および、Cisco Webex が信頼する有効な証明書がオンプレミスの Expressway に存在するかどうかをチェックします。

1. Cisco Webex Control Hub にログインします。
2. [サービス (Services)] を選択します。
3. [ハイブリッド コール (Hybrid Call)] カードで [設定 (Settings)] リンクを選択します。
4. [コール サービス接続 (Call Service Connect)] セクションで、パブリック SIP の SRV アドレスの指定に使用されるドメインを [SIP 宛先 (SIP Destination)] フィールドで確認します。
5. レコードが正しく入力されている場合は、[テスト (Test)] をクリックしてレコードが有効かどうかを確認します。
6. 下の図に示すように、明らかに、パブリック ドメインに対応する SIP SRV レコードが関連付けられていないことがわかります。

SIP Destination ⓘ

mtls.rtp.ciscotac.net Test Save

✖ Your SIP Destination is not configured correctly. [View test results](#)

[テスト結果を表示 (View test results)] を選択すると、図のように、失敗した内容について詳細を表示できます。

Verify SIP Destination

DNS Lookup failed. Check that a DNS or SRV record exists for your SIP Destination and that it resolves to one or more valid IP addresses.

別の方法として、nslookupを使用してSRVレコードを検索することもできます。次に、SIP宛先が存在するかどうかを確認するために実行できるコマンドを示します。

```
C:\Users\pstoiano>nslookup
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
> set type=SRV
> _sips._tcp.mtls.rtp.ciscotac.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8
DNS request timed out.
timeout was 2 seconds.
```



```
DNS request timed out.  
timeout was 2 seconds.  
*** Request to google-public-dns-a.google.com timed-out
```

このコードブロックでわかるように、nslookup コマンドが開始された後で、サーバがパブリック Google DNS サーバである 8.8.8.8 に設定されています。最後に、SRV レコードを検索するレコードタイプを設定しています。この時点で、検索する完全な SRV レコードを発行できません。結果として、最終的には要求がタイムアウトになります。

解決方法

1. それらがパブリック ドメイン名のホストに使用するサイトで、Expressway-E のパブリック SIP の SRV アドレスを設定します。
2. Expressway-E のパブリック IP アドレスに解決されるホスト名を設定します。
3. ステップ 1 で作成した SIP の SRV アドレスに使用するドメインをリストするように、SIP 宛先を設定します。 [Cisco Webex Control Hub にログインします。](#) サービスの選択[ハイブリッド コール (Hybrid Call)] カードで [設定 (Settings)] リンクを選択します。 [コール サービス接続 (Call Service Connect)] セクションで、パブリック SIP の SRV アドレスに使用されるドメインを [SIP 宛先 (SIP Destination)] フィールドに入力します。 [保存 (Save)] を選択します。

注：使用したい SIP SRV レコードがすでに B2B 通信に利用されている場合は、次のようにして、SIP 検出アドレスとして会社ドメインのサブドメインを Cisco Webex Control Hub で指定し、結果としてパブリック DNS SRV レコードにすることを勧めます。

```
サービスとプロトコル ( Service and protocol ) : _sips._tcp.mtls.example.com  
Priority:1  
重量 : 10  
ポート番号 ( Port number ) : 5062  
Target:us-expe1.example.com
```

これらの推奨値は [『Cisco Webex ハイブリッド設計ガイド』](#) から直接引用したものです。

代替策

SIP SRV レコードを持っていない (作成する予定がない) 場合は、代わりにサフィックスを「:5062」とする Expressway パブリック IP アドレスをリストできます。これにより、Webex環境はSRVルックアップを試行せず、%Expressway_Pub_IP%:5062に直接接続します(例 : 64.102.241.236:5062)

1. SIPの宛先を%Expressway_Pub_IP%:5062形式に設定します(例 : 64.102.241.236:5062) [Cisco Webex Control Hub にログインします。](#) サービスの選択[ハイブリッド コール (Hybrid Call)] カードで [設定 (Settings)] リンクを選択します。 [コール サービス接続 (Call Service Connect)] セクションで、 [SIP 宛先 (SIP Destination)] フィールドに「 %Expressway_Pub_IP%:5062」と入力します。 [保存 (Save)] を選択します。

設定を必要とする SIP 宛先アドレスや SRV レコードの詳細については、『Cisco Webex ハイブリッド コール サービス導入ガイド』の「[組織でハイブリッド コール サービス接続を有効にする](#)」の項、または『Cisco Webex ハイブリッド設計ガイド』を参照してください。

問題 2： ソケット障害： ポート 5062 で Expressway への着信がブロックされる

DNS 解決の完了後、Cisco Webex 環境は、DNS ルックアップ中に返された IP アドレスへのポー

ト 5062 経由の TCP 接続を確立しようとする。この IP アドレスが、オンプレミスの Expressway-E のパブリック IP アドレスになります。Cisco Webex 環境がこの TCP 接続を確立できない場合、後続のオンプレミスへの着信コールは失敗します。この特定の状況では、他のほぼすべての Cisco Webex 着信コール障害と同じである、「オンプレミス電話機の着信音が鳴らない」という症状が現れます。

Expressway 診断ログを使用してこの問題をトラブルシューティングしても、Cisco Webex からのトラフィックはまったく確認できません。TCP 接続 (TCP Connecting) を検索しようとしても、Dst-port=5062 の接続試行を確認できず、その後の MTLS ハンドシェイクも Cisco Webex からの SIP Invite も確認できません。この状況では Expressway-E 診断ログが役に立たないため、いくつかの方法で検証を行います。

1. ファイアウォールの外部インターフェイスからパケット キャプチャを取得します。
2. ポート チェック ユーティリティを利用します。
3. ハイブリッド接続テスト ツールを使用します。

ハイブリッド接続テスト ツールは Cisco Webex Control Hub に組み込まれているもので、Cisco Webex 環境からオンプレミスの Expressway への接続試行をシミュレートします。そのため、最も理想的な検証方法として使用できます。組織への TCP 接続をテストするには、次の操作を行います。

1. Cisco Webex Control Hub にログインします。
2. [サービス (Services)] を選択します。
3. [ハイブリッド コール (Hybrid Call)] カードで [設定 (Settings)] リンクを選択します。
4. [コール サービス接続 (Call Service Connect)] セクションで、[SIP 宛先 (SIP Destination)] に入力した値が正しいことを確認します。
5. 図に示すように、[テスト (Test)] をクリックします。

SIP Destination ⓘ

64.102.241.236:5062

Test Save

✖ Your SIP Destination is not configured correctly. [View test results](#)

6. テストが失敗したため、[テスト結果の表示] リンクをクリックして、図に示すように詳細を確認できます。

Verify SIP Destination



IP address lookup

IP

64.102.241.236

Tests	Result	Details
Connecting to IP	Successful	
Socket test	Failed	TCP Connection failure: Check network connectivity, connection speed, and/or firewall configuration.
SSL Handshake	Not performed	
Ping	Not performed	

前の図に示すように、64.102.241.236:5062 への接続を試みたときにソケット テストが失敗したことがわかります。Expressway 診断ログ/pcap に加えてこのデータも接続試行を示していないことから、ファイアウォールの ACL/NAT/ルーティングの設定を調べる十分な根拠が得られました。

解決方法

この特定の問題については、Cisco Webex 環境やオンプレミスのコラボレーションの機器が原因ではないため、ファイアウォールの設定に注目する必要があります。インターフェイスとなるファイアウォールのタイプを予測することは必ずしもできないため、デバイスに詳しい担当者の協力を求める必要があります。問題が、ファイアウォールの ACL、NAT、またはルーティング設定のミスに関連している可能性があります。

問題 3： ソケット障害：Expressway-E がポート 5062 をリッスンしていない

この特定の状況については、正しい診断がされていないケースが多く見られます。多くの場合、ポート 5062 経由のトラフィックがブロックされている理由として、ファイアウォールがその原因と見なされます。この特定の状況をトラブルシューティングするには、前述の「Expressway への着信でポート 5062 がブロックされる」のシナリオで紹介した手法を使用できます。ハイブリッド接続テスト ツールや、ポート接続の確認に使用する他のツールは失敗します。最初の仮説として考えられるのは、「ファイアウォールがトラフィックをブロックしている」です。ほとんどの人が、Expressway-E の診断ログを調べて、TCP 接続を確立しようとしているかどうかを判断します。ログ全体を眺めて、図に示すようなログ行項目を探します。

```
2017-09-19T14:01:46.462-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:46,461"  
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="40342" Dst-ip="172.16.2.2"  
Dst-port="5062" Detail="TCP Connecting"
```

この状況では、前述のような特定のログ エントリは存在しません。そのため、多くの人が誤った診断をして、ファイアウォールが原因だと仮定します。

パケット キャプチャが診断ログと一緒に含まれていれば、ファイアウォールが原因でないことを確認できます。次に示すのは、Expressway-E がポート 5062 経由でリッスンしていないシナリオで出現したパケット キャプチャの例です。このキャプチャは、図に示すように、適用フィルタとして `tcp.port==5062` を使用してフィルタ処理したものです。

Filter Capture Spark TCP SYN packet received

Filter: tcp.ports=5062 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
55	2017-09-19 14:56:46.625745	146.20.193.73	172.16.2.2	TCP	34351	5062	74	34351->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380
56	2017-09-19 14:56:46.625789	172.16.2.2	146.20.193.73	TCP	5062	34351	54	5062->34351 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
57	2017-09-19 14:56:46.653157	146.20.193.73	172.16.2.2	TCP	35883	5062	74	35883->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380
58	2017-09-19 14:56:46.653173	172.16.2.2	146.20.193.73	TCP	5062	35883	54	5062->35883 [RST, ACK] Seq=1 Ack=1 win=0 Len=0

Frame 55: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 Ethernet II, Src: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3), Dst: Vmware_58:9f:31 (00:0c:29:58:9f:31)
 Internet Protocol Version 4, Src: 146.20.193.73 (146.20.193.73), Dst: 172.16.2.2 (172.16.2.2)
 Transmission Control Protocol, Src Port: 34351 (34351), Dst Port: 5062 (5062), Seq: 0, Len: 0

Immediate RST sent from the Expressway

Expressway-E から取得したパケット キャプチャからわかるように、tcp ポート 5062 経由のトラフィックはファイアウォールによってブロックされておらず、実際に着信しています。パケット番号 56 では、最初の TCP SYN パケットが到着した直後に、Expressway-E から RST が送信されていることがわかります。こうした情報から、パケットを受信している Expressway-E については問題から分離することができ、問題を Expressway-E の観点からトラブルシューティングする必要がありますと結論付けることができます。得られた根拠を前提として、なぜ Expressway-E がパケットを RST するのか、その理由の候補を考えてみます。この動作の原因として次の 2 つの可能性が考えられます。

1. Expressway-Eには、トラフィックをブロックしている可能性のある、ある種のファイアウォールルールが設定されています
2. Expressway-Eが相互TLSトラフィックをリッスンしていない、またはポート5062を介したトラフィックをリッスンしていない。

Expressway-E のファイアウォール機能は、[システム (System)] > [保護 (Protection)] > [ファイアウォールルール (Firewall rules)] > [設定 (Configuration)] にあります。この環境でこのことを確認した時点では、ファイアウォールの設定は存在しませんでした。

いくつかの方法で、Expressway-E がポート 5062 経由の相互 TLS トラフィックをリッスンしているかどうかを確認できます。この確認には、Web インターフェイスを使用するか、CLI をルートユーザとして使用できます。

Expressway のルートから、`netstat-an | grep ':5062'`を実行すると、次のような出力が表示されます。

```
~ # netstat -an | grep ':5062'
tcp        0      0 172.16.2.2:5062      0.0.0.0:*          LISTEN    <--- Outside
Interface
tcp        0      0 192.168.1.6:5062     0.0.0.0:*          LISTEN    <--- Inside Interface
tcp        0      0 127.0.0.1:5062      0.0.0.0:*          LISTEN
tcp        0      0 :::1:5062           :::*              LISTEN
```

これらの情報は Expressway-E の Web インターフェイスを使用してキャプチャすることもできます。これらの情報を収集するには、次の手順を参照してください。

1. Expressway-Eにログインします
2. 「メンテナンス・ ツール」 > 「ポートの使用」 > 「ローカル着信ポート」に移動します
3. タイプSIPおよびIPポート5062を検索します (図に示すように赤で強調表示) 。

Type	Description	Protocol	IP address	IP port	Transport	Actions
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP	View/Edit
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP	View/Edit
SIP	TCP port	SIP	192.168.1.6	5060	TCP	View/Edit
SIP	TCP port	SIP	172.16.2.2	5060	TCP	View/Edit
SIP	TLS port	SIP	192.168.1.6	5061	TCP	View/Edit
SIP	TLS port	SIP	172.16.2.2	5061	TCP	View/Edit
SIP	Mutual TLS port	SIP	192.168.1.6	5062	TCP	View/Edit
SIP	Mutual TLS port	SIP	172.16.2.2	5062	TCP	View/Edit

確認すべき内容がわかったので、現在の環境と比較できます。CLI の観点から、`netstat-an | grep ':5062'` の出力は次のようになります。

```
~ # netstat -an | grep ':5062'
tcp        0      0 0.0.0.0:*          LISTEN
tcp        0      0 :::1:5062         LISTEN
~ #
```

さらに、Web UI ではローカルの着信ポートの下に相互 TLS ポートが表示されません。

Type	Description	Protocol	IP address	IP port	Transport
H.323	Call signaling port range	H.323	192.168.1.6	15000-19999	TCP
H.323	Call signaling port range	H.323	172.16.2.2	15000-19999	TCP
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP
SIP	TCP port	SIP	192.168.1.6	5060	TCP
SIP	TCP port	SIP	172.16.2.2	5060	TCP
SIP	TLS port	SIP	192.168.1.6	5061	TCP
SIP	TLS port	SIP	172.16.2.2	5061	TCP

こうしたデータから、Expressway-E が相互 TLS トラフィックをリッスンしていないと判断できます。

解決方法

この問題を解決するには、相互 TLS モードが有効になっていることと、Expressway-E で相互 TLS ポートが 5062 に設定されていることを確認する必要があります。

1. Expressway-E にログインします。
2. [設定 (Configuration)] > [プロトコル (Protocols)] > [SIP] に移動します。
3. 相互 TLS モードが [オン (On)] に設定されていることを確認します。
4. 相互 TLS ポートが [5062] に設定されていることを確認します。
5. 図に示すように、[保存 (Save)] をクリックします。

SIP

Configuration

SIP mode

UDP mode

UDP port

TCP mode

TCP port

TLS mode

TLS port

Mutual TLS mode

Mutual TLS port

問題 4 : Expressway-E または C がプリロード済み SIP ルート ヘッダーをサポートしていない

ハイブリッドコール サービス接続では、コールのルーティングはルート ヘッダーに基づいて行われます。ルート ヘッダーは、ソリューションのコール サービス認識 (Expressway コネクタ) 部分から Cisco Webex に配信される情報に基づいて設定されます。Expressway コネクタ ホストは Unified CM に対して、コール サービスが有効になっているユーザが誰かをクエリし、それらのユーザのディレクトリ URI と、ユーザの Unified CM ホーム クラスタのクラスタ FQDN の両方を抽出します。たとえば、Alice と Bob を使用した次の例を参照してください。

ディレクトリURI 宛先ルート ヘッダー
bob@example.com emea-cucm.example.com
alice@example.com us-cucm.example.com

Alice または Bob がコールを行うと、コールは彼らのオンプレミスの Unified CM にルーティングされます。そのため、着信側のユーザにルーティングする前に彼らの Cisco WebexRD に固定することができます。

Alice が Bob にコールした場合、コールは Alice の Unified CM ホーム クラスタの FQDN (*us-cucm.example.com*) にルーティングされます。Cisco Webex が Expressway-E への着信に送信する SIP INVITE を分析すると、SIP ヘッダーの中で次の情報が見つかります。

リクエスト URI sip:bob@example.com
ルート ヘッダー sip:us-cucm.example.com;lr

Expresswayの観点から見ると、検索ルールは、要求URIではなくルートヘッダ(*us-cucm.example.com*) – を使用してコールをルーティングするように設定されます。この場合は AliceのUnified CMホームクラスタです。

こうした基本的な情報から、Expressway が誤って設定され、前述のロジックが機能しなくなるトラブルシューティングの状況を理解することができます。他のほとんどすべての着信ハイブリッドコール サービス接続のコール セットアップ障害と同じように、オンプレミス電話機で着信音が鳴らないという症状が現れます。

Expressway で診断ログを分析する前に、このコールを特定する方法について考えてみましょう。

1. SIP 要求 URI は、着信側のディレクトリ URI (Directory URI) になります。
2. [SIP FROM]フィールドは、[First Name Last Name]
<sip:WebexDisplayName@subdomain.call.ciscospark.com>と表示される[発呼側]でフォーマットされます

これらの情報を使用して、着信側のディレクトリ URI、発信側の名と姓、または発信側の Cisco Webex SIP アドレスで診断ログを検索できます。この情報がない場合は、「INVITE SIP:」を検索して、Expresswayで実行されているすべてのSIPコールを検索できます。着信コールの SIP INVITE が特定されたら、SIP コール ID を探してコピーできます。この値がわかったら、後はコール ID に基づいて診断ログを検索するだけで、このコール レッグに関連するすべてのメッセージを表示できます。

また、コールが会社にたどり着くまでの距離を調べることもルーティングの問題の分離に役立ちます。前述に示した情報を Expressway-C で検索してみて、コールがそこからルーティングされたものかどうかを調べることができます。コールが Expressway-C からルーティングされている場合は、そこから調査を始める可能性が高くなります。

このシナリオでは、Expressway-C が Expressway-E から INVITE を受信したことがわかります。

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,830"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.5" Local-port="26847"
Src-ip="192.168.1.6" Src-port="7003" Msg-Hash="11449260850208794722"
SIPMSG:
| INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-
id=a82052ef-6fd7-4506-8173-e73af6655b5d;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8ad97fff3c240124;x-cisco-
local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769
6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstoiano test"

;tag=872524918

To: <sip:jorobb@rtp.ciscotac.net>

Max-Forwards: 15

Route:

Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-
e73af6655b5d@192.168.1.6:7003;transport=tls;lr>

Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-
e73af6655b5d@192.168.1.6:5061;transport=tls;lr>

ここで重要なのは、ルートヘッダー(クラスタ FQDN) がまだそのままであることです。ただし、ルートヘッダー(クラスタ FQDN) cucm.rtp.ciscotac.net に基づいて実行されている検索ロジックはありません。そうではなく、メッセージがすぐに 404 Not Found で拒否されています。

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Call Attempted" Service="SIP"
Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" Src-alias="sip:pstoiano-
test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net"
Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-
ddde83b49fd0" Protocol="TLS" Auth="NO" Level="1" UTCTime="2017-09-19 18:16:15,832"

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Attempted" Service="SIP"
Src-alias-type="SIP" Src-alias="pstoiano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-4e95-a70e-
253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="searchtype:INVITE" Level="1"
UTCTime="2017-09-19 18:16:15,834"

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Completed" Reason="Not
Found" Service="SIP" Src-alias-type="SIP" Src-alias="pstoiano-test@dmzlab.call.ciscospark.com"
Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-
4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="found:false,
searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-19 18:16:15,835"

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Call Rejected" Service="SIP"
Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" Src-alias="sip:pstoiano-

test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net"
Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-
ddde83b49fd0" Detail="Not Found" Protocol="TLS" Response-code="404" Level="1" UTCTime="2017-09-
19 18:16:15,835"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,830"
Module="network.sip" Level="INFO": Action="Received" Local-ip="192.168.1.5" Local-port="26847"
Src-ip="192.168.1.6" Src-port="7003" Detail="Receive Request Method=INVITE, CSeq=1, Request-
URI=sip:jorobb@rtp.ciscotac.net, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-
Tag=872524918, To-Tag=, Msg-Hash=11449260850208794722, Local-
SessionID=daf7c278732bb5a557fb57925dffcbf7, Remote-SessionID=00000000000000000000000000000000"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,836"
Module="network.sip" Level="INFO": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-
ip="192.168.1.6" Dst-port="7003" Detail="Sending Response Code=404, Method=INVITE, CSeq=1,
To=sip:jorobb@rtp.ciscotac.net, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-
Tag=872524918, To-Tag=96b9a0eaf669a590, Msg-Hash=254718822158415175, Local-
SessionID=00000000000000000000000000000000, Remote-SessionID=daf7c278732bb5a557fb57925dffcbf7"

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,836"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-
ip="192.168.1.6" Dst-port="7003" Msg-Hash="254718822158415175"
SIPMSG:
|SIP/2.0 404 Not Found
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-
id=a82052ef-6fd7-4506-8173-e73af6655b5d;received=192.168.1.6;rport=7003;ingress-
zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8ad97fff3c240124;x-cisco-
local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769
6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5eld5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
From: "pstoiano test"

;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>;tag=96b9a0eaf669a590
Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.5:5061 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=daf7c278732bb5a557fb57925dffcbf7
Content-Length: 0

作業シナリオと比較してみると、作業シナリオでは検索ロジックがルータのヘッダー (クラスタ FQDN) に基づいて実行されていることがわかります。

2017-09-22T13:56:02.215-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Attempted" Service="SIP"
Src-alias-type="SIP" Src-alias="pstoiano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf" Tag="8bd936da-f2ab-4412-96df-d64558f7597b" Detail="searchtype:INVITE" Level="1"
UTCTime="2017-09-22 17:56:02,215"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,217"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:


```
<routed> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<location clear="yes" url="sip:cucm.rtp.ciscotac.net;lr" diversion="" dest-url-for-
message="sip:jorobb@rtp.ciscotac.net" sip-route-set="" dest-service=""> added
sip:cucm.rtp.ciscotac.net;lr to location set "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<proxy stop-on-busy="no" timeout="0"/> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound MS to CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'multiway' did not match destination
alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'WebEx Search Rule' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'ISDN Inbound' ignored due to source
filtering"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'recalls into CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'CEtcp-rtp12-tpdmz-118-ucmpub' did
not match destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Conference Factory' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound B2B Calling' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Cisco Webex' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'as is local' towards
target 'LocalZone' at priority '1' with alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.219-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Hybrid Call Service
Inbound Routing' towards target 'CUCM11' at priority '2' with alias 'cucm.rtp.ciscotac.net;lr'"
その後、Expressway-C がコールを Unified CM ( 192.168.1.21 ) に正しく転送していることがわ
かります。
```

```
2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-
ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TCP 192.168.1.5:5060;egress-
zone=CUCM11;branch=z9hG4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b
5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-
id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;ingress-
zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-
service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbcd5b79c6cffad9ecd84cc8
337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005
```

```
Via: SIP/2.0/TLS
192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbef9819;received=148.62.40.64;rport=36
149;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-
8c648a16c2c5d7b85fa5c759d59aa190;rport=47732
Call-ID: daala6fa546ce76591fc464f0a50ee32@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscospark.com>;tag=567490631
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 14
Route:
```

```
Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf@192.168.1.5:5060;transport=tcp;lr>
Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-
e2d2bb6fec77@192.168.1.6:7003;transport=tls;lr>
Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-
e2d2bb6fec77@192.168.1.6:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
```

診断ログを分析し、問題を Expressway-C と特定のエラー (404 Not Found) に分離したので、この種の動作を引き起こしている原因の究明に集中することができます。次のことについて考慮する必要があります。

1. コールは、検索ルールを介して Expressway のゾーンを流入出しています。
2. Expressway では、「プリロード済み SIP ルートのサポート」と呼ばれるロジックが使用されます。このロジックは、ルータのヘッダーが含まれている SIP INVITE 要求を処理します。この値を、Expressway-C と Expressway-E の両方の [ゾーン (Zones)] (トラバーサルサーバ、トラバーサルクライアント、ネイバー) でオンまたはオフにすることができます。

これで xConfiguration を使用して、Expressway-E トラバーサルサーバゾーンと Expressway-C クライアントゾーンの両方で、特にハイブリッドコールサービス接続用に設定されているものについて設定を表示できます。ゾーンの設定に加えて、このコールをゾーン間で通過するように設定されている検索ルールを分析することができます。また、Expressway-E から Expressway-C にコールが渡されたこともわかっているので、トラバーサルサーバゾーンの設定が正しい可能性が非常に高くなります。

具体的には、次の xConfig ではこのゾーンがハイブリッドコールサービストラバーサル (Hybrid Call Service Traversal) という名前であることがわかります。これは TraversalServer というゾーンタイプです。このゾーンは、SIP TCP ポート 7003 を経由して Expressway-C への通信を行います。

ハイブリッドコールサービスで重要なのは、プリロード済み SIP ルートのサポートをオンにしている必要があることです。Expressway の Web インターフェイスでは、この値はプリロード済み SIP ルートのサポート (Preloaded SIP routes support) と呼ばれていますが、xConfiguration では SIP PreloadedSipRoutes Accept と表示されます。

Expressway-E

```
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

```

*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Type: "TraversalServer"

```

また、このゾーンには検索ルール 3 (Webex ハイブリッド) が結び付けられていることも判断できます。基本的には、検索ルールはハイブリッド コール サービスの DNS ゾーンを経由して着信する「すべての」エイリアスを送信し、前述のゾーン「ハイブリッド コール サービストラバーサル」に渡しています。予想されたとおり、Expressway-E の検索ルールもトラバーサル サーバゾーンも正しく設定されています。

```

*c xConfiguration Zones Policy SearchRules Rule 3 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Description: "Calls to VCS-C"
*c xConfiguration Zones Policy SearchRules Rule 3 Mode: "AnyAlias"
*c xConfiguration Zones Policy SearchRules Rule 3 Name: "Webex Hybrid"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Behavior: "Strip"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern String:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Type: "Prefix"
*c xConfiguration Zones Policy SearchRules Rule 3 Priority: "15"
*c xConfiguration Zones Policy SearchRules Rule 3 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 3 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 3 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 3 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 3 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 3 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Type: "Zone"

```

Expressway-C の xConfiguration に注目した場合は、最初に Webex ハイブリッドのトラバーサルクライアント ゾーンを探ることができます。簡単に見つける方法の 1 つとして、Expressway-E の xConfiguration からわかったポート番号 (SIP ポート : "7003") で検索します。これを利用して、xConfiguration で正しいゾーンをすぐに見つけることができます。

また前述のように、[ゾーン名 (Zone Name)]として「ハイブリッド コール サービストラバーサル (Hybrid Call Service Traversal)」、[タイプ (Type)]として「トラバーサル クライアント

(Traversal Client)」、および SIP PreloadedSipRoutes Accept の設定内容がわかります。この xConfiguration から、この値はオフに設定されていることがわかります。『Cisco Webex ハイブリッドコール サービス導入ガイド』によれば、この値はオンに設定する必要があります。

さらに、プリロード済み SIP ルートのサポートの定義を調べてみると、この値をオフに設定し、なおかつ INVITE にルート ヘッダーが含まれている場合は、明らかに、Expressway-C がメッセージを「拒否」することがわかります。「このヘッダーが含まれている SIP INVITE 要求をゾーンで拒否するようにするには、[プリロード済み SIP ルートのサポート (Preloaded SIP routes support)] を [オフ (Off)] に切り替えます。」

Expressway-C

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 6 TraversalClient Accept Delegated Credential Checks: "Off"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Password:
"{cipher}qeh8eq+fuVY1GHGgRLder/1lYDd760/6KrHGA7g8bJs="
*c xConfiguration Zones Zone 6 TraversalClient Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 6 TraversalClient Collaboration Edge: "Off"
*c xConfiguration Zones Zone 6 TraversalClient H323 Port: "1719"
*c xConfiguration Zones Zone 6 TraversalClient H323 Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient Peer 1 Address: "amer-expressway01.ciscotac.net"
*c xConfiguration Zones Zone 6 TraversalClient Peer 2 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 3 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 4 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 5 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 6 Address:
*c xConfiguration Zones Zone 6 TraversalClient Registrations: "Allow"
*c xConfiguration Zones Zone 6 TraversalClient RetryInterval: "120"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Port: "7003"
*c xConfiguration Zones Zone 6 TraversalClient SIP PreloadedSipRoutes Accept: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Address:
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Port:
*c xConfiguration Zones Zone 6 TraversalClient SIP Transport: "TLS"
*c xConfiguration Zones Zone 6 Type: "TraversalClient"
```

この時点で、問題が Expressway-C のトラバーサル クライアント ゾーンの設定ミスへと分離されました。[プリロード済み SIP ルートのサポート (Preloaded SIP routes support)] を [オン (On)] に切り替える必要があります。

解決方法

プリロード済み SIP ルートのサポートを正しく設定するには、次の操作を行います。

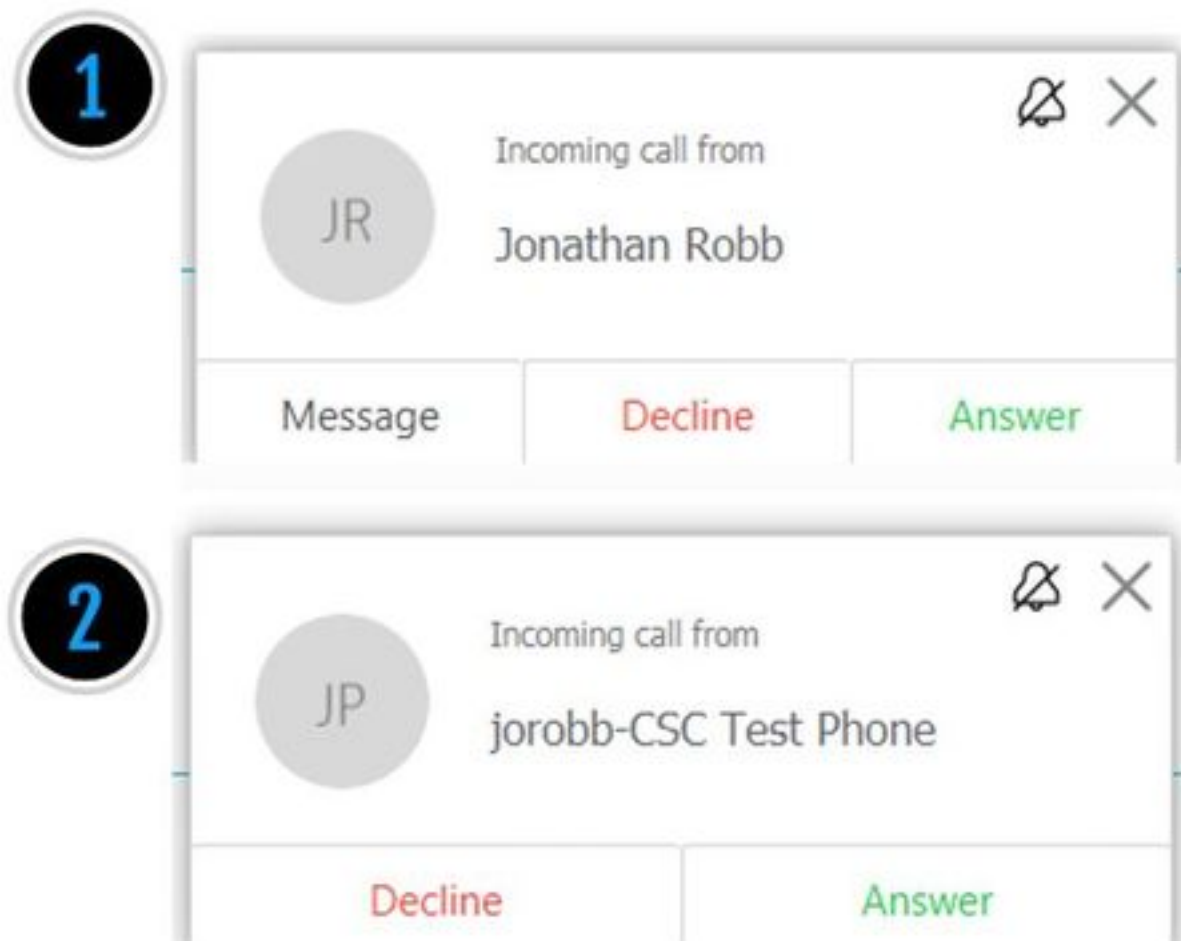
1. Expressway-C にログインします。
2. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
3. [ハイブリッドコール サービストラバーサル クライアント ゾーン (Hybrid Call Service Traversal client zone)] を選択します (名前付けはお客様ごとに異なります) 。
4. [プリロード済み SIP ルートのサポート (Preloaded SIP routes support)] を [オン (On)] に設定します。

5. [保存 (Save)] を選択します。

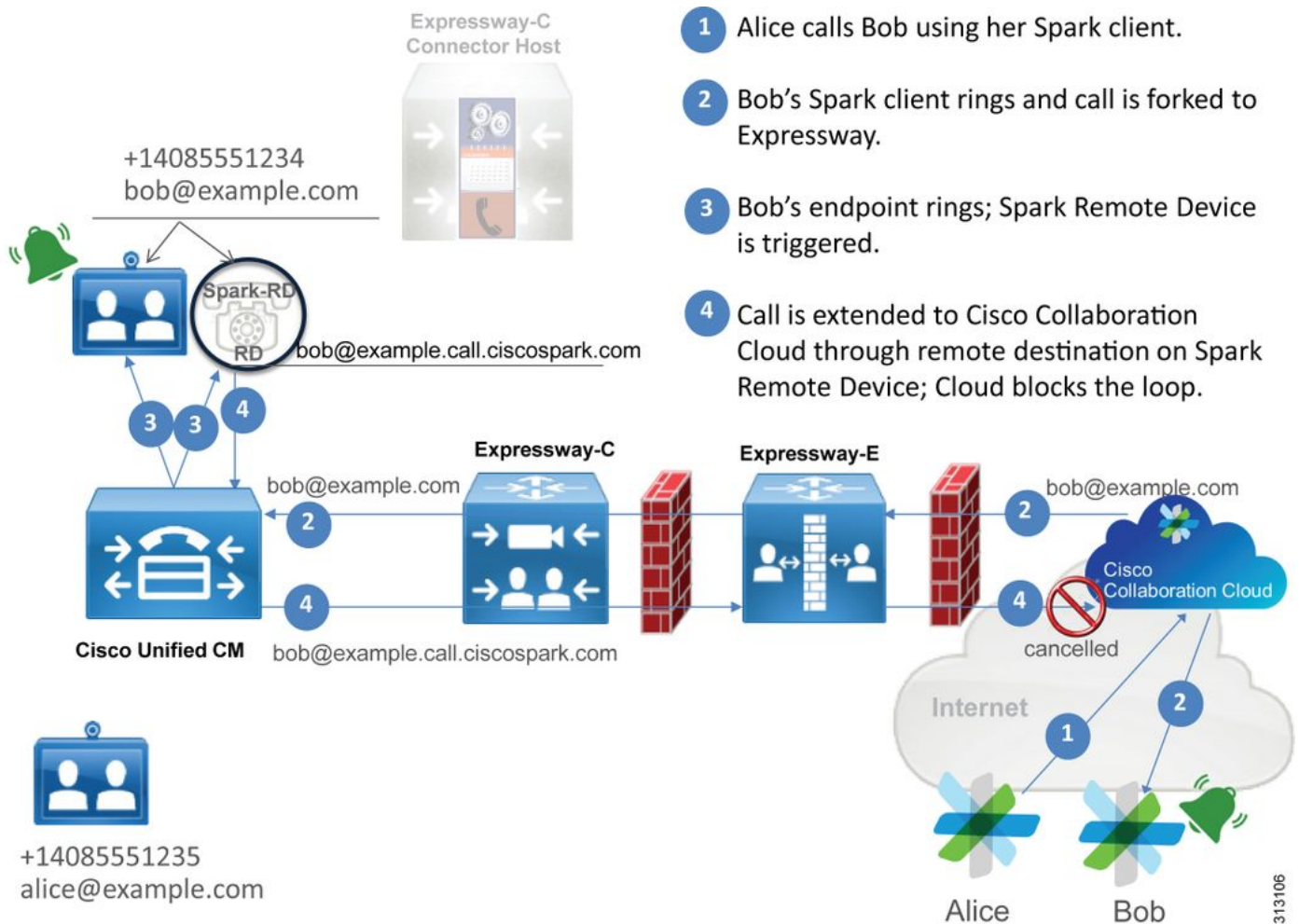
注：このシナリオは Expressway-C での障害例を示していますが、Webex ハイブリッド コールトラバーサル サーバゾーンで [プリロード済み SIP ルートのサポート (Preloaded SIP routes support)] が [オフ (Off)] になっている場合は、Expressway-E でも同じ診断ログエラーが見つかる可能性があります。その場合は、コールが Expressway-C に到達することは決して確認されず、Expressway-E がコール拒否および 404 Not Found を送信する役割を担っていたこととなります。

問題 5： Cisco Webex アプリで 2 つのコール通知 (トースト) を受信している

この特定の問題は、コールのドロップとならない着信コールのシナリオでのみ、偶発的に発生します。この問題では、コールを受信している人 (着信側) がコールを発信した人 (発信側) から 2 つの通知 (トースト) を Cisco Webex アプリで受信しています。1 つ目の通知は Cisco Webex から生成されていて、2 つ目の通知はオンプレミス インフラストラクチャから生成されています。次の図は、受信した 2 つの通知の例です。



1 つ目の通知 (トースト) は、Cisco Webex 側からコールを開始している人物 (発信側) です。この例では、発信者 ID は、そのコールを開始しているユーザの表示名 (Display Name) です。2 つ目の通知 (トースト) は、オンプレミスの CTI から、またはコールを発信しているユーザに割り当てられた Cisco Webex RD から送信されています。一見すると、この動作は不自然に思われます。しかし、Cisco Webex ハイブリッド コール設計ガイドの着信コールの図を見てみると、図に示すように、動作について理解を深めることができます。



- 1 Alice calls Bob using her Spark client.
- 2 Bob's Spark client rings and call is forked to Expressway.
- 3 Bob's endpoint rings; Spark Remote Device is triggered.
- 4 Call is extended to Cisco Collaboration Cloud through remote destination on Spark Remote Device; Cloud blocks the loop.

この図から、Alice は 自身の Cisco Webex アプリから Bob をコールしていて、コールがオンプレミスまでフォークされていることがわかります。このコールは、Bob の電話機に割り当てられているディレクトリ URI (Directory URI) と一致します。問題となるのは、この設計ではディレクトリ URI が Bob の CTI RD または Cisco Webex RD にも割り当てられていることです。したがって、コールが CTI-RD または Cisco Webex RD に提示されたとき、そのコールは Cisco Webex に送り返されます。これは、デバイスのリモート宛先 (Remote Destination) が bob@example.call.ciscospark.com 用に設定されているためです。この状況に対処するため、Cisco Webex は特定のコール レッグをキャンセルします。

コール レッグを正常にキャンセルするため、Cisco Webex は最初に SIP ヘッダーにパラメータを設定する必要がありましたが、与えられたレッグをキャンセルする目的で SIP ヘッダーを探ることになります。Cisco Webex が SIP INVITE に挿入するパラメータは **call-type=squared** と呼ばれるもので、この値が **Contact** ヘッダーに入力されます。この値がメッセージから欠落した場合、Cisco Webex はコールをキャンセルする方法を認識できません。

こうした情報から、前に示したシナリオを再び参照することができます。前のシナリオでは、Cisco Webex ユーザの Jonathan Robb がコールを発信したときに、ユーザの Cisco Webex アプリで 2 つの通知 (トースト) を受信していました。この種の問題をトラブルシューティングするには、常に Expressway-C と Expressway-E から診断ログを収集する必要があります。まず、Expressway-E のログを調べて、SIP INVITE において最初にインバウンド送信された Cisco Webex INVITE の **Contact** ヘッダーに、実際に **call-type=squared** の値が存在することを確かめることができます。これにより、ファイアウォールがメッセージをまったく操作していないことが確かめられます。次に示すのは、このシナリオにおける Expressway-E への着信 INVITE のスニペット例です。

```
2017-09-19T14:01:48.140-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,140"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="5062"
Src-ip="146.20.193.73" Src-port="40342" Msg-Hash="11658696457333185909"
SIPMSG:
|INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71,SIP/2.0/TLS
127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>;call-type=squared
<-- Webex inserted value
From: "Jonathan Robb"
```

```
;tag=540300020
```

To:

コンタクトヘッダーに **call-type=squared** の値が存在します。この時点では、コールで Expressway を介したルーティングを行う必要があります。コールを Webex ハイブリッドトラバーサル サーバゾーンから送信する必要があります。Expressway-E のログを検索して、コールが Expressway-E からどのように送信されたのかを調べることができます。その結果から、Expressway-E が何らかの方法で INVITE を操作しているかどうかを推測します。

```
2017-09-19T14:01:48.468-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,468"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="26686" Msg-Hash="1847271284712495612"
SIPMSG:
INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKec916b02b6d469abad0a30b93753f4b0859;proxy-call-
id=d7372034-85d1-41f8-af84-dffed6d1a9a9;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKd91699370129b4c10d09e269525de00c2;x-cisco-local-
service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdfef078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debc8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=4
0342;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls> <-- Webex inserted value is now missing
From: "Jonathan Robb"
```

```
;tag=540300020
```

To:

Max-Forwards: 15

Route: <sip:cucm.rtp.ciscotac.net;lr>

Expressway-E から Expressway-C に送信されているこの SIP INVITE を調べてみると、コンタクトヘッダーに **call-type=squared** がないことがわかります。また、行項目 4 を見ると、出力ゾーン (egress-zone) が **HybridCallServiceTraversal** に等しくなっていることもわかります。結論として、ダイヤル時に Cisco Webex アプリが 2 つ目の通知 (トースト) を受信しているのは、Expressway-E において SIP INVITE のコンタクトヘッダーから **call-type=squared** タグが欠落しているからだと判断できます。つまり、このヘッダーの欠落を引き起こしている原因を突き止める必要があります。

コールは、Expressway でセットアップしたハイブリッド コール サービス トラバーサルを経由してルーティングする必要があります。そのため、そこから調査を始めるのが適切です。

xConfiguration がある場合は、このゾーンがどのように設定されたのかを確認できます。

xConfiguration でゾーンを特定するには、ログに出力される Via 行に記録された名前を使用します。前の例では egress-zone=HybridCallServiceTraversal という名前になっていました。この名前が SIP ヘッダーの Via 行に出力される時は、スペースが削除されます。xConfiguration の観点から見た実際のゾーン名には、スペースがあり、ハイブリッド コール サービス トラバーサルでフォーマットが設定されています。

```
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "Off" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

設定がハイブリッド コール サービス トラバーサルのものであることが明らかになったので、次のような目立った設定の候補を探ることができます。

- SIP PreloadedSIPRoutes Accept : オン
- SIP ParameterPreservatoin Mode : オフ

任意の Expressway の Web インターフェイスを使用して、これらの値の定義と動作の内容を確認できます。

プリロード済み SIP ルートのサポート (Preloaded SIP routes support)

ルート ヘッダーが含まれている SIP INVITE 要求をこのゾーンで処理できるようにするには、[プリロード済み SIP ルートのサポート (Preloaded SIP routes support)] を [オン (On)] に切り替えます。

このヘッダーが含まれている SIP INVITE 要求をゾーンで拒否するようにするには、[プリロード済み SIP ルートのサポート (Preloaded SIP routes support)] を [オフ (Off)] に切り替えます。

SIP パラメータの保持 (SIP parameter preservation)

Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。

[オン (On)] : このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI パラメータとコンタクト パラメータを保持します。

[オフ (Off)] : このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI パラメータとコンタクト パラメータを B2BUA が必要に応じて書き直すことを許可します。

これらの定義と、xConfiguration の設定、および call-type=squared の値が SIP INVITE の「コンタクト」ヘッダーに設定されていることから、ハイブリッド コール サービストラバーサルゾーンで SIP パラメータの保護値をオフ (Off) にしていることがタグの欠落の原因であり、そのために Cisco Webex アプリで 2 つの着信通知を受信していると結論付けることができます。

解決方法

SIP INVITE のコンタクト ヘッダーで call-type=squared の値を保つためには、Expressway において、コールの処理に関与するすべてのゾーンについて SIP パラメータの保護をサポートする必要があります。

1. Expressway-E にログインします。
2. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
3. ハイブリッド トラバーサル サーバに使用されているゾーンを選択します。
4. [SIP パラメータの保持 (SIP parameter preservation)] の値を [オン (On)] に設定します。
5. 設定を保存します。

#####

注 : このシナリオの例では、Expressway-E の Webex ハイブリッド トラバーサル サーバゾーンの設定が誤っていました。Webex ハイブリッド トラバーサル クライアントまたは CUCM ネイバゾーンにおいても、SIP パラメータの保持の値がオフに設定されている可能性が十分にあることに注意してください。この場合、Expressway-E から Expressway-C に対して call-type=squared 値が送信されて、Expressway-C から削除されることが予想されます。

アウトバウンド: オンプレミスから Cisco Webex へ

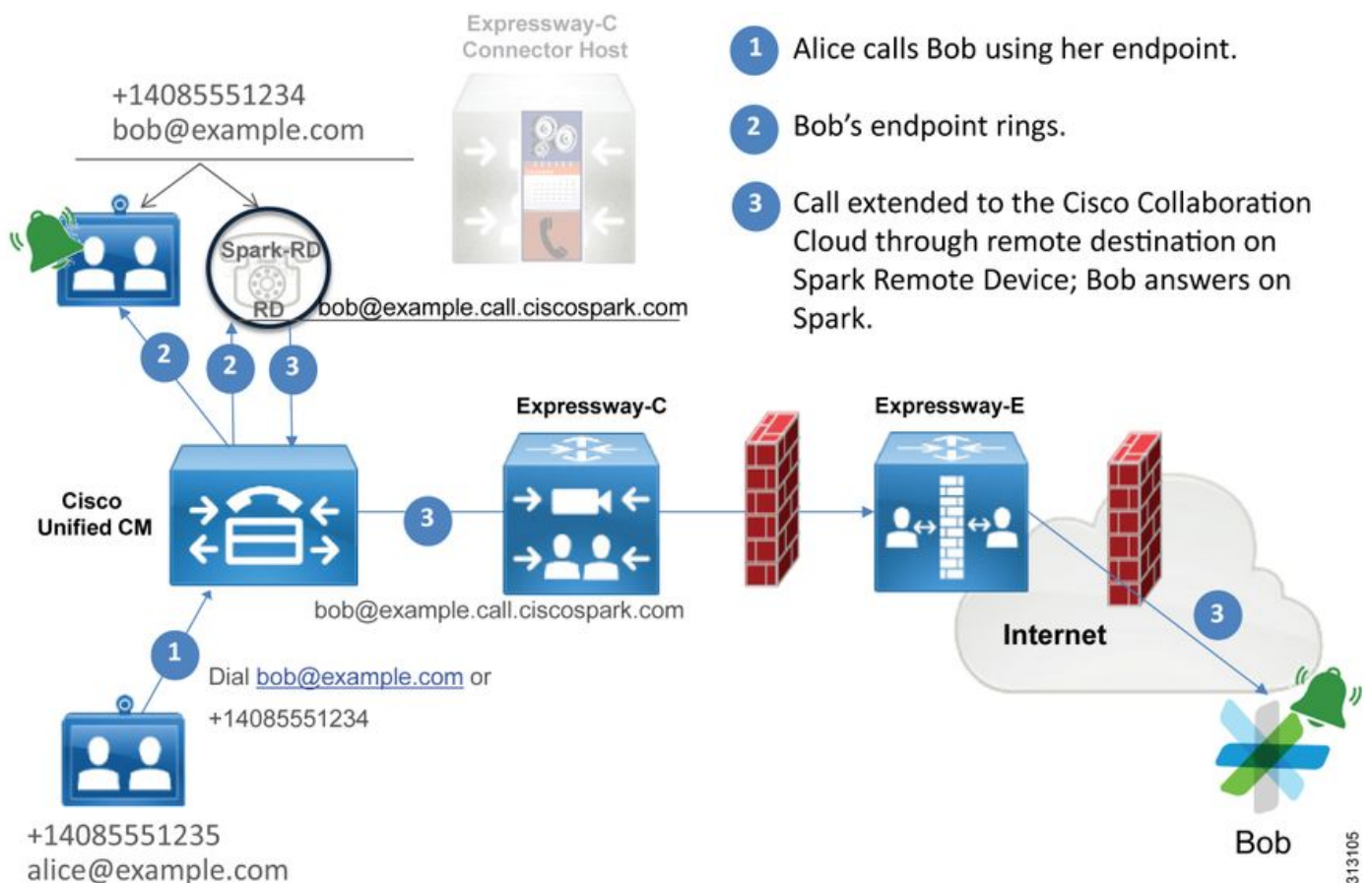
オンプレミスから Cisco Webex への発信障害では、ほとんどすべての場合に同じ症状が報告されています。たとえば、「Unified CM に登録した自分の電話機から、コール サービス接続で有効になっている他のユーザに電話をかけると、相手のオンプレミス電話機では着信音が鳴るが、相手の Cisco Webex アプリでは着信音が鳴らない」などです。このシナリオをトラブルシューティングするためには、この種のコールで発生するコールのフローとロジックの両方について理解しておくことが重要です。

全体的なロジック フロー

1. ユーザ A が自分のオンプレミス電話機から、ユーザ B のディレクトリ URI に電話をかけます。
2. ユーザ B のオンプレミス電話機と CTI RD/Webex RD がコールを受け付けます。
3. ユーザ B のオンプレミス電話で着信音が鳴り始めます。
4. ユーザ B の CTI-RD/Webex-RD によって、このコールが UserB@example.call.ciscopark.com という宛先にフォークされます。
5. Unified CM がこのコールを Expressway-C に渡します。
6. Expressway-C がコールを Expressway-E に送信します。
7. Expressway-E は、callservice.ciscopark.com ドメインで DNS ルックアップを実行します。
8. Expressway-E が、ポート 5062 を経由した Cisco Webex 環境への接続を試みます。
9. Expressway-E と Cisco Webex 環境の間で相互ハンドシェイクが開始されます。
10. Cisco Webex 環境が、ユーザ B の使用可能な Cisco Webex アプリにコールを渡します。
11. ユーザ B が使用できる Cisco Webex アプリで着信音が鳴り始めます。

コールフロー

図のように、[ユーザ B のオンプレミス電話 (User B on-prem phone)] > [Unified CM] > [CTI-RD/Webex-RD] > [Expressway-C] > [Expressway-E] > [Cisco Webex 環境 (Cisco Webex environment)] > [Cisco Webex アプリ (Cisco Webex apps)] に移動します。



注：図は『[Cisco Webex ハイブリッド設計ガイド](#)』からの抜粋です。

ログ分析のヒント

Cisco Webex へのフォークされた発信コールが失敗している状況をトラブルシューティングする場合は、Unified CM、Expressway-C、Expressway-E の各ログを収集します。これらの一連のログを調べることで、コールがどのようにして環境を通過しているのかを確認できます。コールが

オンプレミス環境内でどのくらいの距離から達しているのかを手早く理解する別の方法として、Expressway の「検索履歴」を使用できます。Expressway の検索履歴では、Cisco Webex 宛てのフォークされたコールが Expressway-C または E に達しているかどうかを速やかに調べることができます。

検索履歴を使用するには、次の操作を行います。

1. Expressway-E にログインします。
テスト コールを発信します。
[ステータス (Status)]> [検索履歴 (Search history)] に移動します。
コールを受ける必要がある Webex SIP URI の宛先アドレス
(user@example.call.ciscospark.com) がコールに存在するかどうかを確認めます。
Expressway-E に達しているコールが検索履歴に表示されない場合は、Expressway-C についてこの手順を繰り返します。

Expressway で診断ログを分析する前に、このコールを特定する方法について考えてみましょう。

1. SIP 要求 URI は、Cisco Webex ユーザの SIP アドレスになります。
2. [SIP FROM]フィールドは、[Calling Party]が[First Name Last Name] < sip:Alias@Domain>としてリストされるようにフォーマットされます

これらの情報を使用して、発信側のディレクトリ URI、発信側の名と姓、または着信側の Cisco Webex SIP アドレスで診断ログを検索できます。この情報がない場合は、「INVITE SIP:」で検索を行い、Expressway で実行されているすべての SIP コールを検索できます。発信コールの SIP INVITE が特定されたら、SIP コール ID (Call-ID) を探してコピーできます。この値がわかったら、後はコール ID に基づいて診断ログを検索するだけで、このコール レッグに関連するすべてのメッセージを表示できます。

以下では、コール サービス接続で有効になっているユーザに電話をかけたときに、Unified CM に登録された電話から Cisco Webex 環境への発信コールでよく発生する問題をいくつか紹介します。

問題1: Expresswayがcallservice.ciscospark.comアドレスを解決できない

Expressway DNS ゾーンの標準の操作手順として、要求 URI の右側に表示されるドメインに基づいて DNS ルックアップを実行します。このことを説明するために、例を考えてみましょう。DNSゾーンが要求URIがpstoiano-test@dmzlab.call.ciscospark.comのコールを受信する場合、一般的なExpressway DNSゾーンは、要求URIの右側であるdmzlab.call.ciscospark.comでDNS SRVルックアップロジックを実行します。Expressway がこの処理を行うとすれば、次のルックアップと応答が発生すると予想できます。

```
_sips._tcp.dmzlab.call.ciscospark.com.  
Response: 5 10 5061 12sip-cfa-01.wbx2.com.  
12sip-cfa-01.wbx2.com  
Response: 146.20.193.64
```

詳しく調べてみると、SRV レコードの応答から、サーバのアドレスと、ポート 5062 ではなくポート 5061 が提供されていることがわかります。

つまり、ポート 5062 経由で発生する相互 TLS ハンドシェイクが実行されず、Expressway と Cisco Webex 間のシグナリングに別のポートが使用されます。ここで問題となるのは、『Cisco Webex ハイブリッド コール サービス導入ガイド』ではポート 5061 の使用を明確に指示してい

ないことです。これは、一部の環境で B2B 通話が許可されていないためです。

Expressway におけるこうした標準の DNS ゾーン SRV ルックアップ ロジックを回避する方法として、指定した値に基づいて明示的に検索するように Expressway を設定します。

この特定のコールを分析する際は、(検索履歴を使用して) コールがここまで達していると判断したので、Expressway-E に注目することができます。まず、Expressway-E に着信している 1 つ目の SIP INVITE を調べて、どのゾーンを経由して着信したのか、どの検索ルールが使用されているのか、どのゾーンからコールが送出しているのか、そして、DNS ゾーンに正しく送信されている場合にどのような DNS ルックアップ ロジックが発生しているのかを明らかにします。

```
2017-09-19T13:18:50.562-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,556"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26686" Msg-Hash="4341754241544006348"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK6d734eaf7a6d733bd1e79705b7445ebb46175.1d33be65c99c
56898f85df813f1db3a7;proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK13187594dd412;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 991f7e80-9c11517a-130ac-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"

;tag=332677~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106860
To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 17:18:50 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 2272025a-ce36-49d0-8d93-cb6a5e90ffe0
Session-ID: 75957d4fb66a13e835c10737aa332675;remote=00000000000000000000000000000000
Cisco-Guid: 2568978048-0000065536-000000148-0352430272
Content-Type: application/sdp
Content-Length: 714
```

<SDP Omitted>

このSIP INVITEでは、要求URI(pstojano-test@dmzlab.call.ciscospark.com)、Call-ID(991f7e80-9c11517a-130ac-1501a8c0)、From("Jonathan Rob " <sip:5010@rtp.ciscotac.net>)、To(sip:pstojano-test@dmzlab.call.ciscospark.com)、およびUser-Agent(Cisco-CUCM11.5)。このINVITEの受信後、Expresswayはロジックを決定して、コールを別のゾーンにルーティングできるかどうかを判断する必要があります。Expresswayは検索ルールに基づいてこの判断を実行します。

```
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-
test@dmzlab.call.ciscospark.com'"
```

前述のログスニペットから、Expressway-Eは4つの検索ルールを使用して解析を行ったものの、1つ(Webex Hybrid - to Webex Cloud)しか考慮しなかったことがわかります。検索ルールには90の優先順位があり、ハイブリッドコールサービスDNSゾーンに送ることを目的としていました。コールがDNSゾーンに送信されているので、Expressway-Eで発生しているDNS SRVルックアップを確認できます。

```
2017-09-19T13:18:50.565-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,565"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="dmzlab.call.ciscospark.com" Type="NAPTR (IPv4 and IPv6)"
2017-09-19T13:18:50.718-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,718"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T13:18:50.795-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,795"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4' 'TCP' '146.20.193.64:5061'] (A/AAAA) Hostname:'l2sip-cfa-01.wbx2.com' Port:'5061'
Priority:'5' TTL:'300' Weight:'10' (SRV) Number of relevant records retrieved: 2"
```

上記のスニペットでは、Expressway-Eが要求URI(_sips._tcp.dmzlab.call.ciscospark.com)の右側に基づいてSRVルックアップを実行し、l2cfa-01.wbx2.comとポート5061に解決されています。ホスト名l2sip-cfa-01.wbx2.comは146.20.193.64に解決されます。この情報を使用して、Expresswayが実行する次の論理的な手順は、TCP SYNパケットを146.20.193.64に送信し、コールのセットアップを試行することです。Expressway-Eのログから、このことが起きているかどうかを確認できます。

```
2017-09-19T13:18:51.145-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:51,145"
Module="network.tcp" Level="DEBUG": Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64"
Dst-port="5061" Detail="TCP Connecting"
2017-09-19T13:19:01.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:19:01,289"
Module="network.tcp" Level="ERROR": Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64"
Dst-port="5061" Detail="TCP Connection Failed"
```

前述のExpressway-Eの診断ログスニペットでは、Expressway-Eは前にTCPポート5061経由で解決されたIP 146.20.193.64への接続を試みていることがわかります。同じことは、収集したパケットキャプチャからも確認できます。

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
3878	2017-09-19 17:18:08.801765	68.67.59.22	172.16.2.2	TCP	25876	5061	66	25876->5061 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=231154828 TSecr=410470239
3879	2017-09-19 17:18:08.801923	172.16.2.2	68.67.59.22	TCP	5061	25876	66	5061->25876 [FIN, ACK] Seq=1 Ack=2 Win=0 Len=0 TSval=4111465862 TSecr=231154828
3882	2017-09-19 17:18:08.822153	68.67.59.22	172.16.2.2	TCP	25876	5061	66	25876->5061 [ACK] Seq=2 Ack=1 Win=362 Len=0 TSval=231154849 TSecr=4111465862
8109	2017-09-19 17:18:25.110830	192.33.146.113	172.16.2.2	TCP	50714	5061	60	50714->5061 [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
14878	2017-09-19 17:18:51.145472	172.16.2.2	146.20.193.64	TCP	25010	5061	74	25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 wS=128
15133	2017-09-19 17:18:58.203929	172.16.2.2	146.20.193.64	TCP	25010	5061	74	25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 wS=128
15702	2017-09-19 17:18:58.251324	172.16.2.2	146.20.193.64	TCP	25010	5061	74	TCP Retransmission: 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 wS=128
16770	2017-09-19 17:18:58.283326	172.16.2.2	146.20.193.64	TCP	25010	5061	74	TCP Retransmission: 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 wS=128
17377	2017-09-19 17:19:01.328621	172.16.2.2	146.20.193.64	TCP	25011	5061	74	25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 wS=128
17848	2017-09-19 17:19:02.319327	172.16.2.2	146.20.193.64	TCP	25011	5061	74	TCP Retransmission: 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 wS=128
18423	2017-09-19 17:19:04.421223	172.16.2.2	146.20.193.64	TCP	25011	5061	74	TCP Retransmission: 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 wS=128
19459	2017-09-19 17:19:08.459332	172.16.2.2	146.20.193.64	TCP	25011	5061	74	TCP Retransmission: 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 wS=128

The Expressway-E doesn't receive a SYN-ACK so it retries the SYN packet again 3 times

これらの結果から、ポート 5061 経由のトラフィックが成功していないことは明らかです。ただし、ハイブリッドコール サービス接続は TCP ポート 5061 ではなくポート 5062 の使用を意図していました。したがって、Expressway-E がポート 5062 を返す SRV レコードを解決していない理由について考える必要があります。その答えを見つけるため、Expressway-E の Webex ハイブリッド DNS ゾーンで起こりうる設定の問題を調べることができます。

*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"

*c xConfiguration Zones Zone 6 DNS SIP Authentication Trust Mode: "Off"

*c xConfiguration Zones Zone 6 DNS SIP Default Transport: "TLS"

*c xConfiguration Zones Zone 6 DNS SIP DnsOverride Name: "ciscopark.com"

*c xConfiguration Zones Zone 6 DNS SIP DnsOverride Override: "Off"

*c xConfiguration Zones Zone 6 DNS SIP Media AesGcm Support: "Off"

*c xConfiguration Zones Zone 6 DNS SIP Media Encryption Mode: "On"

*c xConfiguration Zones Zone 6 DNS SIP Media ICE Support: "Off"

*c xConfiguration Zones Zone 6 DNS SIP ParameterPreservation Mode: "Off"

*c xConfiguration Zones Zone 6 DNS SIP Poison Mode: "Off"

*c xConfiguration Zones Zone 6 DNS SIP PreloadedSipRoutes Accept: "On"

*c xConfiguration Zones Zone 6 DNS SIP Record Route Address Type: "IP"

*c xConfiguration Zones Zone 6 DNS SIP SearchAutoResponse: "Off"

*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "On"

*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"

*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscopark.com"

*c xConfiguration Zones Zone 6 DNS SIP UDP BFCP Filter Mode: "Off"

*c xConfiguration Zones Zone 6 DNS SIP UDP IX Filter Mode: "Off"

Expressway-E の xConfiguration には、DNS ルックアップに関連する値として、DNSOverride Name と DNSOverride Override という 2 つの注目すべき値があります。この xConfiguration によると、DNSOverride Override はオフに設定されており、したがって DNSOverride Name は有効になっていません。これらの値の動作について理解を深めるため、Expressway Web UI を使用して値の定義を調べることができます。

DNS 要求の変更 (Modify DNS request) (xConfig の DnsOverride Override に対応)

このゾーンからの発信 SIP コールをダイヤルした宛先内のドメインではなく、手動で指定した SIP ドメインにルーティングします。このオプションは、主に Cisco Webex サービスでの使用を目的としています。www.cisco.com/go/hybrid-services を参照してください。

検索するドメイン (Domain to search for) (xConfig の DnsOverride Name に対応)

発信 SIP URI についてドメインを検索する代わりに DNS で検索する FQDN を入力します。元の SIP URI には影響しません。

以上の定義から、これらの値は正しく設定されている場合に DNS ルックアップ ロジックに完全に適合することは明らかです。これを Cisco Webex ハイブリッドコール サービス導入ガイドの文と組み合わせると、[Modify DNS Request] を [On] に設定し、[Domain to search] を [callservice.ciscopark.com] に設定する必要があります。これらの値を変更して正しい情報を指定すれば、DNS SRV ルックアップ ロジックはまったく異なるものになります。Expressway-E 診断ログの観点から予想できるスニペットを次に示します。

```
2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscopark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4' 'TCP' '146.20.193.70:5062'] (A/AAAA) ['IPv4' 'TCP' '146.20.193.64:5062'] (A/AAAA)
Hostname:'l2sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)
Hostname:'l2sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of
relevant records retrieved: 4"
```

解決方法

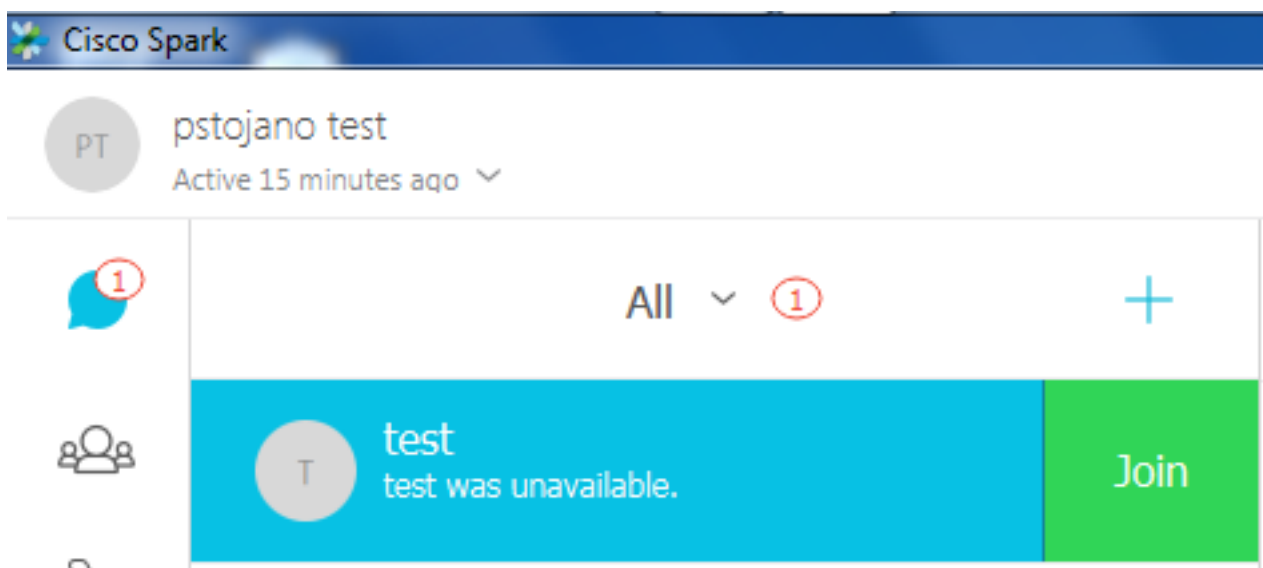
1. Expressway-E にログインします。
2. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
3. 設定済みの Webex ハイブリッド DNS ゾーンを選択します。
4. [DNS 要求の変更 (Modify DNS request)] を [オン (On)] に設定します。
5. 値を検索するドメインを `callservice.ciscopark.com` に設定します
6. 変更を保存

注 : Expressway で使用されている DNS ゾーンが 1 つしかない場合は、別の DNS ゾーンをハイブリッド コール サービスで使用するように設定して、これらの値を利用できるようにする必要があります。

問題 2 : ポート 5062 で Cisco Webex への発信がブロックされる

Cisco Webex へのフォークされた発信コールの障害に関する固有な問題は、クライアントで着信音が鳴らないにもかかわらず着信側の Cisco Webex アプリで [参加 (Join)] ボタンが表示されることです。前述のシナリオと同様に、この問題でも同じツールとログを使用して障害の存在箇所を的確に理解する必要があります。コールの問題の分離やログの分析に関するヒントについては、図に示しているこの記事の項を参照してください。

[参加 (Join)] ボタンが表示されている図



発信コールの問題 1 と同様に、Expressway-E の診断ログで分析を始めることができます。これは、Expressway で検索履歴を使用して、コールがそこまで達していると判断したためです。前と同様に、Expressway-C から Expressway-E に着信する最初の INVITE から開始します。検索する内容は次のとおりです。

1. Expressway-E が INVITE を受信しているかどうか。
2. 検索ルール ロジックによってコールがハイブリッド DNS ゾーンを通過しているかどうか
3. DNS ゾーンが DNS ルックアップを実行しているかどうか、正しいドメインで実行しているかどうか
4. システムによってポート 5062 の TCP ハンドシェイクが試行され正しく確立されたかどうか
5. 相互 TLS ハンドシェイクが成功したかどうか

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,017"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="3732376649380137405"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcddfd62f6ff7e09f9939482.899441b6d60c
444e4ed58951d07b5224;proxy-call-id=696f6f1c-9abe-47f3-96a4-e26f649fb76f;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12d4b77c97a64;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 6a48de80-9c11273a-12d08-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

```
;tag=328867~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106829
```

To:

```
Max-Forwards: 15
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 14:18:34 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: b2967a3b-93fb-4ca4-b0d7-131f75335684
Session-ID: 75957d4fb66a13e835c10737aa328865;remote=00000000000000000000000000000000
Cisco-Guid: 1783160448-0000065536-0000000126-0352430272
Content-Type: application/sdp
Content-Length: 714
<SDP Omitted>
```

前の INVITE でわかるように、INVITE は正常に受信されています。これは「着信」の動作であり、Expressway-C の IP アドレスから送られてきています。次に、検索ルール ロジックを見てみましょう。


```

2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscopark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscopark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-
test@dmzlab.call.ciscopark.com'"

```

上記のログスニペットから、Expressway-Eは4つの検索ルールを使用して解析しましたが、1つだけが解析されていることがわかります（Webex/ハイブリッド-Webexクラウドへ）が考慮された検索ルールのプライオリティは90で、ハイブリッドコールサービスDNSゾーン。コールがDNSゾーンに送信されているので、Expressway-Eで発生しているDNS SRV ルックアップを確認できません。以上はすべて、完全に正常です。続いて、DNS ルックアップ ロジックに注目してみましょう。

```

2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscopark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4' 'TCP' '146.20.193.70:5062'] (A/AAAA) ['IPv4' 'TCP' '146.20.193.64:5062'] (A/AAAA)
Hostname:'l2sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)
Hostname:'l2sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of
relevant records retrieved: 4"

```

この例では、callservice.ciscopark.com SRVレコードが解決されていることがわかります。その応答は4つの異なる有効なレコードであり、すべてがポート5062を使用しています。これは正常な動作です。この時点で、次に来るべきTCPハンドシェイクを分析できます。このドキュメントですでに説明したように、診断ログで「TCP接続(TCP Connecting)」を検索し、Dst-port="5062" がリストされている行項目を探することができます。このシナリオで明らかになる内容の例を次に示します。

```

2017-09-19T10:18:35.474-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,474"
Module="network.tcp" Level="DEBUG": Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connecting"
2017-09-19T10:28:35.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:28:35,289"
Module="network.tcp" Level="ERROR": Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connection Failed"

```

また、図に示すように、診断ログバンドルに含まれていたtcpdumpを使用して、TCPハンドシェイクについての詳細情報をいくつか得ることもできます。

Expressway-E attempts TCP Connection twice

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
2	2017-09-19 14:18:35.474312	172.16.2.2	146.20.193.70	TCP	25026	5062	74	25026->5062 [SYN] Seq=0 win=29200 Len=0
3	2017-09-19 14:18:36.523324	172.16.2.2	146.20.193.70	TCP	25026	5062	74	[TCP Retransmission] 25026->5062 [SYN]
4	2017-09-19 14:18:38.571325	172.16.2.2	146.20.193.70	TCP	25026	5062	74	[TCP Retransmission] 25026->5062 [SYN]
7	2017-09-19 14:18:42.603331	172.16.2.2	146.20.193.70	TCP	25026	5062	74	[TCP Retransmission] 25026->5062 [SYN]
8	2017-09-19 14:18:45.807635	172.16.2.2	146.20.193.64	TCP	25027	5062	74	25027->5062 [SYN] Seq=0 win=29200 Len=0
9	2017-09-19 14:18:46.827328	172.16.2.2	146.20.193.64	TCP	25027	5062	74	[TCP Retransmission] 25027->5062 [SYN]
10	2017-09-19 14:18:48.875336	172.16.2.2	146.20.193.64	TCP	25027	5062	74	[TCP Retransmission] 25027->5062 [SYN]
11	2017-09-19 14:18:52.907335	172.16.2.2	146.20.193.64	TCP	25027	5062	74	[TCP Retransmission] 25027->5062 [SYN]

The Expressway-E doesn't receive a SYN-ACK so it attempts to retransmit.

この時点で、Expressway-E がコールを正しくルーティングしていると判断できます。このシナリオで問題となるのは、Webex 環境で TCP 接続を確立できないことです。その原因として、Webex 環境が TCP SYN パケットに応答していないことが考えられますが、接続を処理しているサーバが多数の顧客間で共有されていることを考慮すると、その可能性は小さいと考えられます。このシナリオで可能性の高い原因として考えられるのは、何らかのタイプの間接デバイス（ファイアウォール、IPS など）で発信トラフィックが許可されていないことです。

解決方法

問題を分離したので、このデータをお客様のネットワーク管理者に提供する必要があります。また、お客様がより詳しい情報を必要としている場合は、さらに証明を裏付けるために、エッジデバイスやファイアウォールの外部インターフェイスからキャプチャを取得することができます。Expressway の観点から見た場合、この問題はそのデバイスには存在しないため、これ以上必要な作業はありません。

問題 3： Expressway-E の検索ルールが正しく設定されていない

検索ルールの設定の誤りは、Expressway の設定に関連する一番大きな問題の 1 つです。検索ルールの設定の問題は双方向になる可能性があります。これは、着信コールの検索ルールが必要であり、発信コールの検索ルールが必要だからです。この問題を調べていくと、Expressway では正規表現の問題がよく発生しますが、それらが必ずしも検索ルールの問題の原因だとは限らないことがわかります。ここでは特に、失敗している発信コールについて詳しく説明します。他のすべてのフォークされた発信コールのシナリオと同様に、症状は同じです。

- 着信ユーザの Cisco Webex アプリに [参加 (Join)] ボタンが表示された
- 発信側の電話に着信音が送り返されていた
- 着信ユーザのオンプレミス電話機では着信音が鳴っていた
- 着信ユーザの Cisco Webex アプリでは着信音が鳴らなかった

他のすべてのシナリオと同様に、Expressway-C および E の診断ログに加えて CUCM SDL トレースを利用することもできます。前と同様に、検索履歴の活用のヒントや、診断ログでコールを特定するためのヒントを参照してください。前と同様に、Expressway-E の検索履歴を使用した結果、このコールはそこから発信していて失敗していると判断されました。次に示すのは分析の最初の部分です。この部分について、Expressway-C から Expressway-E に送られている最初の SIP INVITE を調べることができます。

```
2017-09-25T11:26:02.959-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,959"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="25675" Msg-Hash="1536984498381728689"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972

To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 15:26:02 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 8e8c014d-5d01-4581-8108-5cb096778fc5
Session-ID: 75957d4fb66a13e835c10737aa505813;remote=00000000000000000000000000000000
Cisco-Guid: 3582928512-0000065536-0000000240-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

SIPヘッダーのコールID(d58f2680-9c91200a-1c7ba-1501a8c0)を使用すると、このダイアログに関連するすべてのメッセージをすばやく検索できます。コールIDのログで3つ目のヒット箇所を見てみると、Expressway-E から即座に 404 Not Found が Expressway-C に送信されていることがわかります。

2017-09-25T11:26:13.286-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:13,286"
Module="network.sip" Level="DEBUG": **Action="Sent"** Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="25675" Msg-Hash="12372154521012287279"

SIPMSG:

|SIP/2.0 404 Not Found

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e3863ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE
From: "Jonathan Robb"

;tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972

To:

Server: TANDBERG/4135 (X8.10.2) Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa505813 Content-Length: 0

このデータから2つのことがわかります。

1. Expressway-E は Cisco Webex への INVITE の送信をまったく試行していない。
2. Expressway-E が、404 Not Found エラーでコールを拒否するためのロジックを決定する責任を負っていました。

通常、404 Not Found エラーは、Expressway が宛先アドレスを見つけることができないことを意味します。Expressway は、Expressway 同士の間で、および別の環境にコールをルーティングするために検索ルールを使用します。そのため、最初に Expressway-E の xConfiguration に注目します。この xConfiguration の中で、Webex ハイブリッド DNS ゾーンにコールを渡す検索ルールを探ることができます。Expressway で設定されている検索ルールを xConfiguration の観点から探すには、「xConfiguration Zones Policy SearchRules Rule」を検索します。すると、Expressway で作成された検索ルールごとに検索ルール設定のリストが得られます。「ルール」の後に表示される番号は、最初に作成された検索ルールが1としてマークされているかどうかに基づいて増加します。検索ルールが見つからない場合は、よく使用されている「Webex」などの名前の値を使用すると、検索ルールを見つけやすくなります。ルールを識別するもう1つの方法は、「.*@.*\.ciscopark\.com」に設定されているパターン文字列値を見つけることができます。想定された設定の内容になっています。(パターン文字列が正しく設定されていると仮定)。このシナリオの xConfiguration を調べてみると、検索ルール6が Cisco Webex にコールを渡す正しいルールであることがわかります。

```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern String: ".*@.*\.ciscopark\.com"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Type: "Regex"
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 6 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 6 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 6 Source Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 6 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 6 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 6 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Type: "Zone"
```

このパターンをテストするには、「パターンの確認」機能を使用します。ここで重要なのは、次の値を設定することです。[メンテナンス (Maintenance)] > [ツール (Tools)] > [パターンの確認 (Check pattern)]

- エイリアス : %最初の INVITE にある要求 URI% (例 : pstojano-test@dmzlab.call.ciscopark.com) を設定できます。
- パターン タイプ (Pattern type) : 正規表現
- パターン文字列 . * @ . * \ . c i s c o p a r k \ . c o m
- パターン動作 (Pattern behavior) : 脱退

ルールの正規表現を正しく設定すると、この「パターンの確認」が成功したという結果が表示されます。この様子を次の図に示します。

Check pattern

Alias

Alias i

Pattern

Pattern type Regex ▼ i

Pattern string i

Pattern behavior Leave ▼ i

Result	
Result	Succeeded
Details	Alias matched pattern
Alias	pstoiano-test@dmzlab.call.ciscospark.com

検索ルールが存在して正しく設定されていることを確認できたので、Expressway が実行している検索ロジックを詳しく調べて、404 Not Found を送信している Expressway-E に影響を与えているかどうかを判断できます。Expressway が実行していた検索ルール ロジックの例を次に示します。

```

2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstoiano-test@dmzlab.call.ciscospark.com'"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstoiano-test@dmzlab.call.ciscospark.com'"
2017-09-25T11:26:02.967-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,967"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'to DNS' towards target
'DNS' at priority '100' with alias 'pstoiano-test@dmzlab.call.ciscospark.com'"

2017-09-25T11:26:02.968-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,968"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="dmzlab.call.ciscospark.com"
Type="NAPTR (IPv4 and IPv6)"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Could not resolve hostname"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"

```

この例では、Expressway は 4 つの検索ルールを処理したことがわかります。最初の 3 つはさまざまな理由で考慮されていませんでしたが、4 つ目は考慮されていました。このデータで興味深いのは、考慮の直後に Expressway が直接 DNS ルックアップ ロジックに移動していることです。xConfiguration で確認したことを考えてみると、Webex ハイブリッド用に設定された検索ルールは「Webex Hybrid - to Webex Cloud」という名前ですが、前述の検索ルールでは考慮すらされていませんでした。そこで、考慮された検索ルール (to DNS) がどのように実装されていたのかを調べれば、Webex ハイブリッド検索ルールの使用に影響を与えているかどうかについて理解を深めることができます。そのために、今度は改めて xConfig を調べ、「to DNS」という名前の検索ルールを探します。

```

*c xConfiguration Zones Policy SearchRules Rule 1 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Description:
*c xConfiguration Zones Policy SearchRules Rule 1 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "(?!.*@%localdomains%.*$).*"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: "Regex"

```

```
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 1 Protocol: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Mode: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Name: "Please Select"
*c xConfiguration Zones Policy SearchRules Rule 1 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 1 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Name: "DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Type: "Zone"
```

この検索ルールを調べた結果、次のように結論付けることができます。

- ・パターン文字列は Cisco Webex 要求 URI にマッチすると考えられる
- ・優先度は 100 に設定されている
- ・進行状況 (パターン動作) は「停止 (Stop)」に設定されている

こうした情報から、コールされている側の Cisco Webex 要求 URI はこのルールにマッチすると考えられ、ルールがマッチしたのであれば Expressway は他の検索ルールの検索 (考慮) を停止すると考えられます。以上の考察から、ルールの優先度が重要な要因になります。Expressway における検索ルールの優先度の仕組みでは、最低の優先度のルールが最初に試行されます。次に例を示します。検索ルール : Localパターン動作 (Pattern behavior) : [Continue]優先度1検索ルール : ネイバーパターン動作 (Pattern behavior) : [Continue]priority 10検索ルール : DNSパターン動作 (Pattern behavior) : stop優先度 50この例では、Local (1) という検索ルールが最初に試行され、マッチが見つかった場合は「パターン動作 (Pattern behavior)」が「続行 (Continue)」に設定されているので検索ルール Neighbor (10) に進みます。検索ルール Neighbor にマッチしなかった場合でも、続けて検索ルール DNS (50) に進み、最後に考慮されます。検索ルール DNS がマッチした場合は、50 より高い優先度を持つ別の検索ルールが存在するかどうかに関係なく、「パターン動作 (Pattern behavior)」が「停止 (Stop)」に設定されているため検索が停止します。以上のことを踏まえて、「to DNS」ルールと「Webex Hybrid - to Webex Cloud」の間で検索ルールの優先度を調べることができます。

```
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"

*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"
```

ここでは、「to DNS」ルールの優先度が「Webex Hybrid - to Webex Cloud」ルールよりも低いことが分かります。したがって、「to DNS」ルールが最初に試行されます。「パターン動作 (進行状況) (Pattern behavior (Progress))」が「停止 (Stop)」に設定されているとすれば、Expressway-E が Webex Hybrid - to Webex Cloud ルールを考慮することは決してなく、コールは最終的に失敗します。解決方法ハイブリッド コール サービス接続ではこの種の問題が多くなってきています。ソリューション導入の際に、優先度の高いルールを作成して Cisco Webex の検索に使用する事例が多くなっています。多くの場合、このようにして作成されたルールは呼び出されません。理由は、優先度の低い既存のルールがマッチして結果的に失敗するからです。この問題は、Cisco Webex に対するインバウンド コールとアウトバウンド コールの両方で発生します。これを解決するには、次の手順を実行する必要があります。

1. Expressway-E にログインします。
2. [設定 (Configuration)] > [ダイヤルプラン (Dial Plan)] > [検索ルール (Search rules)] に移動します。
3. Webex ハイブリッドの検索ルールを探してクリックします (例 : [Name] : Webex Hybrid - to Webex Cloud) 。
4. [優先度] の値に、他の検索ルールよりも低い値を設定して、他の検索ルールに影響を与えないようにします (例 : Priority:99) 。

検索ルールの原則として、パターン文字列が具体的なものほど、検索ルールの優先度リストで低い優先度にします。通常、DNS ゾーンで設定されているパターン文字列では、ローカルドメインでないものがすべてマッチしてインターネットに送信されます。そのため、検索ルールのタイプを高優先度に設定して、最後に呼び出されるようにすることをお勧めします。問題 4: Expressway の CPL が正しく設定されていない Expressway ソリューションでは、サーバで使用可能な Call Processing Language (CPL) のロジックを使用することで、通話料金の不正を軽減できます。展開中の Expressway ソリューションが、Cisco Webex ハイブリッドコールサービスと、モバイルおよびリモートアクセス専用の場合は、CPL のポリシーとルールを有効にして実装することを強く推奨します。Expressway で CPL を Cisco Webex ハイブリッド用に設定することは非常に簡単ですが、誤った設定をすると容易にコールの試行が妨げられるおそれがあります。以下のシナリオでは、診断ログを使用して CPL の設定の誤りを特定する方法について説明します。他のすべてのフォークされた発信コールのシナリオと同様に、症状は同じです。

- 着信ユーザの Cisco Webex アプリに [参加 (Join)] ボタンが表示された
- 発信側の電話に着信音が送り返されていた
- 着信ユーザのオンプレミス電話機では着信音が鳴っていた
- 着信ユーザのアプリでは着信音が鳴らなかった

他のすべてのシナリオと同様に、Expressway-C および E の診断ログに加えて CUCM SDL トレースを利用することもできます。前と同様に、[検索履歴(Search History)]と、診断ログでコールを識別するためのヒントを使用します。前と同様に、Expressway-E の検索履歴を使用した結果、このコールはそこに着信していて失敗していると判断されました。次に示すのは分析の最初の部分です。この部分について、Expressway-C から Expressway-E に送られている最初の SIP INVITE を調べることができます。

```
2017-09-25T16:54:43.722-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,722"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26404" Msg-Hash="17204952472509519266"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscopark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

```
;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000
```

To:

```
Max-Forwards: 15
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
```

Date: Mon, 25 Sep 2017 20:54:43 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 4ffffefed-0512-4067-ac8c-35828f0a1150
Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

SIP ヘッダーからのコール ID (c030f100-9c916d13-1cdcb-1501a8c0) を使用して、このダイアログに関連するすべてのメッセージを検索して絞り込むことができます。コール ID のログで 3 つ目のヒット箇所を見てみると、Expressway-E から即座に 403 Forbidden が Expressway-C に送信されていることがわかります。

2017-09-25T16:54:43.727-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,727"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="26404" Msg-Hash="9195436101110134622"
SIPMSG:
|SIP/2.0 403 Forbidden
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0de36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;received=192.168.1.5;rport=26404;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
From: "Jonathan Robb"

;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000

To:

;tag=64fe7f9eab37029d

Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa512577
Content-Length: 0

Expressway-Eがこのコールを拒否し、Expressway-Cに403 Forbiddenエラーを送信した理由を理解するには、Expresswayに入力した403 Forbiddenと元のSIP INVITEの間のログエントリを分析します。検索ルールがまったく呼び出されておらず、Call Process Language (CPL) のロジックが呼び出されていることに注意してください。そのスニペットを次に示します。

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:

前述のログの分析から、CPL がコールを拒否していると判断できます。

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4fffefed-0512-4067-ac8c-35828f0a1150"
Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-25 20:54:43,726"

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Call Rejected" Service="SIP" Src-ip="192.168.1.5" Src-port="26404" Src-alias-type="SIP"

注：この状況では検索ルールの呼び出しは確認されません。なぜなら、CPL、FindMe、およびトランスフォーメーションがすべて検索ルールより前に処理されているからです。ほとんどの場合、Expressway の xConfig を利用して状況を詳しく理解できます。ただし、CPL の場合、定義済みのルールはポリシーが有効になっている場合にしか表示できません。次に示す xConfig の一部分では、Expressway-E がローカル CPL ロジックを使用していることがわかります。

*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"

ルール設定をより深く理解するには、図のように、Expressway-E にログインし、[設定 (Configuration)] > [コール ポリシー (Call Policy)] > [ルール (Rules)] に移動する必要があります。

Call Policy rules

Source	Destination	Action	Rearrange
	@dmzlab.call.ciscospark.com	Reject	

この設定を調べてみると、次のものが設定されていることがわかります。送信元：.*宛先：.*@dmzlab.call.ciscospark.com.*Action:[Reject] 『[Cisco Webex ハイブリッド コール サービス導入ガイド](#)』の内容と比べてみると、送信元 (Source) と宛先 (Destination) が逆方向に設定されていることがわかります。

Field	Setting
Source Type	From address
Rule applies to	Unauthenticated callers
Source pattern	.*@example.call.ciscospark.com.*, where example is your company's subdomain.
Destination pattern	.*
Action	Reject

解決方法この問題を解決するには、CPLルールの設定を修正し、[Source]が。

*@%Webex_subdomain%.call.ciscospark.com.*に設定され、[Destination Pattern]が。*

1. Expressway-E にログインします。
2. [設定 (Configuration)] > [コール ポリシー (Call Policy)] > [ルール (Rules)] に移動します。
3. Cisco Webex ハイブリッド コール サービス用に設定されたルールを選択します。

4. ソースパターンを`*@%Webex_subdomain%\call\ciscopark\com.*`と入力します(例：
`*@dmzlab\call\ciscopark\com.*`)
5. [Destination Pattern]に「`*`」と入力します。
6. [保存 (Save)] を選択します。

Webex ハイブリッドにおける CPL の実装の詳細については、『[Cisco Webex ハイブリッド設計ガイド](#)』を参照してください。双方向：Cisco Webex からオンプレミスへ、またはオンプレミスから Cisco Webex へ 問題 1：IP フォン/コラボレーション エンドポイントで G.711、G.722、または AAC-LD 以外のオーディオコーデックを提供しているハイブリッドコール サービス接続は、G.711、G.722、AAC-LD の 3 つの異なるオーディオコーデックをサポートしています。Cisco Webex 環境でコールが正常に確立されるように、必ずこれらのオーディオコーデックのいずれかを使用してください。オンプレミス環境は多くのタイプのオーディオコーデックを使用するように設定できますが、同時にそれらを制限するように設定することもできます。この操作は、Unified CM のカスタムのリージョン設定やデフォルトのリージョン設定を使用することで意図的に行えますが、意図せずに行われることもあります。この特定の動作については、ロギングのパターンがコールの方向によって異なる場合があります、Unified CM が早期オファー (Early Offer) を使用するように設定されていたか遅延オファー (Delayed Offer) を使用するように設定されていたかによっても異なります。以下では、この動作で生じるさまざまな状況の例をいくつか示します。

1. Cisco Webex が着信 INVITE を送信し、同時に G.711、G.722、または AAC-LD を提供する SDP を送信します。Expressway-C はこのメッセージを Unified CM に送信しますが、Unified CM はこのコールについて G.729 のみを許可するように設定されています。したがって、使用可能なコーデックがないため Unified CM はコールを拒否します。
2. Unified CM が Cisco Webex への発信コールを早期オファー (Early Offer) として試行します。つまり、Expressway-C に送信される最初の INVITE には、G.729 オーディオ「のみ」をサポートする SDP が含まれます。次に、Cisco Webex は G.729 をサポートしていないため、音声をゼロにする 200 OK/SDP(`m=audio 0 RTP/SAVP`)を送信します。Expressway-C がこの INVITE を Unified CM に渡が使用可能がないため、コールがを終了します..
3. Unified CM が Cisco Webex への発信コールを遅延オファー (Delayed Offer) として試行します。つまり、Expressway-C に送信される最初の INVITE には SDP が含まれません。次に、Cisco Webex は 200 OK を送信し、同時に、Cisco Webex がサポートするすべてのオーディオコーデックを含む SDP を送信します。Expressway-C はこの 200 OK を Unified CM に送信しますが、Unified CM はこのコールについて G.729 のみを許可するにしか設定されていません。したがって、使用可能なコーデックがないため Unified CM はコールを拒否します。

この問題に一致する Hybrid Call Service Connect コール障害を特定する場合は、Unified CM SDL トレースに加えて、Expressway ログを取得する必要があります。次のログスニペットの例は、Unified CM が発信コールを Early Offer としてとして試行している状況 #2 に一致します。コールは Cisco Webex に到達していることがわかっているため、Expressway-E からログの分析を始めます。Cisco Webex への最初の INVITE のスニペットを次に示します。優先されるオーディオコーデックは G.729 (ペイロード 18) に設定されていることがわかります。101 は DTMF であり、この特定のシナリオでは関連性はありません。

```
2017-09-19T10:46:10.488-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:10,488"  
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="172.16.2.2" Local-port="25034" Dst-  
ip="146.20.193.64" Dst-port="5062" Msg-Hash="4309505007645007056"  
SIPMSG:  
INVITE sip:pstojano-test@dmzlab.call.ciscopark.com SIP/2.0  
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-  
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-  
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport  
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-  
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone  
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
```

zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Remote-Party-ID: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;privacy=off;screen=no;party=calling
Contact: <sip:172.16.2.2:5073;transport=tls>;video;audio
From: "Jonathan Robb"

Max-Forwards: 14
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aede256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aede256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
Supported: X-cisco-srtp-fallback,replaces,timer
Session-Expires: 1800;refresher=uac
Min-SE: 500
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Length: 1407

v=0
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
c=IN IP4 64.102.241.236
b=AS:384
t=0 0
m=audio 52668 RTP/SAVP 18 101 <-- CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=rtcp:52669 IN IP4 64.102.241.236
m=video 52670 RTP/SAVP 126 97
b=TIAS:384000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801e;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....

UNENCRYPTED_SRTCP

a=sendrecv

a=content:main

a=label:11

a=rtcp:52671 IN IP4 64.102.241.236

この最初の INVITE に対して、Cisco Webex は 200 OK メッセージで応答しています。このメッセージを詳しく調べてみると、オーディオコーデックがゼロで埋められたことがわかります。オーディオポートが割り当てられていなければ、コールがそのストリームをネゴシートできないため、このことは問題になります。

2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"

Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="25034"

Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"

SIPMSG:

SIP/2.0 200 OK

Via: SIP/2.0/TLS 64.102.241.236:5062;egress-

zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-

id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS

172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acdde05b35adc5c157;x-cisco-local-

service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS

192.168.1.6:5061;egress-

zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d

bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-

14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-

zone=HybridCallServiceTraversal;branch=z9hG4bKf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd

66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-

c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-

zone=HybridCallServiceTraversal,SIP/2.0/TCP

192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11

Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21

CSeq: 101 INVITE

Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>

From: "Jonathan Robb"

Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-55aede256d2@64.102.241.236:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-55aede256d2@172.16.2.2:5061;transport=tls;lr>

Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE

User-Agent: Cisco-L2SIP

Supported: replaces

Accept: application/sdp

Allow-Events: kpml

Session-ID: ed35426ed3ade6fdc3b058792333df2b;remote=75957d4fb66a13e835c10737aa329445

Locus: 4711a33f-9d49-11e7-9bf6-dea12d0f2127

Locus-Type: CALL

Content-Type: application/sdp

Content-Length: 503

v=0

o=linus 0 1 IN IP4 146.20.193.109

s=-

c=IN IP4 146.20.193.109

b=TIAS:384000

t=0 0

m=audio 0 RTP/SAVP * <-- Webex is zeroing this port out

m=video 33512 RTP/SAVP 108

c=IN IP4 146.20.193.109

b=TIAS:384000

a=content:main

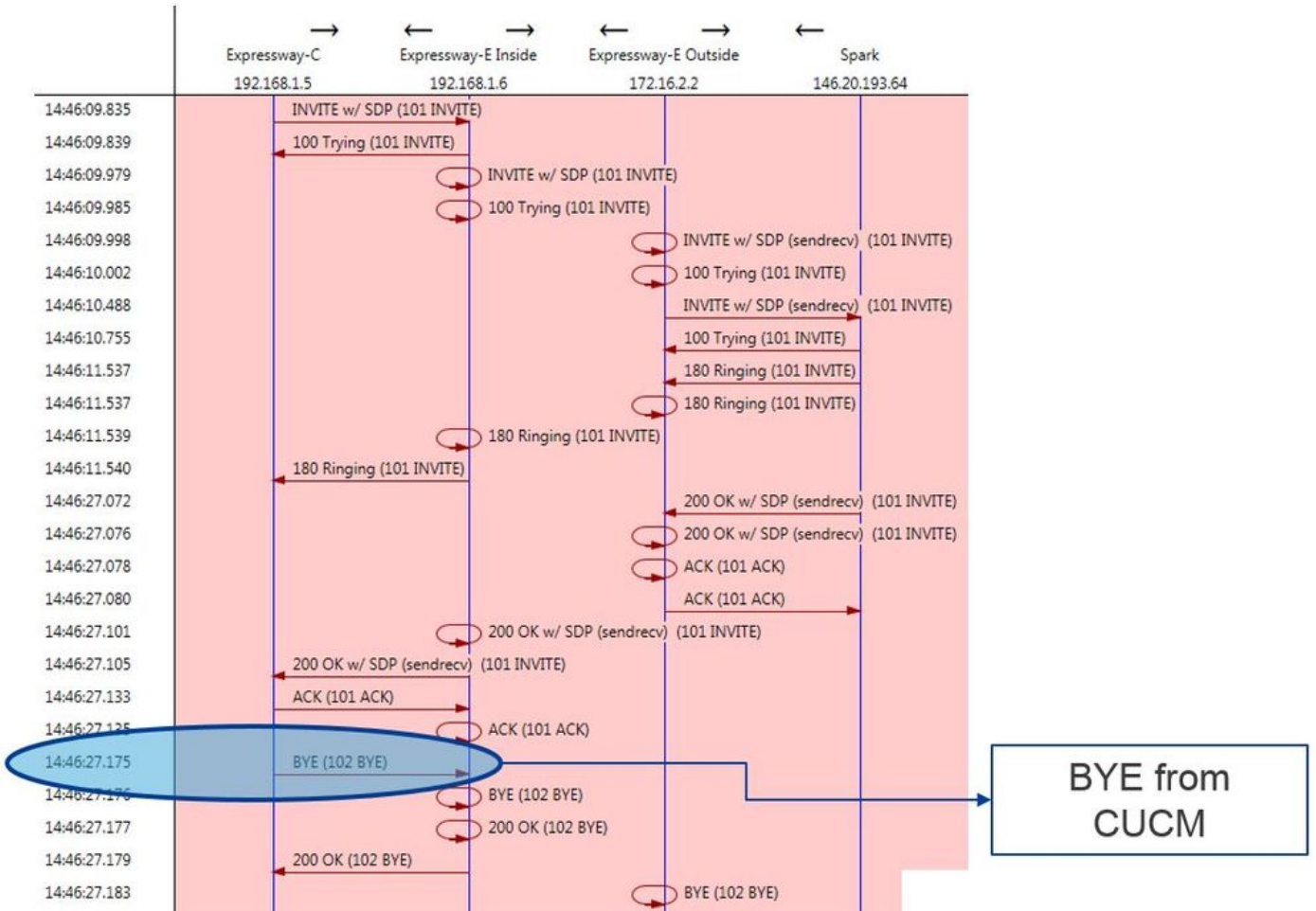
a=sendrecv

```

a=rtpmap:108 H264/90000
a=fmtp:108 profile-level-id=42001E;packetization-mode=1;max-mps=40500;max-fs=1620;max-
fps=3000;max-br=10000;max-dpb=3037;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=label:200

```

ここで、TranslatorX を使用してダイアログの残りの部分を調べてみましょう。ダイアログ自体が ACK で完了していることがわかります。問題は、ダイアログが完了した直後に、図に示すように、Expressway-C の方向から来る BYE が存在することです。



BYEメッセージの詳細な例を次に示します。明らかに、ユーザエージェントは Cisco-CUCM11.5 です。つまり、メッセージは Unified CM によって生成されていることがわかります。別の点で指摘すべきは、原因コードが cause=47 に設定されているということです。この場合の一般的な変換は No resource available です。

```

2017-09-19T10:46:27.175-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,175"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="237943800593485079"
SIPMSG:
BYE sip:192.168.1.6:5071;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK90a666b3461356f8cd605cec91e4538240575.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-c60a8b17a8bd;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12ddd10269d39;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 102 BYE
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=329447~c9cc7ddc-9592-49e8-a13c-
79e26f48eebc-30106833
To: <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=f3734601fb0eb541
Max-Forwards: 69
Route: <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:7003;transport=tls;lr>, <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-

```

14872e007efb@192.168.1.6:5061;transport=tls;lr>
User-Agent: Cisco-CUCM11.5
Date: Tue, 19 Sep 2017 14:46:09 GMT
X-TAAntag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Reason: Q.850 ;cause=47
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=ed35426ed3ade6fdc3b058792333df2b
Content-Length: 0

Cisco Webexコンポーネントは、このコールサンプルのオーディオコーデックをゼロにしたため、次の点に焦点を当てる必要があります。a.Cisco Webex に送信された最初の INVITEb.ポートをゼロで埋めるのに使用された Cisco Webex のロジック最初のINVITEに関して何が固有なのかを見てみましょう。G.729のみが含まれています。この点については、『Cisco Webexハイブリッドコールサービス導入ガイド』を参照し、「ハイブリッドコールサービス接続の前提条件の完了」セクションのステップ5を参照してください。次のような説明があります。Cisco Webex は次のコーデックをサポートしています。

- オーディオ : G.711、G.722、AAC-LD
- ビデオ : H.264

注 : Opusは、Cisco Webexハイブリッドコールのコールのオンプレミスレグでは使用されません。以上のことから、Unified CM がサポートされていないオーディオコーデックを送信していて、それが原因で Cisco Webex がポートをゼロで埋めていると判断できます。ソリューション : この特定の状況に対処するには、オンプレミスでコールをアンカーしているCisco Webex RDとExpressway-CのSIPトランクの間のリージョン設定を確認する必要がある場合があります。確認するには、これらの2つの要素があるデバイスプールを決定します。デバイスプールにはリージョンへのマッピングが含まれています。Expressway-C の SIP トランクのデバイスプールを調べるには、次の操作を行います。

1. Unified CMにログインします。
2. [Device] > [Trunk]に移動します。
3. トランク名を検索するか、[検索]をクリックします。
4. Expressway-Cトランクを選択します。
5. デバイスポールの名前を記録します。

コールをアンカーしたCTI-RDまたはCisco Webex-RDのデバイスプールを確認するには、次の手順に従います。

1. [Device] > [Phone] の順に移動します。
2. 検索時に、[Device Type contains Webex]または[CTI Remote Device] (お客様が何を使用しているかに応じて) を選択できます。
3. デバイスポールの名前を記録します。

各デバイスプールに接続されているリージョンを確認します。

1. [システム(System)] > [デバイスプール(Device Pool)]に移動します。
2. Expressway-C SIPトランクに使用するデバイスプールを検索します。
3. デバイスポールをクリックします。
4. 領域名を記録します。
5. Webex-RDまたはCTI-RDに使用するデバイスプールを検索します。
6. デバイスポールをクリックします。
7. 領域名を記録します。

地域関係の決定 :

1. [システム(System)] > [リージョン情報(Region information)] > [リージョン(Region)]に移動します。
2. 特定された地域のいずれかを検索します。
3. G.729を使用している両方のリージョン間にリージョン関係があるかどうかを確認します。

この時点で、G.729 を使用している関係を特定した場合は、Cisco Webex が使用するサポート対象のオーディオコーデックがサポートされるようにその関係を調整するか、またはその関係をサ

ポートしているリージョンを持つ別のデバイスプールを使用する必要があります。前述のシナリオでは、次のような判断をしました。Expressway-C トランクのリージョン
: ReservingBandwidthWebex RD のリージョン : RTP-Devices図に示すように、RTPデバイスと ReservingBandwidth領域の関係を図示します。

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps
ReservingBandwidth	Use System Default (Factory Default low loss)	8 kbps (G.729)	384 kbps	384 kbps
RTP-Devices	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps
RTP-Infrastructure	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps

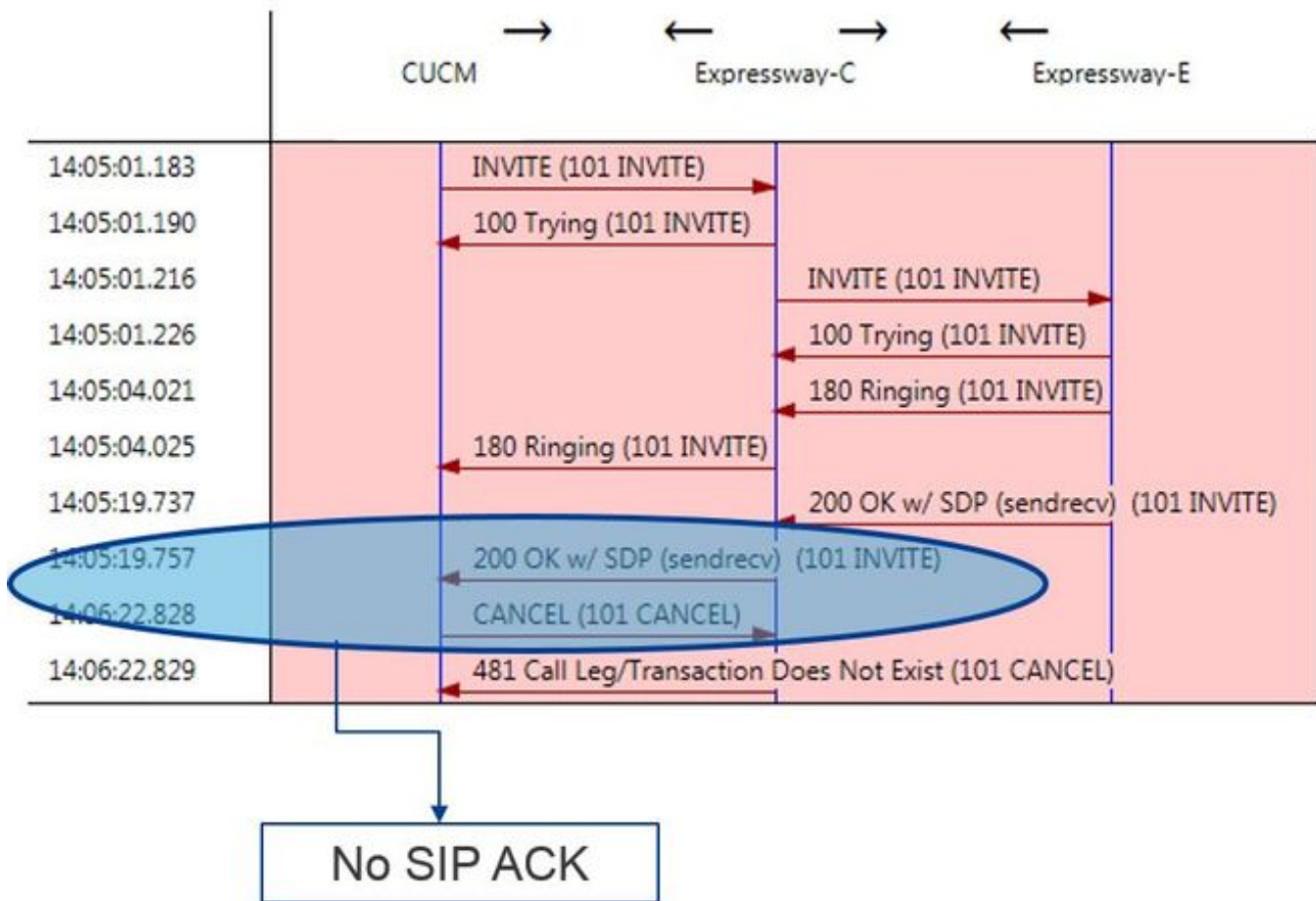
G.729 Not Supported by Spark

Expressway-C トランクが存在していたデバイスプールを変更すると、リージョンの関係が変更されます。新しいデバイスプールのリージョンは RTP-Infrastructure に設定されています。したがって、Cisco Webex-RD と Expressway-C トランク間の新しいリージョン関係は RTP-Devices と RTP-Infrastructure になりました。図に示すように、この関係はCisco Webexでサポートされているオーディオコーデックの1つであるAAC-LDをサポートしているため、コールは正しく設定されます。問題 2 : Unified CM の最大着信メッセージ サイズを超えている企業内でのビデオの普及度が高まっているため、SDP が含まれている SIP メッセージのサイズがかなり大きくなってきています。これらのメッセージを処理するサーバは、大きなパケットを受け入れるように設定する必要があります。呼制御サーバの多くはデフォルト値で対応できます。Cisco Unified Communications Manager (Unified CM) では、過去のリリースにおいて、SDP が含まれている大きなサイズの SIP メッセージを処理するためのデフォルト値が存在しませんでした。Unified CMの新しいリリースでは、SIPメッセージに対して許可される値サイズが増加していますが、この値は新規インストールでのみ設定され、アップグレードでは設定されていません。これで、Hybrid Call Service Connectをサポートするために旧リリースのUnified CMをアップグレードしているお客様は、Unified CMの最大着信メッセージサイズが小さすぎると影響を受ける可能性があります。この問題に一致するハイブリッド コール サービス接続のコール障害を特定しようとする場合は、Unified CM の SDL トレースだけでなく、Expressway のログも必要になります。障害を特定するには、まず何が起こるか、次に障害が発生するシナリオのタイプを理解します。何が起こるのかという質問に答えるには、Unified CMが大きすぎるSIPメッセージを受信すると、TCPソケットを閉じるだけで、Expressway-Cに応答しないことに注意する必要があります。ただし、数多くの状況や手段によってこうした現象が起こる可能性があります。

1. Cisco Webex が、サイズが大きすぎる着信 INVITE と SDP を送信します。Expressway-C はこれを Unified CM に渡しますが、Unified CM は TCP ソケットを閉じ、その後 SIP ダイアログがタイムアウトになります。
2. Unified CM が Webex への発信コールを早期オファー (Early Offer) として試行します。つまり、Expressway-C に送信される最初の INVITE には SDP が含まれます。次に、Cisco Webex は 200 OK と SDP を送信して応答しますが、Expressway-C から Unified CM に渡されたときの 200 OK 応答はサイズが大きすぎます。Unified CM は TCP ソケットを閉じ、その後 SIP ダイアログがタイムアウトになります。
3. Unified CM が Webex への発信コールを遅延オファー (Delayed Offer) として試行します。つまり、Expressway-C に送信される最初の INVITE には SDP が含まれません。次に、Cisco Webex は 200 OK と SDP を送信しますが、Expressway-C から Unified CM に渡されたときの 200 OK オファーはサイズが大きすぎます。Unified CM は TCP ソケットを閉じ、その後 SIP ダイアログがタイムアウトになります。

Expressway-C のログでこの特定の状況を探してみると、メッセージフローを理解しやすくなります。TranslatorXなどのプログラムを使用する場合は、Expressway-CがCisco Webex 200 OKとSDPをUnified CMに渡していることがわかります。ここで問題になるのは、図に示すように、

Unified CM が SIP ACK で決して応答を返さないことです。



応答をしないのは Unified CM の責任であるため、SDL トレースを調べて Unified CM がこの状況をどのように処理しているのかを明らかにすることには意味があります。このシナリオでは、Unified CMはExpressway-Cからの大きなメッセージを無視します。このようなログライン項目が印刷されます。

CUCM Traces

```
53138762.000 |09:05:19.762 |AppInfo |SIPSocketProtocol(5,100,14,707326)::handleReadComplete
send SdlReadRsp: size 5000
53138763.000 |09:05:19.762 |SdlSig |SdlReadRsp |wait
|SIPTcp(5,100,71,1) |SdlTCPConnection(5,100,14,707326)
|5,100,14,707326.4^10.36.100.140^^ |*TraceFlagOverrode
53138763.001 |09:05:19.762 |AppInfo |SIPTcp - SdlRead bufferLen=5000
53138763.002 |09:05:19.762 |AppInfo |//SIP/Stack/Error/0x0/httpish_cache_header_val: DROPPING
unregistered header Locus: c904ecb1-d286-11e6-bfdf-b60ed914549d
53138763.003 |09:05:19.762 |AppInfo |//SIP/Stack/Info/0x0/httpish_msg_process_network_msg:
Content Length 4068, Bytes Remaining 3804
53138763.004 |09:05:19.762 |AppInfo |//SIP/Stack/Info/0x0/ccsip_process_network_message:
process_network_msg: not complete
53138763.005 |09:05:19.762 |AppInfo |SIPTcp - Ignoring large message from %Expressway-
C_IP%:[5060]. Only allow up to 5000 bytes. Resetting connection.
```

SIPダイアログがタイムアウトすると、Cisco Webexはログサンプルに記載されているように、着信SIP 603 DeclineメッセージをExpressway-Eに送信します。

Expressway-E Traces

```
2017-01-04T09:05:40.645-05:00 vcs-expressway tvcs: UTCTime="2017-01-04 14:05:40,645"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="%Exp-E%" Local-port="25150" Src-
ip="%Webex_IP%" Src-port="5062" Msg-Hash="2483073756671246315" SIPMSG: SIP/2.0 603 Decline
```

前述したように、この動作を確認できるシナリオは3つあります。わかりやすくするため、この図では3番目の状況に一致したログの例を示しています。この場合、Cisco Webexへの発信コールが遅延オファー (Delayed Offer) として送られました。ソリューション:

1. Unified CMにログインします。
2. [System] > [Service Parameters] に移動します。

3. Call Managerサービスを実行しているサーバを選択します。
4. サービスの選択を求めるプロンプトが表示されたら、Cisco Call Managerサービスを選択します。
5. [詳細]オプションを選択します。
6. [クラスタ全体に及ぶパラメータ (デバイス - SIP) (Clusterwide Parameters (Device - SIP))] の設定で、[SIP の最大受信メッセージのサイズ (SIP Max Incoming Message Size)] を 18000 に変更します。
7. [Save] を選択します。
8. Cisco Call Manager サービスを実行しているすべての Unified CM ノードで、この手順を繰り返します。

注：IP フォン、コラボレーション エンドポイント、SIP トランクなどでこの設定を利用するためには再起動が必要になります。環境への影響を最小限に抑えるため、これらのデバイスを個別に再起動できます。CUCM上のすべてのデバイスをリセットすることは、絶対に許容できるもので

ない限り避けてください。**付録** Expressway トラブルシューティング ツールパターンの確認ユーティリティ Expressway には、パターンが特定のエイリアスに一致するかどうかをテストする際に役立つパターンチェックユーティリティがあり、期待どおりに変換されます。このユーティリティは、Expressway の [メンテナンス (Maintenance)] > [ツール (Tools)] > [パターンの確認 (Check pattern)] メニュー オプションにあります。通常、これは、検索ルールの正規表現がパターン文字列に対するエイリアスと正しく一致するかどうかをテストし、オプションで文字列の正常な操作を実行する場合に使用されます。ハイブリッド コール サービス接続の場合は、Unified CM クラスタ FQDN が、Unified CM クラスタ FQDN で設定したパターン文字列にマッチするかどうかをテストすることもできます。このユーティリティを使用する際は、宛先 URI ではなくルート ヘッダーにリストされた Unified CM クラスタ FQDN パラメータに基づいてコールがルーティングされることに注意してください。たとえば、次の INVITE が Expressway に着信した場合は、jorobb@rtp.ciscotac.net ではなく cucm.rtp.ciscotac.net に対してパターンの確認機能

```
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eeaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-
local-service=nettle;received=192.168.1.6;rport=41913;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK524f89592d00ffc45b7b53000271676c370.88b5177ac4d7cfcae1eb8f8be78da
055;proxy-call-id=2db939b2-a49b-4307-8d96-23716a2c090b;received=172.16.2.2;rport=25010
Via: SIP/2.0/TLS
192.168.4.150:5062;branch=z9hG4bK92f9ef952712e6610c3e6b72770c1230;received=148.62.40.63;rport=39
986;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-313634-
3d27a6f914badee6420287903c9c6a45;rport=45939
Call-ID: 3e613afb185751cdf019b056285eb574@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscospark.com>;tag=145765215
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

Check pattern を使用して、Hybrid Call Service Connect Route(HCCA)ヘッダー検索ルールルーティングをテストするには、次の手順を実行します。

1. [メンテナンス]> [ツール]> [パターンの確認]に移動します。
2. エイリアスとして、Unified CM Cluster FQDNを入力します。
3. [パターンタイプ]を[プレフィック]に設定します。
4. パターン文字列を[Unified CM Cluster FQDN]に設定します。
5. パターン動作をLeaveに設定します。
6. [パターンの確認]を選択します。

Expressway の検索ルールが正しく設定されていれば、[結果 (Results)] に [成功 (Succeeded)] のメッセージが返されます。図に示すように、正常なCheck pattern testの例を示します。

Check pattern

Alias: cucm.rtp.ciscotac.net

Pattern type: Prefix

Pattern string: cucm.rtp.ciscotac.net

Pattern behavior: Leave

Check pattern

Result

Result	Succeeded
Details	Alias matched pattern
Alias	cucm.rtp.ciscotac.net







これが成功した理由は、このエイリアス(cucm.rtp.ciscotac.net)が(cucm.rtp.ciscotac.net)のプレフィックスパターン文字列と一致するためです。これらの結果に基づいてコールがルーティングされる方法を理解するには、説明されているExpresswayロケートユーティリティを使用します。検索ユーティリティExpressway 検索ユーティリティは、指定した別名に基づいて Expressway がコールを特定のゾーンにルーティングできるかどうかをテストする場合に便利です。テストはすべて、実際にコールを発信せずに実行できます。検索ユーティリティは、Expressway の [メンテナンス (Maintenance)] > [ツール (Tools)] > [検索 (Locate)] メニューにあります。

Expressway-Cの検索機能を使用して、サーバがSIPルートヘッダーで見つかったUnified CMクラスターのFQDNに基づいてコールをルーティングできるかどうかを判断する方法を説明します。

1. [メンテナンス]> [ツール]> [検索]に移動します。
2. [Alias]フィールドにUnified CMクラスターのFQDNを入力します。
3. プロトコルとしてSIPを選択します。
4. ソースのCisco Webex Hybrid Traversalクライアントゾーンを選択します。
5. [検索]を選択します。

インターフェイスの下部に検索結果が表示されます。図に示すように、一致結果を使用して実行されたサンプルテストの例を次に示します。

Locate

Locate	
Alias	* cucm.rtp.ciscotac.net 
Hop count	* 5 
Protocol	SIP 
Source	Hybrid Call Service Traversal 
Authenticated	Yes 
Source alias	<input type="text"/> 

Locate

[Locate]の結果を次に示します。太字は関心価値です。次の結果が表示されます。

- 別名がルーティングされた可能性があるという事実 (True)
- 送信元情報 (ゾーン名/タイプ)
- 宛先情報 (ルーティングされている別名)
- マッチしている検索ルール (ハイブリッド コール サービス着信ルーティング (Hybrid Call Service Inbound Routing))
- コールの送信先ゾーン(CUCM11)

```
Search (1)
State: Completed
Found: True
Type: SIP (OPTIONS)
SIPVariant: Standards-based
CallRouted: True
CallSerial Number: ae73fb64-c305-457a-b7b3-59ea9688c630
Tag: 473a5b19-9a37-40bf-bbee-6f7bc94e7c77
Source (1)
Authenticated: True
Aliases (1)
Alias (1)
Type: Url
Origin: Unknown
Value: xcom-locate
Zone (1)
Name: Hybrid Call Service Traversal
Type: TraversalClient
Path (1)
Hop (1)
Address: 127.0.0.1
Destination (1)
Alias (1)
Type: Url
Origin: Unknown
Value: sip:cucm.rtp.ciscotac.net
StartTime: 2017-09-24 09:51:18
Duration: 0.01
SubSearch (1)
Type: Transforms
Action: Not Transformed
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Admin Policy
Action: Proxy
ResultAlias (1)
```

Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: FindMe
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Search Rules
SearchRule (1)
Name: as is local
Zone (1)
Name: LocalZone
Type: Local
Protocol: SIP
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
Zone (2)
Name: LocalZone
Type: Local
Protocol: H323
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SearchRule (2)
Name: Hybrid Call Service Inbound Routing
Zone (1)
Name: CUCM11
Type: Neighbor
Protocol: SIP
Found: True
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.21:5065
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net

診断ロギングExpressway ソリューションを通過するコールについて、コールまたはメディアの問題をトラブルシューティングする場合は、必ず診断ログを使用する必要があります。エンジニアはこの Expressway 機能を利用して、コールの受け渡し時に Expressway が受けるすべてのロジック上の決定事項について、数多くの詳細情報を得ることができます。SIP メッセージの本体すべてを表示できるほか、Expressway でのコールの受け渡しや Expressway によるメディアチ

チャネルの設定の状況を確認できます。診断ログには、ログを生成するいくつかの異なるモジュールがあります。ログレベルを調整して、「致命的なエラー (FATAL)」、「エラー (ERROR)」、「警告 (WARN)」、「情報 (INFO)」、「デバッグ (DEBUG)」、「トレース (TRACE)」を表示できます。デフォルトでは、すべてがINFOに設定され、問題の診断に必要なほとんどすべてをキャプチャします。場合によっては、何が起きているのかを詳しく理解するために、特定のモジュールのログレベルを「情報 (INFO)」から「デバッグ (DEBUG)」に調整する必要があります。次の手順では、developer.ssl モジュールのロギングレベルを調整する方法を示しています。このモジュールは (相互) TLS ハンドシェイクの情報を提供する役目を果たします。

1. Expresswayサーバにログインします (Expressway-EとExpressway-Cの両方で実行する必要があります)。
2. [メンテナンス(Maintenance)] > [診断(Diagnostics)] > [詳細設定(Advanced)] > [サポートログの設定(Support Log configuration)]に移動します。
3. 調整するモジュール (この例では developer.ssl) までスクロールしてモジュールをクリックします。
4. Level/パラメータの横にあるメニューからDEBUGを選択します。
5. [Save] をクリックします。

この時点で、診断ログをキャプチャする準備ができました。

1. Expresswayサーバにログインします (Expressway-EとExpressway-Cの両方で実行する必要があります)。
2. [メンテナンス] > [診断] > [診断ログ]に移動します。
3. [Start New Log]をクリックします(tcpdumpオプションを必ずオンにします)。
4. 問題を再現します。
5. [ログの停止]をクリックします。
6. [ログのダウンロード]をクリックします。

Expressway の診断ログでは、Expressway-C と Expressway-E の両方から並行してロギングを開始することに注意してください。最初に、Expressway-Eのロギングを開始し、Expressway-Cに移動して開始します。その時点で問題を再現できます。注：現在、Expressway/VCS診断ログバンドルには、Expresswayサーバ証明書または信頼できるCAリストに関する情報が含まれていません。この機能が役立つと思われるケースがある場合は、[「この不具合」](#)にケースをアタッチしてください。

関連情報

- [『Cisco Webex ハイブリッド コール サービス導入ガイド』](#)
- [『Cisco Webex ハイブリッド設計ガイド』](#)
- [『Cisco Expressway Administrator Guide』](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

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。