

Cisco Webex混合呼叫服務連線故障排除指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[呼叫建立問題](#)

[相互TLS握手失敗](#)

[有用的雙向TLS故障排除提示](#)

[問題1. Expressway-E不信任簽署Cisco Webex證書的證書頒發機構\(CA\)](#)

[問題2. Expressway-E Cisco Webex混合DNS區域上的TLS主體驗證名稱不正確](#)

[問題3. Expressway-E不向Cisco Webex傳送完整證書鏈](#)

[問題4. 防火牆終止雙向TLS握手](#)

[問題5. Expressway-E由公共CA簽署，但Cisco Webex控制中心載入了備用證書](#)

[問題6. Expressway未將入站呼叫對映到Cisco Webex混合DNS區域](#)

[問題7. Expressway-E使用預設自簽名證書](#)

[入站：思科Webex到本地](#)

[問題1. Cisco Webex無法解析Expressway-E DNS SRV/主機名](#)

[問題2. 套接字故障：埠5062被阻止入站到Expressway](#)

[問題3. 套接字故障：Expressway-E未在埠5062上偵聽](#)

[問題4. Expressway-E或C不支援預載入的SIP路由報頭](#)

[問題5. Cisco Webex應用正在接收兩個呼叫通知（廣播）](#)

[出站：內部部署至Cisco Webex](#)

[問題1. Expressway無法解析callservice.ciscospark.com地址](#)

[問題2. 埠5062被阻止出站到Cisco Webex](#)

[問題3. Expressway搜尋規則配置錯誤](#)

[問題4. Expressway CPL配置錯誤](#)

[雙向：Cisco Webex到本地或本地到Cisco Webex](#)

[問題1. IP電話/合作終端提供G.711、G.722或AAC-LD以外的音訊編解碼器。](#)

[問題2. 超過Unified CM最大傳入消息大小](#)

[附錄](#)

[Expressway故障排除工具](#)

[檢查模式實用程式](#)

[查詢實用程式](#)

[診斷日誌記錄](#)

[相關資訊](#)

簡介

本文檔介紹思科Webex混合呼叫服務連線解決方案，該解決方案允許您的現有思科呼叫控制基礎設施連線到思科合作雲，以便它們能夠協同工作。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解Cisco Webex產品
- 瞭解Expressway解決方案(B2B)
- 瞭解Cisco Unified Communications Manager(Unified CM)及其與Expressway的整合
- Unified CM 10.5(2)SU5或更高版本。
- Expressway(B2B)版本X8.7.1或更高版本 (建議使用X8.9.1)
- Expressway (聯結器主機) — 有關當前支援的版本，請參閱[適用於Cisco Webex混合服務的Expressway聯結器主機支援](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科整合通訊管理員
- 高速公路
- Windows版Webex
- Webexfor Mac
- Webexfor iOS
- Android版Webex
- 思科協同合作端點
- 協同合作案頭終端
- IP電話
- 軟體使用者端

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

該解決方案提供以下功能：

- 將Webex應用用作音訊和影片呼叫的移動軟客戶端
- 使用該應用從任何地方發出和接收呼叫，就像他們在辦公室一樣
- 使用Webex、Cisco Jabber或其案頭電話進行呼叫，無需擔心使用哪個選項
- 解鎖本地電話中的呼叫歷史記錄，並將該歷史記錄整合到Webex中

本指南涵蓋混合呼叫服務連線獨有的問題。由於混合呼叫服務連線與其他解決方案 (如移動和遠端訪問以及企業到企業呼叫) 運行在同一個Expressway E & C對上，因此其他解決方案的問題可能會影響混合呼叫服務連線。對於部署Expressway對以與呼叫服務連線配合使用的客戶和合作夥伴，在嘗試部署混合呼叫服務連線之前，必須參考[Cisco VCS Expressway和VCS控制基本配置指南](#)。本故障排除指南在附錄3和4中介紹了防火牆/NAT注意事項以及Expressway設計。請詳細閱讀此文檔。此外，本文檔還假設Expressway聯結器主機和混合呼叫服務啟用已完成。

呼叫建立問題

相互TLS握手失敗

混合呼叫服務連線在Cisco Webex和Expressway-E之間使用相互傳輸層安全 (相互TLS) 進行身份驗證。這表示Expressway-E和Cisco Webex都會檢查並檢查彼此存在的證書。由於Expressway伺服器的新部署以及混合呼叫服務連線等解決方案的啟用期間普遍存在相互TLS問題，因此本節提供有用的資訊和提示，用於排除Expressway和Cisco Webex之間的證書問題。

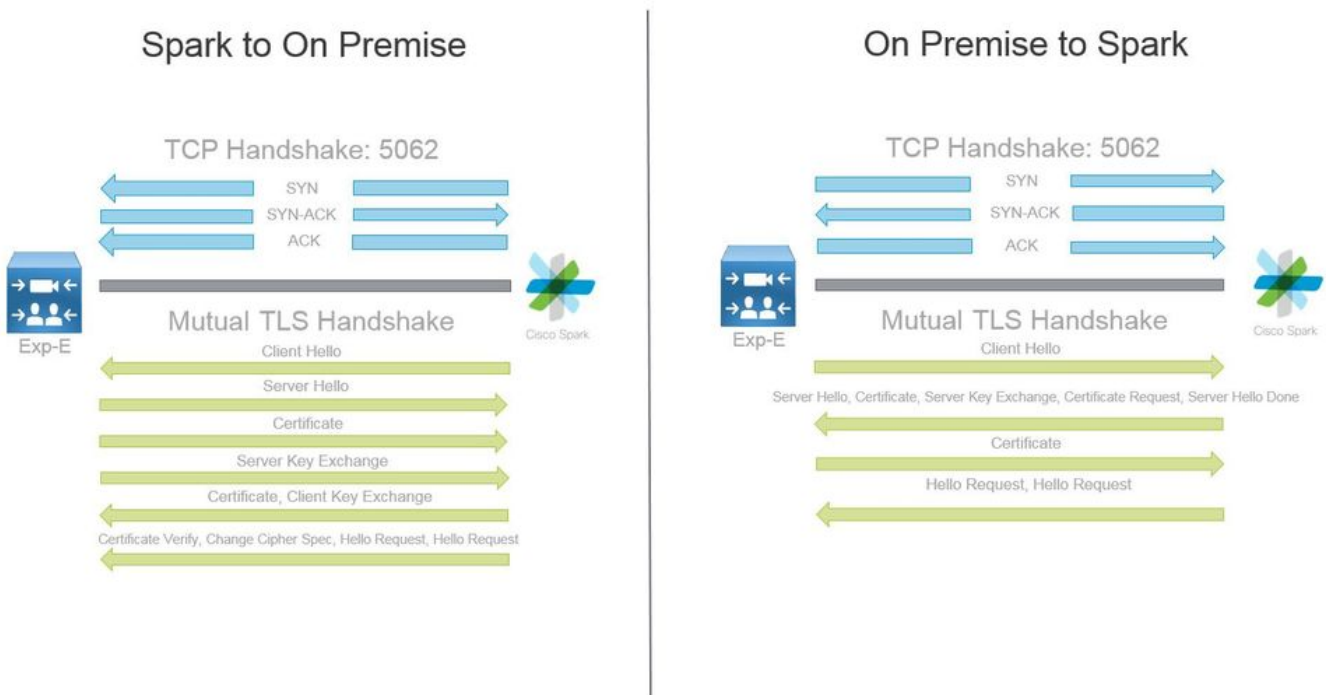
Expressway-E檢查什麼？

- Cisco Webex證書是否由Expressway-E Trusted CA清單中列出的公共CA簽署？
- callservice.ciscospark.com是否在Cisco Webex證書的Subject Alternate Name欄位中？

Cisco Webex會檢查什麼？

- Expressway-E證書是否由Webex信任的一個公共CA簽署？ ([Cisco Webex受信任CA清單](#))
- 如果Expressway-E不使用公開簽名的證書，Expressway證書是否與任何根證書和中間證書一起上傳到Cisco Webex控制中心(<https://admin.ciscospark.com>)？

如下圖所示，對此進行解釋。



有用的雙向TLS故障排除提示

1. 解碼雙向TLS握手

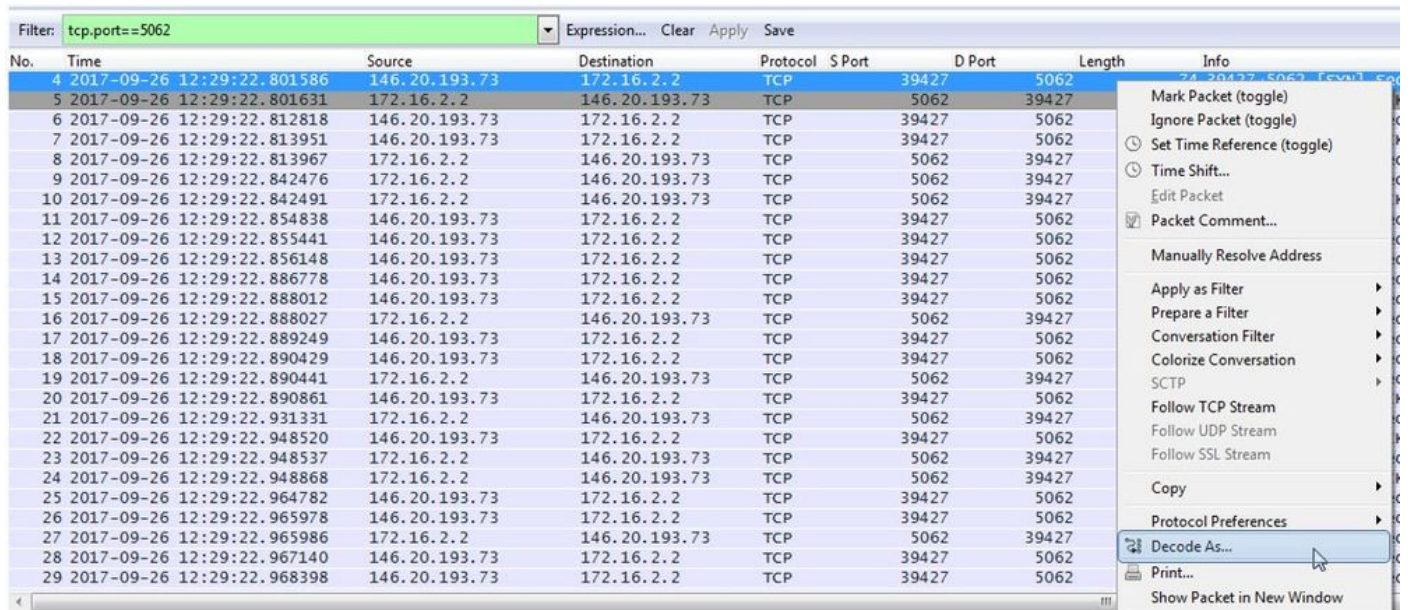
預設情況下，Wireshark將SIP TLS流量標籤為埠5061。這意味著，無論何時您想要分析在埠5062上發生的 (相互) TLS握手，Wireshark都不會知道如何正確解碼流量。以下是發生於連線埠5062上的相互TLS握手的範例，如下圖所示。

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

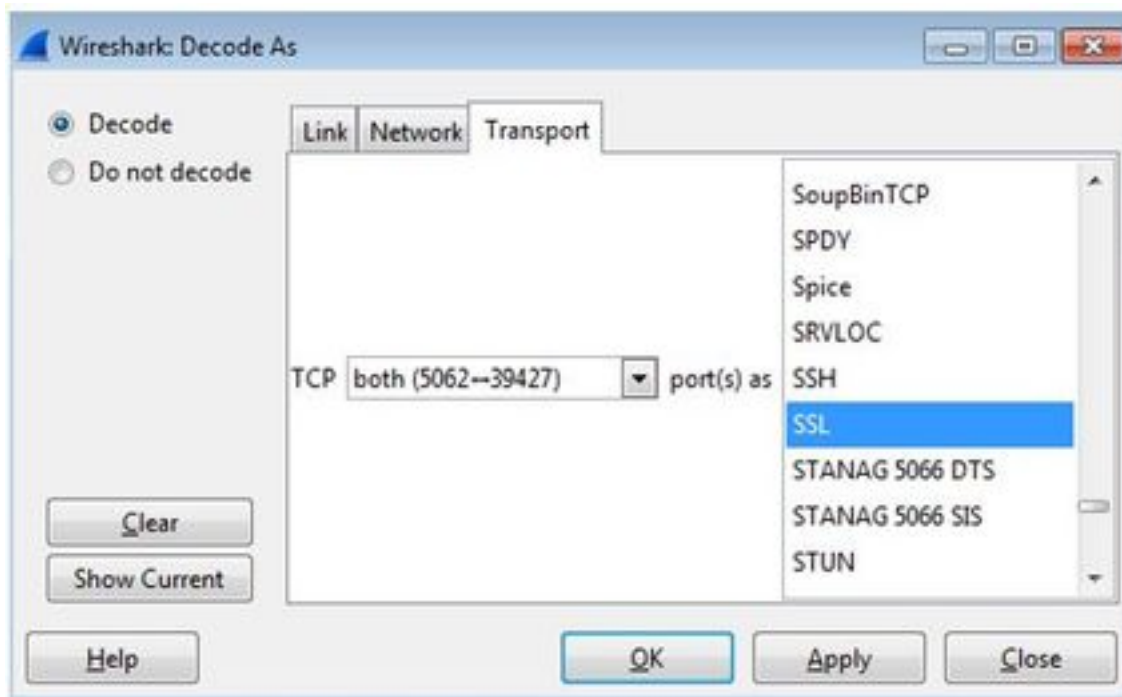
您可以看到，這就是握手在Wireshark中預設設定的顯示方式。資料包編號175是Expressway傳送到Cisco Webex的證書。但是，如果沒有對流量進行解碼，則無法確定這一點。可以使用兩種方法解碼此流量，以便您更容易看到證書資訊和出現的任何錯誤消息。

1a. 將流解碼為SSL

a. 分析相互TLS握手時，首先按tcp.port==5062過濾捕獲。然後，按一下右鍵流中的第一個資料包，然後選擇解碼為..... 如下圖所示。



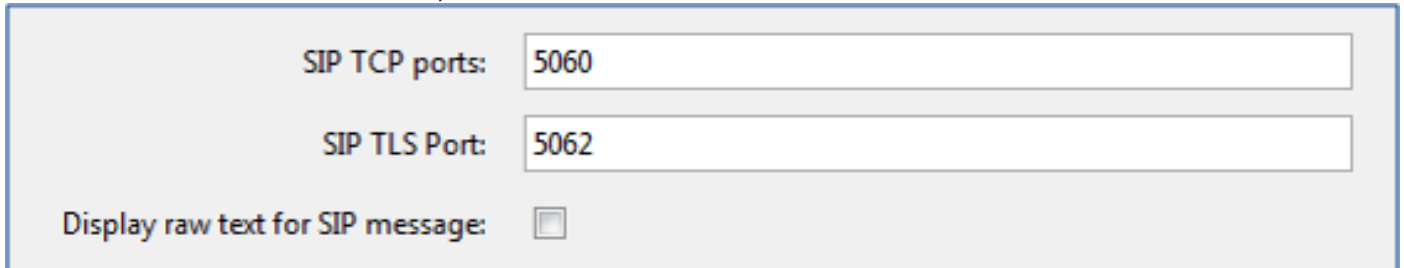
b. 選擇解碼為.....選項後，您會看到一個清單，您可以在其中選擇如何解碼您選擇的流。從清單中選擇SSL，然後按一下Apply並關閉視窗。此時，整個流顯示握手時交換的證書和錯誤消息，如下圖所示。



1b. 調整SIP TLS埠

當您在Wireshark首選項中將SIP TLS埠調整為5062時，您可以看到握手的所有詳細資訊，包括證書。若要進行此更改：

- 開啟Wireshark
- 導航到「編輯」>「首選項」
- 展開協定並選擇SIP
- 將SIP TLS埠設定為5062，然後按一下Apply
- 分析完成時將值設回5061，如下圖所示。



如果現在分析相同的捕獲，您會看到資料包169到175已解碼。封包175顯示Expressway-E憑證，如果對封包進行向下鑽取，可以參閱圖中所示的所有憑證詳細資訊。

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	TLSv1.2	48520	5062	266	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	TLSv1.2	5062	48520	2802	Server Hello
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	1426	Certificate

2. Wireshark過濾

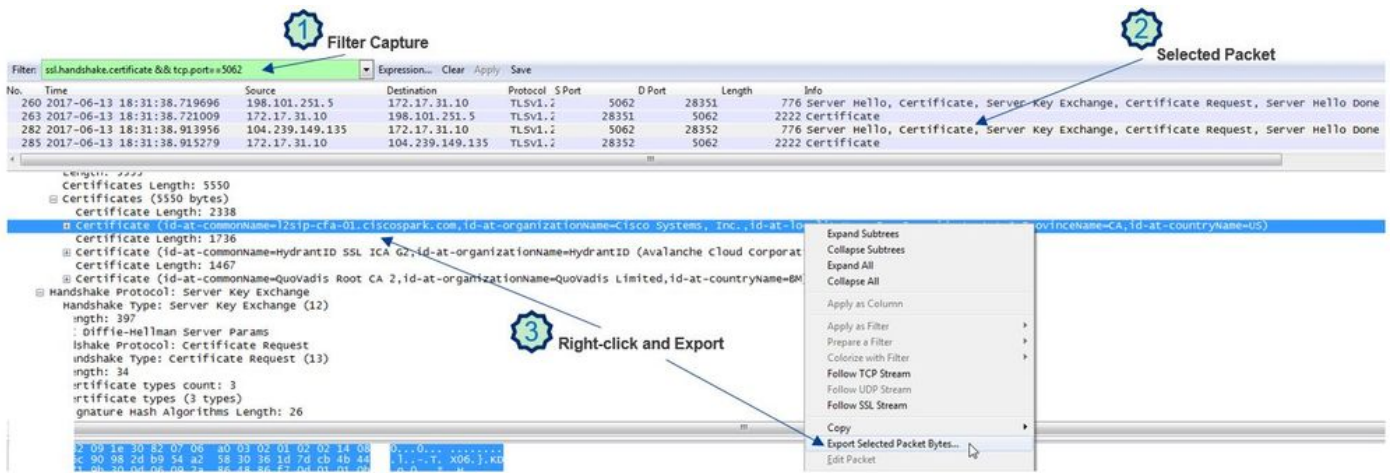
當您分析資料包捕獲時，在給定捕獲中觀察到的資料包數量之多很容易丟失。瞭解您最感興趣的流量型別是非常重要的，這樣您就可以過濾Wireshark來顯示該流量。以下是一些常用的Wireshark過濾器，可用於獲取關於雙方TLS握手的詳細資訊：

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

3. 從Pcap提取證書

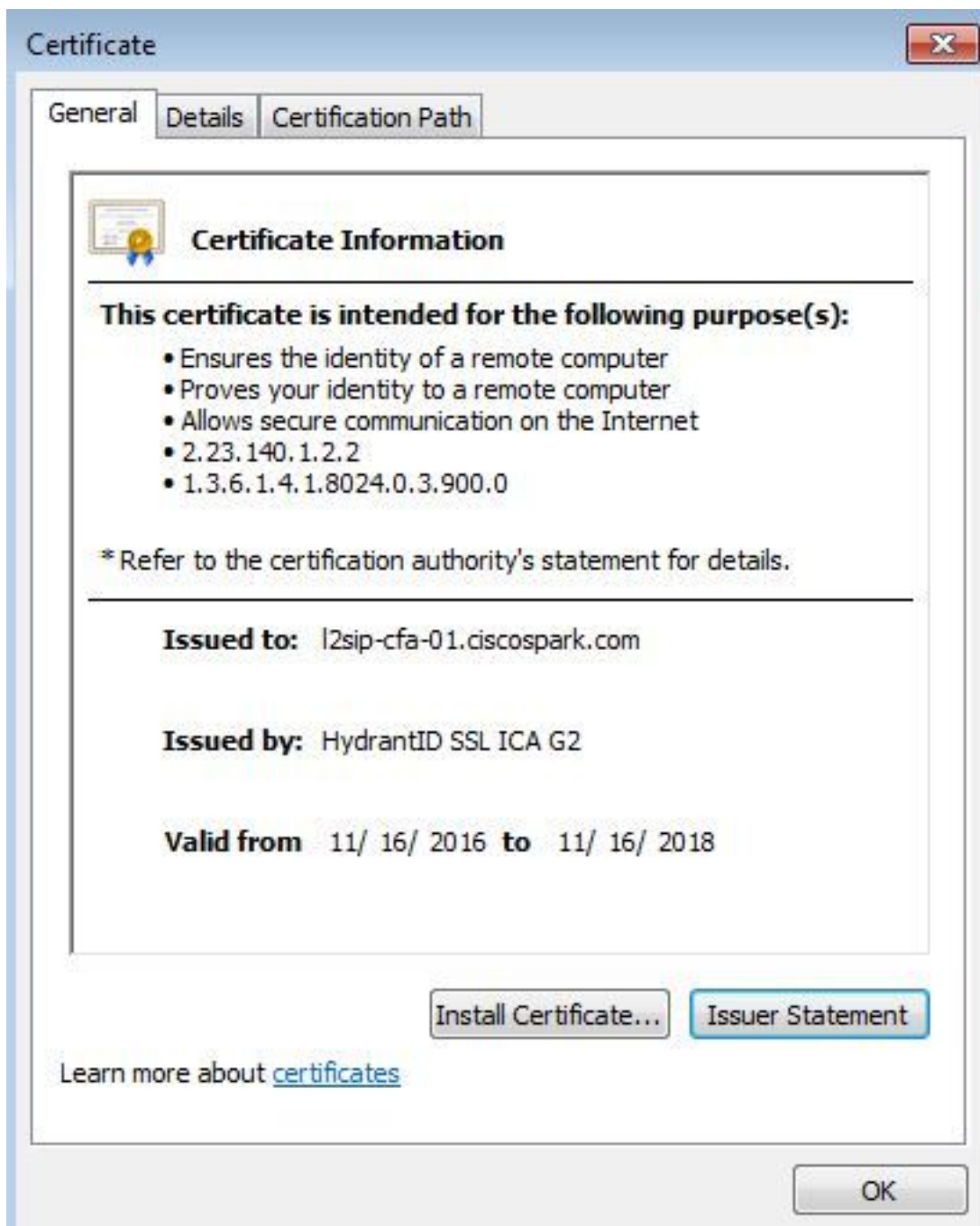
有時您可能需要獲取證書（伺服器、根或中介）的副本。如果您不知道要在哪裡找到您正在搜尋的證書，可以直接從資料包捕獲中提取該證書。以下是如何抽取在雙方TLS握手中提供的Cisco Webex證書的步驟。

1. 使用`ssl.handshake.certificate && tcp.port-5062`過濾==包擷取
2. 找到源自Webex伺服器地址並在「資訊」部分中列印了證書的資料包。
3. 在資料包詳細資訊中，展開安全套接字層> TLS證書>握手協定>證書。附註：鏈中的底部/最後一個憑證是根CA。
4. 按一下右鍵感興趣的證書，然後選擇Export Selected Packet Bytes...（匯出選定的資料包位元組.....），如下圖所示。



5.將檔案儲存為.cer。

6.按兩下儲存的檔案以開啟證書，如下圖所示。



4.調整Expressway日誌記錄級別

Expressway上有兩個日誌記錄模組，可幫助您更好地瞭解Expressway在分析證書時執行的邏輯：

- developer.ssl
- developer.zone.zonemg

預設情況下，這些日誌記錄模組設定為INFO級別。設定為DEBUG級別時，您可以開始看到有關所發生的證書檢查的資訊，以及對映到的區域流量。這兩個功能都與混合呼叫服務相關。

執行Cisco Webex伺服器證書的SAN檢查的Expressway-E示例。

```
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將MTLS連線對映到Cisco Webex混合DNS區域的示例：

```
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"
```

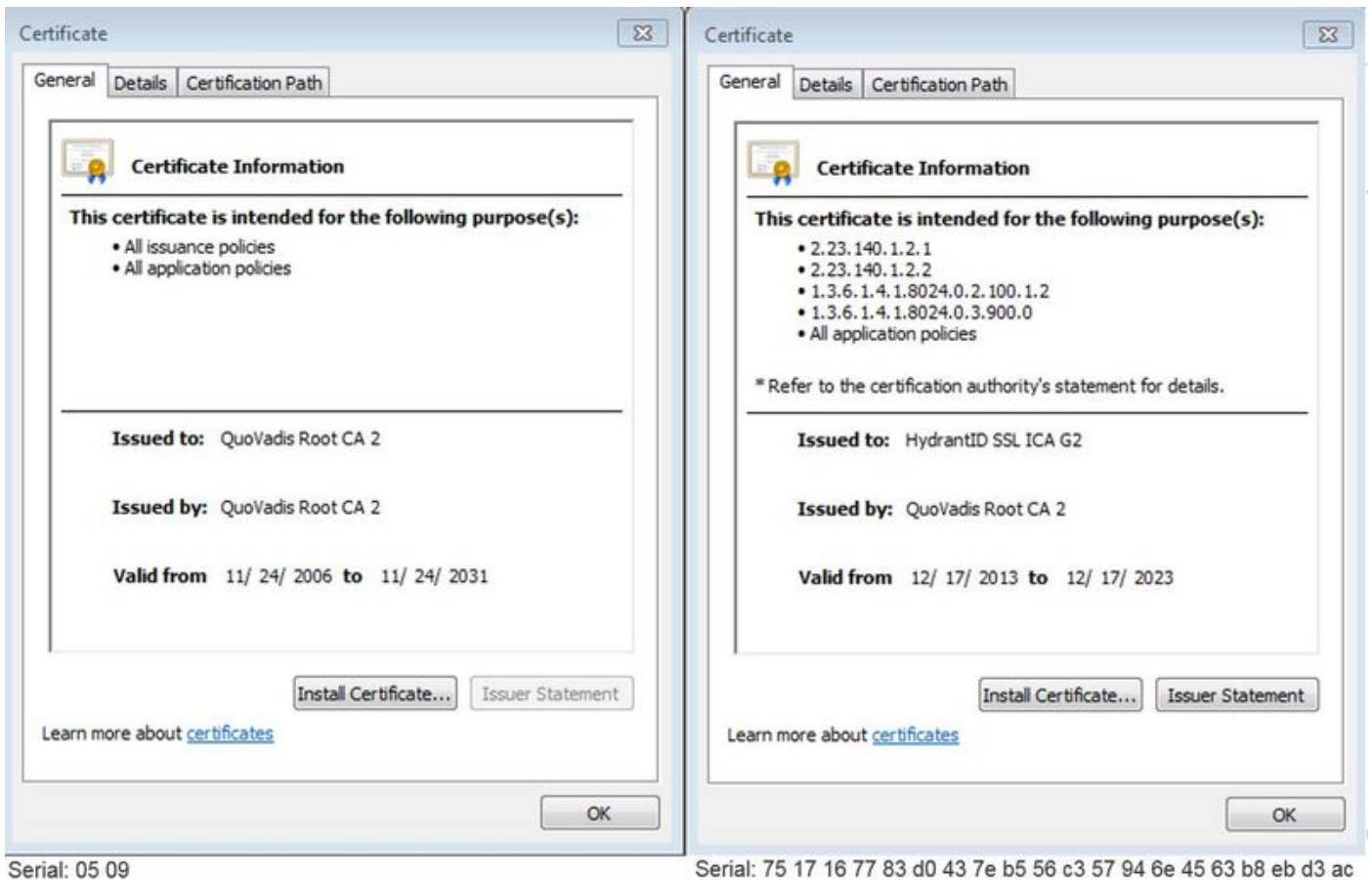
```
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1183)"
Method="ZoneManager::getDNSZoneByTLSVerifySubjectNameList" Thread="0x7f577f0a0700":
this="0x56408ff81220" Detail="Searched for DNS Zones by Subject Name" Found="True"
Candidates="l2sip-cfa-01.ciscospark.coml2sip-cfa-01.ciscospark.coml2sip-cfa-01.wbx2.coml2sip-
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" Identities="{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-l2siproda1-
294-riad-public.wbx2.com, Alt-DNS: l2sip-l2siproda1-817-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"
```

以下列出與Expressway-E和Cisco Webex之間的相互TLS故障相關的最常見問題。

問題1. Expressway-E不信任簽署Cisco Webex證書的證書頒發機構(CA)

與Expressway-E直接通訊的Cisco Webex伺服器稱為L2SIP伺服器。此L2SIP伺服器將由中間伺服器簽署，中間伺服器的公用名稱為Hydant SSL ICA G2。中間伺服器由具有公用名稱QuoVadis Root CA 2的根證書頒發機構簽署，如下圖所示。

附註：這種情況可能會改變。



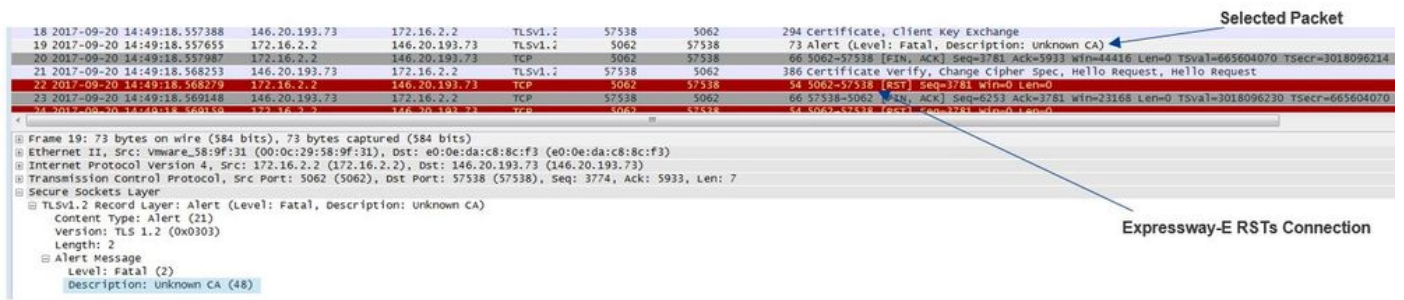
從Expressway診斷角度分析此流量的第一步是搜尋TCP連線。搜尋TCP Connecting後，將會尋找Dst-port=5062值。一旦識別日誌中嘗試並建立此連線的區域，就可以查詢TLS握手，該握手通常由指示正在進行握手的日誌條目表示。

```
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"
```

如果Expressway-E不信任Cisco Webex簽名的證書，您可以預期Expressway-E可以在握手完成後立即拒絕證書。Expressway-E日誌記錄中可通過以下日誌條目發現此問題：

```
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"
```

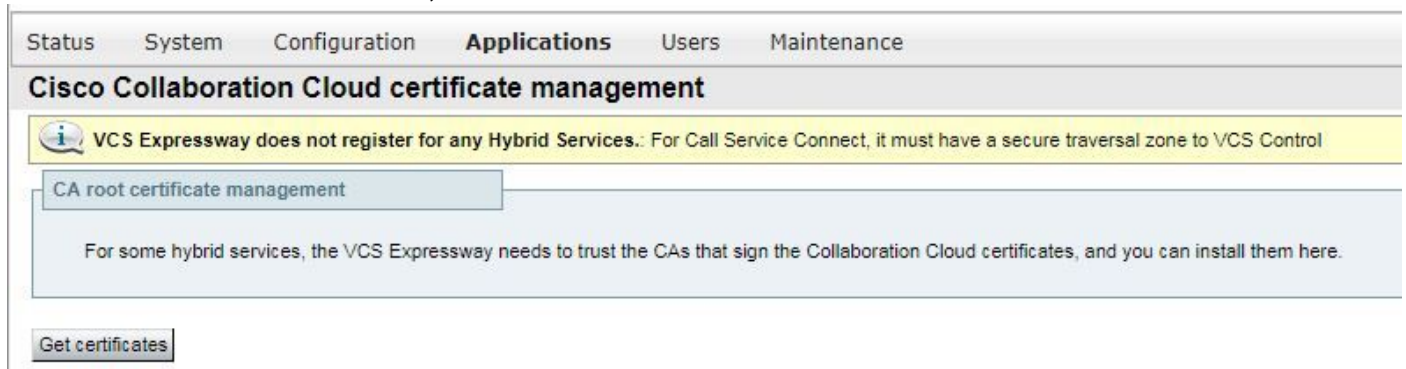
Expressway錯誤消息可能略有誤導，因為它引用了證書鏈中的自簽名證書。Wireshark允許您進一步瞭解交換。從Wireshark資料包捕獲分析的角度來看，您可以清楚地看到，當Webex環境顯示其證書時，Expressway會轉過身，並拒絕具有未知CA錯誤的證書，如下圖所示。



解決方案：

為了解決這種情況，您必須確保Expressway E信任Cisco Webex證書頒發機構。雖然您可以簡單地從Wireshark跟蹤提取這些證書並將其上傳到Expressway上的受信任CA證書儲存區，但Expressway提供了一種更簡單的方法：

- 登入Expressway-E
- 導覽至Applications > Cloud Certificate management
- 選擇Get Certificates選項，如下圖所示。



此時，Cisco Webex證書頒發機構上傳到Expressway-E受信任CA儲存(維護>安全>受信任CA證書)。

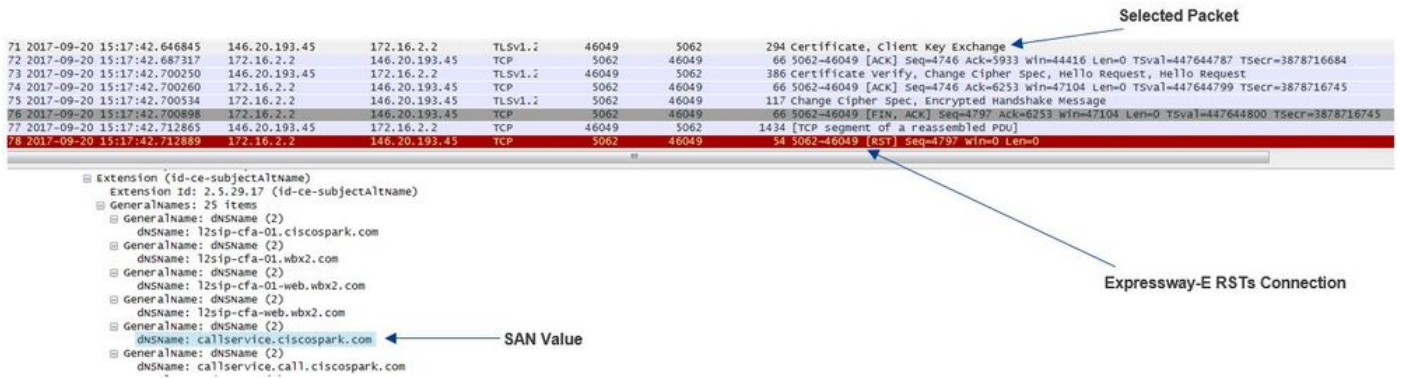
問題2. Expressway-E Cisco Webex混合DNS區域上的TLS主體驗證名稱不正確

作為雙向TLS握手的一部分，混合呼叫服務連線使用TLS驗證。這意味著除了信任Cisco Webex CA證書外，Expressway還會通過檢查所顯示的證書的Subject Alternate Name(SAN)欄位來驗證證書，以確保證書具有callservice.ciscospark.com等值。如果此值不存在，入站呼叫將失敗。

在此特定案例中，Cisco Webex伺服器會將其憑證提供給Expressway-E。證書實際上有25個不同的SAN。請考慮以下情況：Expressway E檢查callservice.ciscospark.com SAN的證書，但找不到該證書。當滿足此條件時，您會在診斷日誌記錄中看到類似以下的錯誤：

```
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"
```

如果您使用Wireshark分析此證書握手，您會發現Cisco Webex出示其證書後，Expressway RST會在不久之後建立連線，如下圖所示。



若要確認此值的設定，您可以前往針對解決方案設定的Webex混合DNS區域。如果具有Expressway-E xConfiguration，則可以查詢「區域配置」部分以確定如何配置TLS驗證主題名稱。對於xConfiguration，請注意，區域是排序的，第一個區域是區域1。以下是來自上述問題環境的xConfiguration。

```
*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"
```

如示例所示，TLS驗證主題名稱設定為callservice.ciscospark.com，而不是callservice.ciscospark.com。（注意額外的「l」）。

解決方案：

為了解決此問題，必須修改TLS驗證使用者名稱：

- 登入Expressway-E
- 導航到Configuration > Zones > Zones
- 選擇Webex Hybrid Services DNS Zone
- 將TLS驗證主題名稱設定為callservice.ciscospark.com
- 選擇儲存

附註：有關基線日誌記錄行為，請參閱。本節顯示Expressway執行憑證驗證以及到Webex混合DNS區域的對應。

附註：Expressway代碼x12.5及更高版本發佈了一個新的「Webex」區域。此Webex區域預填充與Webex進行通訊所需的區域配置。這意味著您不再需要設定「TLS驗證主題模式」和「TLS驗證主題名稱」。為簡化配置，如果您運行Expressway代碼的x12.5或更高版本，建議使用Webex區域。

問題3. Expressway-E不向Cisco Webex傳送完整證書鏈

作為雙向TLS握手的一部分，Cisco Webex必須信任Expressway-E證書。Cisco Webex具有其信任的公共CA的完整清單。通常，當您的Expressway-E證書由Cisco Webex支援的公共CA簽名時，TLS握手會成功。根據設計，Expressway-E在TLS握手期間僅傳送其證書，儘管其證書是由公共CA簽名的。為了傳送完整的憑證鏈結（根憑證和中間憑證），必須在Expressway-E上將這些憑證新增到受信任CA憑證庫中。

如果未滿足此條件，Cisco Webex將拒絕Expressway E證書。對符合此問題的條件進行故障排除時，可以使用Expressway-E中的診斷日誌和tcpdump。分析Expressway-E診斷日誌時，您會看到與以下內容類似的錯誤：


```

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="::TTSSLErrorOutput" 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"

```

如果從Wireshark的角度分析此問題，您會看到Expressway-E出示其證書。如果展開封包，可以看到只傳送伺服器憑證。然後，Cisco Webex會拒絕此TLS握手，並顯示「未知CA」錯誤訊息，如下圖所示。

The image shows a Wireshark capture of a TLS handshake. The top pane lists several packets, with packet 47 selected. The bottom pane shows the details of packet 47, which is a TLS alert with the description "Certificate Unknown". A blue box highlights the certificate field in the handshake details, which is empty, and a label points to it with the text "Expressway-E Server Certificate".

解決方案：

為了解決此案例中的問題，您必須將簽署Expressway-E證書所涉及的中間和根CA上傳到受信任CA證書庫：

- 步驟1. 登入Expressway-E。
- 步驟2. 導覽至Maintenance > Security > Trusted CA certificate。
- 步驟3. 選擇UI底部附近Upload選單下的Choose File。
- 步驟4. 選擇簽署Expressway-E時涉及的CA證書。
- 步驟5. 選擇附加CA憑證。
- 步驟6. 對簽署Expressway-E證書時涉及的所有CA證書（中間、根）重複步驟。
- 步驟7. 選擇附加CA憑證。

完成此過程後，您會看到在金鑰交換中包含Expressway E伺服器證書簽名所涉及的完整證書鏈。以下是使用Wireshark分析封包擷取時將會看到的內容範例。

Selected Packet

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 14:22:13.354815 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 14:22:13.668644 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=444315455

199 2017-09-20 14:22:13.668871 172.16.2.2 146.20.193.45 TCP 5062 48520 66 5062-48520 [FIN, ACK] Seq=746 Ack=209 win=30080 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 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

- Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3933
 - 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=https://certs.godaddy.com/repositor, id-at-organizationName=GoDaddy.com, Inc., id-at-localityName=)
 - 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.防火牆終止雙向TLS握手

Expressway解決方案通常與防火牆連線。很多情況下，該解決方案的內聯防火牆運行某種型別的應用層檢測。通常，使用Expressway解決方案時，當防火牆運行應用層檢測時，管理員會看到不理想的結果。此特定問題可幫助您確定防火牆的應用層檢測何時突然中斷連線。

使用Expressway中的診斷日誌，您可以查詢嘗試的相互TLS握手。如前所述，此握手應該在埠5062上建立TCP連線後不久進行。在這種情況下，當防火牆斷開連線時，您會在診斷日誌記錄中看到這些錯誤。

```
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.ciscopark.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"
```

從資料包捕獲的角度來看，您會看到Expressway-E向Cisco Webex出示了證書。您可以看到來自Cisco Webex方向的TCP RST，如下圖所示。

Selected Packet

263 2017-06-13 18:31:38.721009 172.17.31.10 198.101.251.5 TLSv1.2 28351 5062 2222 certificate

264 2017-06-13 18:31:38.757545 198.101.251.5 172.17.31.10 TCP 5062 28351 66 5062-28351 [ACK] Seq=6087 Ack=5279 win=40448 Len=0 TSval=3255749920 TSecr=3980564402

265 2017-06-13 18:31:38.757559 172.17.31.10 198.101.251.5 TLSv1.2 28351 5062 785 Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message

266 2017-06-13 18:31:38.765000 198.101.251.5 172.17.31.10 TCP 5062 28351 60 5062-28351 [RST] Seq=6087 Win=0 Len=0 TSval=3255749920 TSecr=3980564402

267 2017-06-13 18:31:38.769029 172.17.31.10 198.101.251.5 TCP 28351 5062 74 28351-5062 [ACK] Seq=6087 Ack=2200 Len=0 Win=14608 Src_Ports=28351 TSval=3980564447 TSecr=0 Win=0

268 2017-06-13 18:31:38.769411 198.101.251.5 172.17.31.10 TCP 5062 28351 74 5062-28351 [ACK] Seq=6087 Ack=2200 Len=0 Win=14608 Src_Ports=5062 TSval=3980564447 TSecr=0 Win=0

Frame 261: 2222 bytes on wire (17776 bits), 2222 bytes captured (17776 bits) on Ethernet II, Src: Vmware_80:34:64 (00:50:56:80:34:64), Dst: PaloAlto_00:01:30 (00:1b:17:00:01:30)

Internet Protocol Version 4, Src: 172.17.31.10 (172.17.31.10), Dst: 198.101.251.5 (198.101.251.5)

Transmission Control Protocol, Src Port: 28351 (28351), Dst Port: 5062 (5062), Seq: 3123, Ack: 6087, Len: 2156

[2 Reassembled TCP Segments (5052 bytes): #262(2896), #263(2156)]

Secure Sockets Layer

- Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 5047
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 5043
 - Certificates Length: 5040
 - Certificates (5040 bytes)
 - Certificate Length: 1611
 - Certificate (id-at-commonName=vcse, id-at-organizationalUnitName=Domain Control validated)
 - Certificate Length: 1236
 - Certificate (id-at-commonName=Go Daddy Secure Certificate Authority - G2, id-at-organizationalUnitName=https://certs.godaddy.com/repositor, id-at-organizationName=GoDaddy.com, Inc., id-at-localityName=)
 - Certificate Length: 1153
 - 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)
 - Certificate Length: 1028
 - Certificate (id-at-organizationalUnitName=Go Daddy Class 2 Certification Aut, id-at-organizationName=The Go Daddy Group, Inc., id-at-countryName=US)

乍一看，您可能認為Expressway-E證書存在問題。若要解決此問題，您必須首先確定這些問題的答案：

- Expressway-E是否由Cisco Webex信任的公共CA簽署？
- Expressway-E證書和簽署Expressway-E證書涉及的任何證書是否手動上傳到Cisco Webex控制

中心(<https://admin.ciscospark.com>)?

在此特定情況下，解決方案不是使用Cisco Webex控制中心來管理Expressway-E證書。這意味著Expressway-E證書必須由Cisco Webex信任的公共CA簽署。通過在Wireshark捕獲中選擇證書資料包(如上所示)，您可以看到證書是由公共CA簽名且完整鏈已傳送到Cisco Webex。因此，此問題不應與Expressway E證書相關。

此時，如果需要進一步隔離，您可以從防火牆的外部介面捕獲資料包。但是，診斷日誌中缺少SSL錯誤是一個重要的資料點。如果您回憶上文(問題3.)，如果Cisco Webex不信任Expressway-E證書，您必須看到某種型別的SSL斷開原因。在這種情況下，沒有可用的SSL錯誤。

附註：如果您要從防火牆外部介面獲取資料包捕獲，您將不會看到來自Cisco Webex環境的TCP RST。

解決方案

對於此特定解決方案，您作為合作夥伴或客戶必須依靠您的安全團隊。該團隊必須調查他們是否對Expressway解決方案使用了任何型別的應用層檢查，如果使用了此類檢查，則應禁用該檢查。《[VCS控制和Expressway部署指南](#)》的附錄4說明建議客戶關閉此功能的原因。

問題5. Expressway-E由公共CA簽署，但Cisco Webex控制中心載入了備用證書

當您從頭開始部署Expressway解決方案，並且最初沒有公共CA簽名的Expressway-E證書時，經常會發生此特殊情況。在此場景中，您將Expressway-E伺服器證書(已在內部簽名)上傳到Cisco Webex控制中心，以便成功完成雙方TLS協商。之後，您最終會獲得由公共CA簽名的Expressway-E證書，但是您忘記從Cisco Webex控制中心移除伺服器證書。必須瞭解的是，如果將證書上傳到Cisco Webex控制中心，該證書將優先於Expressway在TLS握手期間顯示的證書和鏈。

從Expressway-E診斷日誌記錄角度來看，此問題可能類似於在Cisco Webex不信任Expressway-E證書時遇到的日誌記錄簽名，例如Expressway-E未傳送其完整鏈或Expressway-E證書未由Cisco Webex信任的公共CA簽名的情況。以下是您在TLS握手期間在Expressway-E日誌記錄中可期待的內容的示例：

```
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"
```

請從Wireshark的角度進行檢視，您可以在這裡看到Expressway E在第175行中顯示其證書。幾行之後，Cisco Webex環境將拒絕該證書，並顯示證書未知錯誤，如下圖所示。

如果您選擇Expressway-E傳送的證書資料包，則可以展開證書資訊以確定Expressway-E

- 1.由Cisco Webex信任的公共CA簽署，且
- 2.把整個鍊子加在簽名中

在這種情況下，滿足這兩個條件。這表明Expressway-E證書沒有錯誤。

解決方案

步驟1.登入Cisco Webex Control Hub。

步驟2.從左窗格中選擇Services。

步驟3.在混合呼叫卡下選擇Settings。

步驟4.滾動到Call Service Connect部分，檢視Certificates for Encrypted SIP Calls下方，檢視是否列出了不需要的證書。如果是，請按一下證書旁邊的垃圾桶圖示。

步驟5.選擇Remove。

附註：執行分析非常重要，確定客戶在刪除之前不使用上傳到Webex控制中心的證書。

有關在Cisco Webex控制中心中上傳Expressway-E證書的詳細資訊，請檢視混合呼叫部署指南的此部分。

問題6. Expressway未將入站呼叫對映到Cisco Webex混合DNS區域

入站TLS對映功能與TLS驗證主題名稱配合使用，兩者均在混合呼叫DNS區域上配置。此場景說明了x12.5之前的Expressway所觀察到的問題和挑戰。在x12及更高版本中，實施了一種稱為「Webex」區域的新區域型別。該區域預填充與Webex整合所需的所有配置。如果您正在運行x12.5並部署Webex混合呼叫，建議使用Webex Zone型別，以便自動配置混合呼叫服務域(callservice.webex.com)。此值與雙向TLS握手期間提供的Webex證書的「主體替代名稱」相匹配，並允許成功連線到Expressway和入站對映。

如果您使用的是x12.5以下的任何代碼版本，或者沒有使用Webex區域，則您需要繼續下面的說明，演示如何識別和糾正Expressway未將入站呼叫對映到Webex混合DNS區域的問題。

該功能分為三個步驟：

1. Expressway-E接受Cisco Webex證書。
2. Expressway-E檢查Cisco Webex證書以確定是否存在與TLS驗證使用者名稱匹配的使用者替代名稱：callservice.ciscopark.com。
3. Expressway-E通過Cisco Webex混合DNS區域對映入站連線。

如果驗證不成功，則表示憑證驗證失敗。如果在Expressway-E上配置了Business-to-business，則呼叫進入預設區域，並根據為Business-to-Business方案提供的搜尋規則進行路由。

與其他情況一樣，您必須同時使用診斷日誌記錄和資料包捕獲來確定此故障的樣子，然後使用資料包捕獲來檢視哪一端正在傳送RST。以下是正在嘗試TCP連線，然後建立的示例。

```
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 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"
```

現在，TCP連線已建立，TLS握手就可以繼續。握手開始後不久，您會看到它很快錯誤地脫離。

```
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"
```

從pcap的角度看這種情況，您可以更好地瞭解

- 誰正在傳送RST，以及
- 傳送哪些證書來確定它們是否正確。

當您分析此特定捕獲時，可以看到Expressway-E傳送了RST。當您檢視通過的Cisco Webex憑證時，可以看到其傳送完整鏈結。此外，您可以斷定，根據診斷日誌中的錯誤消息，您可以排除Expressway-E不信任Cisco Webex公共CA的情況。否則，您會看到類似「憑證鏈結中的自簽署憑證」的錯誤。您可以挖掘封包詳細資訊，如圖所示。

按一下Webex伺服器憑證並將其展開以檢視使用者替代名稱(dnsName) , 可以驗證以確保已列出 **callservice.ciscopark.com**。

導航至Wireshark:Certificate > Extension > General Names > GeneralName > **dnsName:callservice.ciscopark.com**

這完全證實Webex憑證看起來正常。

您現在可以確認TLS驗證使用者名稱是正確的。如上所述，如果您有xConfiguration，則可以查詢「區域配置」部分以確定如何配置TLS驗證主題名稱。關於xConfiguration，需要注意的一點是，首先建立的是與區域1一起訂購的區域。以下是來自上述問題環境的xConfiguration。很顯然，TLS驗證使用者名稱沒有錯誤。

```
*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"
```

接下來必須研究的是TLS驗證入站對映。這將確認是否將TLS連線正確對映到Webex混合DNS區域。也可利用xConfiguration對此進行分析。在xConfiguration中，TLS驗證入站對映稱為DNS ZIP TLS驗證入站分類。如本示例所示，值設定為Off。

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "Off"
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
```

如果此值設定為「關閉」，這意味著阻止VCS嘗試將入站TLS連線對映到此區域。因此，呼叫將進入預設區域，並且如果在Expressway E上配置了「企業到企業」，則將根據為「企業到企業」方案提供的搜尋規則進行檢查和路由。

解決方案

為了解決此問題，您需要將混合呼叫DNS區域上的TLS驗證入站對映設定為「開」。以下是完成此操作的步驟。

1. 登入Expressway-E
2. 導航到Configuration > Zones > Zones
3. 選擇混合呼叫DNS區域
4. 對於TLS驗證入站對映，請選擇On
5. 選擇儲存

附註：有關基線日誌記錄行為，請參閱。本節顯示Expressway執行憑證驗證以及到Webex混合DNS區域的對應。

問題7. Expressway-E使用預設自簽名證書

在一些新的混合呼叫服務連線部署中，Expressway-E證書的簽名被忽略，或者認為可以使用預設伺服器證書。有些人認為，這是可能的，因為Cisco Webex控制中心允許您將自定義證書載入到門戶中。(Services > Settings(在Hybrid Call Card下)> Upload(在Certificates for Encrypted Calls下))

如果您密切注意加密SIP呼叫的證書的措辭，您將看到：'使用思科合作預設信任清單提供的證書或上傳您自己的證書。如果使用自己的名稱，請確保主機名位於已驗證的域中。'該語句的關鍵部分是「確保主機名位於已驗證的域中。」

對符合此情況的問題進行故障排除時，請記住，症狀取決於呼叫方向。如果呼叫是由本地電話發起的，則您預計思科Webex應用不會振鈴。此外，如果您嘗試從Expressway搜尋歷史記錄中跟蹤呼叫，您會發現該呼叫將到達Expressway-E並在此停止。如果呼叫來自Cisco Webex應用並且目的地為本地，則本地電話不會響起。在這種情況下，Expressway-E和Expressway-C搜尋歷史記錄不會顯示任何內容。

在此特定情況下，呼叫源自本地電話。使用Expressway-E搜尋歷史記錄，可以確定呼叫是否到達伺服器。此時，您可以深入瞭解診斷日誌記錄以確定發生了什麼情況。要開始此分析，首先檢視是否嘗試並通過埠5062建立TCP連線。通過在Expressway-E診斷日誌中搜尋「TCP連線」，並搜尋帶有「Dst-port=5062」標籤的行項，可以確定連線是否建立。

```
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"
```

現在您已確認TCP連線已建立，就可以分析緊接著發生的相互TLS握手。正如您在這裡的代碼片斷中所看到的，握手失敗且證書未知(Detail="sslv3 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="sslv3 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:sslv3 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"
```


保Additional alternative names欄位包含Webex Control Hub中列出的Verified Domain按一下「Generate CSR」將CSR提供給第三方公共CA進行簽名返回證書後，導航到維護>安全>伺服器證書在Select the server certificate file旁邊的Upload New Certificate部分，選擇Choose File，然後選擇已簽名的證書選擇上傳伺服器證書資料導覽至Maintenance > Security > Trusted CA certificate在選擇包含受信任CA證書的檔案旁邊的上傳部分，選擇選擇檔案。選擇公共CA提供的任何根和中間CA證書。選擇Append CA certificate。重新啟動Expressway-E。

2a. 將內部CA和Expressway-E證書上傳到Cisco Webex控制中心

1. 以管理員身份登入Cisco Webex控制中心。
2. 選擇服務。
3. 選擇混合呼叫服務卡下的設定。
4. 在Certificates for Encrypted SIP Calls部分中選擇Upload。
5. 選擇內部CA和Expressway-E證書。

入站：思科Webex到本地

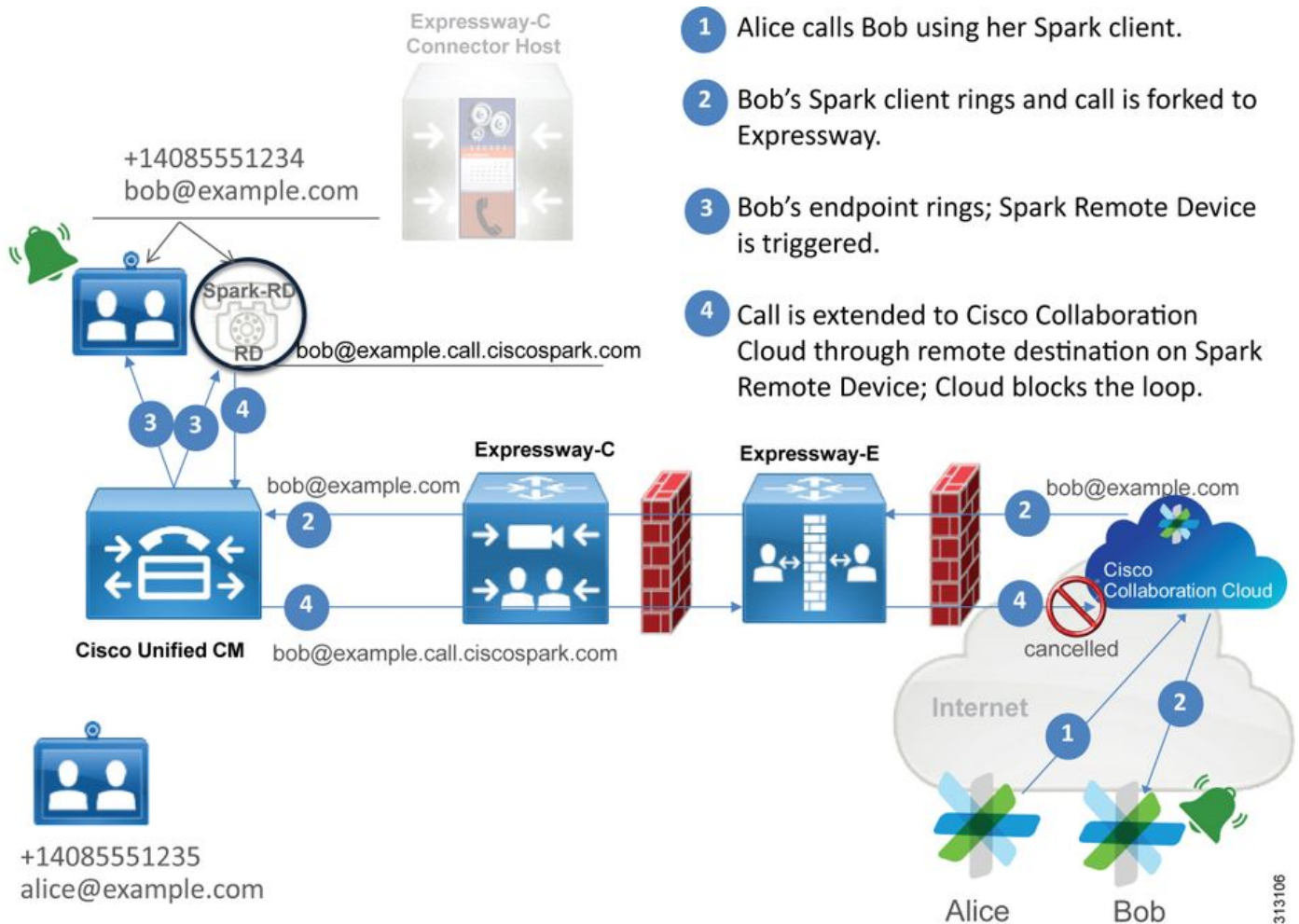
幾乎每個入站思科Webex到本地的故障都會導致相同的故障症狀：「當我從我的Cisco Webex應用呼叫另一位同事的應用時，同事的應用響起，但本地電話卻不響。」為了排除此故障，您會發現瞭解進行此類呼叫時出現的呼叫流程和邏輯都很有幫助。

高級邏輯流

1. Cisco Webex應用呼叫方發起呼叫
2. 被叫方的應用振鈴
3. 呼叫被分流到Cisco Webex環境
4. Cisco Webex環境必須根據客戶在Cisco Webex控制中心中配置的SIP目標執行DNS查詢
5. Cisco Webex環境嘗試通過埠5062連線到Expressway
6. Cisco Webex環境嘗試執行雙向TLS握手
7. Cisco Webex環境向Expressway傳送SIP INVITE，該SIP INVITE向下傳遞到本地合作終端/IP電話
8. Cisco Webex與企業完成SIP協商
9. Cisco Webex和企業開始傳送和接收媒體。

呼叫流

導覽至Cisco Webex app > Cisco Webex environment > Expressway-E > Expressway-C > On-Premises Collaboration Endpoint/IP Phone，如下圖所示。



- 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.

以下是從Webex到本地基礎設施的入站呼叫觀察到的一些常見問題。

問題1. Cisco Webex無法解析Expressway-E DNS SRV/主機名

在考慮思科Webex到本地呼叫流程時，思科Webex的第一個邏輯步驟是如何聯絡本地Expressway。如上所述，Cisco Webex將嘗試根據在[Cisco Webex控制中心](#)的混合呼叫服務設定頁中列出的已配置SIP目標執行SRV查詢，以連線到本地Expressway。

如果您嘗試從Expressway-E診斷日誌角度對此情況進行故障排除，則不會看到來自Cisco Webex的任何流量。如果您嘗試搜尋TCP連線，您將看不到Dst-port=5062，也不會看到來自Cisco Webex的任何後續的MTLS握手或SIP Invite。

如果發生這種情況，您必須檢查SIP目的地在Cisco Webex控制中心中的配置方式。您還可以使用混合連線測試工具來幫助進行故障排除。混合連線測試工具會檢查是否存在有效的DNS地址、Cisco Webex是否可以連線到SRV查詢中返回的埠，以及本地Expressway是否具有Cisco Webex信任的有效證書。

1. 登入[Cisco Webex Control Hub](#)
2. 選擇服務
3. 選擇Hybrid Call card中的SettingsLink。
4. 在「呼叫服務連線」部分中，驗證SIP Destinationfield中用於公共SIP SRV地址的域。
5. 如果輸入的記錄正確，請按一下測試以檢視記錄是否有效。
6. 如下圖所示，您可以清楚地看到公共域沒有與其關聯的相應SIP SRV記錄，如下圖所示。

SIP Destination ⓘ

mtls.rtp.ciscotac.net

Test

Save

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

選擇**View test results**，您可以檢視更多有關失敗原因的詳情，如下圖所示。

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.

作為另一種方法，您還可以使用nslookup查詢SRV記錄。以下是您可以運行以驗證SIP目標是否存在的命令。

```
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
```

如上面的代碼塊所示，nslookup命令被啟動，然後伺服器被設定為8.8.8.8，這是公共Google DNS伺服器。最後，您將設定記錄型別以查詢SRV記錄。此時，您可以發佈要查詢的完整SRV記錄。最終結果是請求最終超時。

解決方案

1. 在用於承載公共域名的站點上為Expressway-E配置公共SIP SRV地址。
2. 配置將解析為Expressway-E的公共IP地址的主機名
3. 配置SIP目標以列出用於步驟1中建立的SIP SRV地址的域。登入[Cisco Webex Control Hub](#)選擇服務選擇混合呼叫卡中的**Settings**連結在Call Service Connect部分，在**SIP Destination**欄位中輸入用於公共SIP SRV地址的域。選擇儲存

附註：如果您想要使用的SIP SRV記錄已被用於企業到企業通訊，我們建議在Cisco Webex Control Hub中指定企業域的子域作為SIP發現地址，然後指定公共DNS SRV記錄，如下所示：

```
服務和協定：_sips._tcp.mtls.example.com
優先順序機制:1
重量:10
埠號：5062
```


目標：us-expe1.example.com

上述建議直接摘自[Cisco Webex混合設計手冊](#)。

替代解決方案

如果客戶沒有SIP SRV記錄（並且不計畫建立記錄），則他們可以列出字尾「:5062」的Expressway公共IP地址。通過執行此操作，Webex環境不會嘗試SRV查詢，而是直接連線到%Expressway_Pub_IP%:5062。（示例：64.102.241.236:5062）

1. 將SIP目標配置為格式化為%Expressway_Pub_IP%:5062。（示例：64.102.241.236:5062）
登入[Cisco Webex Control Hub](#)選擇服務選擇混合呼叫卡中的Settings連結在「呼叫服務連線」部分的「SIP Destination」欄位中輸入%Expressway_Pub_IP%:5062。選擇儲存

有關必須設定的SIP目標地址和/或SRV記錄的詳細資訊。請參閱《Cisco Webex混合呼叫服務部署指南》或《[Cisco Webex混合設計手冊](#)》的[為您的組織啟用混合呼叫服務連線](#)部分。

問題2.套接字故障：埠5062被阻止入站到Expressway

DNS解析完成後，Cisco Webex環境嘗試通過埠5062建立到DNS查詢過程中返回的IP地址的TCP連線。此IP地址將成為本地Expressway-E的公共IP地址。如果Cisco Webex環境無法建立此TCP連線，則隨後對內部部署的入站呼叫將失敗。此特定情況的症狀與幾乎所有其他思科Webex入站呼叫故障相同：本地電話不響。

如果使用Expressway診斷日誌對此問題進行故障排除，您將不會看到來自Cisco Webex的任何流量。如果您嘗試搜尋TCP連線，您將看不到Dst-port=5062的任何連線嘗試，也不會看到來自Cisco Webex的任何後續的MTLS握手或SIP Invite。由於Expressway-E診斷日誌記錄在此情況下沒有用處，因此可以使用以下幾種驗證方法：

1. 從防火牆的外部介面獲取資料包捕獲
2. 利用埠檢查實用程式
3. 使用混合連線測試工具

由於混合連線測試工具直接內建於Cisco Webex控制中心，並模擬嘗試連線到本地Expressway的Cisco Webex環境，因此它是可用的最理想的驗證方法。測試到組織的TCP連線：

1. 登入[Cisco Webex Control Hub](#)
2. 選擇服務
3. 選擇混合呼叫卡中的SettingsLink
4. 在「呼叫服務連線」部分中，確保在SIP目標中輸入的值正確
5. 按一下「Test」，如下圖所示。

SIP Destination ⓘ



64.102.241.236:5062

Test Save

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

6. 由於測試失敗，您可以按一下[檢視測試結果](#)連結檢查詳細資訊，如下圖所示。

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	

如上圖所示，您可以看到在嘗試連線到64.102.241.236:5062時Socket測試失敗。除了Expressway診斷日誌/資料包外，此資料未顯示任何連線嘗試，因此您現在有足夠的證據來調查防火牆ACL/NAT/路由配置。

解決方案

由於此特定問題不是由Cisco Webex環境或本地合作裝置引起的，因此您需要將重點放在防火牆配置上。由於您不一定能預測要連線的防火牆型別，因此您需要依賴熟悉裝置的人員。此問題可能與防火牆ACL、NAT或路由配置錯誤有關。

問題3.套接字故障：Expressway-E未在埠5062上偵聽

這種特殊情況經常被診斷為錯誤的。很多情況下，假設防火牆是導致通過埠5062的流量被阻止的原因。要對此特殊情況進行故障排除，您可以使用上述「埠5062被阻止入站到Expressway」場景中的技術。您會發現混合連線測試工具和用於檢查埠連線的任何其他工具都將失敗。第一個假設是防火牆正在阻止流量。然後，大多數人會再次檢查Expressway-E上的診斷日誌記錄，以確定他們是否可以嘗試建立的TCP連線。它們通常會查詢日誌行專案，如圖所示。

```
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"
```

在這種情況下，上述特定日誌條目將不存在。因此，許多人會誤診情況，以為是防火牆。

如果診斷日誌記錄中包含資料包捕獲，則可以驗證原因是否出在防火牆。以下是Expressway-E未偵聽埠5062的場景中的資料包捕獲示例。此捕獲通過使用tcp.port==5062作為應用的過濾器進行過濾，如下圖所示。

Filter: tcp.port==5062

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

Spark TCP SYN packet received

Immediate RST sent from the Expressway

從Expressway-E獲取的資料包捕獲中可以看到，TCP埠5062上的流量未被防火牆阻止，但實際上到達了。在資料包編號56中，您可以看到Expressway E在初始TCP SYN資料包到達後立即傳送RST。使用此資訊，您可以斷定問題與Expressway-E接收資料包無關；您必須從Expressway-E的角度對問題進行故障排除。根據證據，考慮為什麼Expressway-E會拒絕資料包的可能原因。可歸因於此行為的兩種可能性：

1. Expressway-E設定了一些可能阻止流量的防火牆規則
2. Expressway-E未偵聽相互TLS流量和/或未偵聽通過埠5062的流量。

Expressway-E的防火牆功能位於 *System > Protection > Firewall rules > Configuration* 下。在此環境中檢查此配置時，不存在防火牆配置。

有多種方法可以檢驗Expressway-E是否正在偵聽埠5062上的相互TLS流量。您可以通過Web介面或CLI以超級使用者身份執行此操作。

如果發出 `netstat -an | grep ':5062'`，您應會獲得一些與下面類似的輸出。

```
~ # 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
```

也可通過Expressway-E的Web介面捕獲此資訊。請參閱以下步驟收集此資訊

1. 登入Expressway-E
2. 導航到維護工具>埠使用>本地入站埠
3. 搜尋SIP和IP埠5062型別。(以紅色突出顯示，如下圖所示)

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

現在您已經知道應該看到什麼，可以將其與當前環境進行比較。從CLI角度來看，當您運行 `netstat -an | grep ':5062'`，輸出如下所示：

```
~ # netstat -an | grep ':5062'
tcp        0      0 127.0.0.1:5062       0.0.0.0:*            LISTEN
tcp        0      0 :::1:5062            :::*                  LISTEN
~ #
```

此外，Web UU不會顯示「本地入站埠」下列出的雙方TLS埠

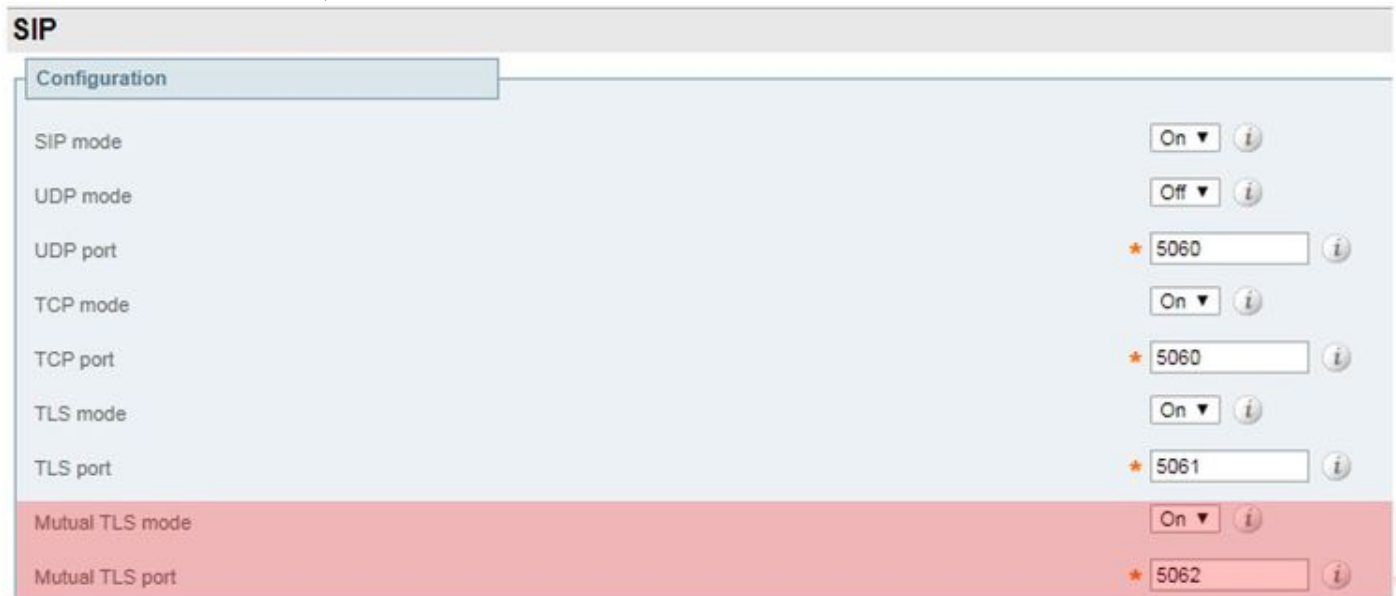
Type	Description	Protocol	IP address	IP port	Transport
H.323	Call signaling port range	H.323	192.168.1.6	15000-19999	TCP
H.323	Call signaling port range	H.323	172.16.2.2	15000-19999	TCP
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP
SIP	TCP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

通過此資料，您可以斷定Expressway-E沒有偵聽相互TLS流量。

解決方案

為了解決此問題，您必須確保啟用相互TLS模式並在Expressway-E上將相互TLS埠設定為5062:

1. 登入Expressway-E
2. 導覽至**Configuration > Protocols > SIP**
3. 確保「相互TLS」模式設定為「開啟」
4. 確保雙向TLS埠設定為**5062**
5. 按一下「**Save**」，如下圖所示。



問題4. Expressway-E或C不支援預載入的SIP路由報頭

使用混合呼叫服務連線，呼叫路由基於路由報頭完成。路由報頭是根據解決方案的呼叫服務感知（Expressway連結器）部分向Cisco Webex提供的資訊填充的。Expressway連結器主機將查詢Unified CM以查詢已啟用呼叫服務的使用者，並提取其Directory URI和Unified CM主群集的群集FQDN。使用Alice和Bob檢視以下示例：

目錄URI	目的地路由報頭
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

如果Alice或Bob進行呼叫，則呼叫將路由到其本地Unified CM，以便在路由到被叫使用者之前可以錨定到其Cisco WebexRD。

如果Alice要呼叫Bob，該呼叫將路由到Alice的Unified CM主群集FQDN(us-cucm.example.com)。如果分析Cisco Webex向Expressway-E傳送入站的SIP INVITE，您將在SIP報頭中找到以下資訊

請求URI sip:bob@example.com

路由報頭 sip:us-cucm.example.com;lr

從Expressway的角度來看，搜尋規則配置為路由呼叫，而不是通過請求URI，而是通過路由報頭(us-cucm.example.com) — 在此情況下，Alice的Unified CM主集群。

通過此基礎設定，您可以瞭解Expressway配置錯誤導致上述邏輯無法工作的故障排除情況。與幾乎所有其他入站混合呼叫服務連線呼叫設定失敗一樣，故障症狀是本地電話沒有響起。

分析Expressway上的診斷日誌之前，請考慮如何識別此呼叫：

1. SIP請求URI將是被叫方的目錄URI。
2. 「SIP FROM」欄位的格式將使用列為「First Name Last Name」
<sip:WebexDisplayName@subdomain.call.ciscospark.com>的主叫方

使用此資訊，您可以按被叫方的目錄URI、主叫方的名字和姓氏或主叫方的Cisco Webex SIP地址搜尋診斷日誌。如果您沒有以上任何資訊，可在「INVITE SIP:」上搜尋，找到通過Expressway運行的所有SIP呼叫。識別出入站呼叫的SIP INVITE後，您可以找到並複製SIP呼叫ID。在擁有該值後，您只需根據呼叫ID搜尋診斷日誌即可檢視與此呼叫段相關的所有消息。

幫助隔離路由問題的另一件事情是確定呼叫進入企業的距離。您可以嘗試在Expressway-C上搜尋上述資訊，檢視該呼叫是否已路由到該處。如果是，您可能希望在那裡開始調查。

在此場景中，可以看到Expressway-C已收到來自Expressway-E的INVITE。

```
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>

重要的是，路由報頭 (群集FQDN) 仍完好。但是，沒有基於路由報頭 (群集FQDN) cucm.rtp.ciscotac.net執行搜尋邏輯。相反，您會看到消息立即被拒絕並顯示404 Not Found。

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:pstojoano-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="pstojoano-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="pstojoano-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:pstojoano-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=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c7696bb;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=35464;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
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

與工作方案相比，您會看到在工作方案中，搜尋邏輯是根據路由器報頭（群集FQDN）執行的

```
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'"**
然後您可以看到Expressway-C將呼叫正確轉發到Unified CM(192.168.1.21)。

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.ciscopark.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)

分析了將問題隔離到Expressway-C的診斷日誌記錄以及特定錯誤(404 Not Found)後，您可以重點
分析導致此類行為的因素。需要考慮的事項如下：

1. 呼叫通過搜尋規則在Expressway上移入和移出區域。
2. Expressway使用稱為預載入SIP路由支援的邏輯，用於處理包含路由器報頭的SIP INVITE請求。該值可以在Expressway-C和Expressway-E上的區域（遍歷伺服器、遍歷客戶端、鄰居）中開啟或關閉。

現在，您可以使用xConfiguration檢視Expressway-E遍歷伺服器與Expressway-C客戶端區域上的配置，特別是針對混合呼叫服務連線設定的那些區域。除了Zone配置之外，您還可以分析配置為將此呼叫從一個區域傳遞到另一個區域的搜尋規則。您還知道Expressway-E確實將呼叫傳遞到Expressway-C，因此遍歷伺服器區域配置很可能正確設定。

為了對此進行細分，下面的xConfig告訴我們此區域的名稱稱為混合呼叫服務遍歷。它屬於TraversalServer區域型別。它通過SIP TCP埠7003與Expressway-C進行通訊。

混合呼叫服務的關鍵部分是，必須啟用預載入SIP路由支援。Expressway Web介面呼叫此值Preloaded SIP routes support，而xConfiguration將顯示為SIP PreloadedSipRoutes Accept

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 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 Type: "TraversalServer"
```

您還可以確定此區域與搜尋規則3 (Webex混合) 關聯。實際上，搜尋規則傳送的是通過混合呼叫服務的DNS區域傳入的「任意」別名，並將其傳遞到上面的區域，即混合呼叫服務遍歷。按照預期，Expressway-E上的搜尋規則和遍歷伺服器區域都配置正確。

```
*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"
```

如果關注Expressway-C的xConfiguration，可以從查詢Webex Hybrid的遍歷客戶端區域開始。查詢該埠的一種簡單方法是搜尋您從Expressway-E xConfiguration(SIP Port: 「7003」)。這有助於您快速確定xConfiguration中的正確區域。

與以前一樣，您可以瞭解區域名稱（混合呼叫服務遍歷）、型別（遍歷客戶端）以及為SIP PreloadedSipRoutes Accept（預載入SIP路由支援）配置的內容。從此xConfiguration中可以看到，該值設定為Off。根據Cisco Webex混合呼叫服務部署指南，此值應設定為On。

此外，如果檢查預載入SIP路由支援的定義，我們可以清楚地看到，如果此值設定為Off且INVITE包含路由報頭，則Expressway-C應拒絕消息：**"如果希望區域拒絕包含此報頭的SIP INVITE請求，則切換預載入SIP路由支援關閉。"**

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/1lYDd76O/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"
```

此時，您將問題歸結為Expressway-C穿越客戶端區域配置錯誤。您必須將預載入SIP路由支援切換為On。

解決方案

要正確設定預載入SIP路由支援，請執行以下操作：

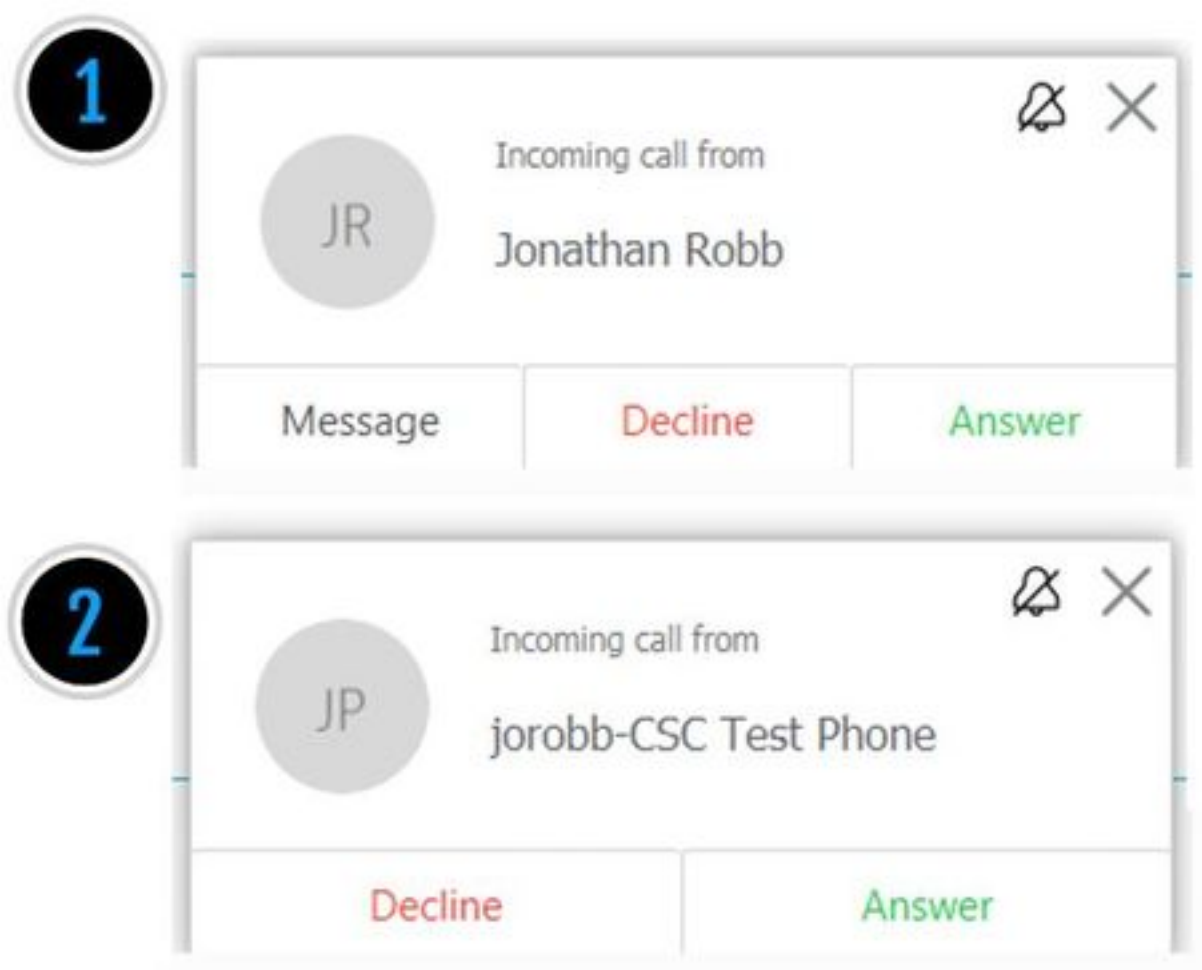
1. 登入Expressway-C
2. 導航到Configuration > Zones > Zones

3. 選擇混合呼叫服務遍歷客戶端區域 (命名因客戶而異)
4. 將Preloaded SIP routs support設定為On
5. 選擇儲存

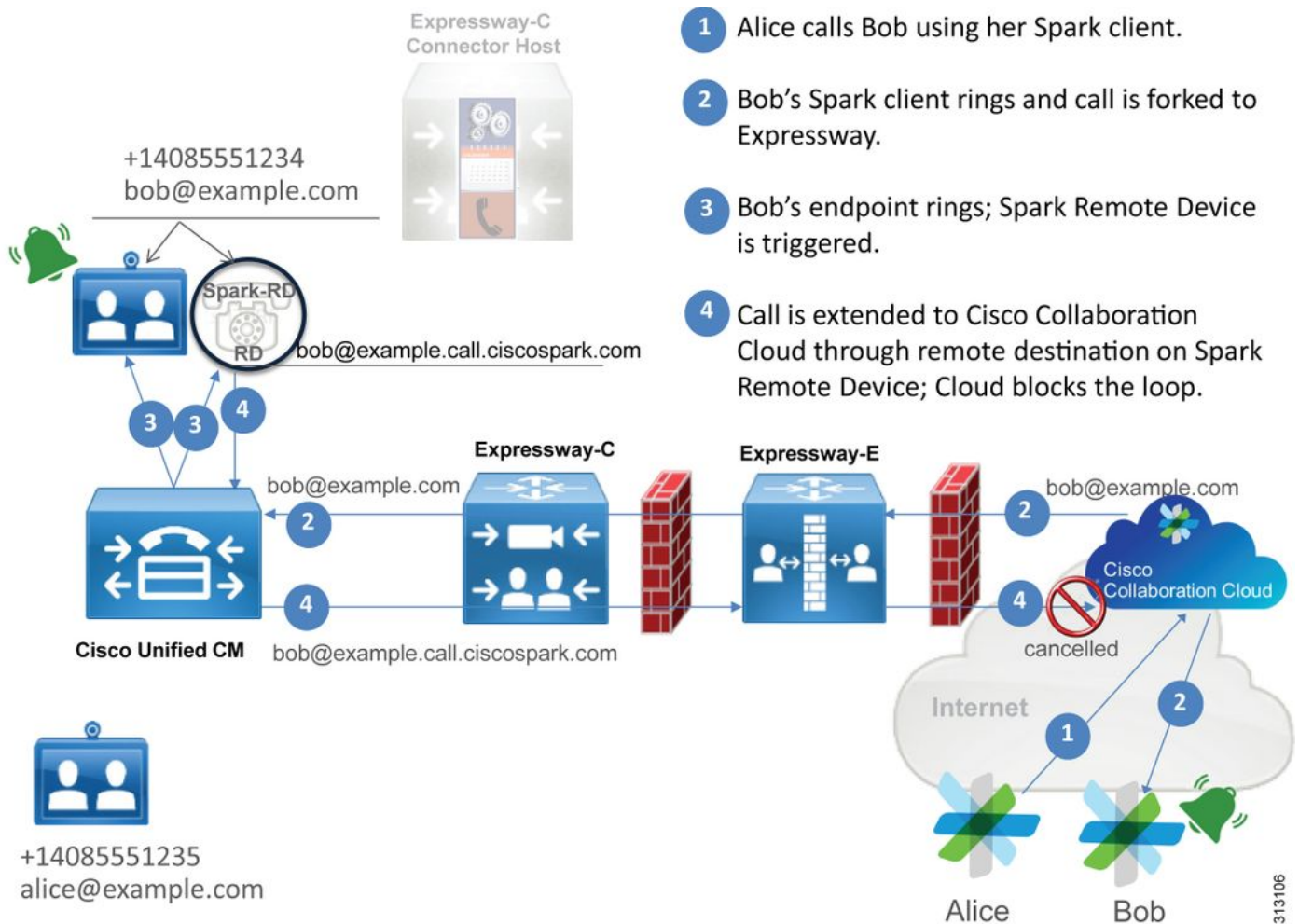
附註：雖然此場景演示了Expressway-C上的故障，但是如果Webex混合呼叫遍歷伺服器區域上的預載入SIP路由支援關閉，則在Expressway-E上可以觀察到相同的診斷日誌記錄錯誤。在這種情況下，您永遠看不到呼叫到達Expressway-C，而Expressway-E將負責拒絕呼叫並傳送404 Not Found。

問題5. Cisco Webex應用正在接收兩個呼叫通知 (廣播)

此特定問題碰巧是唯一不會導致呼叫丟棄的入站呼叫方案。對於此問題，接收呼叫的人 (被叫方) 在Cisco Webex應用中接收來自發出呼叫的人 (主叫方) 的兩條通知 (通知)。第一個通知由Cisco Webex生成，第二個通知由內部基礎設施生成。以下為圖中所示的兩個收到的通知的示例。



第一個通知(toast)來自從Cisco Webex端發起呼叫的人員 (主叫方)。此例項中的呼叫ID是發起該呼叫的使用者的顯示名稱。第二個通知(toast)來自本地CTI或Cisco Webex RD，分配給進行呼叫的使用者。起初，這種行為似乎有些奇怪。但是，如果您檢視入站呼叫圖表 (來自Cisco Webex混合呼叫設計手冊)，則行為會更有意義，如下圖所示。



從圖中，您可以看到Alice正在通過其Cisco Webex應用呼叫Bob，並且呼叫被分流到本地。此呼叫應與分配給Bob電話的目錄URI匹配。問題在於，在此設計中，目錄URI也分配給他的CTI-RD或Cisco Webex RD。因此，當呼叫被提供給CTI-RD或Cisco Webex RD時，該呼叫將傳送回Cisco Webex，因為裝置已為bob@example.call.ciscospark.com配置了遠端目標。Cisco Webex處理此情況的方式是取消特定呼叫段。

為使Cisco Webex正確取消呼叫段，Cisco Webex最初需要在SIP報頭中放置一個引數，它會查詢該引數以取消該給定段。Cisco Webex插入到SIP INVITE中的引數稱為"call-type=squared"，該值輸入到Contact報頭中。如果從消息中刪除此值，Cisco Webex不瞭解如何取消呼叫。

使用此資訊，您可以重新檢視先前顯示的場景，即當思科Webex使用者Jonathan Robb進行呼叫時，使用者的Cisco Webex應用收到兩個通知（廣播）。若要解決此類問題，您始終需要收集Expressway-C和Expressway-E的診斷日誌記錄。作為起點，您可以檢視Expressway-E日誌，確定SIP INVITE實際上在入站傳送的初始Cisco Webex INVITE的Contact標頭中確實存在call-type=squared值。這將確保防火牆不會以任何方式操縱消息。下面是此場景中傳入Expressway-E的INVITE的示例片段。

```
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:

Contact報頭存在call-type=squared值。此時，呼叫必須通過Expressway路由並傳送Webex混合遍歷伺服器區域。我們可以搜尋Expressway-E日誌，以確定如何從Expressway-E發出呼叫。這將給我們一個建議，說明Expressway-E是否以任何方式操縱INVITE。

```
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=z9hG4bK52aac9a181192566e01b98ae0280bdf858.0e65cdf078cabb269e6cb6bce132
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>

檢視從Expressway-E傳送到Expressway-C的此SIP INVITE時，請注意Contact報頭缺少call-type=squared。需要指出的另一點是，在第4行中，您可以看到出口區域等於HybridCallServiceTraversal。現在您可以斷定，Cisco Webex應用在被撥號時收到第二個通知(toast)的原因是Expressway-E從SIP INVITE Contact標頭中去除call-type=squared標籤。要回答的問題是，是什麼原因導致了此剝離標題。

呼叫必須通過您在Expressway上設定的混合呼叫服務遍歷進行路由，因此這是開始調查的良好位置

。如果您有xConfiguration，您可以看到此區域的配置方式。要標識xConfiguration中的區域，您只需使用記錄在Via行中的名稱，該名稱將列印在日誌中。您可以看到上面稱為egress-zone=HybridCallServiceTraversal。將此名稱列印到SIP報頭的Via行時，空格會被刪除。xConfiguration視角中的實際區域名稱將具有空格，並在混合呼叫服務遍歷中格式化。

```
*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: "rtpl2-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"
```

通過為混合呼叫服務遍歷標識的設定，您可以查詢突出的潛在設定，例如：

- SIP預載入SIP路由接受：於
- SIP引數保留模式：Off

使用任何Expressway的Web介面，您可以檢視這些值的定義及其用途。

預載入SIP路由支援

Switch Preloaded SIP routs support On (交換機預載入的SIP路由支援On)，使該區域能夠處理包含路由報頭的SIP INVITE請求。

如果希望區域拒絕包含此報頭的SIP INVITE請求，則切換預載入SIP路由支援關閉。

SIP引數保留

確定Expressway的B2BUA是否保留或重寫通過此區域路由的SIP請求中的引數。

Onpreserves此區域與B2BUA之間路由請求的SIP請求URI和聯絡人引數。

如果需要，B2BUA可以重寫在此區域和B2BUA之間路由請求的SIP請求URI和Contact引數。

根據這些定義、xConfiguration以及 **call-type=squared**值放在SIP INVITE的「聯絡人」標頭中，您可以斷定，在混合呼叫服務遍歷區域上將SIP引數保留值設定為Off是標籤被刪除和Cisco Webex應用獲得雙振鈴通知的原因。

解決方案

要保留SIP INVITE的Contact報頭中的call-type=squared值，您必須確保Expressway支援保留所有參與處理呼叫的區域的SIP引數：

1. 登入Expressway-E
2. 導航到**Configuration > Zones > Zones**
3. 選擇用於混合遍歷伺服器的區域
4. 將SIP引數保留值設定為On
5. 儲存設定。

#####

附註：在此示例場景中，錯誤配置的是Expressway-E上的Webex混合遍歷伺服器區域。請記住，在Webex混合遍歷客戶端或CUCM鄰居區域上，SIP引數保留值完全可以設定為Off。這兩種配置都將在Expressway-C上完成。如果出現這種情況，您可能認為Expressway-E會將 **call-type=squared**值傳送到Expressway-C，並且會是Expressway-C將其剝離。

出站：內部部署至Cisco Webex

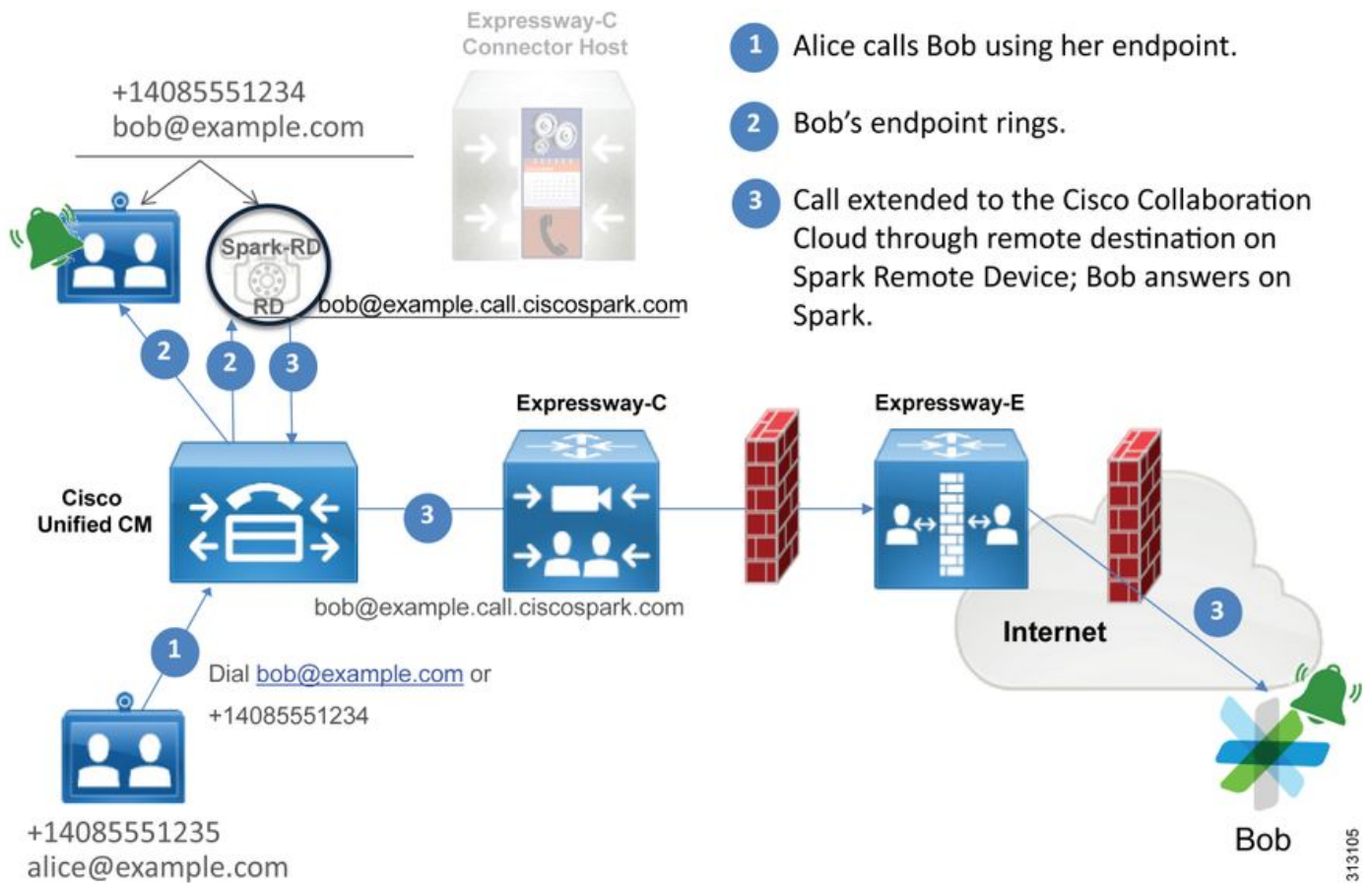
幾乎每次涉及到Cisco Webex的出站本地呼叫失敗都會導致相同的故障症狀：「當我從我的Unified CM註冊電話呼叫支援呼叫服務連線的另一使用者時，其本地電話振鈴，但其Cisco Webex應用未振鈴。」要對此場景進行故障排除，必須瞭解進行此類呼叫時發生的呼叫流程和邏輯。

高級邏輯流

1. 使用者A從自己的內部電話呼叫使用者B的目錄URI
2. 使用者B的本地電話和CTI-RD/Webex-RD接受呼叫
3. 使用者B的本地電話開始響起
4. 使用者B的CTI-RD/Webex-RD將此呼叫轉發到UserB@example.call.ciscospark.com的目標
5. Unified CM將此呼叫傳送到Expressway-C
6. Expressway-C將呼叫傳送到Expressway-E
7. Expressway-E在callservice.ciscospark.com域上執行DNS查詢
8. Expressway-E嘗試通過埠5062連線到Cisco Webex環境。
9. Expressway-E和Cisco Webex環境開始相互握手
10. Cisco Webex環境會將呼叫傳遞到使用者B可用的思科Webex應用
11. 使用者B的可用思科Webex應用開始振鈴。

呼叫流

導覽至**使用者B on-prem phone > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco Webex environment > Cisco Webex app**，如下圖所示。



附註：影象已從[Cisco Webex混合設計手冊](#)中提取。

日誌分析提示

如果您正在排查到Cisco Webex的出站分叉呼叫失敗的情況，您需要收集Unified CM、Expressway-C和Expressway-E日誌。通過這些日誌集，您可以檢視呼叫是如何通過環境的。要瞭解呼叫在本地環境中到達的距離，另一個快速方法是使用Expressway「搜尋歷史記錄」。通過Expressway搜尋歷史記錄，您可以快速檢視對Cisco Webex的分支呼叫是否到達Expressway-C或E。

要使用搜尋歷史記錄，您可以執行以下操作：

1. 登入Expressway-E
發出測試呼叫
導航到狀態>搜尋歷史記錄
驗證您是否看到具有應呼叫的Webex SIP URI的目標地址的呼叫
(user@example.call.ciscospark.com)
如果搜尋歷史記錄未顯示按Expressway-E搜尋歷史記錄進行的呼叫，請在Expressway-C上重複此過程

分析Expressway上的診斷日誌之前，請考慮如何識別此呼叫：

1. SIP請求URI將是Cisco Webex使用者的SIP地址
2. SIP FROM欄位的格式將設定為將主叫方列為「名字姓氏」<sip:Alias@Domain>

使用此資訊，您可以按主叫方的目錄URI、主叫方的名字和姓氏或被叫方的Cisco Webex SIP地址搜尋診斷日誌。如果您沒有以上任何資訊，您可以搜尋「INVITE SIP:」，這將找到通過Expressway運行的所有SIP呼叫。識別出出站呼叫的SIP INVITE後，您可以找到並複製SIP Call-ID。執行此操作後，您只需根據Call-ID搜尋診斷日誌即可檢視與此呼叫段相關的所有消息。

以下是在對已啟用呼叫服務連線的使用者進行呼叫時，觀察到從Unified CM註冊電話到Cisco

Webex環境的出站呼叫的一些最常見問題。

問題1. Expressway無法解析callservice.ciscospark.com地址

Expressway DNS區域的標準操作過程是根據請求URI右側顯示的域執行DNS查詢。要解釋這一點，請考慮一個示例。如果DNS區域將接收請求URI為pstoiano-test@dmzlab.call.ciscospark.com的呼叫，則典型的Expressway DNS區域將在dmzlab.call.ciscospark.com（請求URI的右側）上執行DNS SRV查詢邏輯。如果Expressway要執行此操作，您預計將會發生以下查詢和響應。

```
_sip._tcp.dmzlab.call.ciscospark.com.  
Response: 5 10 5061 l2sip-cfa-01.wbx2.com.  
l2sip-cfa-01.wbx2.com  
Response: 146.20.193.64
```

如果仔細檢視，您會看到SRV記錄響應提供伺服器地址和埠5061，而不是5062。

這意味著不會在埠5062上發生相互TLS握手，並且在Expressway和Cisco Webex之間使用單獨的埠進行信令。此問題的難點在於，《Cisco Webex混合呼叫服務部署指南》沒有明確指出使用埠5061，因為某些環境不允許企業對企業進行呼叫。

在Expressway上通過此標準DNS區域SRV查詢邏輯的工作方式是配置Expressway，使其根據您提供的值執行顯式搜尋。

現在，分析此特定呼叫時，您可以重點關注Expressway-E，因為您確定（使用搜尋歷史記錄）該呼叫已到達此程度。從進入Expressway-E的第一個SIP INVITE開始，檢視它進入哪個區域、正在使用哪些搜尋規則、呼叫發出哪個區域，以及如果正確傳送到DNS區域，將發生什麼DNS查詢邏輯。

```
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:pstoiano-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-remotecallinfo>;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: 2568978048-0000065536-0000000148-0352430272
Content-Type: application/sdp
Content-Length: 714
```

<SDP Omitted>

在此SIP INVITE中，您可以收集請求URI(pstojano-test@dmzlab.call.ciscospark.com)、Call-ID(991f7e80-9c11517a-130ac-1501a8c0)、From("Jonathan Robb" <sip:5010@rtp.ciscotac.net>)、To(sip:pstojano-test@dmzlab.call.ciscospark.com)和User-Agent(Cisco-CUCM11.5)。收到此INVITE後，Expressway現在必須做出邏輯決策，以確定是否可以將該呼叫路由到另一個區域。Expressway將根據搜尋規則執行此操作。

```
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'"
```

根據上面的日誌片段，您可以看到Expressway-E通過四個搜尋規則進行了解析，但是隻考慮了一個(Webex Hybrid — 到Webex Cloud)規則。搜尋規則的優先順序為90，目標為轉至混合呼叫服務DNS區域。現在呼叫正在傳送到DNS區域，您可以檢視Expressway-E上發生的DNS SRV查詢

```
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"
```

在上面的代碼片段中，您可以看到Expressway-E基於請求URI(_sips._tcp.dmzlab.call.ciscospark.com)的右側執行了SRV查詢，並且已解析為主機名為l2sip-cfa-01.wbx2.com和埠5061。hostname l2sip-cfa-01.wbx2.com解析為146.20.193.64。使用此資訊

，Expressway下一步將採取的邏輯步驟是將TCP SYN資料包傳送到146.20.193.64，以便嘗試建立呼叫。通過Expressway-E日誌記錄，您可以檢視是否發生這種情況。

```
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"
```

在上述Expressway-E診斷日誌記錄代碼片段中，可以看到Expressway-E正在嘗試連線到IP 146.20.193.64，該地址以前通過TCP埠5061解析，但此連線完全失敗。從收集的資料包捕獲中也可以看到相同的情況。

Expressway-E attempts TCP Connection

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=4109470239
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=2 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=2 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=0 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
15158	2017-09-19 17:18:52.203326	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
15160	2017-09-19 17:18:54.231324	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
15170	2017-09-19 17:18:55.283326	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
15757	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
17846	2017-09-19 17:19:02.379327	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
18425	2017-09-19 17:19:04.427323	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

根據這些結果，可以清楚地看到，埠5061上的流量無法成功。但是，混合呼叫服務連線應使用TCP埠5062，而不是5061。因此，您需要考慮為什麼Expressway E不解析返回埠5062的SRV記錄。要嘗試回答此問題，您可以在Expressway-E Webex混合DNS區域上查詢可能的配置問題。

```
*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: "ciscospark.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.ciscospark.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"
```

在Expressway-E的xConfiguration中，您可以看到兩個與DNS查詢相關的特殊值：DNSOverride Name和DNSOverride Override。基於此xConfiguration，DNSOverride Override設定為Off，因此DNSOverride Name不會生效。為了更好地瞭解這些值的用途，您可以使用Expressway Web UI查詢這些值的定義。

修改DNS請求(在xConfig中轉換為DnsOverride Override)

將出站SIP呼叫從此區域路由到手動指定的SIP域，而不是撥號目標中的域。此選項主要用於Cisco Webex通話服務。請參閱www.cisco.com/go/hybrid-services。

要搜尋的域(在xConfig中轉換為DnsOverride名稱)

輸入要在DNS中查詢的FQDN，而不是在出站SIP URI上搜尋域。原始SIP URI不受影響。

現在您已經有了這些定義，很顯然，如果設定正確，這些值與我們的DNS查詢邏輯完全相關。如果將此選項與Cisco Webex混合呼叫服務部署指南中的語句相結合，您會發現修改DNS請求必須設定為**On**，而要搜尋的域應設定為**callservice.ciscopark.com**。如果要更改這些值以指定正確的資訊，則DNS SRV查詢邏輯將完全不同。下面是從Expressway-E診斷日誌記錄角度可期待的內容的片段

```
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"
```

解決方案

1. 登入Expressway-E
2. 導航到**Configuration Zones > Zones**
3. 選擇已配置的Webex混合DNS區域
4. 將修改DNS請求設定為**On**
5. 將「域」設定為**callservice.ciscopark.com**
6. 儲存更改

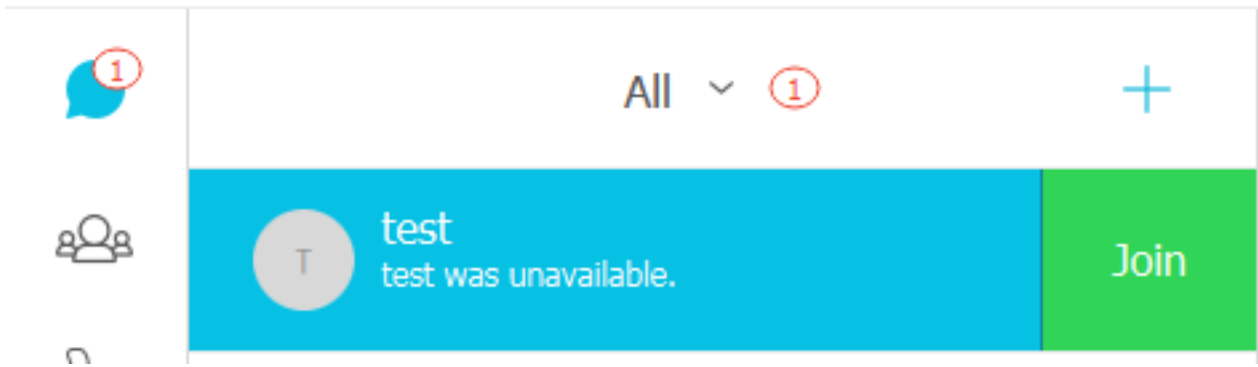
附註：如果Expressway上只使用一個DNS區域，則應配置一個單獨的DNS區域，以便與可以利用這些值的混合呼叫服務一起使用。

問題2.埠5062被阻止出站到Cisco Webex

思科Webex的分叉出站呼叫失敗的一個獨特之處在於，被叫方的Cisco Webex應用將在他們的應用上顯示「加入」按鈕，儘管客戶端從不振鈴。與上面的情況一樣，對於此問題，您將需要再次使用相同的工具和日誌記錄，以更好地瞭解故障所在。有關隔離呼叫問題和分析日誌的提示，請參見本文如圖所示的部分。

顯示的「連線」按鈕的圖示

PT pstoiano test
Active 15 minutes ago



與「撥出呼叫問題#1」類似，您可以在Expressway-E診斷日誌記錄中開始分析，因為您已經使用Expressway上的搜尋歷史記錄來確定呼叫到達了那麼遠。與以前一樣，從Expressway-C進入Expressway-E的初始INVITE開始。請記住您要查詢的內容包括：

- 1. Expressway-E是否收到INVITE
- 2. 搜尋規則邏輯是否將呼叫傳遞到混合DNS區域
- 3. DNS區域是否執行DNS查詢並在正確的域上執行
- 4. 系統是否嘗試並正確建立了埠5062的TCP握手
- 5. 相互TLS握手是否成功

```
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:pstoiano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcd62f6ff7e09f9939482.899441b6d60c
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>
```

如上面的邀請中所示，INVITE接收正常。這是「已接收」操作，來自Expressway-C IP地址。現在，您可以轉到搜尋規則邏輯

```
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.ciscospark.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.ciscospark.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.ciscospark.com'"
```

根據上面的日誌片段，您可以看到Expressway-E通過四個搜尋規則進行了解析，但只有一個搜尋規則（*Webex Hybrid* — 至*Webex Cloud*）都考慮過了。搜尋規則的優先順序為90，目標為 *混合呼叫服務DNS區域*。現在呼叫正在傳送到DNS區域，您可以檢視Expressway-E上發生的DNS SRV查詢。這一切都是正常的。現在，您可以重點關注DNS查詢邏輯

```
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.ciscospark.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"
```

您可以清楚地看到，在此例項中，callservice.ciscospark.com SRV記錄已解析。響應是四個不同的有效記錄，全部使用埠5062。這是正常行為。此時，您現在可以分析接下來應發生的TCP握手。如本文檔前面所述，您可以搜尋診斷日誌中的「TCP連線」，並查詢列出Dst-port="5062"的行專案。下面是您在此場景中看到的內容示例：

```
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"
```

您還可以使用診斷日誌記錄捆綁包中包含的tcpdump，獲取有關TCP握手的更多詳細資訊，如下圖所示。

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.

此時，您可以斷定Expressway-E正確路由呼叫。此場景中的難題是無法與Webex環境建立TCP連線。發生這種情況的原因是Webex環境沒有響應TCP SYN資料包，但是考慮到處理連線的伺服器在許多客戶之間是共用的，這種情況不太可能發生。在此案例中，更有可能的原因是某些型別的中間裝置（防火牆、IPS等）不允許流量流出。

解決方案

由於問題已被隔離，因此應將此資料提供給客戶的網路管理員。此外，如果他們需要更多資訊，您可以將捕獲從邊緣裝置和/或防火牆的外部介面移出，以便進一步驗證。從Expressway的角度來看，由於問題不在該裝置上，因此無需執行進一步的操作。

問題3. Expressway搜尋規則配置錯誤

搜尋規則配置錯誤是Expressway上最大的配置相關問題之一。搜尋規則配置問題可以是雙向的，因為您需要入站呼叫的搜尋規則，並且您需要出站呼叫的搜尋規則。瀏覽此問題時，您會發現，儘管Expressway上的正規表示式問題非常常見，但它們並不總是搜尋規則問題的原因。在此特定網段中，您將處理失敗的出站呼叫。與我們所有其它出站分叉呼叫場景一樣，症狀保持不變：

- 被叫使用者的Cisco Webex應用顯示「加入」按鈕
- 主叫電話正在回鈴
- 被叫使用者的本地電話正在振鈴
- 被叫使用者的Cisco Webex應用從未響起

與所有其他方案一樣，您還需要利用CUCM SDL跟蹤以及Expressway-C和E診斷日誌。與以前一樣，您應該參考以利用搜尋歷史和提示來識別診斷日誌中的呼叫。與以前一樣，使用Expressway-E搜尋歷史記錄確定此呼叫已到達並且失敗。下面是分析的開始，我們將檢視從Expressway-C進入Expressway-E的初始SIP INVITE。

```
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-remotec: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>

使用SIP報頭中的呼叫ID(**d58f2680-9c91200a-1c7ba-1501a8c0**)，您可以快速向下搜尋與此對話方塊關聯的所有消息。在檢視日誌中第三個命中的呼叫ID時，可以看到Expressway-E立即向Expressway-C傳送**404 Not Found**。

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:

這些資料告訴您兩件事：

1. Expressway-E從未嘗試向Cisco Webex傳送INVITE
2. Expressway-E負責作出拒絕呼叫的邏輯決定，並出現404 Not Found錯誤。

404 Not Found錯誤通常表示Expressway無法找到目的地址。由於Expressway使用搜尋規則在它們之間和到不同環境之間路由呼叫，因此首先應重點關注Expressway-E的xConfiguration。在此xConfiguration中，您可以查詢應將呼叫傳遞到Webex混合DNS區域的搜尋規則。要從xConfiguration角度查詢Expressway上配置的搜尋規則，您可以搜尋「xConfiguration Zones Policy SearchRules Rule」。通過執行此操作，您將看到在Expressway上建立的每個搜尋規則的搜尋規則配置清單。「Rule」後面的數字將根據首先建立的搜尋規則（標籤為1）增加。如果您在查詢搜尋規則時遇到問題。您可以使用常用的命名值(如「Webex」)來更好地定位搜尋規則。標識規則的另一種方法是查詢設定為「.*@.*\ciscopark\com」的模式字串值。這是假設要配置的模式字串。（假設模式字串配置正確）在此場景中檢視xConfiguration後，您可以看到搜尋規則6是將呼叫傳遞給Cisco Webex的正確規則。

```
*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"
```

要測試此模式，可以使用中所述的Check pattern函式。這裡需要配置以下值：維護>工具>檢查模式

- 別名：初始INVITE%中的%Request URI(例如：pstoiano-test@dmzlab.call.ciscopark.com)
- 模式型別：正規表示式
- 模式字串。.*@.*\ciscopark\com
- 模式行為：離開

如果規則的Regex設定正確，您應該會看到此檢查模式的結果「成功」。下圖說明了這一點，如下圖所示

:

Check pattern

Alias

Alias *

Pattern

Pattern type Regex ▼ i

Pattern string *

Pattern behavior Leave ▼ i

Result	
Result	Succeeded
Details	Alias matched pattern
Alias	pstojano-test@dmzlab.call.ciscopark.com

現在，您可以確認搜尋規則存在且配置正確，然後仔細檢視Expressway執行的搜尋邏輯，以確定它是否影響傳送404 Not Found的Expressway-E。下面是Expressway執行的搜尋規則邏輯的示例。

```

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 'pstojano-test@dmzlab.call.ciscopark.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 'pstojano-test@dmzlab.call.ciscopark.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 'pstojano-test@dmzlab.call.ciscopark.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.ciscopark.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.ciscopark.com" Type="SRV (IPv4 and IPv6)"

```

在此示例中，您可以看到Expressway處理了四個搜尋規則。由於各種原因未考慮前3項，但考慮第4項。有趣的資料是，在考慮之後，Expressway立即跳轉到DNS查詢邏輯。如果您還記得我們在xConfiguration中看到的內容，則為Webex Hybrid配置的搜尋規則被命名為Webex Hybrid - to Webex Cloud，而上面的搜尋規則邏輯甚至沒有考慮它。此時，值得瞭解考慮搜尋規則（到DNS）的實施方式，以便更好地瞭解它是否影響Webex混合搜尋規則的使用。為此，您可以重新訪問xConfig，查詢名為「to DNS」的搜尋規則

```

*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"
```

檢視此搜尋規則後，您可以得出以下結論：

- 模式字串與Cisco Webex請求URI匹配
- 優先順序設定為100
- Progress(模式行為)設定為Stop。

此資訊告訴我們，正在呼叫的Cisco Webex請求URI將與此規則匹配，如果規則匹配，則Expressway將停止搜尋（考慮）其他搜尋規則。有了這一認識，規則優先順序就成為了一個關鍵因素。Expressway搜尋規則優先順序的工作方式是首先嘗試最低優先順序規則。以下是範例。搜尋規則：本地模式行為：繼續優先順序1搜尋規則：鄰居模式行為：繼續優先順序10搜尋規則：DNS模式行為：停止優先順序50在本示例中，將首先嘗試名為Local(1)的搜尋規則，如果找到匹配項，則它將移至搜尋規則鄰居(10)，因為模式行為設定為Continue。如果搜尋規則Neighbor不匹配，它仍會繼續搜尋規則DNS(50)並考慮最後一個。如果搜尋規則DNS匹配，則無論是否存在優先順序高於50的另一搜尋規則，搜尋都將停止，因為模式行為設定為Stop。通過此瞭解，您可以檢視「到DNS」和「Webex Hybrid - to Webex Cloud」規則之間的搜尋規則優先順序。

```
*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"
```

在這裡，您可以看到「to DNS」規則的優先順序低於「Webex Hybrid - to Webex Cloud」規則，因此，「to DNS」規則將首先嘗試。鑑於模式行為（進度）設定為「停止」，Expressway-E從不考慮Webex Hybrid - to Webex Cloud規則，因此呼叫最終會失敗。解決方案此類問題在混合呼叫服務連線中越來越常見。部署解決方案時，人們會多次建立用於思科Webex搜尋的高優先順序規則。很多時候，由於匹配了現有的低優先順序規則，因此不會呼叫建立的規則，這會導致失敗。對Cisco Webex的入站和出站呼叫都會發生此問題。要解決此問題，您需要執行以下步驟：

1. 登入Expressway-E
2. 導航到Configuration > Dial Plan > Search rules
3. 查詢Webex Hybrid Search規則並按一下它(例如：名稱:Webex Hybrid — 到Webex Cloud)
4. 將Priority值設定為比其他Search規則更低但足夠高的值，以便不會影響其他規則。(例如：優先順序機制:99)

使用搜尋規則的一般經驗法則是Pattern字串越具體，它可放置在Search rule priority清單中的位置就越低。通常，DNS區域配置有模式字串，該字串將捕獲非本地域的任何內容並將其傳送到Internet。因此，我們建議您將該型別的搜尋規則設定為高優先順序，以便最後呼叫。問題4. Expressway CPL配置錯誤Expressway解決方案使用伺服器上提供的呼叫處理語言(CPL)邏輯緩解收費欺詐。如果部署的Expressway解決方案僅用於Cisco Webex混合呼叫服務以及移動和遠端訪問，我們強烈建議啟用和實施CPL策略和規則。Expressway for Cisco Webex Hybrid上的CPL配置相當簡單，但如果配置錯誤，很容易阻止呼叫嘗試。以下場景顯示如何使用診斷日誌記錄來識別CPL配置錯誤。像所有其他出站分叉呼叫場景一樣，症狀保持不變：

- 被叫使用者的Cisco Webex應用顯示「加入」按鈕
- 主叫電話正在回鈴
- 被叫使用者的本地電話正在振鈴
- 被叫使用者的應用從未響起

與所有其他場景一樣，您可以使用CUCM SDL跟蹤以及Expressway-C和E診斷日誌。與先前一樣，您應參考使用搜尋歷史記錄和在診斷日誌中識別呼叫的提示。與之前一樣，使用Expressway-E搜尋歷史記錄確定此呼叫到達並失敗。下面是分析的開始，您可以在其中檢視從Expressway-C進入Expressway-E的初始SIP INVITE。

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.ciscospark.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-remotecallinfo>;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: 3224432896-0000065536-000000264-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

使用SIP報頭中的呼叫ID(c030f100-9c916d13-1cdcb-1501a8c0)，可以快速向下搜尋與此對話方塊關聯的所有消息。在檢視日誌中第三個命中的呼叫ID時，您可以看到Expressway-E立即向Expressway-C傳送403 Forbidden。

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=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0d
e36e16590bae36df388b6;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

要瞭解Expressway-E拒絕此呼叫並將一個403 Forbidden錯誤傳送到Expressway-C的原因，您需要分析輸入到Expressway中的403 Forbidden和原始SIP INVITE之間的日誌條目。通過分析這些日誌條目，您通常可以看到正在作出的所有邏輯決策。請注意，您未看到任何正在呼叫的搜尋規則，但看到正在呼叫的呼叫過程語言(CPL)邏輯。下面是其中的一個片段。

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:

基於以上日誌分析。您可以確定CPL拒絕呼叫。

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="4ffffefed-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"

附註：在這種情況下，您不會看到正在呼叫搜尋規則，因為CPL、FindMe和轉換都在搜尋規則之前處理在大多數情況下，您可以使用Expressway的xConfig來更好地瞭解情況。但是，對於CPL，只有在啟用策略後，您才能看到定義的規則。下面是顯示此Expressway-E正在使用本地CPL邏輯的xConfig部分。

*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"

要更好地瞭解規則配置，您需要登入到Expressway-E並導航到Configuration > Call Policy > Rules，如下圖所示。

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

檢視此配置時，可以看到以下已配置來源：.*目標:.*@dmzlab.call.ciscospark.com.*Action:拒絕與 [Cisco Webex混合呼叫服務部署指南](#)中記錄的內容相比，您可以看到源和目標已反向配置。

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

解決方案若要解決此問題，您需要重新調整CPL規則配置，以便將源設定為。

@%Webex_subdomain%.call.ciscospark.com.，且目標模式為。*

1. 登入Expressway-E
2. 導航到Configuration > Call Policy > Rules
3. 選擇為Cisco Webex混合呼叫服務設定的規則
4. 輸入源模式為.*@%Webex_subdomain%.call.ciscospark.com.*(例如：
.*@dmzlab.call.ciscospark.com.*)
5. 輸入目標模式為。*
6. 選擇保存

有關適用於Webex混合的CPL實作的詳細資訊，請參閱[Cisco Webex混合設計手冊](#)。雙向

: Cisco Webex到本地或本地到Cisco Webex 問題1. IP電話/合作終端提供G.711、G.722或AAC-LD以外的音訊編解碼器。混合呼叫服務連線支援三種不同的音訊編解碼器：G.711、G.722和AAC-LD。要成功建立與Cisco Webex環境的呼叫，必須使用其中一個音訊編解碼器。本地環境可以設定為使用多種型別的音訊編解碼器，但同時也可以設定為限制它們。通過使用Unified CM上的自定義和/或預設區域設定，可能會有意或無意地發生這種情況。對於此特定行為，記錄模式可能會因呼叫方向而異，並且如果Unified CM配置為使用早期或延遲提供，則記錄模式也會有所不同。下面是一些不同情況的示例，在這些情況下，此行為可能會呈現自身：

1. Cisco Webex傳送包含SDP的傳入INVITE，提供G.711、G.722或AAC-LD。Expressway-C將此消息傳送到Unified CM，但Unified CM配置為僅允許G.729進行此呼叫。因此，由於沒有可用的編解碼器，Unified CM將拒絕呼叫。
2. Unified CM嘗試將出站呼叫作為*Early Offer*傳送到Cisco Webex，這意味著傳送到Expressway-C的初始INVITE將包含僅支援G.729音訊的SDP。然後，Cisco Webex會傳送一個200 OK (帶SDP)，將音訊清零(*m=audio 0 RTP/SAVP*)，因為它不支援G.729。當Expressway-C將此INVITE傳遞到Unified CM後，Unified CM會因為不存在可用的編解碼器而終止呼叫。
3. Unified CM嘗試將出站呼叫作為*Delayed Offer*至Cisco Webex，這意味著傳送到Expressway-C的初始INVITE將不包含SDP。然後，Cisco Webex會傳送一個200 OK (帶SDP)，其中包含Cisco Webex支援的所有支援語音編解碼器。Expressway-C將此200 OK傳送到Unified CM，但Unified CM配置為僅允許G.729進行此呼叫。因此，由於沒有可用的編解碼器，Unified CM將拒絕呼叫。

如果您嘗試識別與此問題相匹配的混合呼叫服務連線呼叫失敗，則除Unified CM SDL跟蹤之外，您還必須獲取Expressway日誌。下面的示例日誌代碼片段與Unified CM嘗試以*Early Offer*進行出站呼

叫的情況相#2。由於我們知道呼叫將傳至Cisco Webex，因此日誌分析開始於Expressway-E。以下是思科Webex的初始INVITE片段。您可以看到首選的音訊編解碼器設定為G.729（負載18）。101用於DTMF，對於此特定方案不相關。

```
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.ciscospark.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=rtptime:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtptime: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

響應此初始INVITE，Cisco Webex使用200 OK消息進行響應。如果仔細檢視此消息，您可以看到音訊編解碼器已歸零。這是有問題的，因為如果沒有分配音訊埠，呼叫將無法協商該流。

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"

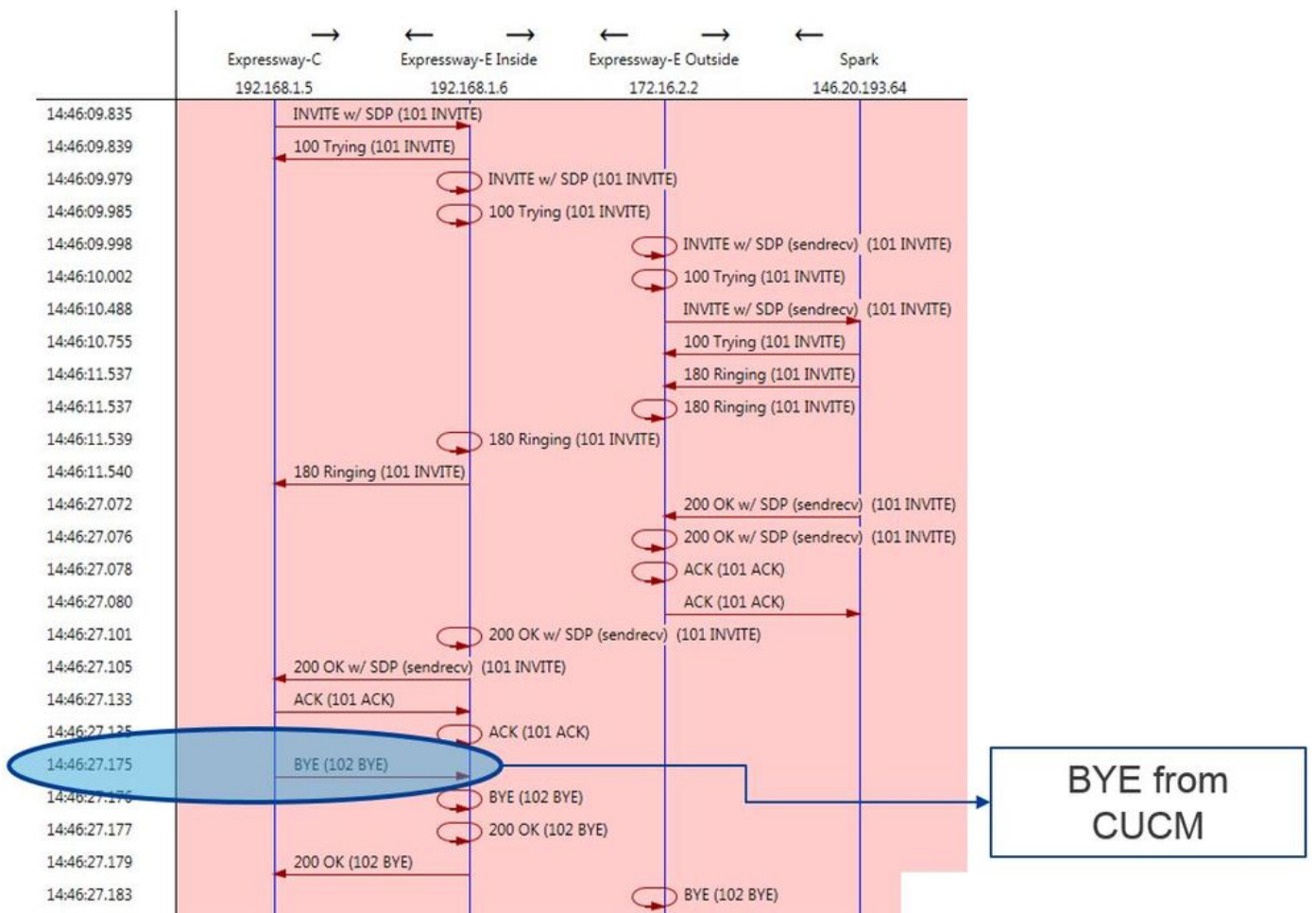
Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aede256d2@64.102.241.236:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aede256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE
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

```

現在可以使用TranslatorX檢視對話方塊的其餘部分。您可以看到對話方塊本身使用ACK完成。問題出在對話方塊完成之後，立即出現來自Expressway-C方向的BYE，如下圖所示。



以下是BYE消息的詳細示例。您可以清楚地看到使用者代理是Cisco-CUCM11.5，這意味著該消息是由Unified CM生成的。需要指出的另一點是，原因代碼設定為cause=47。此原因的常見轉換是無可用資源。

```

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-TAAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Reason: Q.850 ;cause=47
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=ed35426ed3ade6fdc3b058792333df2b
Content-Length: 0

由於Cisco Webex元件清除了此呼叫示例的音訊編解碼器，因此重點必須放在：a.傳送到Cisco Webex的初始INVITE和b.思科Webex用於將該埠歸零的邏輯是什麼。現在要瞭解初始INVITE的獨特之處，可以發現它只包含G.729。瞭解此資訊，請檢視Cisco Webex混合呼叫服務部署指南，並特別檢視「準備環境」一章，其中[完成混合呼叫服務連線的先決條件](#)(Complete the Prerequisites for Hybrid Call Service Connect)一節的步驟5列出了支援的特定編解碼器。我們可以看到：Cisco Webex支援以下編解碼器：

- 音訊 — G.711、G.722、AAC-LD
- 影片 — H.264

附註：*Opus*不用於Cisco Webex混合呼叫的本地呼叫段。有了這些資訊，您可以斷定Unified CM正在傳送不受支援的音訊編解碼器，這是Cisco Webex將埠歸零的原因。解決方案：要解決此特定情況，您可能需要檢視本地錨定呼叫的Cisco Webex RD和Expressway-C的SIP中繼之間的區域配置。為此，請確定這兩個元素所在的裝置池。裝置池包含到區域的對映。要確定Expressway-C SIP中繼的裝置池，請執行以下操作：

1. 登入到Unified CM。
2. 導覽至Device > Trunk。
3. 搜尋Trunk名稱或按一下Find。
4. 選擇Expressway-C中繼。
5. 記錄裝置池的名稱。

要確定錨定呼叫的CTI-RD或Cisco Webex-RD的裝置池，請執行以下操作：

1. 導覽至Device > Phone。
2. 搜尋時，您可以選擇Device Type contains Webex or CTI Remote Device (取決於客戶使用的裝置)。
3. 記錄裝置池的名稱。

確定連線到每個裝置池的區域：

1. 導覽至System > Device Pool。
2. 搜尋用於Expressway-C SIP中繼的裝置池。
3. 按一下Device Pool。
4. 記錄區域名稱。
5. 搜尋用於Webex-RD或CTI-RD的裝置池。
6. 按一下Device Pool。
7. 記錄區域名稱。

確定區域關係：

1. 定位至系統>區域資訊>區域。
2. 搜尋已確定的區域之一。

3. 確定使用G.729的兩個區域之間是否存在區域關係。

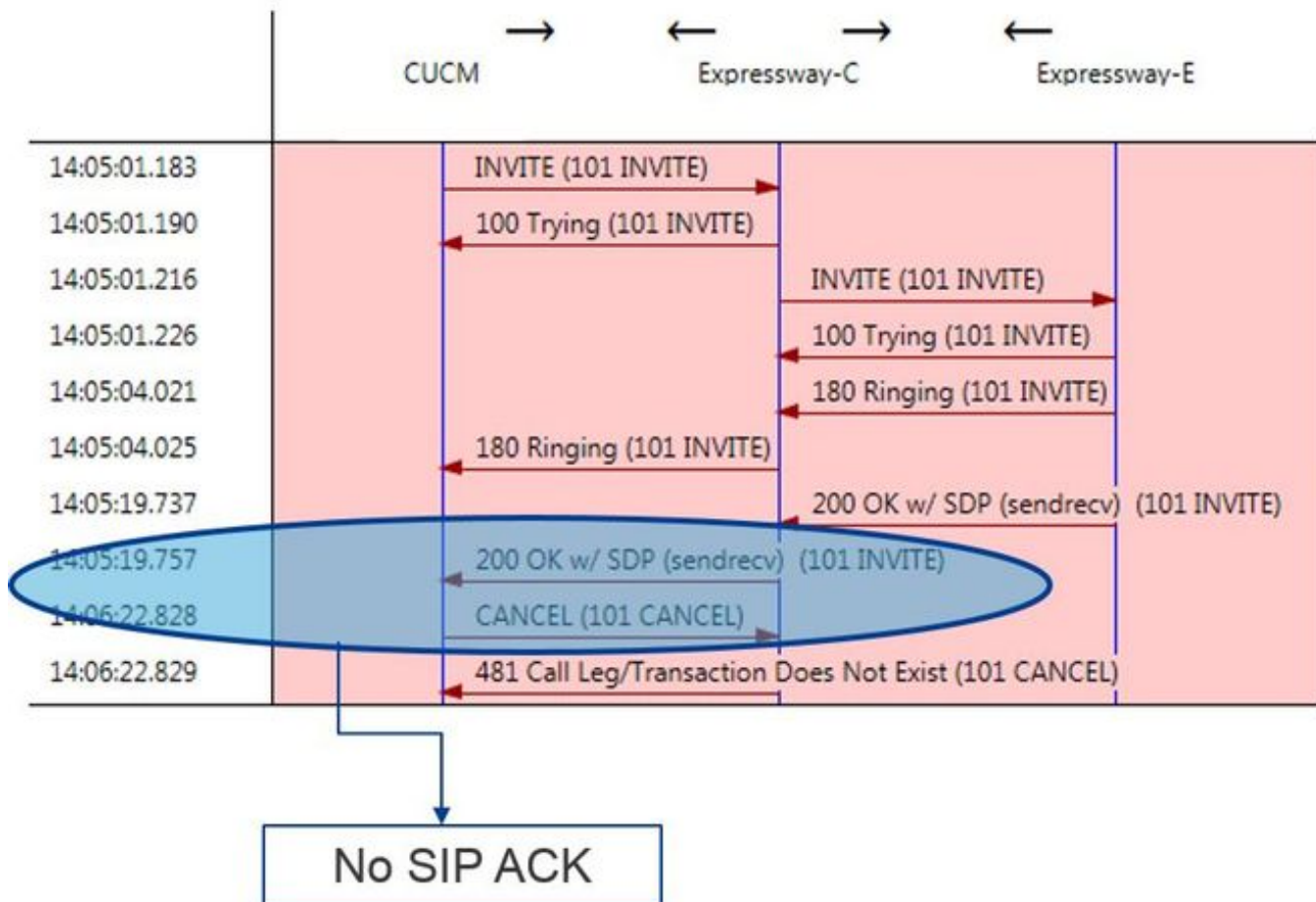
此時，如果您確定使用G.729的關係，則需要調整該關係以支援Cisco Webex使用的受支援的音訊編解碼器，或使用另一個具有支援此功能的區域的裝置池。在上述場景中，確定了以下內容：
Expressway-C中繼區域：保留頻寬Webex-RD區域：RTP裝置
以下是RTP-Devices和ReservingBandwidth區域之間關係的圖形說明，如圖所示。

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

通過更改Expressway-C中繼所在的裝置池，您可以更改Region關係。新的裝置池的區域設定為RTP-Infrastructure，因此Cisco Webex-RD和Expressway-C中繼之間的新區域關係是RTP-Devices和RTP-Infrastructure。如圖所示，您可以看到此關係支援AAC-LD（Cisco Webex支援的音訊編解碼器之一），因此呼叫將正確設定。問題2.超過Unified CM最大傳入消息大小由於影片在企業中越來越普遍，包含SDP的SIP消息的大小已大幅增加。處理這些消息的伺服器必須配置為能夠接受大型資料包。在許多呼叫控制伺服器上，預設值是正常的。使用Cisco Unified Communications Manager(Unified CM)時，過去版本中處理包含SDP的大型SIP消息的預設值是不存在的。在Unified CM的更高版本中，允許的SIP消息值大小已增加，但是此值僅在新安裝而非升級時設定。綜上所述，如果客戶要升級其舊版本的Unified CM以支援混合呼叫服務連線，可能會受到Unified CM上的最大傳入消息大小過低的影響。如果您正在嘗試識別與此問題匹配的混合呼叫服務連線呼叫故障，除Unified CM SDL跟蹤外，還必須獲取Expressway日誌。為了識別故障，首先要瞭解發生了什麼情況，然後瞭解故障可能發生的情形型別。要回答發生什麼的問題，您必須知道，一旦Unified CM收到過大的SIP消息，它就會關閉TCP套接字而不響應Expressway-C。因此，可能出現多種情況及方式：

1. Cisco Webex傳送的傳入INVITEw/ SDP過大。Expressway-C將此消息傳遞到Unified CM，Unified CM關閉TCP套接字，然後SIP對話方塊將超時。
2. Unified CM嘗試將出站呼叫作為Early Offer to Webex，這意味著傳送到Expressway-C的初始INVITE將包含SDP。然後，Cisco Webex會傳送一個200 OK（帶SDP）作為響應，且從Expressway-C傳遞到Unified CM時的200 OK響應太大。Unified CM關閉TCP套接字，然後SIP對話方塊將超時。
3. Unified CM嘗試將出站呼叫作為Delayed Offer to Webex，這意味著傳送到Expressway-C的初始INVITE將不包含SDP。然後，Cisco Webex會傳送一個200 OK和SDP，當從Expressway-C傳遞到Unified CM時，200 OK選項太大。Unified CM關閉TCP套接字，然後SIP對話方塊將超時。

檢視Expressway-C日誌以瞭解此特定情況，有助於了解消息流。如果您使用TranslatorX之類的程式，您可以看到Expressway-C正在將Cisco Webex 200 OK（帶SDP）傳遞到Unified CM。難題是Unified CM永遠不會以SIP ACK進行響應，如圖所示。



由於Unified CM是無法響應的責任方，因此有必要檢視SDL跟蹤以瞭解Unified CM如何處理這種情況。在此方案中，您會發現Unified CM忽略來自Expressway-C的大型消息。將列印此類日誌行專案

```

o
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.

```

在SIP對話方塊超時後，Cisco Webex將向日誌示例中記錄的Expressway-E傳送入站SIP 603拒絕消息。

```

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

```

如前所述，您可以在三種不同的場景中看到此行為。為清楚起見，此圖中所提供的日誌樣本與情況3相匹配，即呼叫作為延遲提議被傳送到出站Cisco Webex。解決方案：

1. 登入到Unified CM。
2. 導覽至System > Service Parameters。
3. 選擇運行Call Manager服務的伺服器。
4. 當系統提示選擇「服務」時，選擇Cisco Call Manager服務。

5. 選擇Advanced選項。
6. 在Clusterwide Parameters(Device - SIP)設定下，將SIP Max Incoming Message Size更改為18000。
7. 選擇儲存。
8. 對運行Cisco Call Manager服務的每個Unified CM節點重複此過程。

附註：要使IP電話、合作終端和/或SIP中繼利用此設定，必須重新啟動該終端。可以單獨重新啟動這些裝置，以最大程度地減少對環境的影響。除非您知道這樣做是完全可以接受的，否則不要重置

CUCM上的每個裝置。**附錄Expressway故障排除工具**檢查模式實用程式Expressway具有模式檢查實用程式，當您希望測試模式是否與特定別名匹配並以預期方式轉換時，該實用程式非常有用。該實用程式可在Expressway上的維護>工具>檢查模式選單選項下找到。最常見的情況是，如果您要測試搜尋規則正規表示式是否將別名與模式字串正確匹配，然後可以選擇執行字串的成功操作，則會使用此方法。對於混合呼叫服務連線，您還可以測試Unified CM集群FQDN是否與為Unified CM集群FQDN設定的模式字串匹配。使用此實用程式時，請記住呼叫將根據路由報頭中列出的Unified CM集群FQDN引數（而不是目標URI）進行路由。例如，如果以下邀請進入Expressway，請根據cucm.rtp.ciscotac.net而不是jorobb@rtp.ciscotac.net測試Check pattern功能。

```
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eeae-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:
```

要使用檢查模式測試混合呼叫服務連線路由報頭搜尋規則路由，請執行以下步驟：

1. 導航到維護>工具>檢查模式。
2. 對於別名，輸入Unified CM集群FQDN。
3. 將Pattern Type設定為Prefix。
4. 將模式字串設定為Unified CM集群FQDN。
5. 將Pattern行為設定為Leave。
6. 選擇Check pattern。

如果Expressway上的搜尋規則配置正確，您將會看到Results return a Succeeded消息。以下是成功的Check模式測試的範例，如下圖所示。

Check pattern

Alias

Alias

Pattern

Pattern type

Pattern string

Pattern behavior

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

成功的原因是，此別名(cucm.rtp.ciscotac.net)與的字首模式字串(cucm.rtp.ciscotac.net)匹配。為了瞭解呼叫如何根據這些結果進行路由，您可以使用描述的Expressway定位實用程式。查詢實用程式如果要測試Expressway能否根據給定別名將呼叫路由到特定區域，Expressway的定位實用程式非常有用。所有這一切都無需實際呼叫即可完成。在Expressway上的Maintenance > Tools > Locate選單下可以找到Locate實用程式。您將看到有關如何使用Expressway-C上的「查詢」功能來確定伺服器是否可以根據SIP路由報頭中的Unified CM集群FQDN路由呼叫的一些說明。

1. 導航到維護>工具>定位。
2. 在「別名」欄位中輸入Unified CM集群FQDN。
3. 選擇SIP作為協定。
4. 為源選擇Cisco Webex混合遍歷客戶端區域。
5. 選擇Locate。

現在，您將在介面底部看到搜尋結果。以下是已執行的範例測試，搭配結果如下圖所示。

Locate

Locate

Alias

Hop count

Protocol

Source

Authenticated

Source alias

以下是定位的結果。粗略計算的是利息價值。結果表明：

- 可以路由別名的事實(True)
- 源資訊 (區域名稱/型別)
- 目標資訊 (正在路由的別名)
- 匹配的搜尋規則 (混合呼叫服務入站路由)
- 呼叫將傳送到的地區(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

診斷日誌記錄無論何時對通過Expressway解決方案的呼叫進行呼叫或媒體問題故障排除，都必須使用診斷日誌記錄。此Expressway功能可為工程師提供大量詳細資訊，瞭解Expressway在呼叫通過時進行的所有邏輯決策。您可以看到全文SIP消息、Expressway如何通過該呼叫以及Expressway如何設定媒體通道。診斷日誌記錄包含許多不同的模組。可以調整日誌記錄級別以顯示致命、錯誤、警告、資訊、調試、跟蹤。預設情況下，所有內容都設定為INFO，幾乎可以捕獲診斷問題所需的所有內容。有時您可能需要將特定模組的日誌記錄級別從「資訊」調整為「調試」，以便更好地瞭解正在發生的情況。以下步驟說明如何調整developer.ssi模組的日誌記錄級別，該模組負責為（相互）TLS握手提供資訊。

1. 登入到Expressway伺服器（必須在Expressway-E和C上完成）。
2. 導航到Maintenance > Diagnostics > Advanced > Support Log configuration。
3. 滾動到要調整的模組（在此例項中為developer.ssi），然後按一下它。
4. 在Level引數旁邊，從選單中選擇DEBUG。
5. 按一下「Save」。

此時，您已準備好捕獲診斷日誌記錄：

1. 登入到Expressway伺服器（必須在Expressway-E和C上完成）。
2. 導航到維護>診斷>診斷日誌記錄。
3. 按一下Start New Log（確保選中tcpdump選項）。
4. 重現問題。
5. 按一下Stop Logging。
6. 按一下「Download Log」。

對於Expressway診斷日誌記錄，請記住，您將並行從Expressway-C和Expressway-E開始日誌記錄：首先，在Expressway-E上開始日誌記錄，然後轉到Expressway-C並啟動日誌記錄。此時，您就可以重現該問題。附註：目前，Expressway/VCS診斷日誌捆綁包不包含有關Expressway伺服器證書或受信任CA清單的資訊。如果您遇到擁有此功能有益的案例，請將您的案例附加到此[缺陷中](#)。

相關資訊

- [Cisco Webex混合呼叫服務部署指南](#)
- [Cisco Webex混合設計手冊](#)

- [Cisco Expressway管理員指南](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。