Guida alla risoluzione dei problemi per Cisco Webex Hybrid Call Service Connect

Sommario

Informazioni correlate

Introduzione

Questo documento descrive la soluzione Cisco Webex Hybrid Call Service Connect che consente all'infrastruttura di controllo delle chiamate Cisco esistente di connettersi a Cisco Collaboration Cloud in modo che possano funzionare insieme.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza dell'offerta Cisco Webex
- Conoscenza della soluzione Expressway (B2B)
- Conoscenza di Cisco Unified Communications Manager (Unified CM) e relativa integrazione con Expressway
- Unified CM 10.5(2) SU5 o versioni successive.
- Expressway (B2B) versione X8.7.1 o successiva (si consiglia X8.9.1)
- Expressway (Connector Host): per le versioni attualmente supportate, vedere Supporto di Expressway Connector Host per Cisco Webex Hybrid Services

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Unified Communications Manager
- Expressways
- Webex per Windows
- Webex per Mac
- Webex per iOS
- Webex per Android
- Endpoint Cisco Collaboration
- Endpoint Collaboration da scrivania
- Telefoni IP
- Software client

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La soluzione offre le seguenti funzionalità:

- Usa l'app Webex come soft client per dispositivi mobili per chiamate audio e video
- Usa l'app per effettuare e ricevere chiamate da qualsiasi luogo, come se si trovassero in ufficio
- Usa Webex, Cisco Jabber o il loro telefono da tavolo per chiamare, senza preoccuparti di quale opzione usano
- Sbloccare la cronologia delle chiamate nei telefoni locali e integrarla in Webex

Scopo di questa guida è trattare i problemi specifici di Hybrid Call Service Connect. Poiché Hybrid Call Service Connect viene eseguito sulla stessa coppia E & C Expressway di altre soluzioni, ad esempio l'accesso remoto e mobile e le chiamate Business to Business, i problemi con le altre soluzioni possono influire su Hybrid Call Service Connect. Per i clienti e i partner che distribuiscono una coppia Expressway da utilizzare con Call Service Connect, è necessario fare riferimento alla guida alla configurazione base di Cisco VCS Expressway e VCS Control prima di tentare di distribuire Hybrid Call Service Connect. La presente guida alla risoluzione dei problemi descrive le considerazioni su Firewall/NAT e il progetto Expressway nelle appendici 3 e 4. Consultare la presente documentazione. Inoltre, in questo documento si presume che l'host del connettore Expressway e l'attivazione del servizio Hybrid Call siano state completate.

Problemi di configurazione delle chiamate

Errori di handshake TLS reciproci

Hybrid Call Service Connect utilizza la mutua TLS (Transport Layer Security) per l'autenticazione tra Cisco Webex e Expressway-E. Ciò significa che Expressway-E e Cisco Webex controllano e ispezionano i rispettivi certificati. Poiché i problemi TLS reciproci sono così diffusi durante le nuove installazioni dei server Expressway e l'abilitazione di soluzioni come Hybrid Call Service Connect, questa sezione fornisce informazioni utili e suggerimenti per la risoluzione dei problemi basati sui certificati tra Expressways e Cisco Webex.

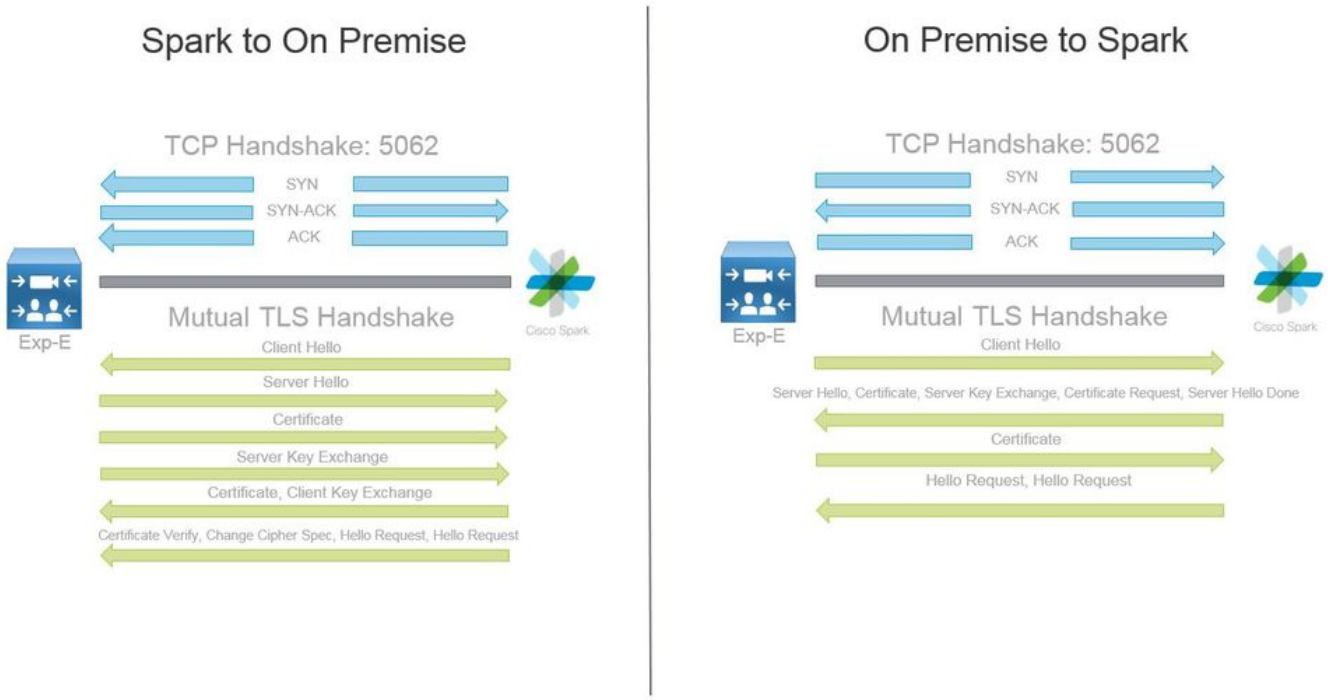
Che cosa controlla Expressway-E?

- Il certificato Cisco Webex è stato firmato da una CA pubblica elencata nell'elenco delle CA attendibili di Expressway-E?
- Nel campo Subject Alternate Name (Nome alternativo soggetto) del certificato Cisco Webex è presente callservice.ciscospark.com?

Cosa controlla Cisco Webex?

- Il certificato Expressway-E è stato firmato da una delle CA pubbliche considerate attendibili da Webex? (Cisco Webex Trusted CA List)
- Se Expressway-E non utilizza un certificato firmato pubblicamente, il certificato Expressway insieme a tutti i certificati radice e intermedi sono stati caricati in Cisco Webex Control Hub (https://admin.ciscospark.com)?

Questo viene spiegato come mostrato nell'immagine.



Suggerimenti utili per la risoluzione dei problemi Mutual TLS

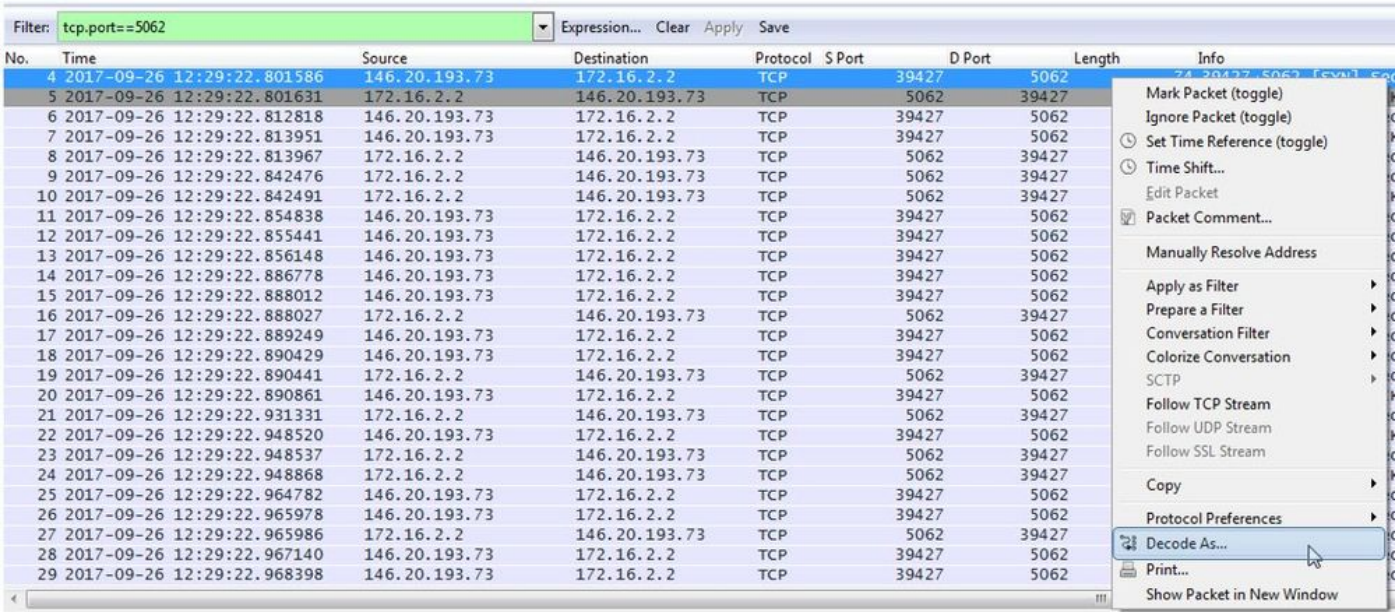
1. Decodifica handshake TLS reciproco

Per impostazione predefinita, Wireshark contrassegna il traffico TLS SIP come porta 5061. Ciò significa che ogni volta che si desidera analizzare un handshake TLS (reciproco) che si verifica sulla porta 5062, Wireshark non saprà come decodificare correttamente il traffico. Di seguito è riportato un esempio dell'handshake TLS reciproco che si verifica sulla porta 5062, come mostrato nell'immagine.

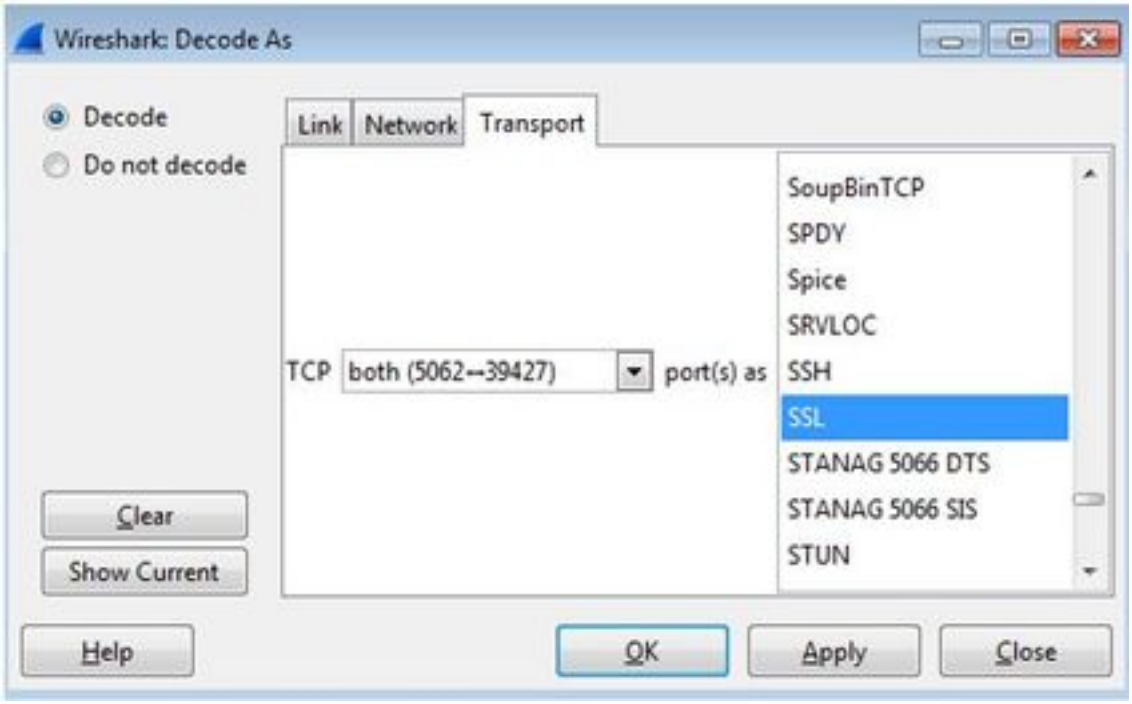
Come si può vedere, questo è l'aspetto della stretta di mano con le impostazioni predefinite in Wireshark. Il pacchetto numero 175 è il certificato che Expressway invia a Cisco Webex. Tuttavia, non è possibile determinarlo senza decodificare il traffico. Esistono due metodi per decodificare il traffico in modo da poter visualizzare più facilmente le informazioni sul certificato e gli eventuali messaggi di errore presenti.

1 bis. Decodifica flusso come SSL

r. Quando si analizza l'handshake TLS reciproco, filtrare prima l'acquisizione in base a **tcp.port==5062**. Quindi, fare clic con il pulsante destro del mouse sul primo pacchetto nel flusso e selezionare **Decodifica con nome...** come mostrato nell'immagine.



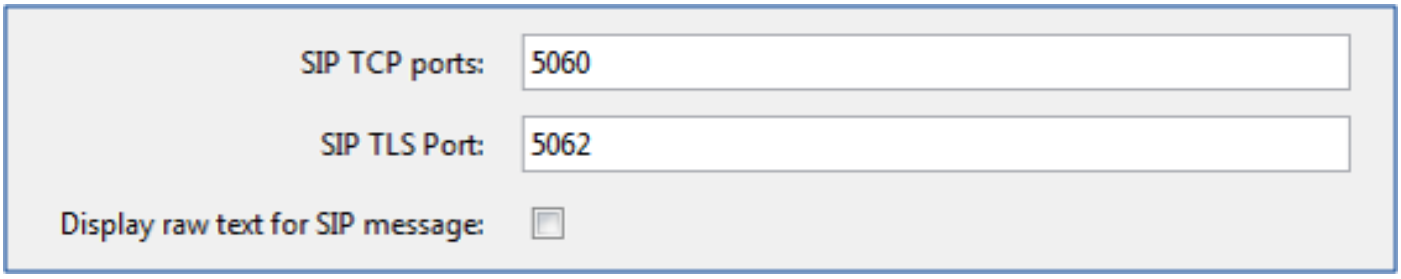
b. Una volta selezionata l'opzione **Decodifica con nome**, viene visualizzato un elenco in cui è possibile selezionare la modalità di decodifica del flusso selezionato. Dalla lista, selezionare **SSL,** fare clic su **Applica**, quindi chiudere la finestra. A questo punto, l'intero flusso mostra il certificato e i messaggi di errore scambiati al momento dell'handshake, come mostrato nell'immagine.



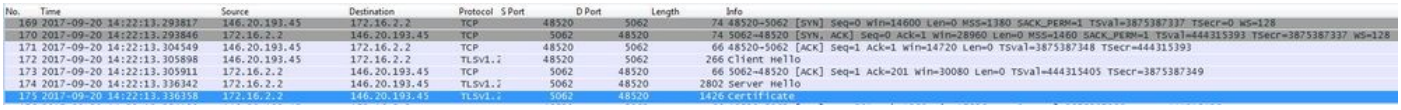
1 ter. Regola porta SIP TLS

Quando si regola la porta SIP TLS su 5062 nelle preferenze di Wireshark, è possibile visualizzare tutti i dettagli che circondano l'handshake, inclusi i certificati. Per apportare tale modifica:

- Apri Wireshark
- Selezionare **Modifica > Preferenze**
- Espandere Protocolli e selezionare **SIP**
- Impostare la porta TLS SIP su 5062 e fare clic su **Apply**
- Impostate nuovamente il valore su 5061 al termine dell'analisi, come mostrato nell'immagine.



Se analizziamo ora la stessa cattura, vedrete i pacchetti da 169 a 175 decodificati. Il pacchetto 175 mostra il certificato Expressway-E e se si espande il pacchetto, è possibile visualizzare tutti i dettagli del certificato, come mostrato nell'immagine.



2. Filtraggio Wireshark

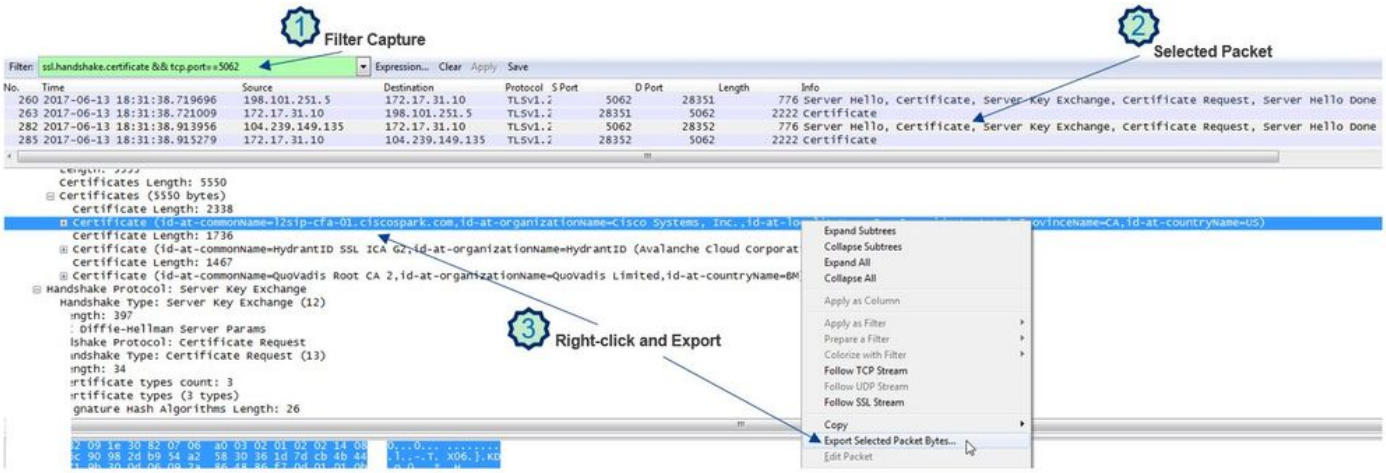
Quando si analizzano le acquisizioni dei pacchetti, è facile perdersi nella quantità di pacchetti osservati in una determinata acquisizione. È importante capire a quale tipo di traffico sei più interessato in modo da poter filtrare Wireshark per visualizzare solo questo. Di seguito sono riportati alcuni filtri Wireshark comuni che possono essere utilizzati per ottenere dettagli su un handshake TLS reciproco:

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

3. Estrai certificato da Pcap

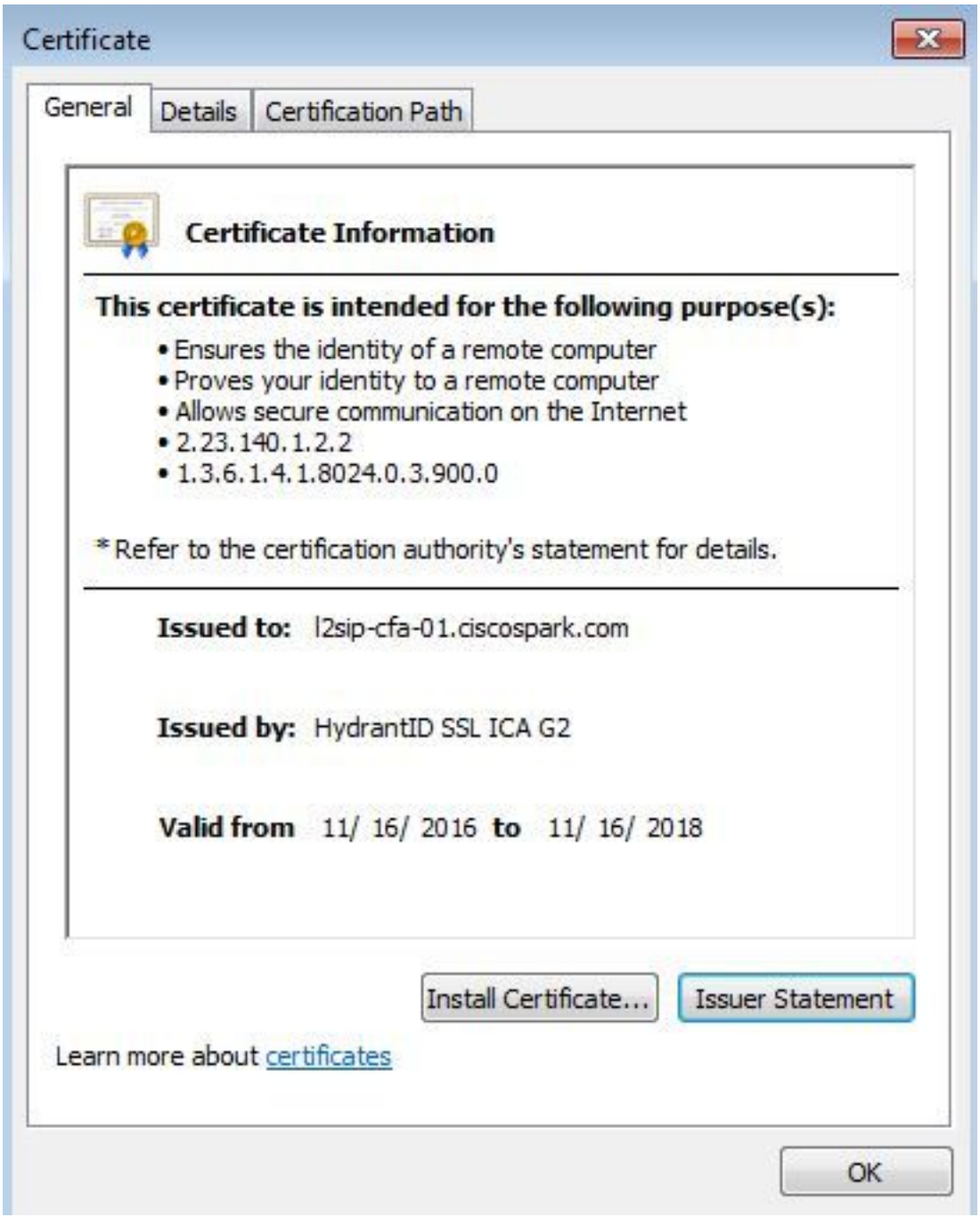
Occasionalmente potrebbe essere necessario ottenere una copia di un certificato (server, radice o intermediario). Se non si sa dove trovare il certificato cercato, è possibile estrarlo direttamente da un'acquisizione pacchetto. Di seguito vengono riportati i passaggi per ottenere il certificato Cisco Webex presentato in un handshake TLS reciproco.

1. Filtrare l'acquisizione del pacchetto con **ssl.handshake.certificate && tcp.port==5062**
2. Individuare il pacchetto originato dall'indirizzo del server Webex su cui è stampato il certificato nella sezione Info.
3. Nei dettagli del pacchetto, espandere **Secure Socket Layer > Certificato TLS > Protocollo handshake > Certificati**. **Nota:** L'ultimo certificato nella catena è la CA radice.
4. Fare clic con il pulsante destro del mouse sul certificato di interesse e selezionare **Esporta byte pacchetto selezionato**... come mostrato nell'immagine.



5. Salvare il file come **file con estensione cer**.

6. Fare doppio clic sul file salvato per aprire il certificato come mostrato nell'immagine.



4. Regolare i livelli di registrazione di Expressway

In Expressway sono disponibili due moduli di registrazione che consentono di comprendere meglio la logica eseguita da Expressway durante l'analisi dei certificati:

- developer.ssl
- developer.zone.zonemg

Per impostazione predefinita, questi moduli di registrazione sono impostati su un livello INFO. Quando è impostato su un livello DEBUG, è possibile iniziare a visualizzare le informazioni relative all'ispezione del certificato eseguita, insieme alla zona a cui viene mappato il traffico. Entrambe queste funzioni sono rilevanti per il servizio Hybrid Call.

Esempio di Expressway-E che esegue un'ispezione SAN del certificato server di Cisco Webex.

```
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"
```

Esempio di mapping Expressway-E della connessione MTLS alla zona DNS ibrida Cisco Webex:

```
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1226)"
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
```

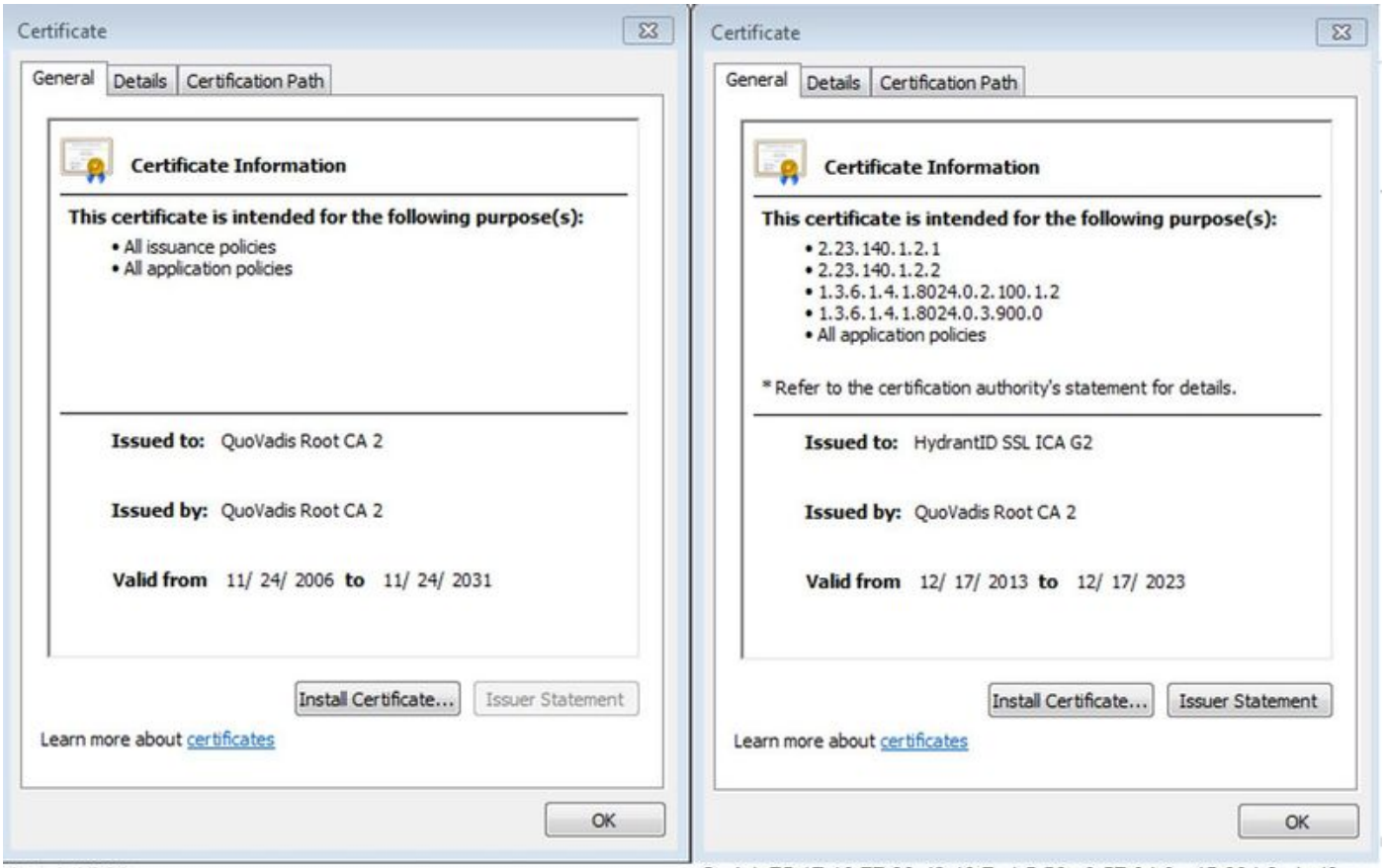
this="0x56408ff81220" **getDNSZoneByTLSVerifySubjectName classified subject name callservice.ciscospark.com into DNS zone Hybrid Call Services DNS**
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.zone.zonemgr" Level="DEBUG" CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1183)"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

Di seguito è riportato un elenco dei problemi più comuni relativi ai guasti TLS reciproci tra Expressway-E e Cisco Webex.

Problema 1. Expressway-E non considera attendibile l'Autorità di certificazione (CA) che ha firmato il certificato Cisco Webex

Il server Cisco Webex in comunicazione diretta con Expressway-E è denominato server L2SIP. Questo server L2SIP deve essere firmato da un server intermedio con un nome comune **Hydrant SSL ICA G2**. L'intermediario deve essere firmato da un'autorità di certificazione radice con un nome comune **QuoVadis Root CA 2** come mostrato nell'immagine.

> **Nota:** Questo potrebbe essere soggetto a cambiamenti.



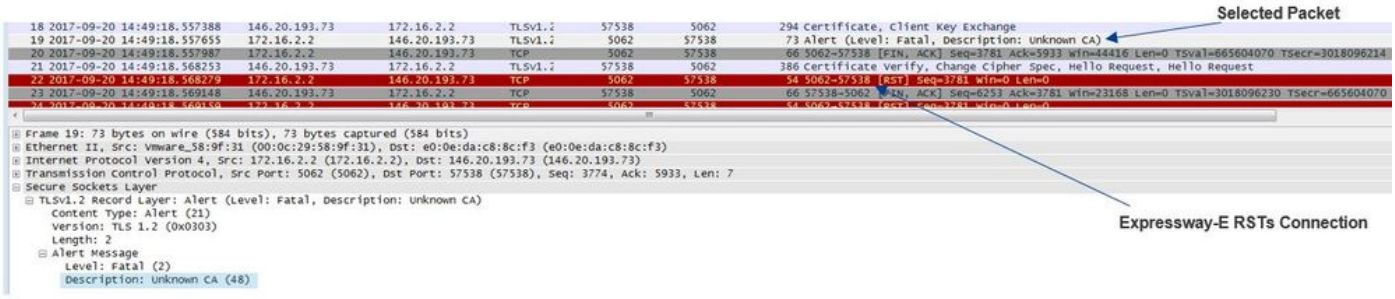
Il primo passaggio per analizzare questo traffico dalla prospettiva diagnostica di Expressway è la ricerca di **TCP Connecting**. Dopo aver eseguito la ricerca in **TCP Connecting**, verrà cercato il valore **Dst-port=5062**. Dopo aver identificato l'area nei log in cui è stata tentata e stabilita la connessione, è possibile cercare l'handshake TLS, in genere indicato dalle voci di log che indicano che l'handshake è in corso.

```
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"
```

Se Expressway-E non considera attendibili i certificati Cisco Webex firmati, è possibile prevedere che Expressway-E possa rifiutare il certificato subito dopo il completamento dell'handshake. È possibile individuare questa condizione nella registrazione di Expressway-E dalle seguenti voci di registro:

```
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="::TTSSLErrorOutput" 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"
```

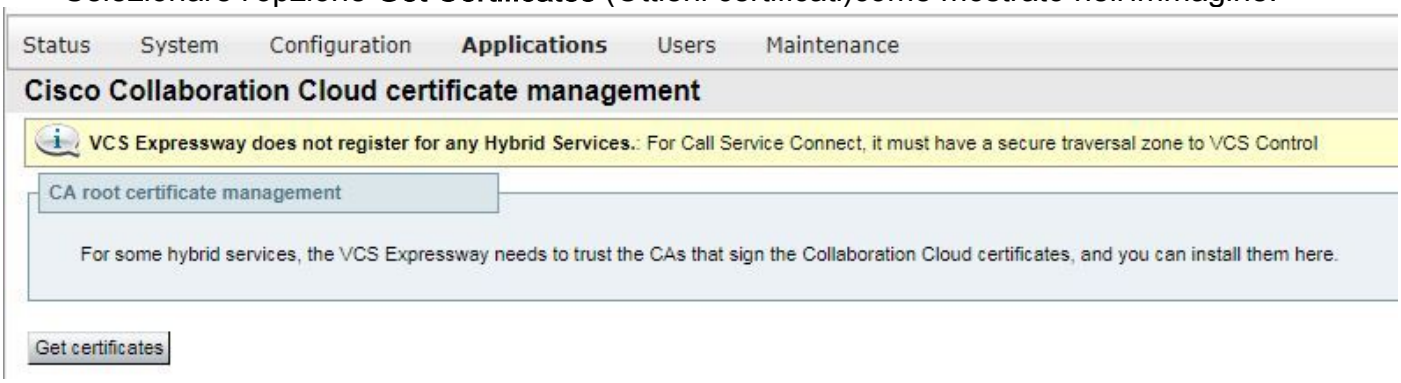
Il messaggio di errore di Expressway può essere leggermente fuorviante in quanto fa riferimento a un certificato autofirmato nella catena di certificati. Wireshark vi permette di osservare da vicino lo scambio. Dal punto di vista dell'analisi dell'acquisizione dei pacchetti Wireshark, è possibile vedere chiaramente che quando l'ambiente Webex presenta il proprio certificato, Expressway si attiva e rifiuta con un certificato contenente un errore CA sconosciuto, come mostrato nell'immagine.



Soluzione:

Per risolvere questa situazione, è necessario verificare che Expressway-E consideri attendibili le autorità di certificazione Cisco Webex. Sebbene sia sufficiente estrarre questi certificati da una traccia Wireshark e caricarli nell'archivio certificati CA attendibile in Expressway, Expressway offre un metodo più semplice:

- Accedere a Expressway-E
- Selezionare **Applicazioni > Gestione certificati cloud**
- Selezionare l'opzione **Get Certificates** (Ottieni certificati)come mostrato nell'immagine.



A questo punto, le autorità di certificazione Cisco Webex vengono caricate nell'archivio delle CA attendibili di Expressway-E **(Manutenzione > Sicurezza > Certificato CA attendibile)**.

Problema 2. Nome non corretto per il nome di verifica del soggetto TLS nella zona DNS ibrida Expressway-E Cisco Webex

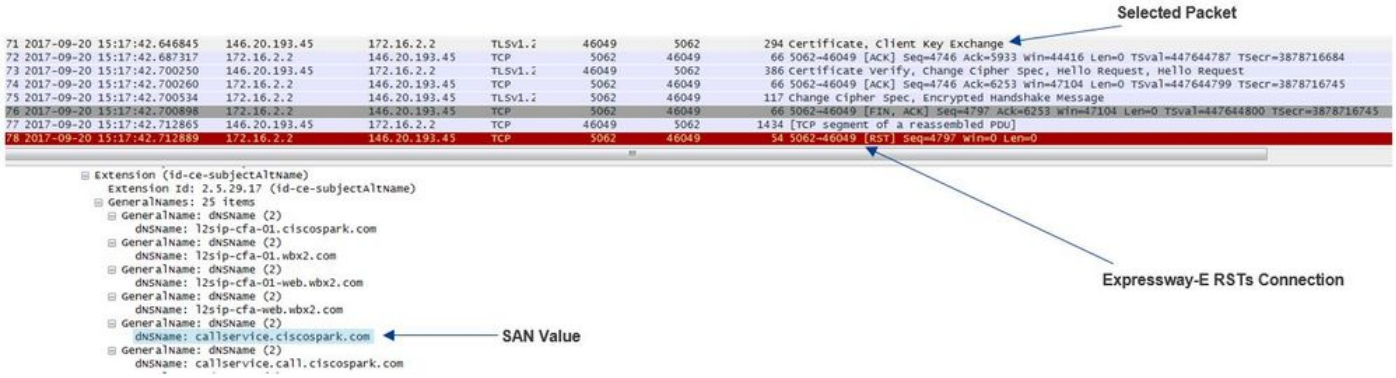
Nell'ambito dell'handshake TLS reciproco, Hybrid Call Service Connect utilizza la verifica TLS. Ciò significa che oltre a considerare attendibili i certificati Cisco Webex CA, Expressway verifica il certificato verificando il campo Nome alternativo soggetto (SAN) del certificato presentato per assicurarsi che abbia un valore come **callservice.ciscospark.com** presente. Se questo valore non è presente, la chiamata in ingresso non riesce.

In questo particolare scenario, il server Cisco Webex presenta il proprio certificato a Expressway-E. Il certificato ha in realtà 25 SAN diverse. Si consideri il caso in cui Expressway-E controlla il certificato per la SAN callservice.ciscospark.com ma non lo trova. Quando questa condizione viene soddisfatta, è possibile visualizzare un errore simile a questo all'interno della registrazione

diagnostica:

```
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"
```

Se si utilizza Wireshark per analizzare l'handshake con certificato, è possibile notare che dopo la presentazione del certificato da parte di Cisco Webex, Expressway RST effettua la connessione subito dopo, come mostrato nell'immagine.



Per confermare la configurazione di questo valore, è possibile passare alla zona DNS ibrida Webex configurata per la soluzione. Se si dispone di Expressway-E xConfiguration, è possibile cercare la sezione di configurazione Zona per determinare come è stato configurato il nome soggetto della verifica TLS. Per xConfiguration, si noti che le zone sono ordinate in base all'ordine della Zona 1. Di seguito è riportata una configurazione x dall'ambiente problematico analizzato sopra.

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

Come si può vedere nell'esempio, il campo TLS Verify Subject Name (Verifica nome soggetto) è impostato su **callservice.ciscospark.com** anziché su **callservice.ciscospark.com**. (notare la lettera "l" extra).

Soluzione:

Per risolvere il problema, è necessario modificare il nome soggetto della verifica TLS:

- Accedere a Expressway-E
- Selezionare **Configurazione > Zone > Zone**
- Seleziona **zona DNS servizi ibridi Webex**
- Impostare il **nome soggetto di verifica TLS** su **callservice.ciscospark.com**
- Selezionare **Salva**

Nota: Per informazioni sul comportamento della registrazione di base, vedere la. Questa sezione illustra Expressway che esegue la verifica dei certificati e il mapping alla zona DNS ibrida Webex.

Nota: A partire dal codice Expressway x12.5 e successivamente è stata rilasciata una nuova zona "Webex". Questa zona Webex prepopola la configurazione della zona necessaria per la comunicazione con Webex. Ciò significa che non è più necessario impostare la modalità di verifica del soggetto TLS e il nome del soggetto di verifica TLS. Per semplificare la configurazione, si consiglia di utilizzare la zona Webex se si esegue x12.5 o versioni successive del codice Expressway.

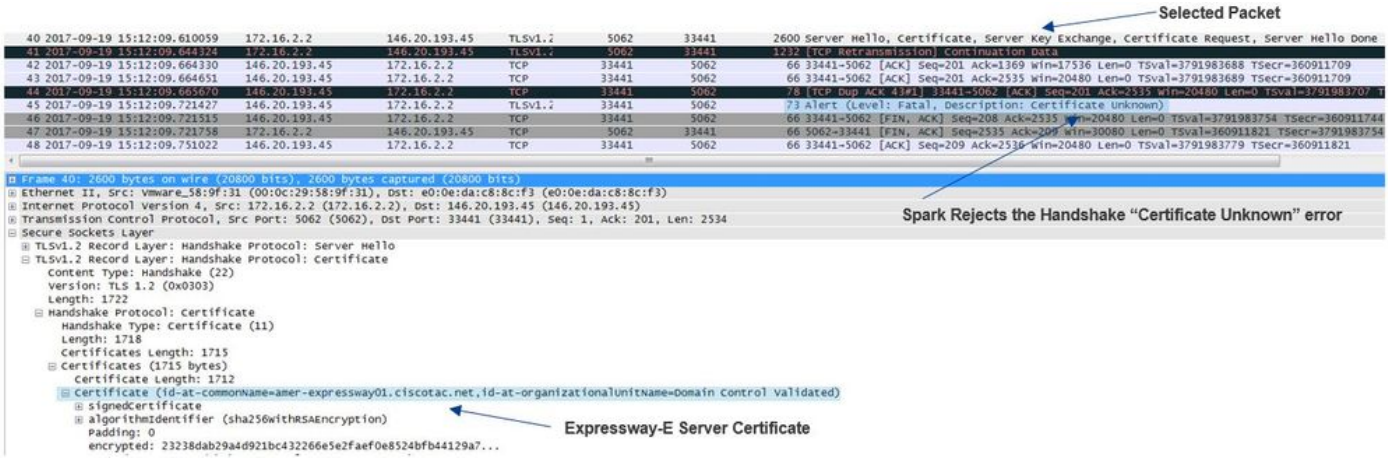
Problema 3. Expressway-E non invia una catena di certificati completa a Cisco Webex

Come parte dell'handshake TLS reciproco, Cisco Webex deve considerare attendibile il certificato Expressway-E. Cisco Webex ha un elenco completo delle CA pubbliche affidabili. In genere, un handshake TLS ha esito positivo quando il certificato Expressway-E è firmato da una CA pubblica supportata da Cisco Webex. In base alla progettazione, Expressway-E invia il proprio certificato solo durante un handshake TLS nonostante sia stato firmato da una CA pubblica. Per inviare l'intera catena di certificati (radice e intermedio), è necessario aggiungere tali certificati all'archivio certificati CA attendibile in Expressway-E.

Se questa condizione non viene soddisfatta, Cisco Webex rifiuta il certificato Expressway-E. Quando si risolve un problema relativo a una condizione, è possibile utilizzare i registri diagnostici e tcpdump di Expressway-E. Quando si analizzano i registri diagnostici di Expressway-E, verrà visualizzato un errore simile a quello riportato di seguito:

```
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"
```

Se analizzate questo dal punto di vista di Wireshark, vedrete che Expressway-E presenta il suo certificato. Se si espande il pacchetto, si noterà che viene inviato solo il certificato del server. Cisco Webex rifiuta quindi questo handshake TLS con un messaggio di errore CA sconosciuto, come mostrato nell'immagine.

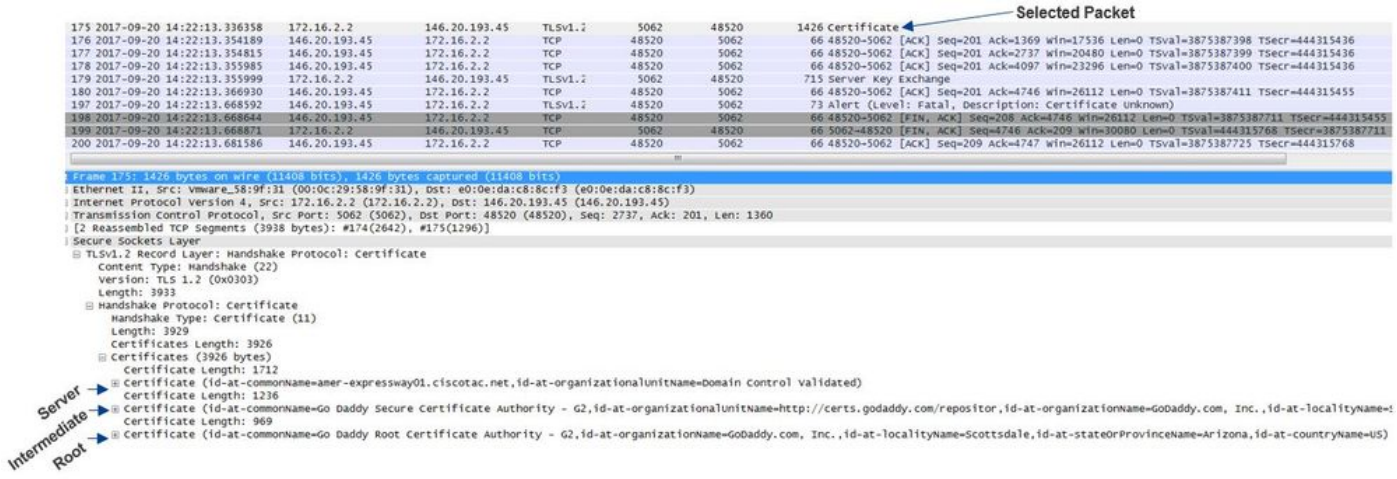


Soluzione:

Per risolvere il problema in questo scenario, è necessario caricare le CA intermedie e radice coinvolte nella firma del certificato Expressway-E nell'archivio certificati delle CA attendibili:

Passaggio 1. Accedere a Expressway-E.
Passaggio 2. Passare a **Manutenzione > Sicurezza > Certificato CA attendibile**.
Passaggio 3. Selezionare **Scegli file** dal menu Carica nella parte inferiore dell'interfaccia utente.
Passaggio 4. Scegliere il certificato CA coinvolto nella firma di Expressway-E.
Passaggio 5. Selezionare **Aggiungi certificato CA**.
Passaggio 6. Ripetere i passaggi per tutti i certificati CA coinvolti nella firma del certificato Expressway-E (intermedio, radice).
Passaggio 7. Selezionare **Aggiungi certificato CA**.

Al termine di questo processo, sarà possibile verificare che l'intera catena di certificati coinvolti nella firma del certificato del server Expressway-E è inclusa nello scambio di chiave. Ecco un esempio di quello che vedreste analizzando un pacchetto catturato con Wireshark.



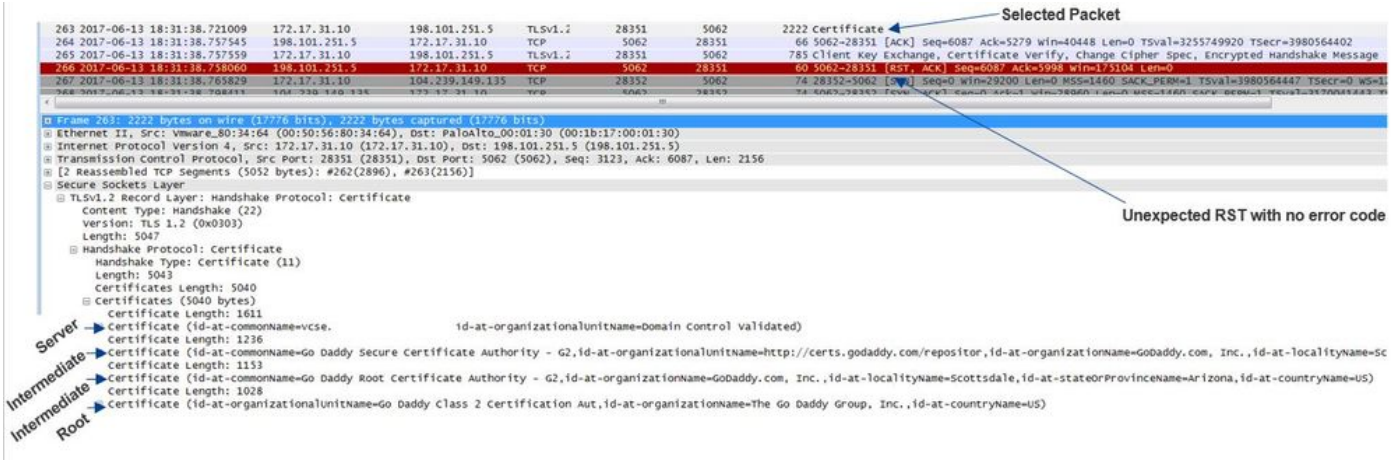
Problema 4. Il firewall termina l'handshake TLS reciproco

La soluzione Expressway in genere si interfaccia con un firewall. Spesso, il firewall in linea per la soluzione esegue un tipo di ispezione a livello di applicazione. Spesso con la soluzione Expressway, quando il firewall esegue l'ispezione a livello di applicazione, gli amministratori possono vedere risultati indesiderati. Questo particolare problema consente di identificare quando l'ispezione a livello di applicazione di un firewall interrompe improvvisamente la connessione.

Utilizzando i log di diagnostica di Expressway, è possibile cercare l'handshake Mutual TLS tentato. come accennato in precedenza, questa handshake deve essere eseguita poco dopo la connessione TCP sulla porta 5062. In questo scenario, quando il firewall interrompe la connessione, questi errori vengono visualizzati nella registrazione diagnostica.

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

Dal punto di vista dell'acquisizione dei pacchetti, vedrai che Expressway-E presenta il suo certificato a Cisco Webex. Si vede un RST TCP provenire dalla direzione di Cisco Webex, come mostrato nell'immagine.



A prima vista, si potrebbe pensare che qualcosa non vada con il certificato Expressway-E. Per risolvere questo problema, è necessario innanzitutto determinare le risposte alle seguenti domande:

- Expressway-E è firmato da una CA pubblica considerata attendibile da Cisco Webex?
- Il certificato Expressway-E e tutti i certificati coinvolti nella firma del certificato Expressway-E vengono caricati manualmente in Cisco Webex Control Hub (https://admin.ciscospark.com)?

In questa particolare condizione, la soluzione non consisteva nell'utilizzare Cisco Webex Control Hub per gestire i certificati Expressway-E. Il certificato Expressway-E deve essere firmato da un'autorità di certificazione pubblica considerata attendibile da Cisco Webex. Selezionando il pacchetto Certificate nell'acquisizione Wireshark (come mostrato sopra), si osserverà che il certificato è stato firmato da una CA pubblica e che l'intera catena è stata inviata a Cisco Webex. Pertanto, il problema non deve essere correlato al certificato Expressway-E.

A questo punto, se è necessario un ulteriore isolamento, è possibile trasferire un pacchetto dall'interfaccia esterna del firewall. Tuttavia, la mancanza di errore SSL nel registro diagnostico è un punto dati importante. Se si ricorda quanto sopra (Numero 3.1), se Cisco Webex non considera attendibile il certificato Expressway-E, è necessario visualizzare un motivo di disconnessione SSL. In questa condizione non è disponibile alcun errore SSL.

> **Nota:** Se si dovesse acquisire un pacchetto dal firewall all'esterno dell'interfaccia, non si vedrebbe un RST TCP provenire dall'ambiente Cisco Webex.

Soluzione

Per questa particolare soluzione, i partner o i clienti devono affidarsi al team di sicurezza. Il team deve verificare se viene utilizzato un tipo qualsiasi di controllo a livello di applicazione per la soluzione Expressway e, in caso affermativo, è necessario disattivare questa funzionalità. Nell'Appendice 4 della **Guida alla distribuzione di VCS Control and Expressway** viene illustrato il motivo per cui è consigliabile disattivare questa funzionalità.

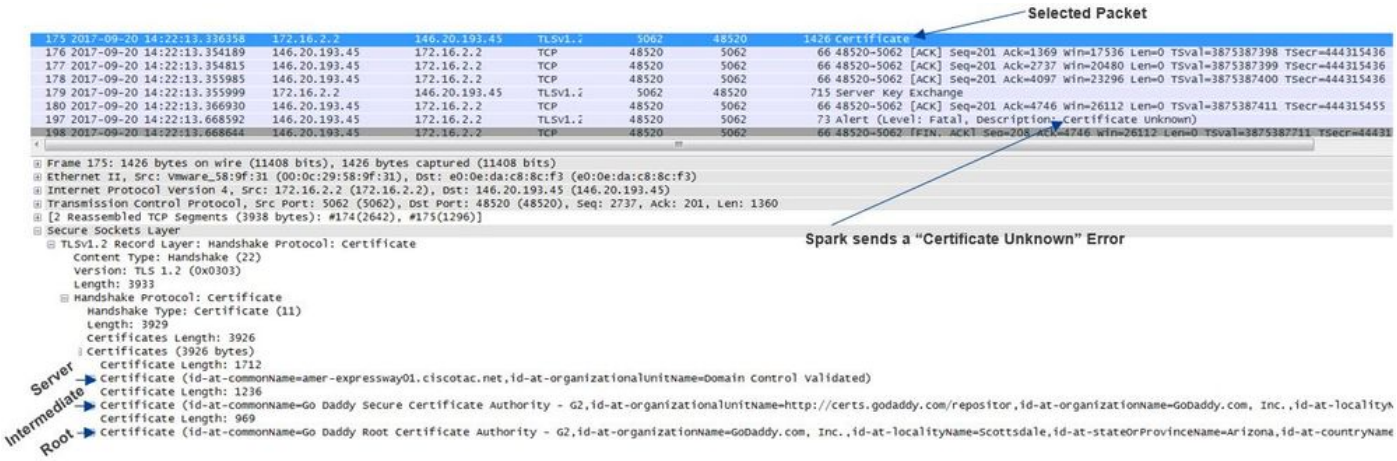
Numero 5. Expressway-E è firmato da una CA pubblica, ma Cisco Webex Control Hub ha caricato certificati alternativi

Questa condizione può spesso verificarsi quando si distribuisce la soluzione Expressway da zero e non si dispone inizialmente del certificato Expressway-E firmato da una CA pubblica. In questo scenario viene caricato il certificato del server Expressway-E (firmato internamente) in Cisco Webex Control Hub per completare correttamente la negoziazione TLS reciproca. In seguito, si ottiene il certificato Expressway-E firmato da una CA pubblica, ma si dimentica di rimuovere il certificato del server da Cisco Webex Control Hub. È importante sapere che quando un certificato viene caricato in Cisco Webex Control Hub, ha la priorità sul certificato e sulla catena presentati da Expressway durante l'handshake TLS.

Dal punto di vista della registrazione diagnostica di Expressway-E, questo problema può avere un aspetto simile alla firma di registrazione soddisfatta quando Cisco Webex non considera attendibile il certificato Expressway-E, ad esempio nel caso in cui Expressway-E non invii l'intera catena o il certificato Expressway-E non sia firmato da una CA pubblica considerata attendibile da Cisco Webex. Di seguito è riportato un esempio di quanto ci si può aspettare nella registrazione di Expressway-E durante l'handshake TLS:

```
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="::TTSSLErrorOutput" 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"
```

Dal punto di vista di Wireshark, è possibile osservare che Expressway-E presenta il proprio certificato alla voce 175. Dopo alcune righe, l'ambiente Cisco Webex rifiuta il certificato con un errore Certificate Unknown (Certificato sconosciuto), come mostrato nell'immagine.



Se si seleziona il pacchetto di certificato inviato da Expressway-E, è possibile espandere le informazioni sul certificato per determinare se Expressway-E

1. sia firmato da una CA pubblica considerata attendibile da Cisco Webex, e

2. è compresa la sua catena completa coinvolta nella firma.

In questa situazione, entrambe le condizioni sono soddisfatte. Ciò suggerisce che non c'è nulla di sbagliato nel certificato Expressway-E.

Soluzione

Passaggio 1. Accedere a Cisco Webex Control Hub.
Passaggio 2. Selezionare **Servizi** dal riquadro di sinistra.

Passaggio 3. Scegliere **Impostazioni** sotto la scheda Hybrid Call.

Passaggio 4. Scorrere fino alla sezione Call Service Connect (Connessione al servizio di chiamata) ed esaminare la sezione Certificati per chiamate SIP crittografate per verificare se sono elencati certificati indesiderati. In tal caso, fare clic sull'icona del cestino accanto al certificato.

passaggio 5. Selezionare **Rimuovi**.

> **Nota:** È importante eseguire l'analisi e verificare che il cliente non stia utilizzando i certificati caricati in Webex Control Hub prima di rimuoverli.

Per ulteriori informazioni sul caricamento del certificato Expressway-E in Cisco Webex Control Hub, vedere questa sezione della Guida alla distribuzione delle chiamate ibride.

Problema 6. Expressway non esegue il mapping della chiamata in ingresso alla zona DNS ibrida Cisco Webex

La funzionalità di mapping TLS in ingresso funziona in combinazione con il nome soggetto di verifica TLS, entrambi configurati nella zona DNS della chiamata ibrida. In questo scenario vengono illustrati problemi e problematiche osservati con Expressway prima di x12.5. In x12 e versioni successive è stato implementato un nuovo tipo di zona denominato "Webex". Questa zona pre-popola tutta la configurazione richiesta per l'integrazione con Webex. Se si esegue x12.5 e si distribuisce Webex Hybrid Call, si consiglia di utilizzare il tipo di zona **Webex** in modo che il dominio dei servizi di chiamata ibrida (callservice.webex.com) sia configurato automaticamente. Questo valore corrisponde al nome soggetto alternativo del certificato Webex presentato durante l'handshake TLS reciproco e consente la connessione e il mapping in ingresso nell'Expressway.

Se si utilizza una versione di codice inferiore a x12.5 o non si utilizza la zona Webex, procedere con la spiegazione seguente che mostra come identificare e correggere i problemi in cui Expressway non esegue il mapping della chiamata in entrata alla zona DNS ibrida Webex.

La funzione si suddivide in tre fasi:

1. Expressway-E accetta il certificato Cisco Webex.
2. Expressway-E controlla il certificato Cisco Webex per determinare se esiste un nome soggetto alternativo che corrisponde al nome soggetto di verifica TLS: callservice.ciscospark.com.
3. Expressway-E esegue il mapping della connessione in entrata tramite la zona DNS ibrida Cisco Webex.

Se l'autenticazione ha esito negativo, la convalida del certificato non è riuscita. La chiamata entra nella zona predefinita e viene instradata in base alle regole di ricerca fornite per gli scenari business-to-business, se business-to-business è configurato su Expressway-E.

Come negli altri scenari, è necessario usare sia la registrazione diagnostica che le acquisizioni dei pacchetti per determinare l'aspetto dell'errore, quindi usare l'acquisizione dei pacchetti per vedere da che parte sta inviando l'RST. Di seguito è riportato un esempio della connessione TCP che si sta tentando di stabilire.

```
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"
```

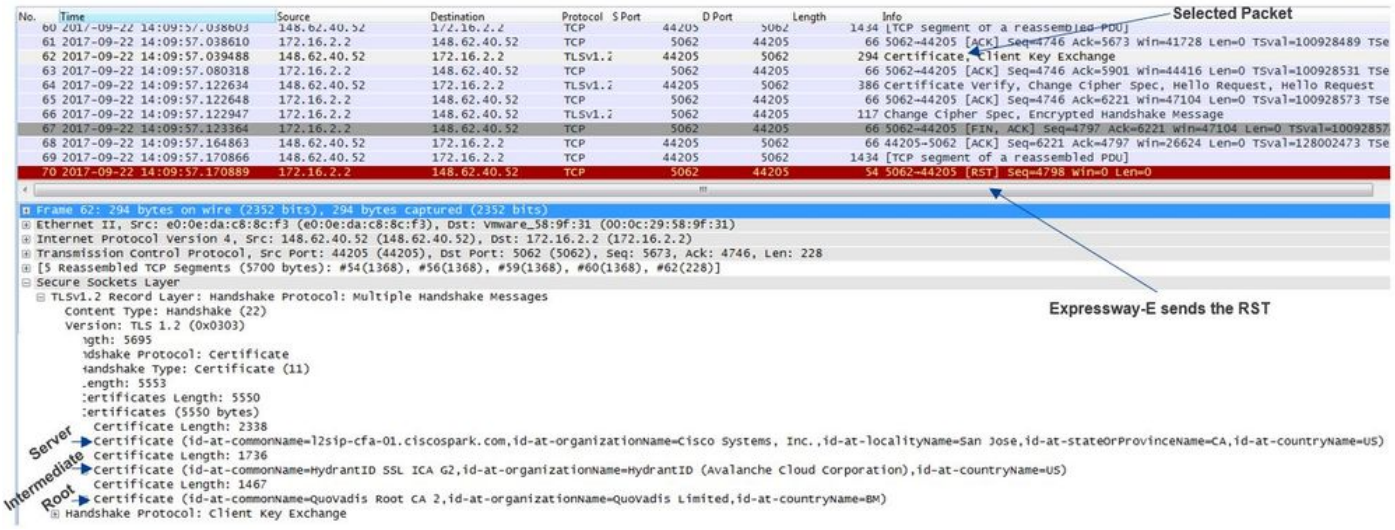
Ora che la connessione TCP è stata stabilita, è possibile eseguire l'handshake TLS. Potete vedere che poco dopo l'avvio della stretta di mano, si verifica rapidamente un errore.

```
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"
```

Osservando la situazione da una prospettiva basata sulla PAC, si può avere un'idea migliore

- chi invia l'RST e
- quali certificati vengono passati per determinare se sono corretti.

Quando si analizza questa particolare acquisizione, è possibile notare che Expressway-E invia l'RST. Se si controlla il certificato Cisco Webex passato, si osserverà che invia l'intera catena. Inoltre, è possibile concludere che, in base al messaggio di errore nel log di diagnostica, è possibile escludere lo scenario in cui Expressway-E non considera attendibili le CA pubbliche Cisco Webex. In caso contrario, verrà visualizzato un errore come "**certificato autofirmato nella catena di certificati**". È possibile esaminare i dettagli del pacchetto come mostrato nell'immagine.



Fare clic sul certificato del server Webex ed espanderlo per visualizzare i nomi soggetto alternativi (dnsName) che è possibile verificare per verificare che **callservice.ciscospark.com sia** elencato.

Selezionare **Wireshark: Certificato > Estensione > Nomi generali > NomeGenerale > dNSName: callservice.ciscospark.com**

Ciò conferma che il certificato Webex ha esattamente lo stesso aspetto.

A questo punto è possibile verificare che il nome soggetto di verifica TLS sia corretto. Come accennato, se si dispone di xConfiguration è possibile cercare la sezione di configurazione Zona per determinare come è stato configurato il nome soggetto della verifica TLS. Una cosa da notare su xConfiguration è che le zone sono ordinate con la Zona 1 è la prima zona creata. Di seguito è riportata una configurazione x dall'ambiente problematico analizzato sopra. È evidente che il nome soggetto della verifica TLS non presenta alcun problema.

```
*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"
```

Il passo successivo da esaminare è il **mapping in ingresso per la verifica TLS**. Ciò conferma se si sta mappando correttamente la connessione TLS alla zona DNS ibrida Webex. Anche xConfiguration può essere utilizzata per analizzare questo aspetto. In xConfiguration il **mapping di verifica TLS in entrata** è denominato **DNS ZIP TLS Verify InboundClassification**. Come si può vedere in questo esempio, il valore è impostato su Off.

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

Poiché questo valore è impostato su Off, il sistema VCS non è in grado di eseguire il mapping delle connessioni TLS in entrata a questa zona. La chiamata entra quindi nella zona predefinita e viene controllata e instradata in base alle regole di ricerca fornite per gli scenari business-to-business, se la connessione business-to-business è configurata su Expressway-E.

Soluzione

Per risolvere questo problema, è necessario impostare su On il mapping di verifica TLS in ingresso nella zona DNS per le chiamate ibride. Di seguito sono riportati i passaggi per completare l'operazione.

1. Accedere a Expressway-E
2. Selezionare **Configurazione > Zone > Zone**
3. Seleziona **zona DNS per le chiamate ibride**
4. Per la **verifica TLS del mapping in ingresso**, scegliere **Attivato**
5. Selezionare **Salva**

Nota: Vedere per il comportamento di registrazione della baseline. Questa sezione illustra Expressway che esegue la verifica dei certificati e il mapping alla zona DNS ibrida Webex.

Problema 7. Expressway-E utilizza il certificato autofirmato predefinito

In alcune nuove distribuzioni di Hybrid Call Service Connect, la firma del certificato Expressway-E viene ignorata o si ritiene che sia possibile utilizzare il certificato server predefinito. Alcuni pensano che ciò sia possibile perché Cisco Webex Control Hub consente di caricare un certificato personalizzato nel portale. (**Servizi > Impostazioni** (**In Scheda di chiamata ibrida**) **> Carica** (**In Certificati per chiamate crittografate**))

Se si presta particolare attenzione al testo relativo ai **certificati per chiamate SIP crittografate,** verrà visualizzato quanto segue: 'Utilizzare i certificati forniti dall'elenco di attendibilità predefinito di Cisco Collaboration o caricare i propri. Se utilizzi il tuo, assicurati che i nomi host si trovino in un dominio verificato.' L'elemento chiave dell'istruzione è **"assicurarsi che i nomi host si trovino in un dominio verificato".**

Quando si risolve un problema che soddisfa questa condizione, tenere presente che il sintomo dipenderà dalla direzione della chiamata. Se la chiamata ha avuto origine da un telefono locale, è probabile che l'app Cisco Webex non squilli. Inoltre, se si tenta di tracciare la chiamata dalla cronologia di ricerca di Expressways, si troverà che la chiamata lo farà fino a Expressway-E e si fermerà lì. Se la chiamata ha avuto origine da un'app Cisco Webex ed è stata destinata all'ufficio, il telefono locale non squilla. In questo caso, la cronologia di ricerca di Expressway-E e Expressway-C non mostra nulla.

In questo particolare scenario, la chiamata è stata effettuata da un telefono locale. Utilizzando Expressway-E Search History, è possibile determinare che la chiamata è stata effettuata sul server. A questo punto, è possibile analizzare la registrazione diagnostica per determinare l'evento. Per avviare questa analisi, verificare innanzitutto se è stata tentata e stabilita una connessione TCP sulla porta 5062. Ricercando "TCP Connecting" nei log di diagnostica di Expressway-E e ricercando la voce di riga con il tag "Dst-port=5062", è possibile determinare se la connessione viene stabilita.

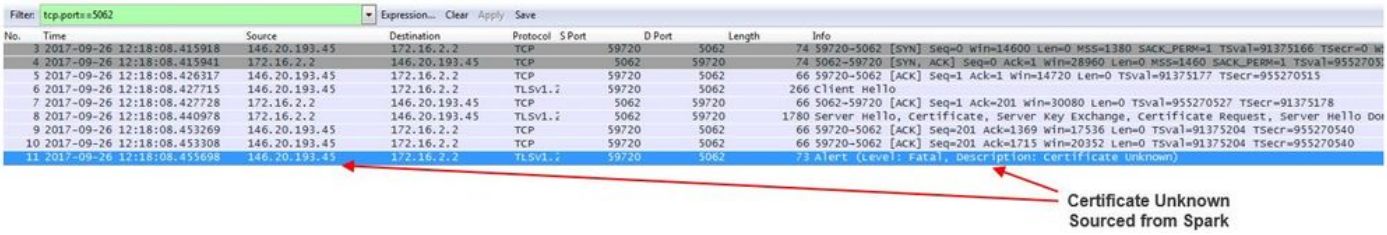
```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG":  Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26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

Dopo aver confermato la connessione TCP stabilita, è possibile analizzare l'handshake TLS reciproco che si verifica immediatamente dopo. Come si può vedere nel frammento qui, l'handshake ha esito negativo e il certificato è sconosciuto **(Detail="sslv3 alert certificate known")**

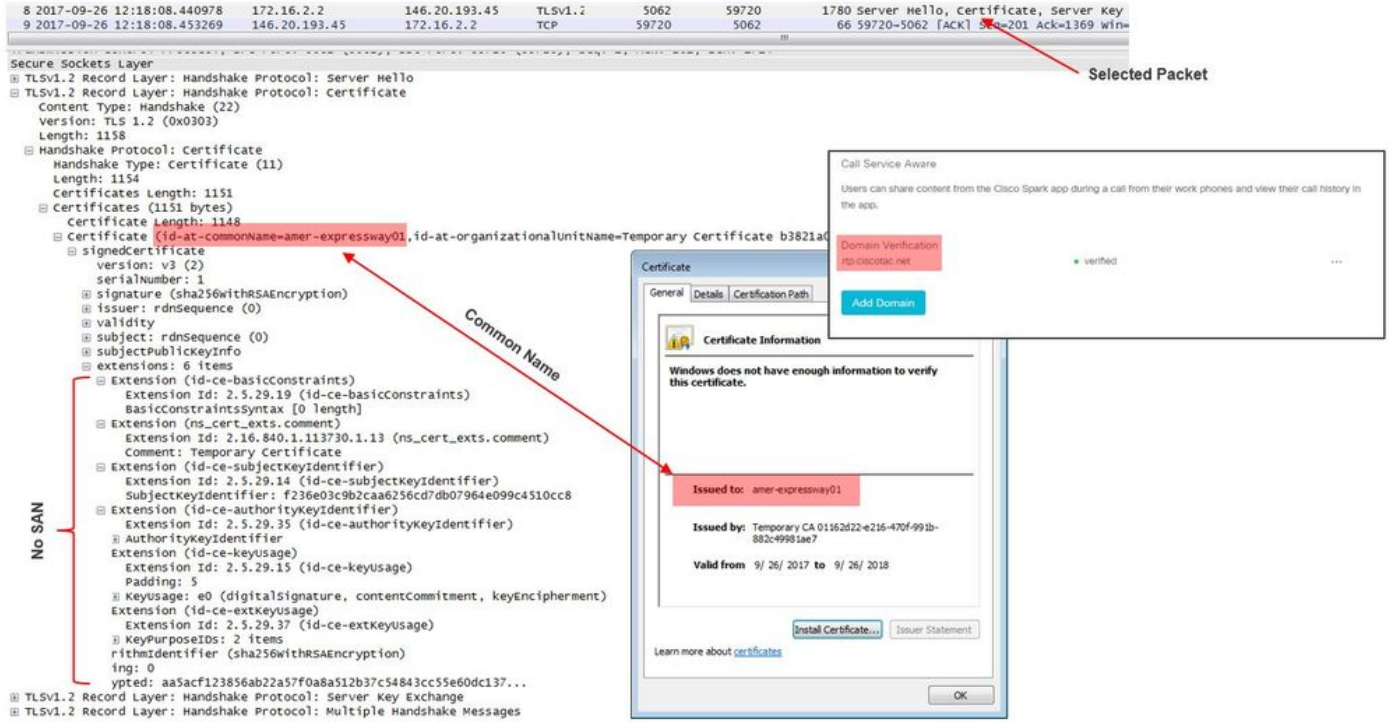
```
2017-09-26T08:18:08.441-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,441"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700":  Detail="Handshake in progress"
Reason="want read/write"
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="::TTSSLErrorOutput" 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"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Se si osserva più da vicino l'acquisizione dei pacchetti fornita con la registrazione diagnostica

Expressway-E, si osserverà che l'errore Certificate Unknown (Certificato sconosciuto) proviene dalla direzione di Cisco Webex, come mostrato nell'immagine.



Se si controlla il certificato del server predefinito da Expressway-E, è possibile verificare che 'Nome comune' e 'Nomi soggetto alternativi' non contengano il 'Dominio verificato' **(rtp.ciscotac.net)**. Si hanno poi prove su cosa causa questo problema, come mostrato nell'immagine.



A questo punto è stato determinato che il certificato del server Expressway-E deve essere firmato da una CA pubblica o da una CA interna.

Soluzione

Per risolvere questo problema, sono disponibili due opzioni:

1. Richiedere che il certificato Expressway-E sia firmato da una [CA pubblica considerata attendibile da Cisco Webex].
   Accedere a Expressway.Selezionare **Manutenzione > Sicurezza > Certificato server**.Selezionare **Genera CSR**.Immettere le informazioni richieste sul certificato e verificare che il campo **Altri nomi alternativi** contenga il **dominio verificato** elencato in Webex Control Hub.Fare clic su **Genera CSR**.Fornire il CSR a una CA pubblica di terze parti per la firma.Al ritorno del certificato, passare a **Manutenzione > Sicurezza > Certificati server**.Nella sezione **Carica nuovo certificato** accanto a **Selezionare il file del certificato del server**, selezionare **Scegli file** e selezionare il **certificato firmato**.Selezionare **Carica dati certificato server**.Passare a **Manutenzione > Sicurezza > Certificato CA attendibile**.Nella sezione

Upload accanto a **Selezionare il file contenente i certificati CA attendibili** selezionare **Scegli file**.Selezionare i certificati CA radice e intermedi forniti dalla CA pubblica.Selezionare **Aggiungi certificato CA**.Riavviare Expressway-E.

2. Richiedere il certificato Expressway-E firmato da una CA interna e quindi caricare le CA interne ed Expressway-E in Cisco Webex Control Hub.
   Accedi a ExpresswaySelezionare **Manutenzione > Sicurezza > Certificato server**.Selezionare **Genera CSR**Immettere le informazioni richieste sul certificato assicurandosi che il *campo Nomi alternativi aggiuntivi* contenga il **Dominio verificato** elencato in Webex Control HubFare clic su **Genera CSR**Fornire CSR a una CA pubblica di terze parti per la firmaAl ritorno del certificato, passare a *Manutenzione > Sicurezza > Certificati server*Nella *sezione Carica nuovo certificato* accanto a *Selezionare il file del certificato del server*, selezionare **Scegli file** e selezionare il certificato firmatoSelezionare **Carica dati certificato server**Passare a **Manutenzione > Sicurezza > Certificato CA attendibile**Nella sezione **Carica** accanto a **Selezionare il file contenente i certificati CA attendibili** selezionare **Scegli file**.Selezionare i certificati CA radice e intermedi forniti dalla CA pubblica.Selezionare **Aggiungi certificato CA**.Riavviare Expressway-E.

2 bis. Caricare il certificato CA interno ed Expressway-E in Cisco Webex Control Hub.

1. Accedere a Cisco Webex Control Hub come amministratore.
2. Selezionare **Servizi**.
3. Selezionare **Settings** (Impostazioni) nella scheda Hybrid Call Service (Servizio di chiamata ibrido).
4. Nella **sezione Certificati per chiamate SIP crittografate** selezionare **Upload**.
5. Scegliere i certificati CA interna ed Expressway-E.

In ingresso: Cisco Webex to On-Premises

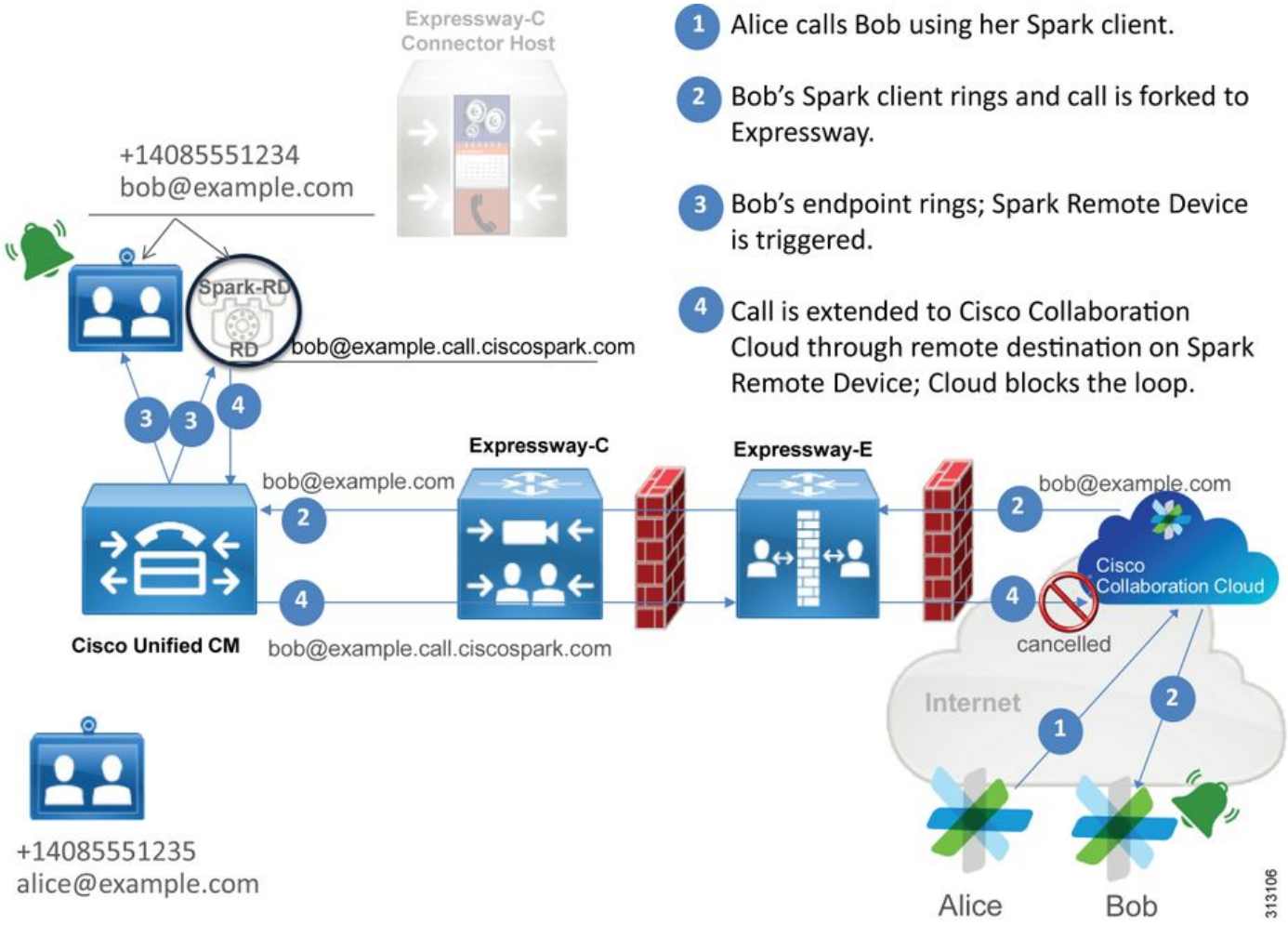
Quasi tutti i guasti in entrata di Cisco Webex a livello locale hanno lo stesso sintomo segnalato: "Quando chiamo dalla mia app Cisco Webex all'app di un altro collega, l'app di quest'ultimo squilla ma il telefono locale no." Per risolvere questo scenario, è utile comprendere sia il flusso di chiamata che la logica che si verifica quando viene eseguito questo tipo di chiamata.

Flusso logico ad alto livello

1. Il chiamante dell'app Cisco Webex avvia la chiamata
2. Anelli app del destinatario chiamata
3. La chiamata viene inoltrata all'ambiente Cisco Webex
4. L'ambiente Cisco Webex deve eseguire una ricerca DNS in base alla destinazione SIP configurata dal cliente in Cisco Webex Control Hub
5. L'ambiente Cisco Webex tenta di connettersi ad Expressway sulla porta 5062
6. L'ambiente Cisco Webex cerca di eseguire un handshake TLS reciproco
7. L'ambiente Cisco Webex invia un INVITE SIP a Expressway che viene trasmesso all'endpoint di collaborazione locale/telefono IP
8. Cisco Webex e l'azienda completano la negoziazione SIP
9. Cisco Webex e le aziende iniziano a inviare e ricevere contenuti multimediali.

Flusso di chiamata

Passare a **Cisco Webex app > Cisco Webex environment > Expressway-E > Expressway-C > On-Premises Collaboration Endpoint/IP Phone** come mostrato nell'immagine.



Di seguito sono riportati alcuni dei problemi comuni osservati con le chiamate in entrata da Webex all'infrastruttura locale.

Problema 1. Cisco Webex non è in grado di risolvere Expressway-E DNS SRV/hostname

Quando si pensa al flusso di chiamate da Cisco Webex a locale, il primo passaggio logico di Cisco Webex è come contattare Expressway locale. Come accennato in precedenza, Cisco Webex tenterà di connettersi a Expressway locale eseguendo una ricerca SRV in base alla **destinazione SIP** configurata elencata nella pagina **Hybrid Call Service Settings** in Cisco Webex Control Hub.

Se si cerca di risolvere questa situazione dal punto di vista del registro diagnostico di Expressway-E, non viene visualizzato alcun traffico proveniente da Cisco Webex. Se si cerca la connessione TCP, non viene visualizzato Dst-port=5062, né alcun handshake MTLS o invito SIP successivo da Cisco Webex.

In questo caso, è necessario verificare in che modo la **destinazione SIP** è stata configurata in Cisco Webex Control Hub. È inoltre possibile utilizzare lo **strumento Hybrid Connectivity Test Tool** per la risoluzione dei problemi. Lo strumento di test della connettività ibrida verifica se è disponibile un indirizzo DNS valido, se Cisco Webex può connettersi alla porta restituita nella ricerca SRV e se Expressway locale dispone di un certificato valido considerato attendibile da Cisco Webex.

1. Accedere a Cisco Webex Control Hub
2. **SelezionaServizi**
3. Selezionare il collegamento Settings (Impostazioni) nella **scheda Hybrid Call (Chiamata**

ibrida).

4. Nella sezione Call Service Connect verificare il dominio utilizzato per l'indirizzo SRV SIP pubblico **nel** campo Destinazione **SIP**.
5. Se il record è stato immesso correttamente, fare clic su **Test** per verificare se il record è valido.
6. Come mostrato di seguito, è possibile notare chiaramente che al dominio pubblico non è associato alcun record SIP SRV corrispondente, come mostrato nell'immagine.

selezionare **Visualizza risultati test** per visualizzare ulteriori dettagli sugli errori, come mostrato nell'immagine.

In alternativa, è possibile cercare il record SRV utilizzando nslookup. Di seguito sono riportati i comandi che è possibile eseguire per verificare se la destinazione SIP esiste.

```
C:\Users\pstojano>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
```

Come si può vedere nel blocco di codice sopra riportato, il comando nslookup è stato avviato e il server è impostato su 8.8.8.8, che è un server DNS Google pubblico. Infine, si impostano i tipi di record per la ricerca nei record SRV. A questo punto, è possibile inviare il record SRV completo da cercare. Il risultato è che le richieste alla fine scadono.

Soluzione

1. Configurare un indirizzo SIP SRV pubblico per Expressway-E nel sito utilizzato per ospitare i nomi di dominio pubblico.
2. Configurare un nome host che verrà risolto nell'indirizzo IP pubblico di Expressway-E
3. Configurare la destinazione SIP in modo da elencare il dominio utilizzato per l'indirizzo SRV

SIP creato nel passaggio 1. Accedere a Cisco Webex Control HubSeleziona **servizi**Selezionare il collegamento **Impostazioni** nella *scheda Hybrid Call*Nella sezione Connessione servizio di chiamata immettere il dominio utilizzato per l'indirizzo SRV SIP pubblico nel campo **Destinazione SIP**. Selezionare Salva

Nota: Se il record SRV SIP che si desidera utilizzare è già utilizzato per le comunicazioni business-to-business, si consiglia di specificare un sottodominio del dominio aziendale come indirizzo di rilevamento SIP in Cisco Webex Control Hub e, di conseguenza, un record SRV DNS pubblico, come indicato di seguito:

Servizio e protocollo: _sips._tcp.mtls.example.com
Priority: 1
Peso: 10
Numero porta: 5062
Destinazione: us-expe1.example.com

La raccomandazione di cui sopra è stata ricavata direttamente dalla Cisco Webex Hybrid Design Guide.

Soluzione alternativa

Se il cliente non dispone di un record SIP SRV (e non intende crearne uno), può elencare in alternativa l'indirizzo IP pubblico di Expressway con suffisso ":5062". In questo modo, l'ambiente Webex non tenterà una ricerca SRV ma si connetterà direttamente a **%Expressway_Pub_IP%:5062**. (Esempio: 64.102.241.236:5062)

1. Configurare la destinazione SIP in modo che venga formattata come **%Expressway_Pub_IP%:5062**. *(Esempio: 64.102.241.236:5062)* Accedere a Cisco Webex Control HubSeleziona **servizi**Selezionare il collegamento **Impostazioni** nella *scheda Hybrid Call*Nella sezione Connessione servizio di chiamata immettere **%Expressway_Pub_IP%:5062** nel campo **Destinazione SIP**. Selezionare Salva

Per ulteriori informazioni sull'indirizzo di destinazione SIP e/o sul record SRV da configurare, Fare riferimento alla sezione Enable Hybrid Call Service Connect for Your Organization della Cisco Webex Hybrid Call Service Deployment Guide o alla Cisco Webex Hybrid Design Guide.

Problema 2. Errore socket: La porta 5062 è bloccata in entrata in Expressway

Al termine della risoluzione DNS, l'ambiente Cisco Webex tenterà di stabilire una connessione TCP sulla porta 5062 all'indirizzo IP restituito durante la ricerca DNS. Questo indirizzo IP sarà l'indirizzo IP pubblico di Expressway-E locale. Se l'ambiente Cisco Webex non è in grado di stabilire questa connessione TCP, la chiamata in entrata nella sede avrà esito negativo. Il sintomo di questa particolare condizione è lo stesso di quasi tutti gli altri errori delle chiamate in arrivo di Cisco Webex: il telefono locale non squilla.

Se si sta risolvendo il problema utilizzando i log di diagnostica di Expressway, non verrà visualizzato alcun traffico proveniente da Cisco Webex. Se si cerca la connessione TCP, non verranno visualizzati i tentativi di connessione per Dst-port=5062, né gli handshake MTLS o gli inviti SIP di Cisco Webex successivi. Poiché la registrazione diagnostica Expressway-E non è utile in questa situazione, è possibile utilizzare alcuni metodi di verifica:

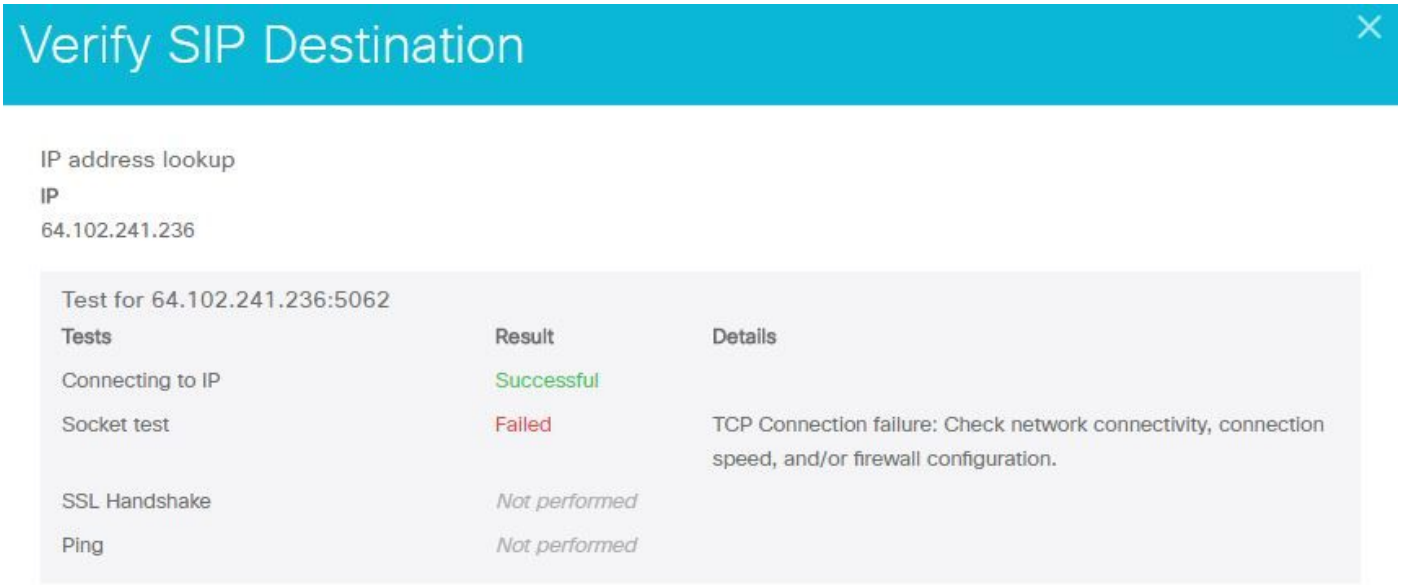
1. Acquisire un pacchetto dall'interfaccia esterna del firewall

2. Utilizzo di un'utility di controllo delle porte
3. Utilizzare lo strumento Hybrid Connectivity Test

Poiché lo strumento Hybrid Connectivity Test è integrato direttamente in Cisco Webex Control Hub e simula l'ambiente Cisco Webex tentando di connettersi a Expressway locale, è il metodo di verifica più ideale disponibile. Per verificare la connettività TCP nell'organizzazione:

1. Accedere a Cisco Webex Control Hub
2. **SelezionaServizi**
3. Selezionare il collegamento Settings (Impostazioni) nella **scheda Hybrid Call (Chiamata ibrida)**
4. Nella sezione Call Service Connect (Connessione servizio di chiamata), verificare che il valore immesso nella destinazione SIP sia corretto
5. Fare clic su Prova come illustrato nell'immagine.

6. Poiché il test non è riuscito, è possibile fare clic sul collegamento **Visualizza risultati test** per controllare i dettagli come mostrato nell'immagine.



Come si osserva nell'immagine precedente, il test Socket non è riuscito durante il tentativo di connessione a 64.102.241.236:5062. Se questi dati, oltre ai log/pcaps di diagnostica di Expressway, non mostrano alcun tentativo di connessione, si dispone ora di prove sufficienti per esaminare la configurazione di ACL/NAT/Routing del firewall.

Soluzione

Poiché questo particolare problema non è causato dall'ambiente Cisco Webex o dalle apparecchiature di collaborazione in sede, è necessario concentrarsi sulla configurazione del firewall. Poiché non è necessariamente possibile prevedere il tipo di firewall con il quale si interagirà, è necessario affidarsi a un utente con familiarità con il dispositivo. È possibile che il

problema sia relativo a un ACL del firewall, a un NAT o a una configurazione errata del routing.

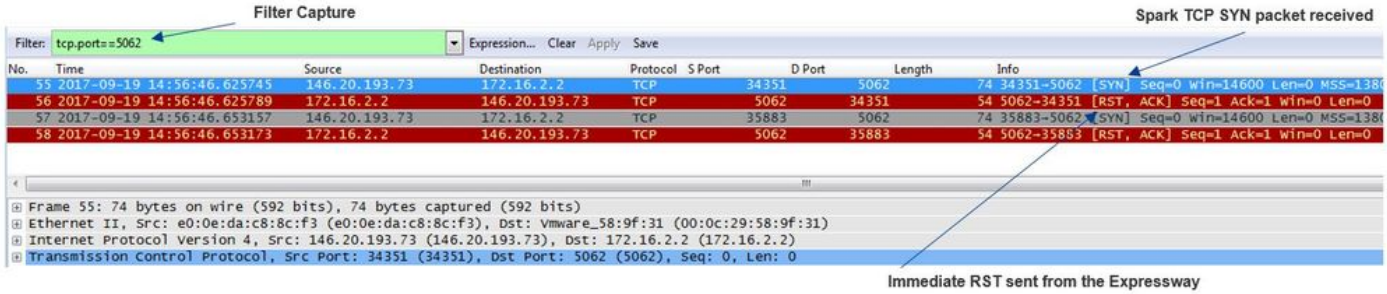
Problema 3. Errore socket: Expressway-E non è in ascolto sulla porta 5062

Questa particolare condizione viene spesso diagnosticata in modo errato. In molti casi, si presume che il firewall sia la causa del blocco del traffico sulla porta 5062. Per risolvere questa condizione particolare, è possibile utilizzare le tecniche descritte nello scenario precedente "Port 5062 is locked inbound to the Expressway". Lo strumento Hybrid Connectivity Test e qualsiasi altro strumento utilizzato per verificare la connettività delle porte avranno esito negativo. Il primo presupposto è che il firewall stia bloccando il traffico. La maggior parte delle persone controlla quindi nuovamente la registrazione diagnostica da Expressway-E per determinare se può vedere la connessione TCP che tenta di stabilire. Cercheranno una voce di log come questa, come mostrato nell'immagine.

```
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"
```

In questa condizione, la voce di log specifica indicata sopra non esisterà. Pertanto, molte persone diagnosticheranno erroneamente la condizione e presupporranno che si tratti del firewall.

Se l'acquisizione di un pacchetto è inclusa nella registrazione diagnostica, è possibile verificare che la causa non sia il firewall. Di seguito viene riportato un esempio di acquisizione di pacchetti dallo scenario in cui Expressway-E non era in ascolto sulla porta 5062. Questa acquisizione è stata filtrata utilizzando **tcp.port==5062** come filtro applicato, come mostrato nell'immagine.



Come si può vedere nell'acquisizione di pacchetti ottenuta da Expressway-E, il traffico sulla porta TCP 5062 non viene bloccato dal firewall, ma sta arrivando. Nel pacchetto numero 56, è possibile notare che Expressway-E sta inviando l'RST subito dopo l'arrivo del pacchetto TCP SYN iniziale. Con queste informazioni, si può concludere che il problema è isolato per l'Expressway-E che riceve il pacchetto; è necessario risolvere il problema dal punto di vista di Expressway-E. Considerate le prove, considerare le possibili ragioni per cui Expressway-E avrebbe inviato il pacchetto. Due possibilità che possono essere attribuite a questo comportamento sono:

1. Expressway-E dispone di alcuni tipi di regole firewall impostate che potrebbero bloccare il traffico

2. Expressway-E non è in ascolto del traffico TLS reciproco e/o non è in ascolto del traffico sulla porta 5062.

La funzionalità firewall di Expressway-E è disponibile in *Sistema > Protezione > Regole firewall > Configurazione*. Quando è stato eseguito il controllo in questo ambiente, non era presente alcuna configurazione firewall.

Esistono diversi modi per verificare se Expressway-E è in ascolto del traffico TLS reciproco sulla porta 5062. A tale scopo, è possibile utilizzare l'interfaccia Web o la CLI come utente root.

Dalla radice di Expressway, se si esegue il comando **netstat -an | grep ':5062' ,** si dovrebbe ottenere un output simile a quello che si vede di seguito.

```
~ # 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
```

Queste informazioni possono essere acquisite anche tramite l'interfaccia Web di Expressway-E. Per ottenere queste informazioni, vedere i passaggi seguenti

1. Accedere a Expressway-E

2. Passare a **Strumenti di manutenzione > Uso porta > Porte in entrata locali**

3. Cercare il tipo SIP e la porta IP 5062 (evidenziati in rosso come mostrato nell'immagine).

Ora che sapete cosa dovreste vedere, potete confrontarlo con l'ambiente attuale. Dal punto di vista della CLI, quando si esegue **netstat -an | grep ':5062' ,** l'output è il seguente:

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

Inoltre, l'unità Web non visualizza la porta TLS reciproca elencata in Porte in ingresso locali

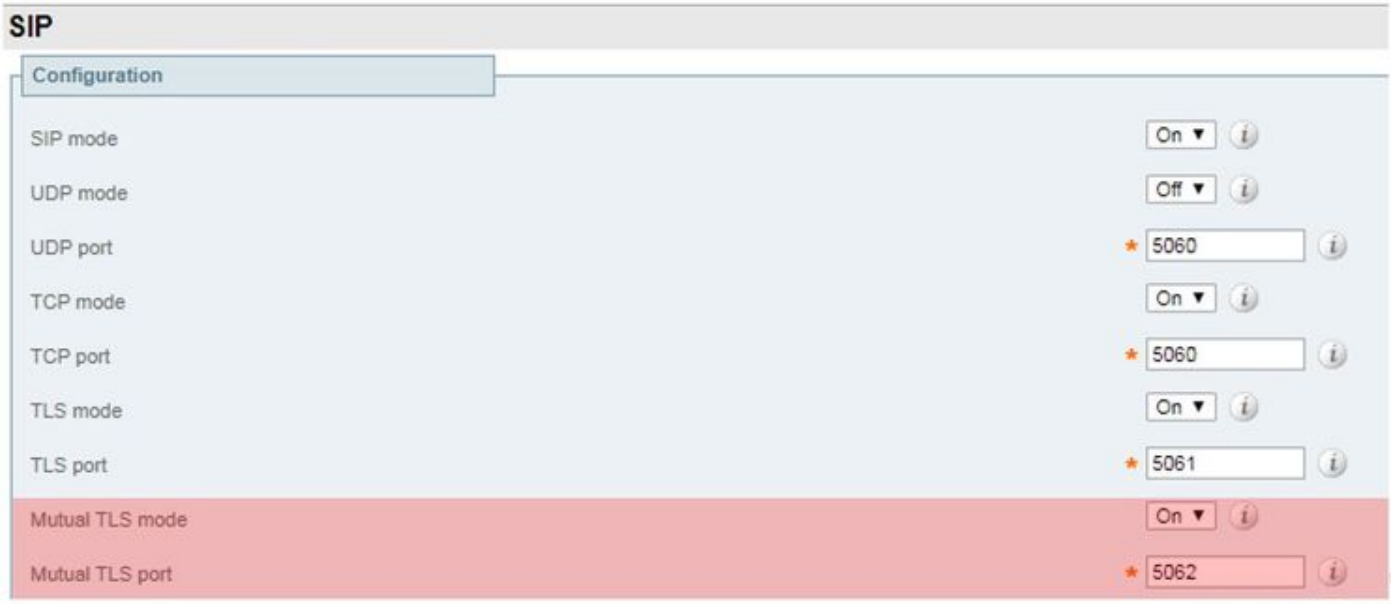
Con questi dati, è possibile concludere che Expressway-E non è in ascolto del traffico TLS reciproco.

Soluzione

Per risolvere questo problema, è necessario verificare che la modalità Mutual TLS sia abilitata e che la porta Mutual TLS sia impostata su 5062 su Expressway-E:

1. Accedere a Expressway-E

2. Selezionare **Configurazione > Protocolli > SIP**
3. Assicurarsi che la modalità Mutual TLS sia impostata su **On**
4. Verificare che la porta Mutual TLS sia impostata su **5062**
5. Fare clic su **Save** (Salva) come mostrato nell'immagine.



Problema 4. Expressway-E o C non supportano intestazioni route SIP precaricate

Con Hybrid Call Service Connect, il routing delle chiamate viene eseguito in base all'**intestazione della route**. L'intestazione del percorso viene compilata in base alle informazioni fornite a Cisco Webex dalla sezione relativa al supporto del servizio di chiamata (Expressway Connector) della soluzione. L'host del connettore Expressway esegue una query su Unified CM per gli utenti abilitati per il servizio di chiamata ed esegue il pull sia dell'**URI di directory** che del **nome di dominio completo (FQDN) del cluster della relativa home di Unified CM**. Vedere questi esempi, utilizzando Alice e Bob:

URI directory	Intestazione route di destinazione
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

Se la chiamata viene effettuata da Alice o Bob, verrà instradata a Unified CM locale in modo che possa essere ancorata a Cisco WebexRD prima di essere indirizzata all'utente chiamato.

Se Alice dovesse chiamare Bob, la chiamata verrebbe indirizzata all'*FQDN del cluster di rete principale di CM unificato di Alice (us-cucm.example.com).* Se si analizza l'INVITE SIP inviato da Cisco Webex in entrata a Expressway-E, nell'intestazione SIP saranno disponibili le informazioni seguenti

URI richiesta	sorso: bob@example.com
Intestazione route	sip:us-cucm.example.com;lr

Dal punto di vista di Expressway, le regole di ricerca sono configurate in modo da instradare la chiamata non dall'URI della richiesta ma dall'**intestazione della route (us-cucm.example.com),** in questo caso il cluster home di Alice Unified CM.

Con questo set di basi, è possibile comprendere le situazioni di risoluzione dei problemi in cui Expressways è configurato in modo errato, il che fa sì che la logica precedente non funzioni.

Come quasi tutti gli altri errori di configurazione delle chiamate alla connessione del servizio di chiamata ibrida in entrata, il sintomo è che *il telefono locale non squilla*.

Prima di analizzare i log di diagnostica in Expressway, considerare come identificare la chiamata:

1. L'URI della richiesta SIP sarà l'**URI** *della* **directory della parte chiamata.**
2. Il campo SIP FROM verrà formattato con il **chiamante** indicato come **"Nome Cognome" <sip:WebexDisplayName@subdomain.call.ciscospark.com>**

Con queste informazioni, è possibile cercare nei log di diagnostica per **URI directory della parte chiamante, nome e cognome della parte chiamante o indirizzo SIP Cisco Webex della parte chiamante**. Se non si dispone di alcuna di queste informazioni, è possibile eseguire una ricerca in "**INVITE SIP:**" per individuare tutte le chiamate SIP in esecuzione su Expressway. Dopo aver identificato l'INVITE SIP per la chiamata in ingresso, è possibile individuare e copiare l'ID chiamata SIP. Dopo aver ottenuto questo valore, è possibile eseguire una semplice ricerca nei log di diagnostica in base all'ID chiamata per visualizzare tutti i messaggi correlati a questa tappa chiamata.

Un'altra cosa per isolare il problema di routing è determinare la distanza della chiamata nell'azienda. È possibile cercare le informazioni indicate in precedenza in Expressway-C per verificare se la chiamata è stata inoltrata fino a quel punto. In caso affermativo, è probabile che tu voglia iniziare la tua indagine da lì.

In questo scenario è possibile osservare che Expressway-C ha ricevuto INVITE da Expressway-E.

```
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: "pstojano 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>

Èimportante che l'**intestazione della route (FQDN cluster)** sia ancora intatta. Non viene tuttavia eseguita alcuna logica di ricerca in base all'intestazione della route (FQDN cluster) **cucm.rtp.ciscotac.net**. Viene invece visualizzato il messaggio che viene rifiutato immediatamente con il valore **404 Non trovato**.

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

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

464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: **9062bca7eca2afe71b4a225048ed5101**@127.0.0.1
CSeq: 1 INVITE
From: **"pstojano 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

Rispetto a uno scenario di lavoro, lo scenario di lavoro mostra che la logica di ricerca viene eseguita in base all'intestazione del router (FQDN del cluster)

2017-09-22T13:56:02.215-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="**Search Attempted**" Service="SIP"
Src-alias-type="SIP" **Src-alias="pstojano-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'"
```

Èpossibile osservare che Expressway-C inoltra correttamente la chiamata in uscita a 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=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbed5b79c6cffad9ecd84cc8
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=z9hG4bK043ca6360f253c6abed9b23fbeff9819;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: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstojano test" <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=567490631
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 14
Route:
```

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

Dopo aver analizzato la registrazione diagnostica che ha isolato il problema a Expressway-C e un errore specifico (404 Non trovato), è possibile concentrarsi su ciò che causerebbe questo tipo di comportamento. Di seguito sono riportati alcuni aspetti da considerare:

1. Le chiamate vengono spostate all'interno e all'esterno delle zone di Expressway tramite regole di ricerca.
2. La logica utilizzata da Expressways, denominata route SIP precaricate, supporta l'elaborazione delle richieste SIP INVITE contenenti l'intestazione del router. Questo valore può essere attivato o disattivato nelle zone (server trasversale, client trasversale, router adiacente) su Expressway-C ed Expressway-E.

Èora possibile utilizzare xConfiguration per visualizzare la configurazione sia nelle zone Expressway-E Traversal Server che nelle zone client Expressway-C, in particolare quelle impostate per la connessione Hybrid Call Service. Oltre alla configurazione della zona, è possibile analizzare le regole di ricerca configurate per passare la chiamata da una zona all'altra. È inoltre noto che Expressway-E ha passato la chiamata a Expressway-C in modo che la configurazione della zona server Traversal sia probabilmente configurata correttamente.

Per scomporre il problema, il codice xConfig seguente indica che il nome di questa zona è denominato **Hybrid Call Service Traversal**. È di tipo zona **TraversalServer**. Comunica con Expressway-C tramite la porta TCP SIP **7003**.

Il fattore chiave per il servizio Hybrid Call è che deve avere il supporto delle route SIP precaricate su On. L'interfaccia Web di Expressway chiama questo valore. Le **route SIP precaricate supportano** il valore, mentre xConfiguration lo visualizza come **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"
```

Èinoltre possibile stabilire che a questa zona è associata la regola di ricerca 3 (Webex Hybrid). In pratica, la regola di ricerca invia un alias "Any" che arriva attraverso la zona DNS dei servizi di chiamata ibrida e lo passa alla zona sopra indicata, Hybrid Call Service Traversal. Come previsto, sia la regola di ricerca che la zona Traversal Server su Expressway-E sono configurate correttamente.

```
*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"
```

Se si concentra l'attenzione su xConfiguration di Expressway-C, è possibile iniziare cercando la zona Traversal Client per Webex Hybrid. Un modo semplice per trovarlo è ricercare il numero di porta appreso da Expressway-E xConfiguration (**porta SIP: "7003"**). Ciò consente di identificare rapidamente la zona corretta in xConfiguration.

Come in precedenza, è possibile conoscere il nome della zona (Hybrid Call Service Traversal), il tipo (Traversal Client) e cosa è stato configurato per l'accettazione delle route SIP precaricate (supporto delle route SIP precaricate). Come si può vedere da questa configurazione x, questo valore è impostato su Off. In base alla Guida alla distribuzione per Cisco Webex Hybrid Call Services, questo valore deve essere impostato su On.

Inoltre, se si controlla la definizione del supporto delle route SIP precaricate, è possibile vedere chiaramente che Expressway-C deve RIFIUTARE un messaggio se questo valore è impostato su Off E l'invito contiene un'intestazione di route: "**Disattiva il supporto delle route SIP precaricate se si desidera che la zona rifiuti le richieste SIP INVITE contenenti questa intestazione**."

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"
```

A questo punto, il problema è stato isolato a causa di una configurazione errata della configurazione della zona client di Expressway-C Traversal. È necessario attivare il supporto delle route SIP precaricate.

Soluzione

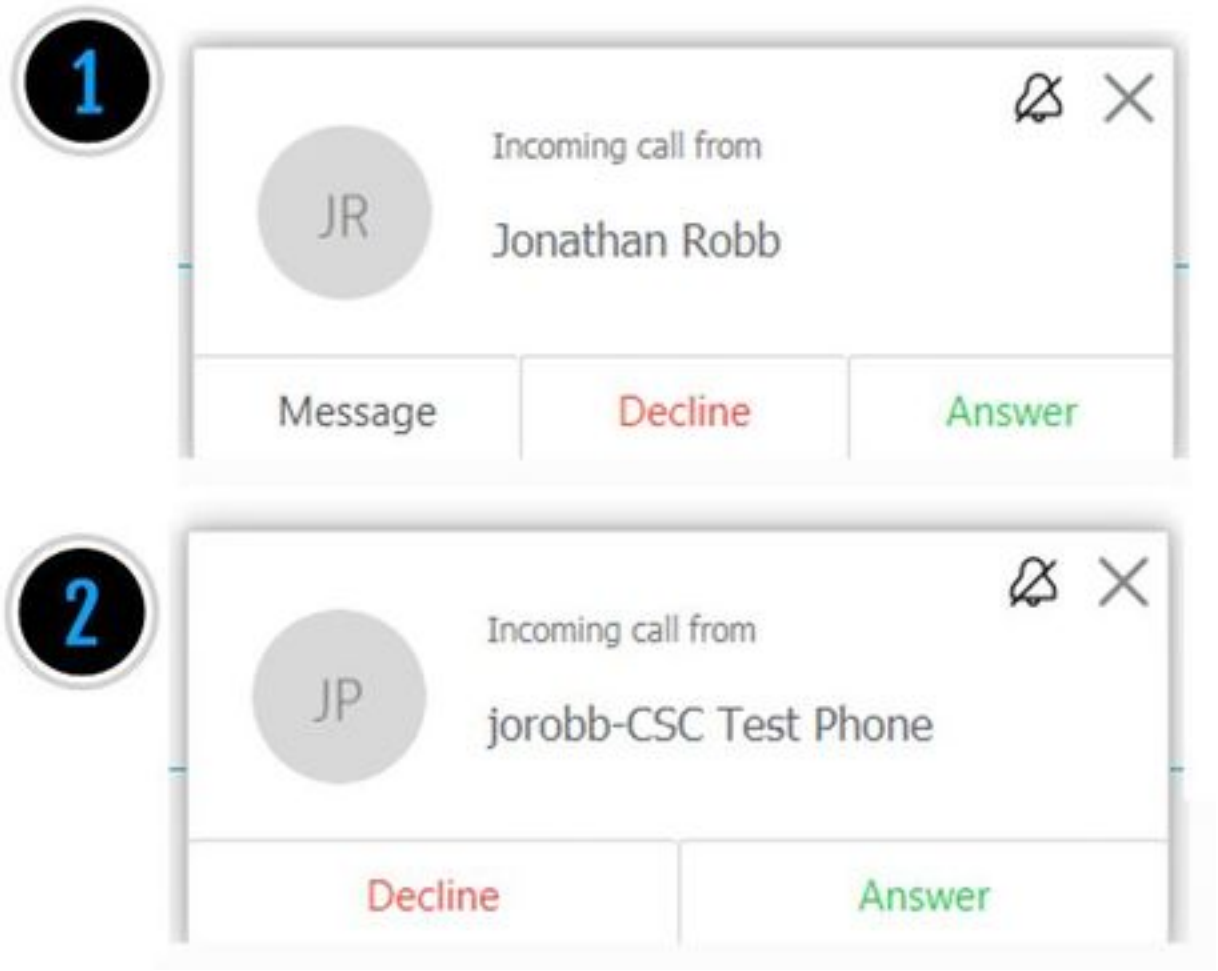
Per impostare correttamente il supporto delle route SIP precaricate:

1. Accedere a Expressway-C
2. Selezionare **Configurazione > Zone > Zone**
3. Selezionare l'area client attraversamento chiamata Hybrid Call (la denominazione varia da cliente a cliente)
4. Impostare il **supporto delle route SIP precaricate** su **On**
5. Selezionare **Salva**

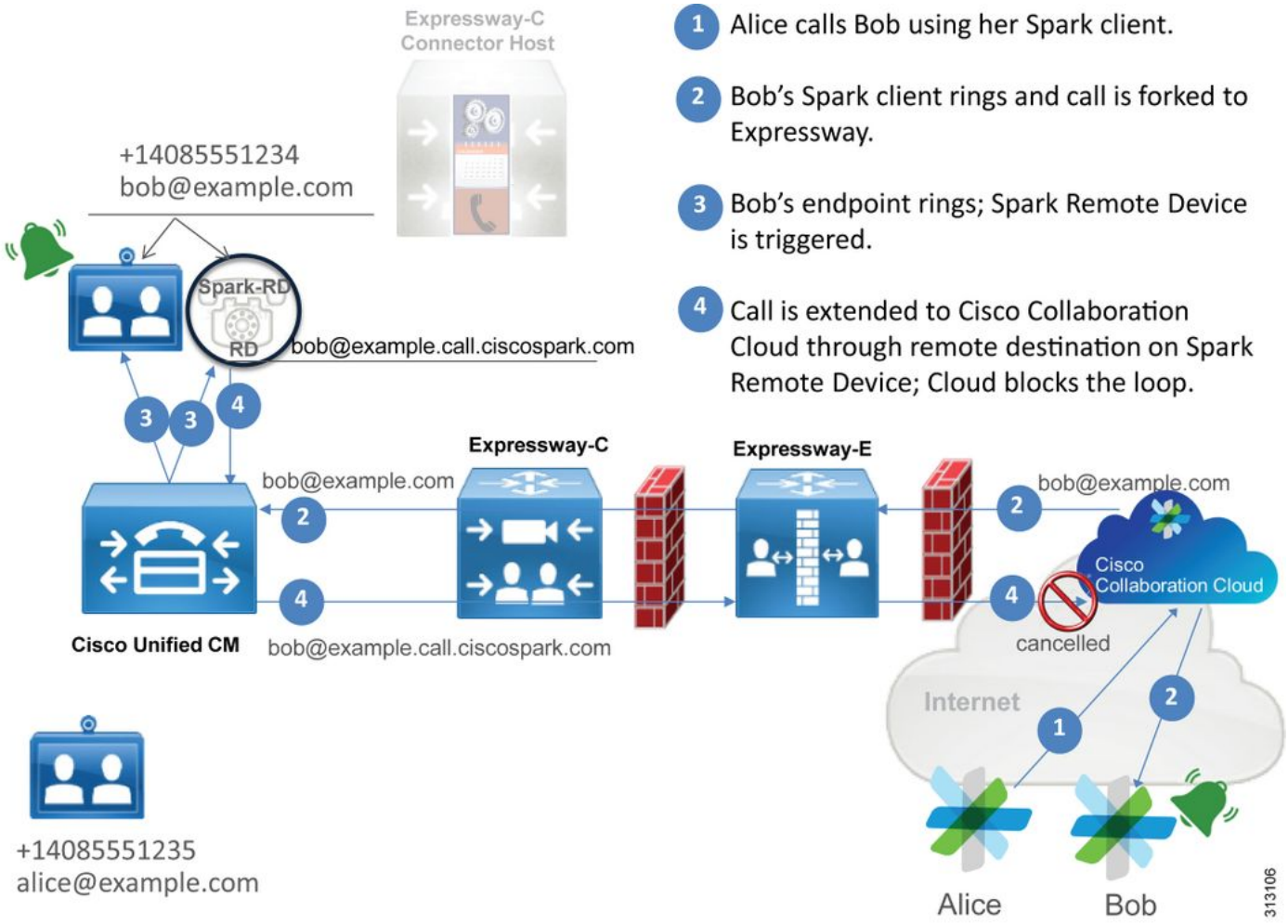
> **Nota:** Anche se questo scenario ha dimostrato il guasto su Expressway-C, è stato possibile osservare gli stessi errori di registrazione diagnostica su Expressway-E se il **supporto delle route SIP precaricate** è disattivato nella zona del server di attraversamento delle chiamate ibride Webex. In quel caso non avreste mai visto la chiamata raggiungere l'Expressway-C e l'Expressway-E sarebbe stato responsabile di rifiutare la chiamata e inviare il 404 Non trovato.

Problema 5. L'app Cisco Webex sta ricevendo due notifiche di chiamata (avvisi popup)

Questo particolare problema si verifica quando è l'unico scenario di chiamata in ingresso che non determina l'interruzione della chiamata. Per questo problema, la persona che riceve la chiamata (il destinatario della chiamata) sta ricevendo due notifiche (avvisi popup) nell'app Cisco Webex dalla persona che ha effettuato la chiamata (il destinatario della chiamata). La prima notifica viene generata da Cisco Webex, la seconda dall'infrastruttura locale. Di seguito sono riportati alcuni esempi delle due notifiche ricevute, come mostrato nell'immagine.



La prima notifica (avviso popup) viene dalla persona che ha iniziato la chiamata (il chiamante) dal lato Cisco Webex. L'ID chiamante in questa istanza è il nome visualizzato dell'utente che avvia la chiamata. La seconda notifica (avviso popup) proviene dalla CTI o da Cisco Webex RD locale e viene assegnata all'utente che sta effettuando la chiamata. All'inizio, questo comportamento sembra strano. Tuttavia, se si rivede lo schema delle chiamate in entrata (dalla Guida alla progettazione delle chiamate ibride di Cisco Webex), il comportamento ha più senso, come mostrato nell'immagine.



Dalla figura, si può vedere che Alice sta chiamando Bob dalla sua app Cisco Webex e che la chiamata è stata inoltrata fino all'edificio. Questa chiamata deve corrispondere all'URI di directory assegnato al telefono di Bob. Il problema è che con questo progetto, l'URI di directory viene assegnato anche al CTI-RD o Cisco Webex RD. Pertanto, quando la chiamata viene offerta al CTI-RD o a Cisco Webex RD, la chiamata viene inviata di nuovo a Cisco Webex perché il dispositivo ha una destinazione remota configurata per bob@example.call.ciscospark.com. Il modo in cui Cisco Webex gestisce questa situazione è che cancella la particolare coda di chiamata.

Per fare in modo che Cisco Webex annulli correttamente la tappa della chiamata, Cisco Webex ha inizialmente bisogno di inserire un parametro nell'intestazione SIP che avrebbe cercato per annullare la tappa specificata. Il parametro che Cisco Webex inserisce nell'INVITE SIP è denominato "**call-type=squared"** e questo valore viene immesso nell'intestazione del contatto. Se il valore viene eliminato dal messaggio, Cisco Webex non è in grado di annullare la chiamata.

Con queste informazioni, è possibile rivisitare lo scenario presentato in precedenza in cui l'app Cisco Webex dell'utente stava ricevendo due notifiche (toast) quando l'utente Cisco Webex Jonathan Robb stava effettuando una chiamata. Per risolvere questo tipo di problema, è sempre necessario raccogliere la registrazione diagnostica di Expressway-C ed Expressway-E. Come punto di partenza, è possibile esaminare i log Expressway-E per determinare che SIP INVITE contiene effettivamente il valore **call-type=squared** presente nell'intestazione Contact dell'iniziale richiesta Cisco Webex INVITE inviata in entrata. In questo modo il firewall non modificherà in alcun modo il messaggio. Di seguito è riportato un frammento di codice di esempio di INVITE in ingresso in Expressway-E da questo scenario.

```
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:
```

Nell'intestazione del contatto è presente il valore call-type=squared. A questo punto, la chiamata deve attraversare Expressway e uscire dalla zona del server di attraversamento ibrido Webex. È possibile eseguire una ricerca nei registri Expressway-E per determinare come la chiamata è stata inviata da Expressway-E. Questo ci darà un'idea se Expressway-E sta in qualche modo manipolando 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=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdfe078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debcd8;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>
```

Quando si esamina questo INVITE SIP inviato da Expressway-E a Expressway-C, si noti che nell'intestazione del contatto manca il **call-type=squared**. Un'altra cosa da sottolineare è che alla voce 4, potete vedere che la zona di uscita è uguale a **HybridCallServiceTraversal**. Si può ora concludere che il motivo per cui l'app Cisco Webex riceve una seconda notifica (avviso popup) quando viene chiamata è lo stripping **call-type=squared** tag dall'intestazione SIP INVITE Contact. La domanda da porsi è: cosa potrebbe causare questa intestazione spogliata?

La chiamata deve passare attraverso l'attraversamento del servizio di chiamata ibrida impostato su Expressway, in modo che sia un buon punto per iniziare l'indagine. Se si dispone di xConfiguration, è possibile verificare come è stata configurata questa zona. Per identificare la Zona in xConfiguration, è sufficiente utilizzare il nome registrato nella riga Via che viene stampato nei log. È possibile vedere sopra che è stato chiamato uscita-zone=HybridCallServiceTraversal. Quando questo nome viene stampato nella riga Via dell'intestazione SIP, gli spazi vengono rimossi. Il nome della zona reale dalla prospettiva xConfiguration contiene spazi ed è formattato in 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: "Off" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On"   <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

Con le impostazioni identificate per l'attraversamento del servizio Hybrid Call, è possibile cercare le impostazioni potenziali che spiccano, ad esempio:

- SIP PreloadedSIPRoutes Accept: On
- ParameterPreservation Mode SIP: Spento

Utilizzando l'interfaccia Web di qualsiasi Expressway, è possibile visualizzare la definizione di questi valori e le relative operazioni.

Supporto route SIP precaricate

Attivare il supporto per le route SIP precaricate per consentire a questa zona di elaborare le richieste SIP INVITE contenenti l'intestazione della route.

Disattiva il supporto di route SIP precaricate se si desidera che la zona rifiuti le richieste SIP INVITE contenenti questa intestazione.

Conservazione dei parametri SIP

Determina se B2BUA di Expressway mantiene o riscrive i parametri nelle richieste SIP instradate tramite questa zona.

Onmantiene i parametri SIP Request URI e Contact del routing delle richieste tra questa zona e B2BUA.
Offconsente a B2BUA di riscrivere, se necessario, i parametri URI richiesta SIP e contatto delle richieste di routing tra questa zona e B2BUA.
In base a queste definizioni, xConfiguration, e al fatto che il valore **call-type=squared** viene inserito nell'intestazione "Contact" (Contatto) di SIP INVITE, è possibile concludere che se il valore di conservazione del parametro SIP è Off nella zona di transito del servizio di chiamata ibrida, il tag viene eliminato e l'app Cisco Webex riceve notifiche a doppio anello.

Soluzione

Per mantenere il valore call-type=squared nell'intestazione Contact di SIP INVITE, è necessario verificare che Expressways supporti la conservazione dei parametri SIP per tutte le zone coinvolte nella gestione della chiamata:

1. Accedere a Expressway-E
2. Selezionare **Configurazione > Zone > Zone**
3. Selezionare la zona utilizzata per Hybrid Traversal Server
4. Impostare il valore di conservazione dei parametri SIP su **On**
5. Salvare le impostazioni.

##
Nota: In questo scenario di esempio, la configurazione errata era relativa alla zona Webex Hybrid Traversal Server su Expressway-E. Tenere presente che è assolutamente possibile impostare il valore di conservazione dei parametri SIP su Off nel client Webex Hybrid Traversal o nelle zone adiacenti CUCM. Entrambe queste configurazioni verrebbero eseguite su Expressway-C. In questo caso ci si potrebbe aspettare che Expressway-E invii il valore **call-type=squared** a Expressway-C e che Expressway-C lo spogli.

In uscita: On-Premises to Cisco Webex

Quasi tutti gli errori delle chiamate in uscita da Cisco Webex in locale hanno lo stesso sintomo segnalato: "Quando effettuo una chiamata dal mio telefono Unified CM registrato a un altro utente abilitato per Call Service Connect, il telefono locale squilla, a differenza dell'app Cisco Webex." Per risolvere questo scenario, è importante comprendere sia il flusso di chiamata che la logica che si verifica quando viene effettuato questo tipo di chiamata.

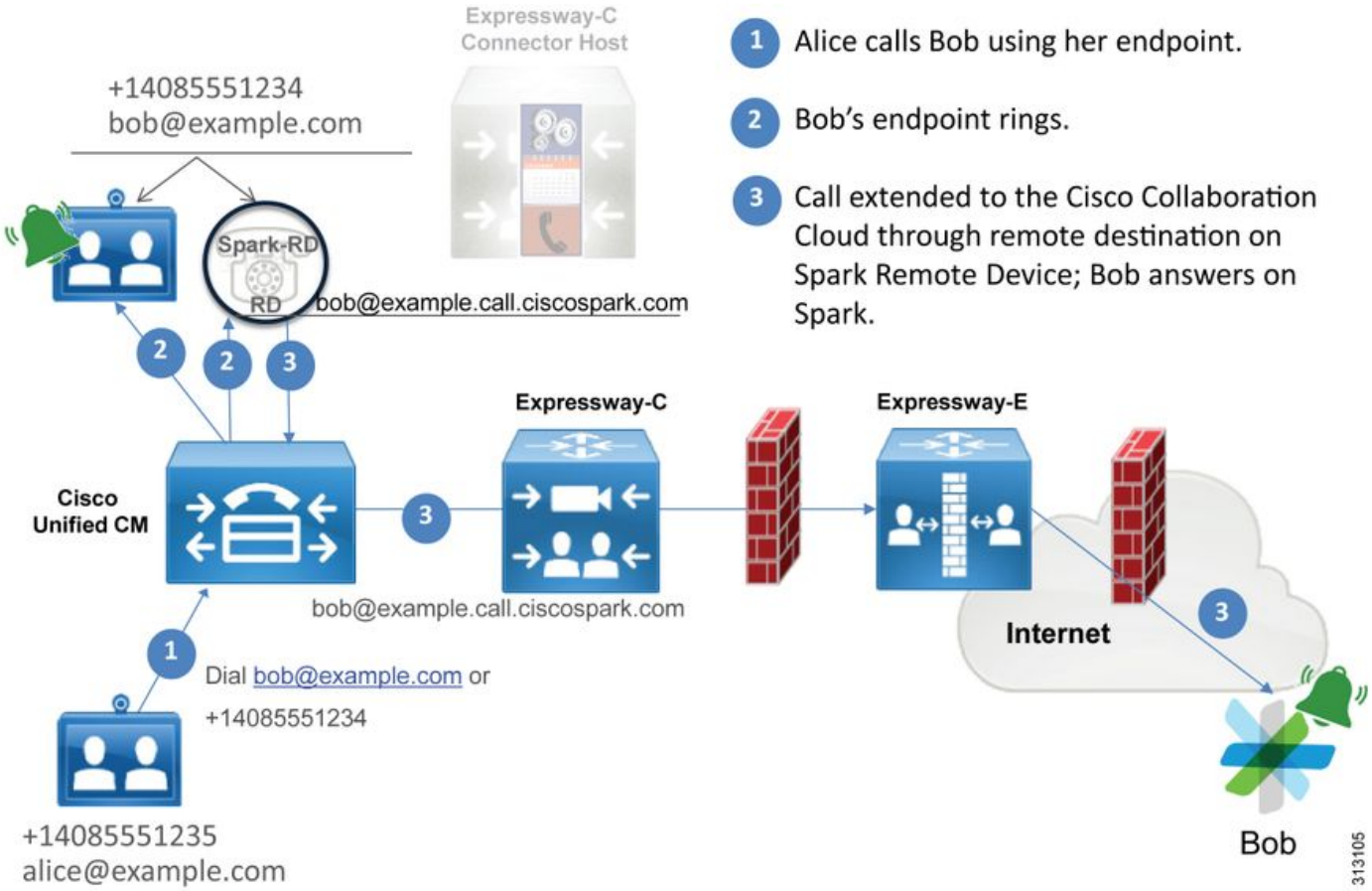
Flusso logico ad alto livello

1. L'utente A effettua una chiamata dal telefono locale all'URI di directory dell'utente B
2. Telefono locale dell'utente B e CTI-RD/Webex-RD accettano la chiamata

3. Il telefono locale dell'utente B inizia a squillare
4. Il CTI-RD/Webex-RD dell'utente B rimanda questo invito alla destinazione di UserB@example.call.ciscospark.com
5. Unified CM trasmette questa chiamata a Expressway-C
6. Expressway-C invia la chiamata a Expressway-E
7. Expressway-E esegue una ricerca DNS nel dominio callservice.ciscospark.com
8. Expressway-E tenta di connettersi all'ambiente Cisco Webex tramite la porta 5062.
9. Expressway-E e l'ambiente Cisco Webex iniziano un handshake reciproco
10. L'ambiente Cisco Webex passa la chiamata all'app Cisco Webex disponibile nell'utente B
11. L'app Cisco Webex disponibile dell'utente B inizia a squillare.

Flusso di chiamata

Passare all'**utente B tramite telefono locale > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco Webex environment > Cisco Webex app** come mostrato nell'immagine.



Nota: L'immagine è stata estratta dalla Cisco Webex Hybrid Design Guide.

Suggerimenti per l'analisi dei log

Se durante la risoluzione di un problema si verifica un errore nelle chiamate biforcate in uscita verso Cisco Webex, è possibile raccogliere i log di Unified CM, Expressway-C ed Expressway-E. Grazie a questi insiemi di registri, è possibile verificare il modo in cui la chiamata passa nell'ambiente. Un altro modo rapido per comprendere quanto la chiamata si stia spingendo all'interno dell'ambiente locale è utilizzare Expressway "Search History". La cronologia di ricerca di Expressway consente di verificare rapidamente se la chiamata biforcata verso Cisco Webex sta raggiungendo Expressway-C o E.

Per utilizzare Cronologia ricerche, è possibile effettuare le seguenti operazioni:

1. Accedere a Expressway-E
   Effettua una chiamata di prova
   Selezionare **Stato > Cronologia ricerca**
   Verificare se viene visualizzata una chiamata con un indirizzo di destinazione dell'URI SIP Webex da chiamare (user@example.call.ciscospark.com)
   Se nella cronologia di ricerca non viene visualizzata la chiamata che ha raggiunto la cronologia di ricerca Expressway-E, ripetere questa procedura in Expressway-C

Prima di analizzare i log di diagnostica in Expressway, considerare come identificare la chiamata:

1. L'URI della richiesta SIP sarà l'indirizzo SIP dell'utente Cisco Webex
2. Il campo SIP FROM verrà formattato in modo che la parte chiamante sia elencata come "Nome Cognome" <sip:Alias@Domain>

Con queste informazioni è possibile cercare nei log di diagnostica per URI directory della parte chiamante, nome e cognome della parte chiamante o indirizzo SIP Cisco Webex della parte chiamata. Se non si dispone di nessuna di queste informazioni, è possibile eseguire una ricerca in **"INVITE SIP:"** per individuare tutte le chiamate SIP in esecuzione su Expressway. Dopo aver identificato l'INVITE SIP per la chiamata in uscita, è possibile individuare e copiare l'**ID chiamata** SIP. Dopo aver ottenuto questo risultato, è possibile eseguire una semplice ricerca nei log di diagnostica in base al **Call-ID** per visualizzare tutti i messaggi correlati a questa tappa della chiamata.

Di seguito sono elencati alcuni dei problemi più comuni osservati con le chiamate in uscita dal telefono registrato in Unified CM all'ambiente Cisco Webex quando viene effettuata una chiamata a un utente abilitato per Call Service Connect.

Problema 1. Impossibile risolvere l'indirizzo callservice.ciscospark.com

La procedura operativa standard per una zona DNS Expressway prevede l'esecuzione di ricerche DNS basate sul dominio visualizzato a destra di un URI di richiesta. Per spiegare questo, consideri un esempio. Se la zona DNS dovesse ricevere una chiamata con un URI di richiesta **pstojano-test@dmzlab.call.ciscospark.com**, una tipica zona DNS Expressway eseguirebbe la logica di ricerca DNS SRV su **dmzlab.call.ciscospark.com** che è il lato destro dell'URI di richiesta. Se Expressway eseguisse questa operazione, è possibile prevedere che si verificheranno la ricerca e la risposta seguenti.

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

Se si controlla attentamente, si noterà che la risposta del record SRV fornisce un indirizzo del server e la porta 5061, non 5062.

Ciò significa che l'handshake TLS reciproco che si verifica sulla porta 5062 non verrà eseguito e che verrà utilizzata una porta separata per la segnalazione tra Expressway e Cisco Webex. Il problema è che la *Deployment Guide for Cisco Webex Hybrid Call Services* non richiede esplicitamente l'uso della porta 5061 perché alcuni ambienti non consentono le chiamate business-to-business.

Per superare la logica di ricerca SRV standard della zona DNS in Expressway, è necessario configurare Expressway in modo che esegua ricerche esplicite in base a un valore specificato dall'utente.

Quando si analizza questa particolare chiamata, è possibile concentrarsi su Expressway-E perché è stato determinato (utilizzando Cronologia ricerche) che la chiamata è arrivata a questo punto. Iniziare con il primo INVITE SIP che arriva in Expressway-E per vedere quale zona è arrivata, quali regole di ricerca sono in uso, quale zona la chiamata esce e, se viene inviata correttamente alla zona DNS, quale logica di ricerca DNS si verifica.

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



        ;tag=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>
```

In questo INVITE SIP è possibile ottenere l'URI della richiesta (pstojano-test@dmzlab.call.ciscospark.com), l'**ID chiamata** (991f7e80-9c11517a-130ac-1501a8c0), **From** ("Jonathan Robb" <sip:5010@rtp.ciscotac.net>), **To** (sip:pstojano-test@dmzlab.call.ciscospark.com) e **User-Agent** (Cisco-CUCM11.5). Dopo la ricezione di INVITE, Expressway deve prendere decisioni logiche per determinare se è possibile instradare la chiamata a un'altra zona. Expressway eseguirà questa operazione in base alle regole di ricerca.

```
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'"
```

Come si può notare dallo snippet di log riportato sopra, l'Expressway-E è stato analizzato tramite quattro regole di ricerca, tuttavia ne è stata presa in considerazione solo una *(da* Webex Hybrid a Webex Cloud*)*. La regola di ricerca ha una priorità di 90 ed è stata indirizzata alla zona DNS dei servizi di chiamata ibrida. Ora che la chiamata viene inviata a una zona DNS, è possibile esaminare le ricerche DNS SRV in corso in Expressway-E

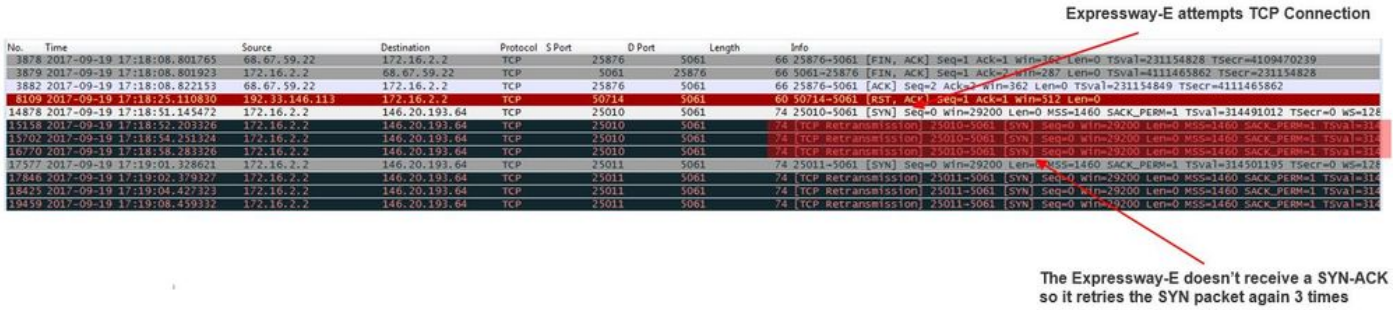
```
2017-09-19T13:18:50.565-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,565"
Module="network.dns" Level="DEBUG":  Detail="Sending DNS query"
Name="dmzlab.call.ciscospark.com" Type="NAPTR (IPv4 and IPv6)"
2017-09-19T13:18:50.718-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,718"
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"
```

Nello snippet di codice riportato sopra, è possibile notare che Expressway-E ha eseguito la ricerca SRV in base alla parte destra dell'URI della richiesta (_sips._tcp.dmzlab.call.ciscospark.com) e si è risolta in un nome host of l2sip-cfa-01.wbx2.com e porta 5061. Il hostname l2sip-cfa-01.wbx2.com si risolve in 146.20.193.64. Con queste informazioni, il passaggio logico successivo che Expressway eseguirà è inviare un pacchetto TCP SYN a 146.20.193.64 in modo che possa provare a configurare la chiamata. Dalla registrazione di Expressway-E è possibile verificare se questo accade.

```
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"
```

Nello snippet di registrazione diagnostica Expressway-E di cui sopra, è possibile notare che Expressway-E sta tentando di connettersi all'IP 146.20.193.64 precedentemente risolto sulla porta

TCP 5061, ma questa connessione è completamente in errore. Lo stesso risultato può essere ottenuto dall'acquisizione del pacchetto raccolta.



Sulla base di questi risultati, è chiaro che il traffico sulla porta 5061 non ha esito positivo. Tuttavia, Hybrid Call Service Connect ha intenzione di utilizzare la porta TCP 5062, non 5061. Pertanto, è necessario considerare il motivo per cui Expressway-E non risolve un record SRV che restituirebbe la porta 5062. Per provare a rispondere a questa domanda, è possibile cercare possibili problemi di configurazione nella zona DNS ibrida Expressway-E Webex.

```
*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"
```

In xConfiguration di Expressway-E, è possibile vedere che esistono due valori particolari di interesse relativi alle ricerche DNS: **DNSOverride Nome e DNSOverride Override**. In base a questa configurazione x, l'override di DNSOverride è impostato su Off, pertanto il nome DNSOverride non avrà effetto. Per comprendere meglio le funzionalità di questi valori, è possibile utilizzare l'interfaccia utente Web di Expressway per cercare la definizione dei valori.

Modifica richiesta DNS *(converte in override DnsOverride in xConfig)*

Instrada le chiamate SIP in uscita da questa zona a un dominio SIP specificato manualmente anziché al dominio nella destinazione chiamata. Questa opzione è destinata principalmente all'uso con Cisco Webex Call Service. Vedere www.cisco.com/go/hybrid-services.

Dominio da cercare *(convertito in nome DnsOverride in xConfig)*

Immettere un FQDN da trovare in DNS anziché cercare il dominio nell'URI SIP in uscita. L'URI SIP originale non è interessato.

Ora che si dispone di queste definizioni, è chiaro che questi valori, se impostati correttamente, sarebbero del tutto rilevanti per la logica di ricerca DNS. Se a questo si aggiungono le istruzioni della Guida alla distribuzione di Cisco Webex Hybrid Call Services, è necessario impostare

Modifica richiesta DNS su **On** e il dominio da cercare su **callservice.ciscospark.com**. Se si modificano questi valori per specificare le informazioni corrette, la logica di ricerca DNS SRV sarà completamente diversa. Di seguito è riportato un frammento di quanto ci si potrebbe aspettare dalla prospettiva di registrazione diagnostica di Expressway-E

```
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"
```

Soluzione

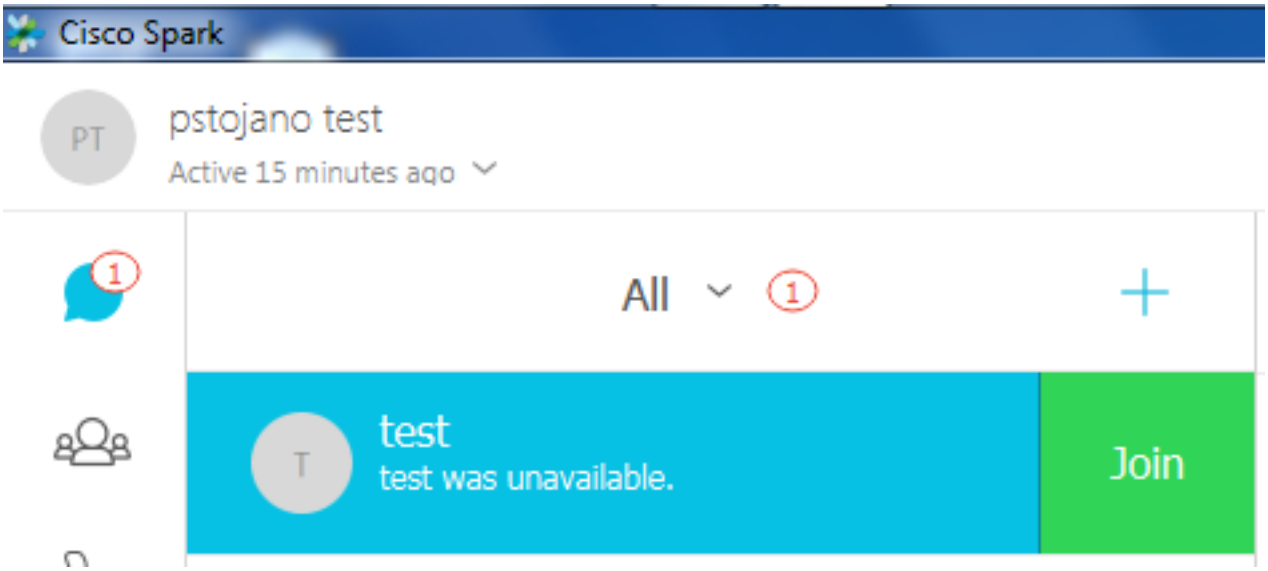
1. Accedere a Expressway-E
2. Passare a **Zone di configurazione > Zone**
3. Selezionare la zona DNS ibrida Webex configurata
4. Impostare la richiesta Modifica DNS su **Attivata**
5. Impostare il dominio in cui cercare il valore su **callservice.ciscospark.com**
6. Salva le modifiche

> **Nota:** Se in Expressway viene utilizzata una sola zona DNS, è necessario configurare una zona DNS separata da utilizzare con il servizio di chiamata ibrida in grado di sfruttare questi valori.

Problema 2. La porta 5062 è bloccata in uscita su Cisco Webex

Una cosa che è unica riguardo gli errori delle chiamate in uscita biforcate verso Cisco Webex è che l'app Cisco Webex del destinatario presenterà un pulsante di accesso alla sua app anche se il client non squilla mai. Analogamente allo scenario precedente, anche in questo caso è necessario utilizzare gli stessi strumenti e la stessa registrazione per individuare la causa del problema. Per suggerimenti sull'isolamento dei problemi relativi alle chiamate e sull'analisi dei registri, vedere la sezione di questo articolo come mostrato nell'immagine.

Illustrazione della visualizzazione del pulsante Partecipa



Analogamente alla chiamata in uscita n. 1, è possibile avviare l'analisi alla registrazione diagnostica di Expressway-E, perché è stata utilizzata la cronologia di ricerca di Expressway per determinare che la chiamata sta raggiungendo tale obiettivo. Come in precedenza, iniziare con l'INVITO iniziale che viene in Expressway-E da Expressway-C. Ricordare che le cose che si desidera cercare sono:

1. Se Expressway-E riceve INVITE
2. Indica se la logica della regola di ricerca passa la chiamata alla zona DNS ibrida
3. Se la zona DNS esegue la ricerca DNS e nel dominio corretto
4. Se il sistema ha tentato di stabilire correttamente un handshake TCP per la porta 5062
5. Se l'handshake TLS reciproco è riuscito

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



        ;tag=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>
```

Come si può vedere nel precedente messaggio INVITE, INVITE viene ricevuto normalmente. Azione "ricevuta" proveniente dall'indirizzo IP di Expressway-C. È ora possibile passare alla logica della regola di ricerca

```
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'"
```

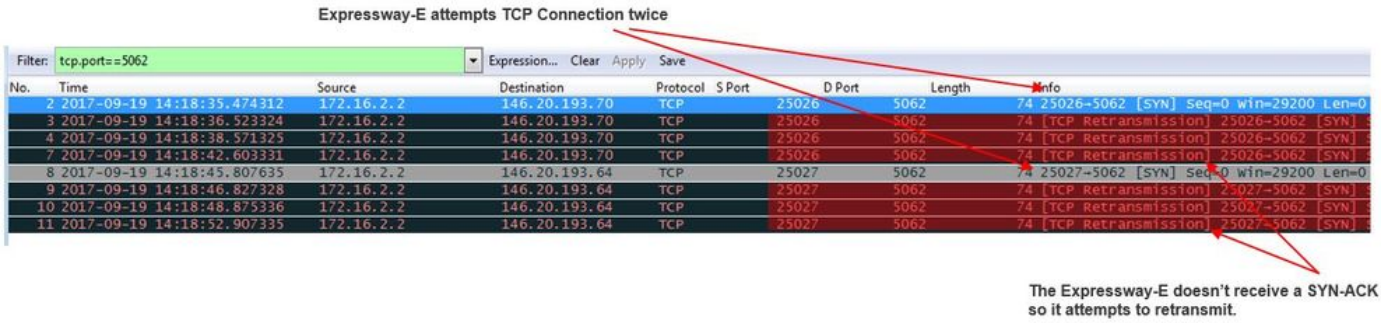
In base al frammento di registro sopra riportato, è possibile notare che Expressway-E ha analizzato quattro regole di ricerca, ma solo una *(Webex Hybrid - Webex Cloud)* è stato preso in considerazione. La regola di ricerca aveva una priorità di 90 ed era destinata a *Zona DNS dei servizi Hybrid Call*. Ora che la chiamata viene inviata a una zona DNS, è possibile esaminare le ricerche DNS SRV in corso in Expressway-E. Tutto ciò è del tutto normale. È ora possibile concentrarsi sulla logica di ricerca DNS

```
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"
```

Potete chiaramente vedere che in questo caso, il record callservice.ciscospark.com SRV viene risolto. La risposta è costituita da quattro record validi diversi che utilizzano tutti la porta 5062. Si tratta di un comportamento normale. A questo punto, è ora possibile analizzare l'handshake TCP che dovrebbe seguire. Come accennato in precedenza nel documento, è possibile cercare "TCP Connecting" nei log di diagnostica e cercare la voce che elenca Dst-port="5062". Di seguito è riportato un esempio di quanto verrà visualizzato in questo scenario:

```
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"
```

Èinoltre possibile utilizzare tcpdump incluso con il bundle di registrazione diagnostica per ottenere informazioni più dettagliate sull'handshake TCP, come mostrato nell'immagine.



A questo punto, è possibile concludere che Expressway-E sta instradando correttamente la chiamata. In questo scenario, la difficoltà è che non è possibile stabilire una connessione TCP con l'ambiente Webex. Questo problema può verificarsi perché l'ambiente Webex non risponde al pacchetto TCP SYN, ma ciò è improbabile se si considera che il server che gestisce la connessione è condiviso tra molti clienti. La causa più probabile in questo scenario è un tipo di dispositivo intermedio (firewall, IPS, ecc.) che non consente l'uscita del traffico.

Soluzione

Poiché il problema era isolato, questi dati devono essere forniti all'amministratore di rete del cliente. Inoltre, se hanno bisogno di ulteriori informazioni, è possibile rimuovere un'acquisizione dall'interfaccia esterna del dispositivo periferico e/o del firewall per un'ulteriore prova. Dal punto di vista di Expressway, non è necessario eseguire ulteriori azioni poiché il problema non risiede in tale dispositivo.

Problema 3. Configurazione errata della regola di ricerca di Expressway

La configurazione errata delle regole di ricerca è uno dei problemi più gravi correlati alla configurazione in Expressways. I problemi di configurazione delle regole di ricerca possono essere bidirezionali, perché sono necessarie regole di ricerca per le chiamate in entrata e regole di ricerca per le chiamate in uscita. Mentre si esamina questo problema, si scoprirà che mentre i problemi regex sono abbastanza comuni su Expressway, non sono sempre la causa di un problema di regola di ricerca. In questo particolare segmento, si esaminerà una chiamata in uscita che ha avuto esito negativo. Come tutti gli altri scenari di chiamate interurbane in uscita, i sintomi rimangono gli stessi:

- L'app Cisco Webex dell'utente chiamato ha presentato il pulsante Partecipa
- Il telefono chiamante stava riproducendo un squillo
- Il telefono locale dell'utente chiamato stava suonando
- L'app Cisco Webex dell'utente chiamato non ha mai squillato

Come tutti gli altri scenari, è possibile utilizzare le tracce SDL CUCM insieme ai log di diagnostica Expressway-C ed E. Come in precedenza, è necessario fare riferimento alla per utilizzare la cronologia di ricerca e ai suggerimenti per identificare una chiamata nei log di diagnostica. Come

in precedenza, è stato determinato utilizzando Expressway-E Search History che la chiamata stava effettuando lì e non riuscendo. Di seguito è riportato l'inizio dell'analisi per la quale si esamina l'INVITO SIP iniziale che arriva in Expressway-E da Expressway-C.

```
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-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
 Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
 Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
 From: "Jonathan Robb"




        tag=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>
```

Utilizzando l'ID chiamata (**d58f2680-9c91200a-1c7ba-1501a8c0**) dall'intestazione SIP, è possibile cercare rapidamente tutti i messaggi associati a questa finestra di dialogo. Se si controlla il terzo hit nei log per Call-ID, si nota che Expressway-E invia immediatamente un **404 Not Found** a Expressway-C.

```
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.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
 CSeq: 101 INVITE
 From: "Jonathan Robb"




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




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

Questi dati forniscono due indicazioni:

1. Expressway-E non ha mai tentato di inviare INVITE a Cisco Webex
2. Expressway-E è stato il responsabile della decisione logica di rifiutare la chiamata con un errore 404 Not Found.

Un errore 404 Not Found in genere indica che Expressway non è in grado di trovare l'indirizzo di destinazione. Poiché le Expressway utilizzano le regole di ricerca per instradare le chiamate tra se stesse e in ambienti diversi, iniziare concentrandosi sulla configurazione x di Expressway-E. In questa configurazione x, è possibile cercare la regola di ricerca che deve trasmettere la chiamata alla zona DNS ibrida Webex. Per trovare le regole di ricerca configurate in Expressway dal punto di vista xConfiguration, è possibile cercare "Regola regole di ricerca criteri zone xConfiguration". In questo modo, verrà visualizzato un elenco di configurazione delle regole di ricerca per ogni regola di ricerca creata in Expressway. Il numero che segue "Regola" aumenterà in base alla regola di ricerca che è stata creata e contrassegnata per la prima volta 1. In caso di problemi nella ricerca della regola di ricerca. è possibile utilizzare i valori di denominazione comunemente utilizzati, ad esempio "*Webex*", per individuare meglio la regola di ricerca. Un altro modo per identificare la regola è trovare il valore Stringa modello impostato su ".*@.*\.ciscospark\.com". Si tratta della stringa del motivo che si suppone debba essere configurata. *(Presupponendo che la stringa modello sia configurata correttamente)*Dopo aver esaminato xConfiguration in questo scenario, è possibile notare che la regola di ricerca 6 è la regola corretta per passare la chiamata a Cisco Webex.

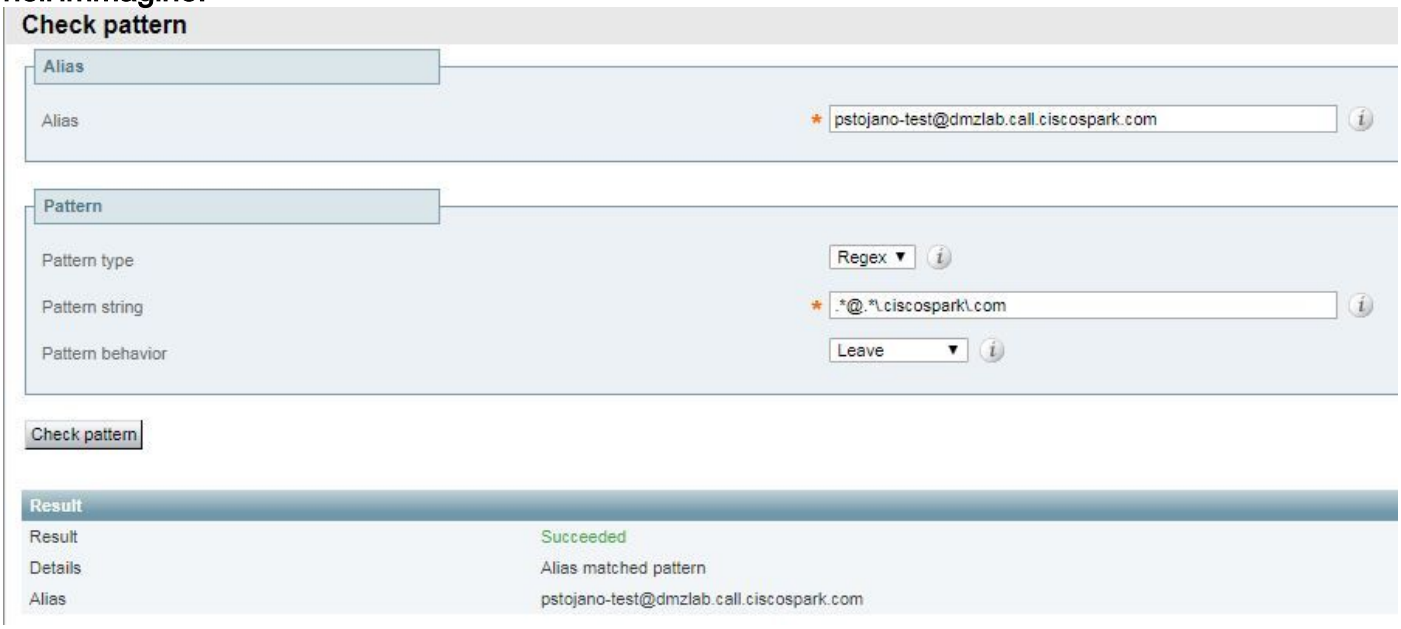
```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex 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: ".*@.*\.ciscospark\.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"
```

Per provare questo modello, è possibile utilizzare la funzione Controlla modello descritta in. La chiamata importante qui è che vogliamo i seguenti valori configurati:Manutenzione > Strumenti > Schema di controllo

- Alias: %URI richiesta nell'INVITE iniziale% (ad esempio: pstojano-test@dmzlab.call.ciscospark.com)
- Tipo motivo: Regex
- Stringa modello .*@.*\.ciscospark\.com
- Comportamento motivo: Esci

Se il Regex per la regola è impostato correttamente, dovrebbe essere visualizzato il risultato di questo criterio di controllo riuscito. Di seguito è riportata un'illustrazione che mostra questa condizione, come mostrato
nell'immagine:



Dopo aver verificato che la regola di ricerca sia presente e configurata correttamente, è possibile esaminare con maggiore attenzione la logica di ricerca eseguita da Expressway per determinare se influisce sull'Expressway-E che invia l'oggetto 404 Non trovato. Di seguito è riportato un esempio della logica della regola di ricerca eseguita da Expressway.

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

2017-09-25T11:26:02.968-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,968"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="dmzlab.call.ciscospark.com"
Type="NAPTR (IPv4 and IPv6)"
```

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

In questo esempio, è possibile vedere che Expressway ha elaborato quattro regole di ricerca. Le prime tre non sono state prese in considerazione per vari motivi, tuttavia la quarta è stata presa in considerazione. La parte interessante dei dati è che subito dopo aver preso in considerazione Expressway passa direttamente alla logica di ricerca DNS. Se si ricordano i risultati ottenuti con xConfiguration, la regola di ricerca configurata per Webex Hybrid è stata denominata Webex Hybrid - per Webex Cloud e non è stata nemmeno considerata nella logica della regola di ricerca sopra riportata. A questo punto, vale la pena esaminare come la regola di ricerca considerata (a DNS) è stata implementata in modo da poter capire meglio se sta avendo un impatto sull'uso della regola di ricerca ibrida Webex. A tale scopo, è possibile rivedere xConfig questa volta cercando la regola di ricerca denominata "a DNS"

```
*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"
```

Dopo aver esaminato questa regola di ricerca, è possibile concludere quanto segue:

- La stringa del modello corrisponderà all'URI della richiesta Cisco Webex
- La priorità è impostata su 100
- L'avanzamento (comportamento del modello) è impostato su Interrompi.

Queste informazioni indicano che l'URI della richiesta Cisco Webex richiamato corrisponde a questa regola e che, se la regola viene soddisfatta, Expressway interrompe la ricerca (prendendo in considerazione) altre regole di ricerca. In questo modo, la priorità della regola diventa un fattore chiave. La priorità della regola di ricerca Expressway funziona quando viene tentata per prima la regola con priorità più bassa. Di seguito è riportato un esempio.Regola di ricerca: LocaleComportamento motivo: ContinuaPriorità 1Regola di ricerca: AdiacenteComportamento motivo: ContinuaPriorità 10Regola di ricerca: DNSComportamento motivo: InterrompiPriorità 50In questo esempio, viene tentata prima la regola di ricerca denominata Locale (1) e, se viene trovata una corrispondenza, viene spostata nella regola di ricerca Adiacente (10) a causa del comportamento Pattern impostato su Continua. Se la regola di ricerca Neighbor non corrisponde, continuerà a cercare DNS regola (50) e prenderà in considerazione quest'ultima. Se il DNS della regola di ricerca corrisponde, la ricerca viene interrotta indipendentemente dal fatto che vi sia un'altra regola di ricerca con una priorità superiore a 50, in quanto il comportamento Pattern è impostato su Stop. Sulla base di queste informazioni, è possibile esaminare le priorità della regola di ricerca tra le regole "to DNS" e "Webex Hybrid - to Webex Cloud".

```
*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"
```

Qui, potete vedere che la regola "to DNS" ha una priorità più bassa della regola "Webex Hybrid - to Webex Cloud" — quindi, la regola "to DNS" verrà provata per prima. Poiché il comportamento del modello (Progress) è impostato su Stop, Expressway-E non considera mai la regola Webex Hybrid - to Webex Cloud e la chiamata alla fine non riesce. SoluzioneQuesto tipo di problema è sempre più comune con Hybrid Call Service Connect. In molti casi, quando la soluzione viene implementata, gli utenti creano una regola con priorità alta da utilizzare per le ricerche Cisco Webex. In molti casi la regola creata non viene richiamata perché le regole con priorità inferiore esistenti vengono confrontate e si verifica un errore. Questo problema si verifica su chiamate in entrata e in uscita verso Cisco Webex. Per risolvere il problema, è necessario eseguire la procedura seguente:

1. Accedere a Expressway-E
2. Passare a Configurazione > Piano di composizione > Regole di ricerca
3. Individuare la regola Webex Hybrid Search e fare clic su di essa *(ad esempio, Nome: Webex Hybrid (a Webex Cloud)*
4. Impostare il valore di Priorità su un valore inferiore rispetto alle altre regole di ricerca, ma sufficientemente alto da non influire sugli altri. *(es: Priority: 99)*

La regola generale con le regole di ricerca è che più specifica è la stringa Pattern, minore è la sua posizione nell'elenco di priorità delle regole di ricerca. In genere una zona DNS è configurata con una stringa Pattern che intercetta qualsiasi elemento che non sia un dominio locale e lo invia a Internet. Per questo motivo, è consigliabile impostare il tipo di regola di ricerca su una priorità alta in modo che venga richiamato per ultimo. Problema 4. Configurazione errata di CPL ExpresswayLa soluzione Expressway consente di ridurre le frodi mediante l'utilizzo della logica CPL (Call Processing Language) disponibile sul server. Se la soluzione Expressway in fase di implementazione viene utilizzata solo per il servizio Cisco Webex Hybrid Call e per l'accesso remoto e mobile, si consiglia di abilitare e implementare i criteri e le regole della licenza CPL. Mentre la configurazione CPL su Expressway per Cisco Webex Hybrid è abbastanza semplice, se configurata in modo errato può facilmente bloccare i tentativi di chiamata. Gli scenari riportati di seguito mostrano come utilizzare la registrazione diagnostica per identificare una configurazione errata del file CPL.Come tutti gli altri scenari di chiamate interurbane in uscita, i sintomi sono rimasti gli stessi:

- L'app Cisco Webex dell'utente chiamato ha presentato un pulsante di accesso
- Il telefono che ha chiamato stava riproducendo un squillo
- Squilla il telefono locale dell'utente chiamato
- L'app dell'utente chiamato non ha mai squillato

Come tutti gli altri scenari, è possibile utilizzare le tracce SDL CUCM insieme ai log di diagnostica Expressway-C ed E. Come in precedenza, è necessario fare riferimento alla per utilizzare Cronologia ricerche e suggerimenti per identificare una chiamata nei log di diagnostica. Come in precedenza, è stato determinato utilizzando la Cronologia ricerche Expressway-E che la chiamata è arrivata lì e non è riuscita. Di seguito è riportato l'inizio dell'analisi in cui è possibile esaminare l'INVITO SIP iniziale in arrivo in Expressway-E da Expressway-C.

```
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-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
 Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
 Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
 From: "Jonathan Robb"




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




 Max-Forwards: 15
 Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5061;transport=tls;lr>
 Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5060;transport=tcp;lr>
 Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
 User-Agent: Cisco-CUCM11.5
 Expires: 180
 Date: Mon, 25 Sep 2017 20:54:43 GMT
 Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
 Session-Expires: 1800
 Min-SE: 1800
 Allow-Events: presence
 X-TAATag: 4fffefed-0512-4067-ac8c-35828f0a1150
 Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
 Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
 Content-Type: application/sdp
 Content-Length: 714

<SDP Omitted>
```

Utilizzando l'ID chiamata (c030f100-9c916d13-1cdcb-1501a8c0) dall'intestazione SIP, è possibile cercare rapidamente tutti i messaggi associati a questa finestra di dialogo. Quando si osserva il terzo hit nei log per Call-ID, si nota che Expressway-E invia immediatamente un 403 Vietato a Expressway-C.

```
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
```

Per comprendere il motivo per cui Expressway-E ha negato la chiamata e ha inviato un errore 403 Vietato a Expressway-C, è necessario analizzare le voci di log comprese tra la 403 Vietato e l'INVITO SIP originale immesso in Expressway. L'analisi di queste voci di log consente in genere di visualizzare tutte le decisioni logiche in corso. Si noti che non viene visualizzata alcuna regola di ricerca richiamata, ma viene visualizzata la logica CPL (Call Process Language) richiamata. Di seguito ne viene riportato un frammento.

```
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:

          "
```

In base all'analisi del registro di cui sopra. è possibile stabilire che la CPL rifiuta la chiamata.

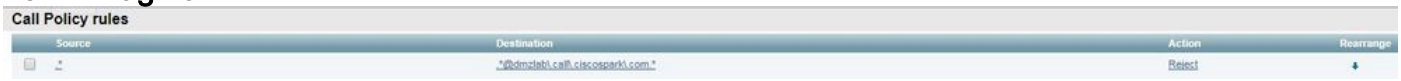
```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-
alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-
number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4fffefed-0512-4067-ac8c-35828f0a1150"
Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-25
20:54:43,726"
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Call Rejected" Service="SIP" Src-
ip="192.168.1.5" Src-port="26404" Src-alias-type="SIP"
```

*Nota: In questa situazione non sarà possibile visualizzare le regole di ricerca richiamate perché le CPL, FindMe e Transforms vengono elaborate prima di una regola di ricerca*Nella maggior parte dei casi, è possibile utilizzare xConfig di Expressway per comprendere meglio le circostanze. Tuttavia, per le CPL, non è possibile visualizzare le regole definite, solo se il criterio è abilitato. Di seguito è riportata la parte di xConfig che mostra come Expressway-E stia utilizzando la logica CPL locale.

```
*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"
```

Per comprendere meglio la configurazione della regola, è necessario accedere a Expressway-E e selezionare Configurazione > Criterio di chiamata > Regole come mostrato

nell'immagine.



Durante il controllo di questa configurazione, è possibile verificare quanto segue è configuratoFonte: .*Destinazione: .*@dmzlab\.call\.ciscospark\.com.*Azione: RifiutaRispetto a quanto documentato nella *Cisco Webex Hybrid Call Service Deployment Guide*, è possibile notare che l'origine e la destinazione sono state configurate in senso inverso.

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**

SoluzionePer risolvere il problema, è necessario modificare la configurazione della regola CPL in modo che l'origine sia impostata su .*@%Webex_subdomain%\.call\.ciscospark\.com.* e il modello di destinazione sia .*

1. Accedere a Expressway-E
2. Selezionare Configurazione > Criterio chiamata > Regole
3. Selezionare la regola impostata per il servizio Cisco Webex Hybrid Call
4. Immettere il modello di origine come .*@%Webex_subdomain%\.call\.ciscospark\.com.*(ad esempio: .*@dmzlab\.call\.ciscospark\.com.*)
5. Immettere il modello di destinazione come .*
6. Selezionare Salva

Per ulteriori informazioni sull'implementazione CPL di Webex Hybrid, consultare la Cisco Webex Hybrid Design Guide. Bidirezionale: Cisco Webex per operazioni locali o Cisco Webex per operazioni locali Problema 1. IP Phone/Collaboration Endpoint offre un codec audio diverso da G.711, G.722 o AAC-LD.Hybrid Call Service Connect supporta tre codec audio diversi: G.711, G.722 e AAC-LD. Per effettuare correttamente una chiamata con l'ambiente Cisco Webex, è necessario utilizzare uno di questi codec audio. L'ambiente locale può essere configurato in modo da utilizzare molti tipi di codec audio, ma allo stesso tempo può essere configurato per limitarli. Questo può accadere intenzionalmente o involontariamente utilizzando le impostazioni di area personalizzate e/o predefinite in Unified CM. Per questo particolare comportamento, i modelli di registrazione possono variare in base alla direzione della chiamata e se Unified CM è stato configurato per l'utilizzo di un'offerta anticipata o ritardata. Di seguito sono riportati alcuni esempi di diverse situazioni in cui questo comportamento potrebbe presentarsi:

1. Cisco Webex invia un INVITE in entrata con SDP che offre G.711, G.722 o AAC-LD. Expressway-C invia questo messaggio a Unified CM, ma Unified CM è configurato per consentire solo la chiamata G.729. Unified CM rifiuta la chiamata perché non è disponibile alcun codec.
2. Unified CM tenta la chiamata in uscita come *offerta anticipata* a Cisco Webex, il che significa che l'INVITE iniziale inviato a Expressway-C conterrà SOLO SDP che supporta l'audio G.729. Cisco Webex invia quindi un messaggio OK 200 con SDP che azzera l'audio (*m=audio 0 RTP/SAVP*) perché non supporta G.729. Una volta che Expressway-C passa questo INVITE a Unified CM, quest'ultimo termina la chiamata perché non è disponibile un

codec.

3. Unified CM tenta la chiamata in uscita come *offerta ritardata* a Cisco Webex, il che significa che l'INVITE iniziale inviato a Expressway-C non conterrà SDP. Cisco Webex invia quindi un messaggio con 200 OK e SDP contenente tutti i codec audio supportati da Cisco Webex. Expressway-C invia il messaggio 200 OK a Unified CM, ma Unified CM è configurato solo per consentire la chiamata a G.729. Unified CM rifiuta la chiamata perché non è disponibile alcun codec.

Se si sta tentando di identificare un errore di chiamata alla connessione del servizio di chiamata ibrida che corrisponde a questo problema, è necessario ottenere i log di Expressway oltre alle tracce SDL di Unified CM. I frammenti di log di esempio riportati di seguito corrispondono alla situazione n. 2 in cui Unified CM sta tentando di effettuare la chiamata in uscita come *offerta anticipata*. Poiché sappiamo che la chiamata sta per arrivare a Cisco Webex, l'analisi del registro inizia su Expressway-E.Di seguito è riportato un estratto dell'invito iniziale a Cisco Webex. Il codec audio preferito è impostato su G.729 (Payload 18). Il valore 101 è per DTMF e per questo particolare scenario non è rilevante.

```
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-55aedea256d2;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=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
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-
55aedea256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aedea256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
Supported: X-cisco-srtp-fallback,replaces,timer
Session-Expires: 1800;refresher=uac
Min-SE: 500
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Length: 1407

v=0
```

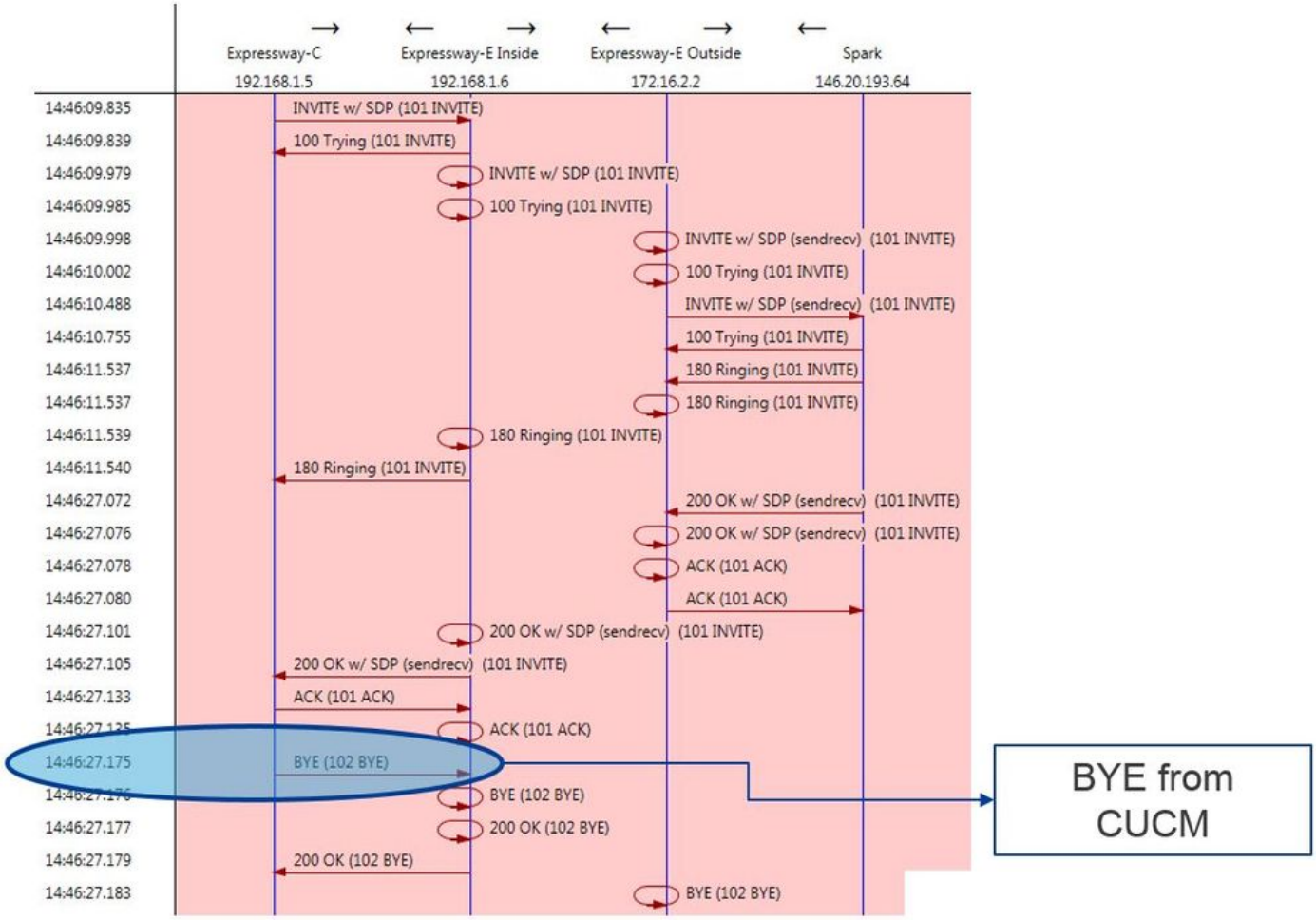
```
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
c=IN IP4 64.102.241.236
b=AS:384
t=0 0
m=audio 52668 RTP/SAVP 18 101  <-- CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....................................
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....................................
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....................................
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....................................
UNENCRYPTED_SRTCP
a=sendrecv
a=rtcp:52669 IN IP4 64.102.241.236
m=video 52670 RTP/SAVP 126 97
b=TIAS:384000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801e;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....................................
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....................................
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....................................
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....................................
UNENCRYPTED_SRTCP
a=sendrecv
a=content:main
a=label:11
a=rtcp:52671 IN IP4 64.102.241.236
```

In risposta all'INVITO iniziale, Cisco Webex risponde con un messaggio di 200 OK. Se guardate più da vicino questo messaggio, potete vedere che il codec audio è stato azzerato. Questo è un problema perché senza una porta audio assegnata, la chiamata non sarà in grado di negoziare il flusso.

```
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-55aedea256d2;rport=38245;received=192.168.5.26,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,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=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
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-55aedea256d2@64.102.241.236:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aedea256d2@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-mbps=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
```

Èora possibile utilizzare TranslatorX per esaminare il resto della finestra di dialogo. Potete vedere che la finestra di dialogo stessa viene completata con un ACK. Il problema si verifica subito dopo il completamento della finestra di dialogo ed è presente un BYE che proviene dalla direzione di Expressway-C, come mostrato
nell'immagine.



Di seguito è riportato un esempio dettagliato del messaggio BYE. L'agente utente è Cisco-CUCM11.5, il che significa che il messaggio è stato generato da Unified CM. Un'altra cosa da sottolineare è che il codice motivo è impostato su cause=47. La traduzione comune per questa opzione è Nessuna risorsa disponibile.

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

Poiché il componente Cisco Webex ha azzerato il codec audio per questo esempio di chiamata, lo stato attivo deve essere su:r. L'INVITE iniziale che è stato inviato a Cisco Webex eb. In che modo Cisco Webex ha azzerato questa porta?Esaminando ora l'aspetto unico di INVITE iniziale, è

possibile notare che contiene solo G.729. Sapendo ciò, consultare la Cisco Webex Hybrid Call Service Deployment Guide e consultare in modo specifico il capitolo Prepare Your Environment in cui il passo 5 della sezione Complete the Prerequisites for Hybrid Call Service Connect richiama i codec specifici supportati. Lì vedremmo questo:Cisco Webex supporta i seguenti codec:

- Audio: G.711, G.722, AAC-LD
- Video: H.264

Nota: Opus non viene utilizzato nella fase in sede della chiamata per Cisco Webex Hybrid Call. Con queste informazioni a portata di mano, è possibile concludere che Unified CM sta inviando un codec audio non supportato; questa è la ragione per cui Cisco Webex sta azzerando la porta. Soluzione:Per risolvere questa particolare situazione, potrebbe essere necessario rivedere la configurazione dell'area tra il dispositivo Cisco Webex RD che sta ancorando la chiamata in locale e il trunk SIP per Expressway-C. A tale scopo, determinare il pool di dispositivi in cui si trovano questi due elementi. Il pool di dispositivi contiene i mapping alle aree. Per determinare il pool di dispositivi del trunk SIP Expressway-C:

1. Accedere a Unified CM.
2. Selezionare Dispositivo > Trunk.
3. Cercare il nome del trunk o fare clic su Trova.
4. Selezionare il trunk Expressway-C.
5. Registrare il nome del pool di dispositivi.

Per determinare il pool di dispositivi del CTI-RD o Cisco Webex-RD a cui è stata ancorata la chiamata:

1. Selezionare Dispositivo > Telefono.
2. Durante la ricerca, è possibile selezionare Tipo di dispositivo contiene Webex o CTI Remote Device (a seconda del tipo di dispositivo utilizzato dal cliente).
3. Registrare il nome del pool di dispositivi.

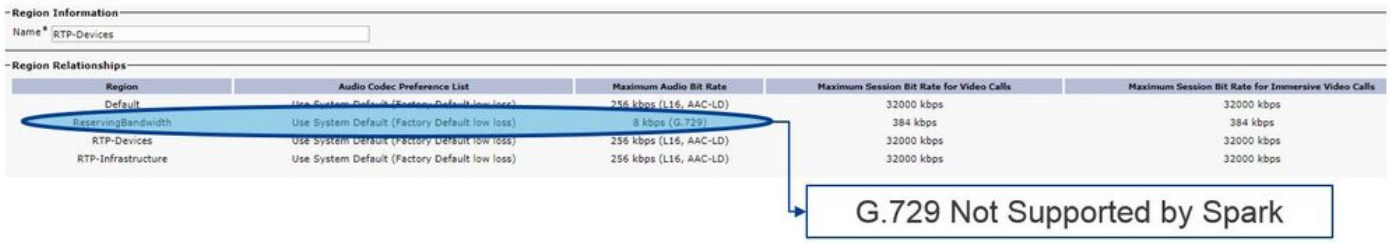
Determinare la regione collegata a ciascun pool di dispositivi:

1. Selezionare Sistema > Pool di dispositivi.
2. Cercare il pool di dispositivi utilizzato per il trunk SIP Expressway-C.
3. Fare clic su Pool di dispositivi.
4. Registrare il nome dell'area.
5. Cercare il pool di dispositivi utilizzato per Webex-RD o CTI-RD.
6. Fare clic su Pool di dispositivi.
7. Registrare il nome dell'area.

Determinare la relazione di area:

1. Passare a Sistema > Informazioni area > Area.
2. Cercare in una delle aree identificate.
3. Determinate se esiste una relazione di regione tra entrambe le regioni che utilizzano G.729.

A questo punto, se si identifica la relazione che sta utilizzando G.729, sarà necessario regolare la relazione in modo che supporti i codec audio supportati da Cisco Webex o utilizzare un pool di dispositivi diverso con un'area che supporti questo tipo di relazione. Nello scenario sopra descritto, è stato determinato quanto segue:Area trunk Expressway-C: Prenotazione larghezza di bandaRegione Webex-RD: Dispositivi RTPDi seguito è riportata un'illustrazione grafica della relazione tra le aree RTP-Devices e ReservingBandwidth, come mostrato nell'immagine.



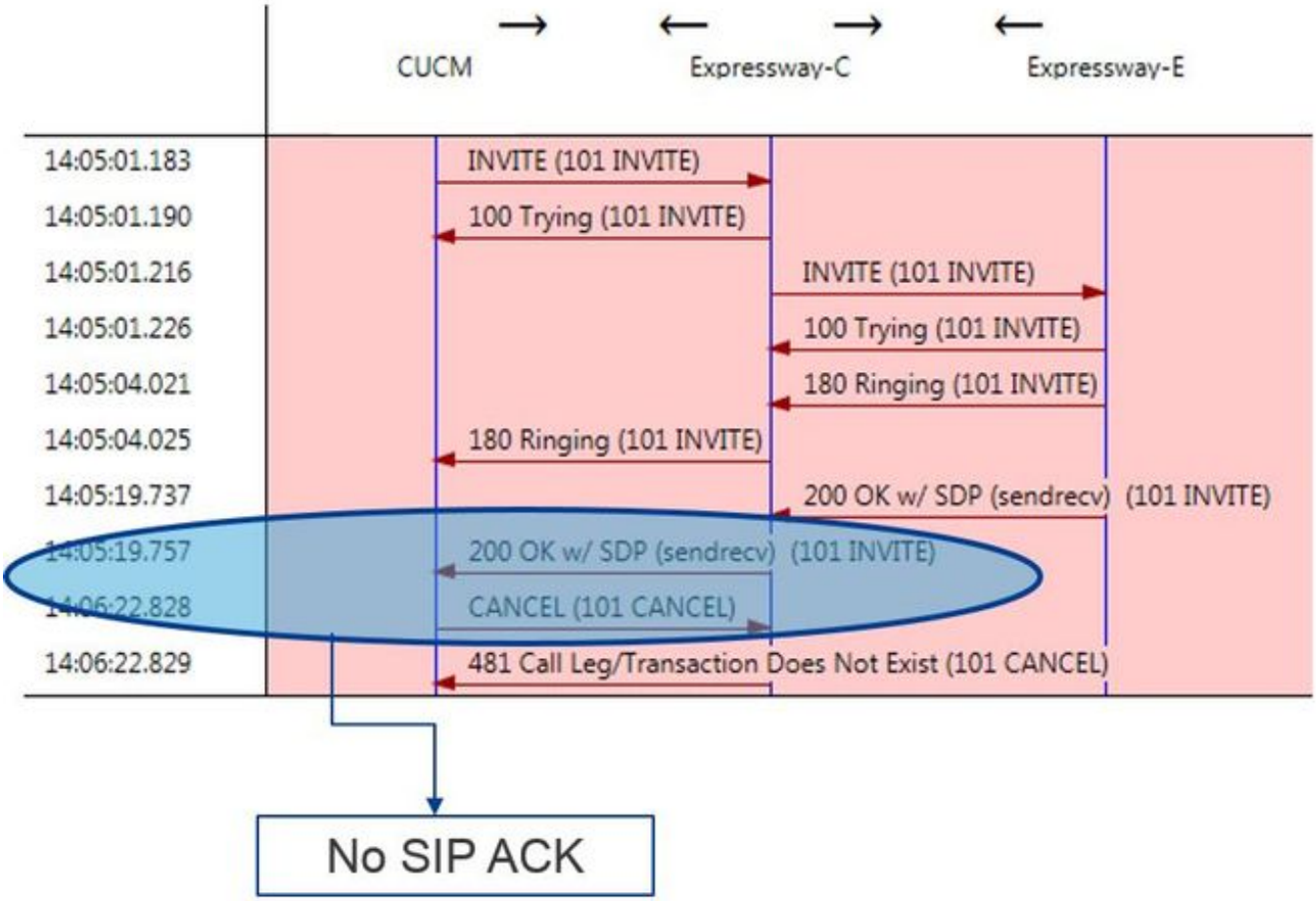
Modificando il pool di dispositivi in cui si trovava il trunk Expressway-C, si modifica la relazione Region. Il nuovo pool di dispositivi ha una regione impostata su RTP-Infrastructure, quindi la nuova relazione della regione tra il trunk Cisco Webex-RD e Expressway-C è RTP-Devices e RTP-Infrastructure. Come mostrato nell'immagine, questa relazione supporta AAC-LD, che è uno dei codec audio supportati da Cisco Webex, quindi la chiamata verrà configurata correttamente. Problema 2. È stata superata la dimensione massima dei messaggi in arrivo di Unified CMPoiché i video sono diventati sempre più diffusi all'interno dell'azienda, la dimensione dei messaggi SIP che contengono SDP è aumentata in modo sostanziale. I server che elaborano questi messaggi devono essere configurati in modo da poter accettare un pacchetto di grandi dimensioni. In molti server di controllo delle chiamate i valori predefiniti sono corretti. In Cisco Unified Communications Manager (Unified Communications Manager), i valori predefiniti per la gestione di un messaggio SIP di grandi dimensioni contenente SDP non erano supportati nelle versioni precedenti. Nelle versioni più recenti di Unified CM, le dimensioni consentite per un messaggio SIP sono state aumentate, ma questo valore viene impostato solo nelle nuove installazioni, non negli aggiornamenti. Ciò detto, i clienti che stanno aggiornando le release precedenti di Unified CM per supportare Hybrid Call Service Connect potrebbero essere interessati dal fatto che il valore di Dimensione massima messaggi in arrivo su Unified CM è troppo basso.Se si sta tentando di identificare un errore di chiamata Hybrid Call Service Connect che corrisponde a questo problema, è necessario ottenere i log di Expressway oltre alle tracce SDL di Unified CM. Al fine di identificare il guasto, prima di tutto, capire cosa succede e poi i tipi di scenari in cui il guasto può verificarsi.Per rispondere alla domanda relativa a cosa accade, è necessario sapere che quando Unified CM riceve un messaggio SIP troppo grande, chiude semplicemente il socket TCP e non risponde a Expressway-C.Detto questo, ci sono molte situazioni e modi in cui questo può accadere:

1. Cisco Webex invia un INVITE in entrata con SDP troppo grande. Expressway-C passa questo messaggio a Unified CM e Unified CM chiude il socket TCP, quindi la finestra di dialogo SIP si interrompe.

2. Unified CM tenta la chiamata in uscita come Early Offer to Webex, il che significa che l'INVITE iniziale inviato a Expressway-C conterrà SDP. Cisco Webex invia quindi un messaggio di conferma di 200 OK con SDP in risposta e la risposta di conferma di 200 OK, quando passata da Expressway-C a Unified CM, è troppo grande. Unified CM chiude il socket TCP, quindi la finestra di dialogo SIP si interrompe.

3. Unified CM tenta la chiamata in uscita come offerta ritardata a Webex, il che significa che l'invito iniziale inviato a Expressway-C non conterrà SDP. Cisco Webex invia quindi un messaggio di 200 OK con SDP e l'offerta 200 OK, quando viene passata da Expressway-C a Unified CM, è troppo grande. Unified CM chiude il socket TCP, quindi la finestra di dialogo SIP si interrompe.

L'analisi dei registri di Expressway-C per questa particolare condizione consente di comprendere il flusso dei messaggi. Se si dovesse utilizzare un programma come TranslatorX, si potrebbe notare che Expressway-C sta passando Cisco Webex 200 OK w/ SDP a Unified CM. Il problema è che Unified CM non risponde mai con un SIP ACK, come mostrato nell'immagine.



Dal momento che Unified CM è il responsabile della mancata risposta, è opportuno esaminare le tracce SDL per vedere come Unified CM gestisce questa condizione. In questo scenario si noterà che il CM unificato ignora il messaggio di grandi dimensioni inviato da Expressway-C. Verrà stampato un elemento della riga di registro di questo tipo.

```
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.
```

Quando la finestra di dialogo SIP scade, Cisco Webex invia un messaggio di rifiuto SIP 603 in entrata a Expressway-E, come indicato nell'esempio di registro.

```
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
```

Come accennato, ci sono tre diversi scenari in cui potete vedere questo comportamento. Per chiarezza, gli esempi di log forniti in questa illustrazione corrispondono alla situazione 3 in cui la chiamata è stata inviata in uscita a Cisco Webex come offerta ritardata. Soluzione:

1. Accedere a Unified CM.
2. Passare a Sistema > Parametri servizio.
3. Selezionare il server che esegue il servizio Gestione chiamate.

4. Quando viene richiesto di selezionare un servizio, scegliere il servizio Cisco Call Manager.
5. Selezionare l'opzione avanzata.
6. Nelle impostazioni Clusterwide Parameters (Device - SIP), modificare SIP Max Incoming Message Size (Dimensione massima messaggi in arrivo SIP) in 18000.
7. Selezionare Salva.
8. Ripetere questa procedura per ogni nodo Unified CM che esegue il servizio Cisco Call Manager.

Nota: Affinché un telefono IP, un endpoint di collaborazione e/o un trunk SIP possano sfruttare questa impostazione, è necessario riavviarlo. Questi dispositivi possono essere riavviati singolarmente per ridurre al minimo l'impatto sull'ambiente. NON reimpostare ogni dispositivo su CUCM a meno che non sia assolutamente accettabile.

Appendice

Strumenti di risoluzione dei problemi di Expressway

Utilità verifica motivo

Expressway dispone di un'utilità di verifica dei pattern utile quando si desidera verificare se un pattern corrisponde a un particolare alias e viene trasformato nel modo previsto. L'utilità è disponibile in Expressway nell'opzione di menu Manutenzione > Strumenti > Controlla pattern. In genere, questa opzione viene utilizzata se si desidera verificare se il regex della regola di ricerca deve corrispondere correttamente a un alias di una stringa di modello e quindi, facoltativamente, eseguire la modifica della stringa. Per la connessione Hybrid Call Service, è inoltre possibile verificare che il nome di dominio completo (FQDN) del cluster CM unificato corrisponda alla stringa Pattern impostata per il nome di dominio completo del cluster CM unificato. Quando si utilizza questa utilità, tenere presente che la chiamata verrà instradata in base al parametro FQDN del cluster CM unificato elencato nell'intestazione della route, non in base all'URI di destinazione. Ad esempio, se il seguente invito è stato inviato in Expressway, verificare la funzionalità di verifica del motivo confrontandola con cucm.rtp.ciscotac.net, non con jorobb@rtp.ciscotac.net.

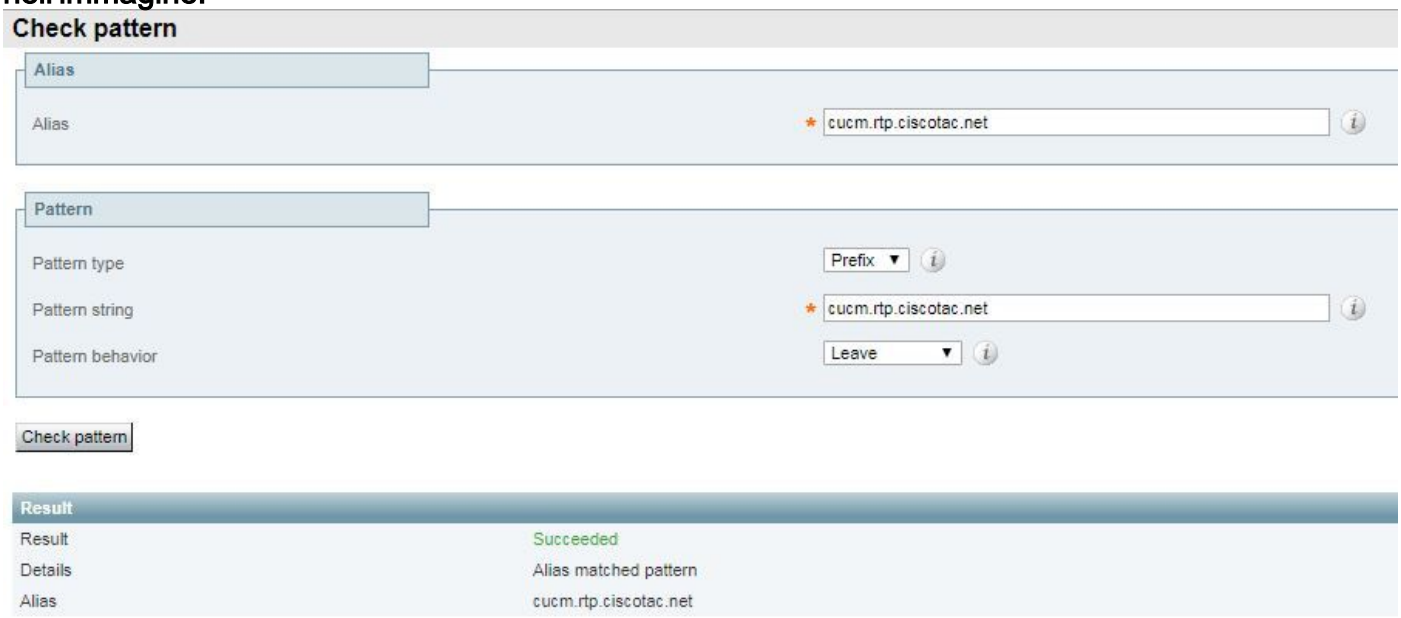
```
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-
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: "pstojano test" <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=145765215
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

Per utilizzare il criterio Check per verificare il routing della regola di ricerca dell'intestazione della route di connessione del servizio chiamate ibride, eseguire la procedura seguente:

1. Passare a Manutenzione > Strumenti > Modello di controllo.
2. Per l'alias, immettere l'FQDN del cluster CM unificato.

3. Impostate il tipo di serie su Prefisso (Prefix).
4. Impostare la stringa del modello su FQDN cluster CM unificato.
5. Impostate il comportamento Pattern su Leave (Esci).
6. Selezionare Modello di controllo.

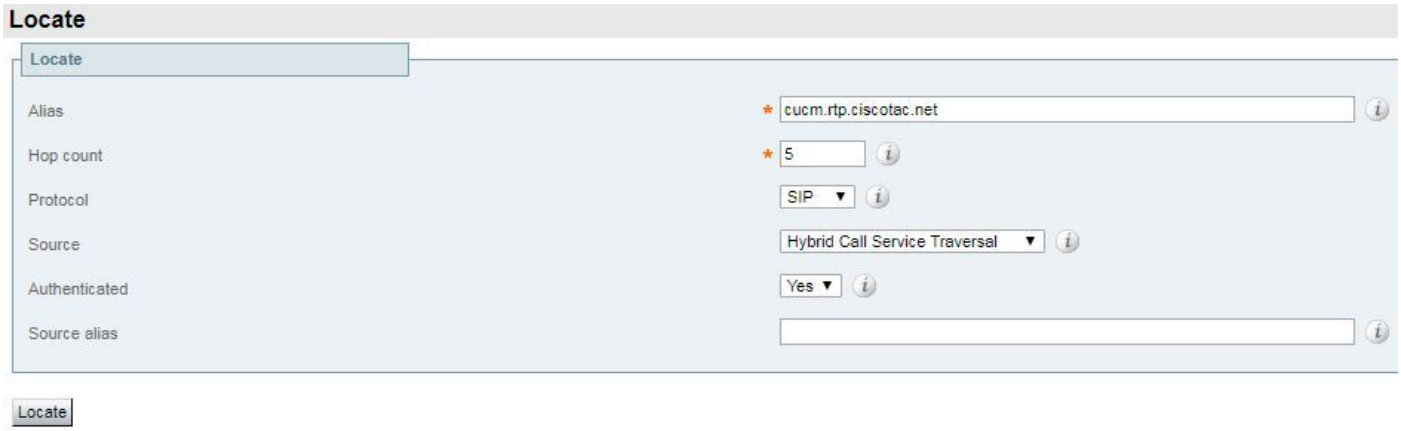
Se le regole di ricerca in Expressway sono configurate correttamente, è possibile che venga visualizzato il messaggio Risultati restituiti: Operazione completata. Di seguito è riportato un esempio di test riuscito del motivo Check, come mostrato nell'immagine.



L'esito di questa operazione è dovuto al fatto che l'alias (cucm.rtp.ciscotac.net) corrisponde alla stringa del motivo Prefisso di (cucm.rtp.ciscotac.net). Per comprendere come viene instradata una chiamata in base a questi risultati, è possibile utilizzare l'utilità di ricerca di Expressway descritta.Utilità TrovaL'utilità Individua di Expressway è utile se si desidera verificare se Expressway è in grado di instradare una chiamata a una particolare zona in base a un determinato alias. Tutto questo può essere completato senza dover fare una vera chiamata. L'utilità Trova è disponibile in Expressway nel menu Manutenzione > Strumenti > Trova. Verranno visualizzate alcune istruzioni su come utilizzare la funzionalità Individua in Expressway-C per determinare se il server può instradare una chiamata in base all'FQDN del cluster CM unificato trovato nell'intestazione della route SIP.

1. Passare a Manutenzione > Strumenti > Individua.
2. Immettere il nome di dominio completo (FQDN) del cluster CM unificato nel campo Alias.
3. Selezionare SIP come protocollo.
4. Selezionare la zona client Cisco Webex Hybrid Traversal per l'origine.
5. Selezionare Individua.

Nella parte inferiore dell'interfaccia verranno visualizzati i risultati della ricerca. Di seguito è riportato un esempio del test di esempio eseguito con i risultati corrispondenti, come mostrato nell'immagine.



Ecco i risultati della ricerca. I valori di interesse sono in grassetto. Questi risultati mostrano:

- Possibilità di instradare l'alias (True)
- Informazioni origine (nome/tipo zona)
- Informazioni sulla destinazione (alias da instradare)
- Regola di ricerca corrispondente (routing in entrata servizio chiamate ibride)
- Zona a cui verrà inviata la chiamata (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
```

Registrazione diagnosticaIn qualsiasi momento si stia risolvendo un problema relativo a una chiamata o ai supporti per una chiamata che attraversa la soluzione Expressway, è necessario utilizzare la registrazione diagnostica. Questa funzionalità di Expressway offre a un tecnico un elevato livello di dettaglio delle informazioni relative a tutte le decisioni logiche che Expressway è in grado di gestire durante il passaggio della chiamata. Potete vedere il corpo completo dei messaggi SIP, il modo in cui Expressway passa il collegamento e come Expressway imposta i canali multimediali. La registrazione diagnostica dispone di diversi moduli che alimentano la

registrazione. I livelli di registrazione possono essere regolati in modo da visualizzare FATAL, ERROR, WARN, INFO, DEBUG, TRACE. Per impostazione predefinita, è impostato su INFO che acquisisce quasi tutto ciò che è necessario per diagnosticare un problema. Di tanto in tanto, potrebbe essere necessario regolare un livello di log di un particolare modulo da INFO a DEBUG per avere una migliore comprensione di ciò che sta accadendo. La procedura riportata di seguito illustra come è possibile modificare i livelli di log del modulo developer.ssl, responsabile della fornitura di informazioni per gli handshake (reciproci) TLS.

1. Accedere al server Expressway (deve essere eseguito sia su Expressway-E che su C).
2. Selezionare Manutenzione > Diagnostica > Avanzate > Configurazione log di supporto.
3. Scorrere fino al modulo che si desidera regolare, in questa istanza developer.ssl e fare clic su di esso.
4. Accanto al parametro Level, scegliere DEBUG dal menu.
5. Fare clic su Salva.

A questo punto è possibile acquisire la registrazione diagnostica:

1. Accedere al server Expressway (deve essere eseguito sia su Expressway-E che su C).
2. Selezionare Manutenzione > Diagnostica > Registrazione diagnostica.
3. Fare clic su Start New Log (assicurarsi di selezionare l'opzione tcpdump).
4. Riprodurre il problema.
5. Fare clic su Interrompi registrazione.
6. Fare clic su Scarica registro.

Per la registrazione diagnostica di Expressway, tenere presente che la registrazione verrà avviata sia da Expressway-C che da Expressway-E in parallelo: iniziare la registrazione su Expressway-E, quindi passare a Expressway-C e avviarlo. A quel punto, si può riprodurre il problema.Nota: Attualmente, il bundle del registro di diagnostica di Expressway/VCS non contiene informazioni sul certificato del server Expressway o sull'elenco di CA attendibili. Se si verifica un caso in cui l'utilizzo di questa funzionalità risulta utile, allegare la richiesta a questo problema.

Informazioni correlate

- Guida all'implementazione dei servizi Cisco Webex Hybrid Call
- Cisco Webex Hybrid Design Guide
- Guida per l'amministratore di Cisco Expressway
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).