マルチドメイン展開での Expressway/VCS 経由の Mobile and Remote Access の設定

目次

概要

このドキュメントでは、複数のドメインを使用する場合に、Mobile Remote Access（MRA）に対応するため Cisco TelePresence Video Communication Server（VCS）を設定する方法を説明します。

ドメインが 1 つだけの MRA セットアップは比較的単純であり、導入ガイドに記載されている手順に従って作業できます。 複数のドメインを使用する導入の場合、これは複雑になります。 このドキュメントは構成ガイドではありませんが、複数ドメインを使用する場合の重要な側面について説明します。 主な設定については、『Cisco TelePresence Video Communication Server (VCS) 導入ガイド』で説明しています。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

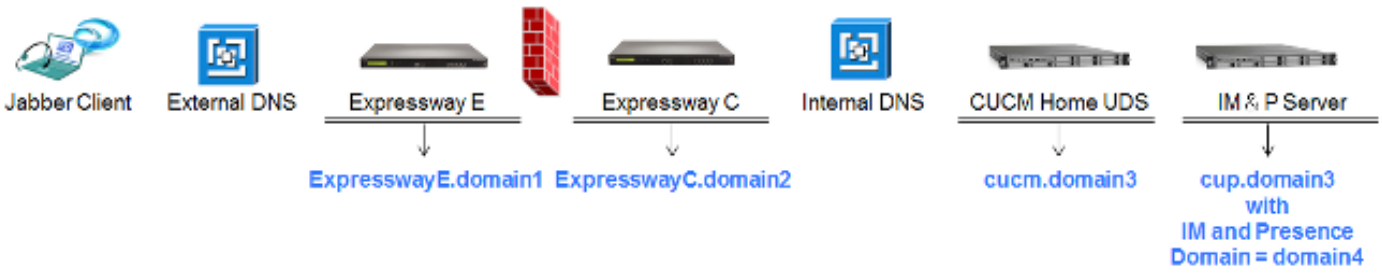
このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

この項で説明する情報を使用して、VCS を設定します。

ネットワーク図

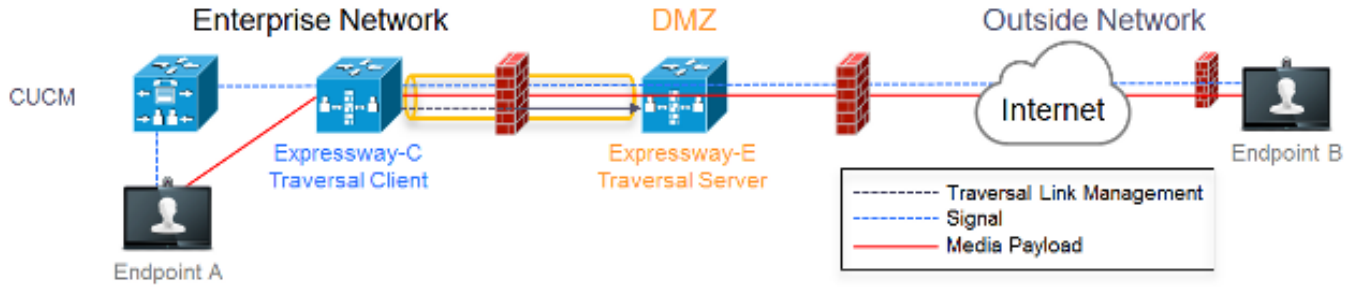


各ドメインの簡単な概要を次に示します。

- **domain1**：これは、クライアントがエッジ サーバの位置を検出するために使用するエッジ ドメインです。このドメインを介して、ユーザ データ サービス（UDS）が検出されます。
- **domain2 および domain3** ：サーバ検出に使用されるドメインです。
- **domain4** ：Extensible Communications Platform（XCP）トラフィックおよび Extensible Messaging and Presence Protocol（XMPP）トラフィックにより使用される Instant Messaging and Presence（IM&P）ドメインです。

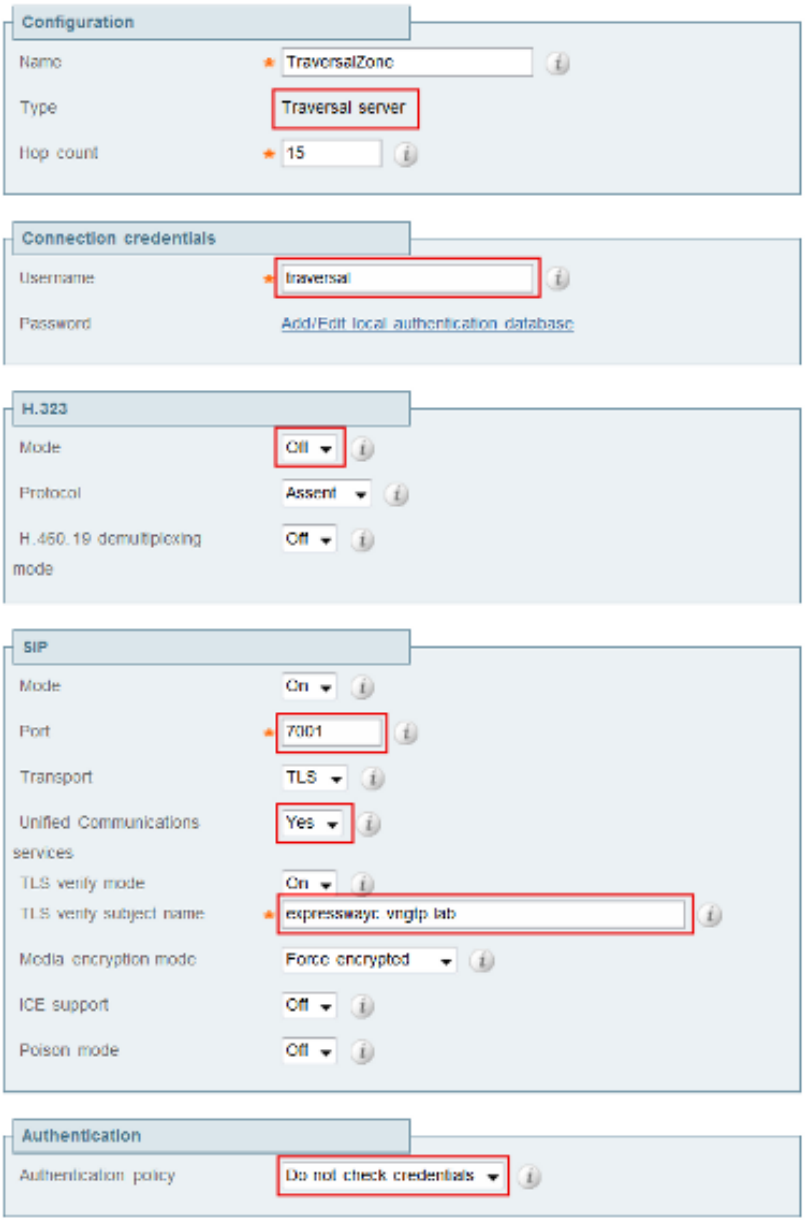
トラバーサル ゾーン

トラバーサル ゾーンは、非武装地帯（DMZ）にあるトラバーサル サーバ（**expresswayE**）と、ネットワーク内部にあるトラバーサル クライアント（**expresswayC**）で構成されています。



Traversal Server

トラバーサル サーバは、Expressway E のゾーン構成にあります。



Select type as Traversal Server

Configure username for Traversal Client to authenticate with with server

H.323 Mode must be set to off

Port 7001 is default listening port for Traversal Client connection

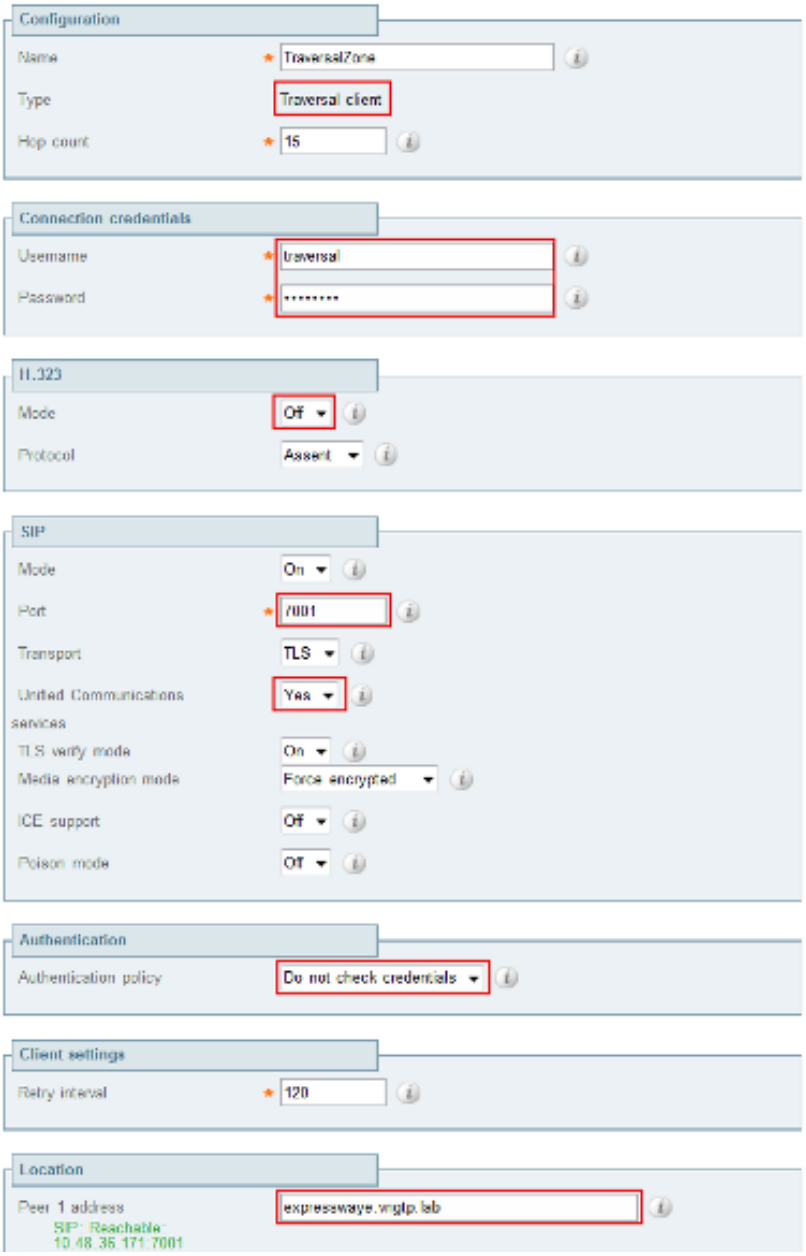
Unified Communications services must be enabled

Must match CN from certificate presented by Traversal Client (Expressway C)

Must be set to 'Do not check credentials' as expressway does not register any endpoints

Traversal Client

トラバーサル クライアントは、Expressway C のゾーン構成にあります。



Select Traversal Client as Type

Configure same username and password as added on the Traversal Server (Expressway E)

H.323 mode must be set to off

Destination port Traversal Server is listening on

Unified Communications must be enabled

Must be set to 'Do not check credentials' as expressway does not register any endpoints

Must be FQDN
Must be DNS resolvable
Must match CN from certificate presented by Traversal Server (Expressway E)

音声サービス ドメイン

内外でのユーザ エクスペリエンスで違いがないようにするため、ユーザは常に **userid@domain4** を使用してログインします。 つまり、**domain1** が **domain4** と異なる場合、Jabber クライアントで音声サービス ドメインを設定する必要があります。 これは、サービス（SRV）レコード検索を使用した Collaboration Edge サービスの検出に、ログインのドメイン部分が使用されるためです。

クライアントは **_collab-edge._tls.<domain>** に対するドメイン ネーム システム（DNS）SRV レコード クエリを実行します。 つまり、ログイン ユーザ ID のドメインが Expressway E のドメインと異なる場合、音声サービス ドメイン設定を使用する必要があります。 Jabber は、Collaboration Edge と UDS の検出にこの設定を使用します。

このタスクを実行するために使用できるオプションが複数あります。

1. メディア サービス インターフェイス（MSI）を使用して Jabber をインストールするときに、次をパラメータとして追加します。

```
msiexec /i CiscoJabberSetup.msi VOICE_SERVICES_DOMAIN=domain1 CLEAR=1
```

2. [%APPDATA%] > [Cisco] > [Unified Communications] > [Jabber] > [CSF] > [Config] に移動し、ディレクトリ内に次の **jabber-config-user.xml** ファイルを作成します。

```
<?xml version="1.0" encoding="utf-8"?>
<config version ="1.0">
<Policies> <VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
</config>
```

注: この手法は試験的なものであり、シスコは公式にサポートしていません。

3. **jabber-config.xml** ファイルを編集します。 このためには、クライアントが最初に内部でログインする必要があります。 JabberConfig ファイル ジェネレータ をこの目的で使用できます。

```
<Policies>
<VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
```

4. また、音声サービス ドメインを使用してモバイル Jabber クライアントを先行して設定できます。これにより、クライアントが最初に内部でログインする必要がありません。 これについては、『導入およびインストール ガイド』のサービス検出の章で説明します。 ユーザがクリックする必要がある設定 URL を作成する必要があります。

```
ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1
```

注: 外部ドメイン（**domain1**）に対して Collaboration Edge SRV レコードの検索を実行できるようにする必要があるため、音声サービス ドメインを使用する必要があります。

DNS レコード

ここでは、外部および内部 DNS レコードの構成設定について説明します。

外部

タイプ	エントリ	解決後
SRV レコード	_collab-edge._tls.domain1	ExpresswayE.domain1
A レコード	ExpresswayE.domain1	IP アドレス ExpresswayE

次の点に留意してください。

- SRV レコードは完全修飾ドメイン名（FQDN）を返しますが、IP アドレスは返しません。
- SRV レコードにより返される FQDN は、Expressway-E の実際の FQDN に一致している必要があります。一致していない場合、SRV レコードのターゲットが CNAME であり、エイリアスが Expressway-E と同じドメイン内のサーバを指し示します（保留中の Cisco Bug ID CSCuo82526）。

Expressway-E は、専用ドメイン（**domain1**）のクライアントに Cookie を設定するため、これは必須です。FQDN により返されるドメインと一致しない場合、クライアントはこれを受け入れません。 この状況における機能向上のため、Cisco Bug ID CSCuo83458 が登録されました。

内部

タイプ	エントリ	解決後
SRV レコード	_cisco-uds._tcp.domain1	cucm.domain3
A レコード	cucm.domain3	IP アドレス CUCM

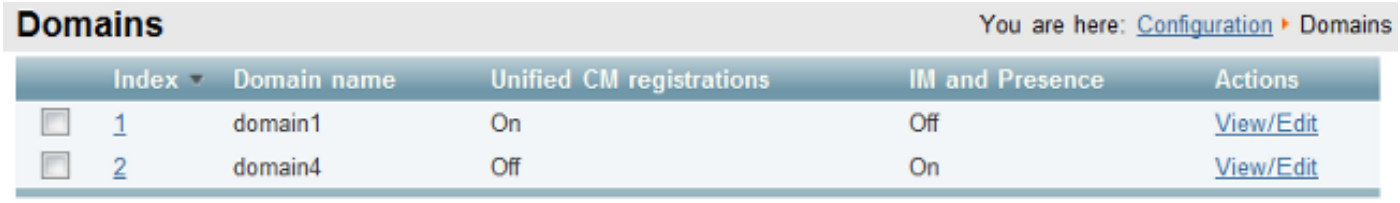
音声サービス ドメインが **domain1** に設定されているので、Collaboration Edge 設定の検出（**get edge_config**）のための変換後 URL に、Jabber により **domain1** が埋め込まれます。 受信後に、Expressway-E は **domain1** に対して SRV UDS レコード クエリを実行し、**200 OK** メッセージでレコードを返します。

タイプ	エントリ	解決後
SRV	_cisco-uds._tcp.domain4	cucm.domain3
A レコード	cucm.domain3	IP アドレス CUCM

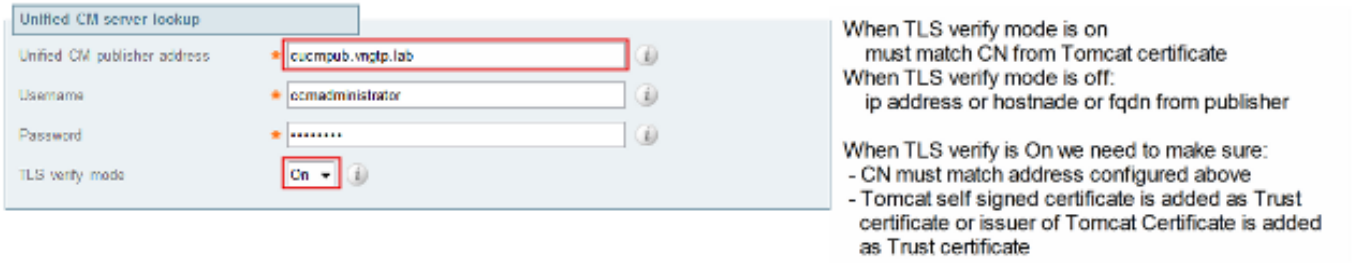
クライアントがネットワークに接続中の場合、**domain4** で SRV UDS レコードの検出が必要です。

Expressway-C の SIP ドメイン

Expressway-C で Session Initiation Protocol（SIP）ドメインを追加し、MRA のために有効にする必要があります。



CUCM サーバのホスト名/IP アドレス



Cisco Unified Communications Manager（CUCM）サーバを設定するとき、2 つのシナリオがあります:

- Expressway-C（**domain2**）が、CUCM サーバと同じドメイン（**domain3**）で設定されている場合、CUCM サーバ（[System] > [Servers]）の次の項目を設定する必要があります。

  IP アドレスホスト名FQDN
- Expressway-C（**domain2**）が、CUCM サーバとは異なるドメイン（**domain3**）で設定されている場合、CUCM サーバの次の項目を設定する必要があります。

  IP アドレスFQDN

Expressway-C が CUCM サーバを検出してホスト名が返されると、**hostname.domain2** に対する

DNS ルックアップが実行されるため、これは必須です。この DNS ルックアップは、**domain2** と **domain3** が異なる場合には機能しません。

証明書

一般的な証明書の要件の他に、証明書のサブジェクト代替名（SAN）に追加する必要がある項目があります。

- Expressway-C

  IM&P サーバで設定されたチャット ノード エイリアスを追加する必要があります。 これは、Transport Layer Security（TLS）およびグループ チャットの両方を使用するユニファイド コミュニケーション XMPP フェデレーション導入環境でのみ必須です。 IM&P サーバがすでに検出されている場合、証明書署名要求（CSR）にこれが自動的に追加されます。

  CUCM 内で、暗号化 TLS に対して設定されており、リモート アクセスを必要とするデバイスに使用されるすべての電話セキュリティ プロファイルの名前（FQDN 形式）を、追加する必要があります。
  注: FQDN 形式が必要となるのは、認証局（CA）で SAN のホスト名構文が許可されていない場合だけです。
- Expressway-E

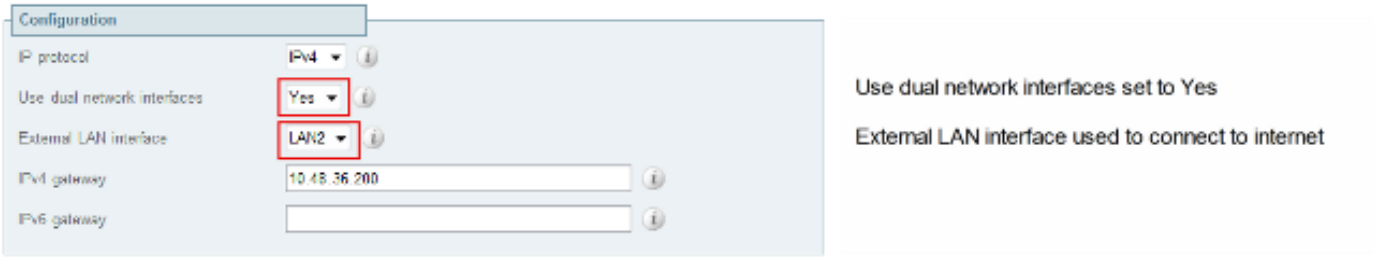
  サービス ディスカバリ（**domain1**）に使用するドメインは追加する必要があります。 XMPP フェデレーション ドメイン。IM&P サーバで設定されたチャット ノード エイリアスを追加する必要があります。 これは、TLS およびグループ チャットの両方を使用するユニファイド コミュニケーション XMPP フェデレーションの導入環境でのみ必須です。 これらは Expressway-C で生成された CSR からコピーできます。

デュアル NIC

ここでは、デュアル ネットワーク インターフェイス カード（NIC）を使用している場合の構成設定について説明します。

2 つのインターフェイス

デュアル ネットワーク インターフェイスを使用するために Expressway-E を設定する場合、両方のインターフェイスを必ず設定および使用することが重要です。



[Use Dual Network Interfaces] に値 [Yes] が設定されている場合、Expressway-E は内部インターフェイスでのみ Expressway-C との XMPP 通信をリッスンします。 したがって、このインターフェイスが正しく設定され、動作していることを確認する必要があります。

1 つのインターフェイス：パブリック IP アドレス

1 つのインターフェイスだけを使用しており、パブリック IP アドレスを使用して Expressway-E を設定する場合、考慮すべき特別な事項はありません。

1 つのインターフェイス：プライベート IP アドレス

1 つのインターフェイスだけを使用し、プライベート IP アドレスを使用して Expressway-E を設定する場合、スタティック ネットワーク アドレス変換（NAT）アドレスも設定する必要があります。

この場合、次の点を確認することが重要です。

- ファイアウォールで、Expressway-C に対しパブリック IP アドレスへのトラフィックの送信が許可されている。 これは *NAT リフレクション* とも呼ばれています。
- Expressway-C のトラバーサル クライアント ゾーンは、Expressway-E のスタティック NAT アドレス（この場合は **20.20.20.20**）と一致するピア アドレスを使用して設定されています。

  ヒント： 高度なネットワーク導入の詳細については、『Cisco TelePresence Video Communication Server の基本設定（Control および Expressway）展開ガイド』の「**付録 4**」を参照してください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

いくつかの特定のシナリオはこのセクションで力バーされますが、また MRA ログイン試行に診断 ログに基づいてすべての通信およびトラブルシューティング情報の詳細な考察を提供するコラボレーション ソリューション アナライザを使用できます。

トラバーサル ゾーン

ピア アドレスが IP アドレスとして設定されているか、またはピア アドレスが共通名（CN）に一致しない場合は、ログに次の情報が記録されます。

```
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.80.161"
Src-port="25697" Dst-ip="10.48.36.171" Dst-port="7001" Detail="Peer's TLS
certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.36.171"
```

パスワードが正しくない場合は、Expressway-E のログに次の情報が記録されます。

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found in
directory for identity: traversal"

Module="developer.nomodule" Level="WARN" CodeLocation="ppcmains/sip/sipproxy/
SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::
checkDigestSAResponse" Thread="0x7f2485cb0700": calculated response does not
match supplied response, calculatedResponse=769c8f488f71eebdf28b61ab1dc9f5e9,
response=319a0bb365decf98c1bb7b3ce350f6ec

Event="Authentication Failed" Service="SIP" Src-ip="10.48.80.161"
Src-port="25723" Detail="Incorrect authentication credential for user"
Protocol="TLS" Method="OPTIONS" Level="1"
```

デュアル NIC

デュアル NIC が有効であるが、2 番目のインターフェイスが使用されていないかまたは接続されていない場合、Expressway-C はポート 7400 での XMPP 通信のために Expressway-E に接続できず、Expressway-C のログに次の情報が記録されます。

```
xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,843" ThreadID=
"139747212576512" Module="Jabber" Level="INFO " CodeLocation="mio.c:1109"
Detail="Connecting on fd 28 to host '10.48.36.171', port 7400"xwayc

XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID="139747212576512"
Module="Jabber" Level="ERROR" CodeLocation="mio.c:1121" Detail="Unable to
connect to host '10.48.36.171', port 7400:(111) Connection refused"

xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID=
"139747406935808" Module="Jabber" Level="ERROR" CodeLocation=
"base_connection.cpp:104" Detail="Failed to connect to component
jabberd-port-1.expresswayc-vngtp-lab"
```

DNS

Collaboration Edge での SRV レコード検索で返される FQDN が、Expressway-E で設定されている FQDN と一致しない場合、Jabber のログに次のエラーが記録されます。

```
WARNING [9134000] - [csf.edge][executeEdgeConfigRequest] XAuth Cookie expiration
time is invalid or not available. Attempting to Failover.

DEBUG [9134000] - [csf.edge][executeEdgeConfigRequest]Failed to retrieve
EdgeConfig with error:INTERNAL_ERROR
```

Expressway-E の診断ログでは、HTTPS メッセージでどのドメインの Cookie が設定されている

かを確認できます。

```
Set-Cookie: X-Auth=1e1111e1-dddb-49e9-ad0d-ab34526e2b00; Expires=Fri,
09 May 2014 20:21:31 GMT; Domain=.vngtp.lab; Path=/; Secure
```

SIP ドメイン

必要な SIP ドメインが Expressway-C に追加されていない場合、Expressway-E はこのドメインのメッセージを受け入れず、診断ログに、クライアントに送信された 403 Forbidden メッセージが記録されます。

```
ExpresswayE traffic_server[15550]:
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response"
Txn-id="2" Dst-ip="10.48.79.80" Dst-port="50314"
HTTPMSG:
|HTTP/1.1 403 Forbidden
Date: Wed, 21 May 2014 14:31:18 GMT
Connection: close
Server: CE_E
Content-Length: 0

ExpresswayE traffic_server[15550]: Event="Sending HTTP error response"
Status="403" Reason="Forbidden" Dst-ip="10.48.79.80" Dst-port="50314"
```