Collaboration Edgeの最も一般的な問題の解決

内容

概要

このドキュメントでは、導入フェーズで顧客が直面するCollaboration Edgeの最も一般的な問題をトラブルシューティングする方法について説明します。

背景説明

Mobile & Remote Access(MRA)は、Virtual Private Network-less(VPN)Jabber機能の導入ソリューションです。このソリューションでは、エンドユーザが世界のどこからでも内部エンタープライズ リソースに接続できます。このガイドは、Collaboration Edge ソリューションのトラブルシューティングを行うエンジニアが、導入段階で発生する可能性がある最も一般的な問題を迅速に特定、解決できるようにする目的で作成されました。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager（CUCM）
- Cisco Expressway Core
- Cisco Expressway Edge
- Cisco IM and Presence(IM&P)
- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for Android
- Cisco Jabber for iOS
- セキュリティ証明書
- ドメイン ネーム システム（DNS）

使用するコンポーネント

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

- ExpresswayバージョンX8.1.1以降
- CUCMリリース9.1(2)SU1以降およびIM&Pバージョン9.1(1)以降
- Cisco Jabberバージョン9.7以降

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

ログインの問題

JabberがMRA経由でサインインできない

この症状は、さまざまな問題が原因で発生する可能性があります。その一部については、ここで説明します。

1. Collaboration Edge Service Record(SRV)が作成されない、またはポート8443が到達不能

JabberクライアントがMRAで正常にログインできるようにするには、特定のコラボレーションエ

ッジSRVレコードを作成し、外部からアクセスできるようにする必要があります。Jabberクライアントが最初に起動すると、DNS SRVクエリが作成されます。

1. **_cisco-uds**：このSRVレコードは、CUCMサーバが使用可能かどうかを判別するために使用されます。

2. **_cuplogin**：このSRVレコードは、IM&Pサーバが使用可能かどうかを判別するために使用されます。

3. **_collab-edge**：このSRVレコードは、MRAが使用可能かどうかを判別するために使用されます。

Jabberクライアントが起動していて、_cisco-udsおよび**_cuplogin**のSRV応答を受信せず、**_collab-edge**の応答を受信しない場合、Jabberはこの応答を使用してSRV応答にリストされているExpressway-Eへの接続を試みます。

_collab-edge SRVレコードは、Expressway-Eの完全修飾ドメイン名(FQDN)をポート**8443**で指しています。**_collab-edge** SRVが作成されていない場合、または外部から使用できない場合、あるいはSRVが使用可能であってもポート8443に到達できない場合、Jabberクライアントはログインに失敗します。

Collaboration Solutions Analyzer(CSA)のSRVチェッカーを使用して、**_collab-edge** SRVレコードが解決可能で、TCPポート8443が到達可能かどうかを確認できます。

ポート8443に到達できない場合は、セキュリティデバイス（ファイアウォール）がポートをブロックしているか、デフォルトゲートウェイ(GW)またはExp-Eのスタティックルートの設定ミスが原因である可能性があります。

2. VCS Expresswayで証明書が受け入れられない、または使用できない

Jabberクライアントは、**_collab-edge**に対する応答を受信すると、ポート8443経由でTransport Layer Security(TLS)を使用してExpresswayに接続し、Expresswayから証明書を取得して、JabberクライアントとExpressway間の通信用にTLSを設定します。

Expresswayに、ExpresswayのFQDNまたはドメインのいずれかを含む有効な署名付き証明書がない場合、この操作は失敗し、Jabberクライアントはログインできません。

この問題が発生した場合は、Expresswayで証明書署名要求(CSR)ツールを使用します。このツールには、サブジェクト代替名(SAN)としてExpresswayのFQDNが自動的に含まれています。

> **注**:MRAでは、Expressway-CとExpressway-Eの間、およびExpressway-Eと外部エンドポイントの間のセキュアな通信が必要です。

機能別のExpressway証明書要件に関する次の表は、『MRA導入ガイド』に記載されています。

Table 1. CSR Alternative Name Element and Unified Communications Features

Add These Items as Subject Alternative Names	When Generating a CSR for These Purposes			
	Mobile and Remote Sccess	Jabber guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence Service chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	

3.エッジ設定にUDSサーバが見つからない

JabberクライアントがExpressway-Eとのセキュアな接続を正常に確立した後、エッジ設定(**get_edge_config**)を要求します。このエッジ設定には、**_cuplogin**および**_cisco-uds**のSRVレコードが含まれています。**_cisco-uds** SRVレコードがエッジ設定に返されない場合、Jabberクライアントはログインを続行できません。

これを修正するには、**_cisco-uds** SRVレコードが内部で作成され、Expressway-Cで解決可能であることを確認します。

DNS SRVレコードの詳細については、『X8.11用MRA導入ガイド』を参照してください。

これは、デュアルドメインの場合によくみられる症状でもあります。デュアルドメインで実行しても、JabberクライアントがUser Data Service(UDS)に返されないことが判明した場合は、_cisco-uds SRVレコードが外部ドメインを持つ内部DNSに作成されていることを確認する必要があります。

> **注**:ExpresswayバージョンX12.5以降では、_cisco-UDS SRVレコードを内部DNSに追加する必要はなくなりました。この拡張機能の詳細については、『Cisco Expresswayを介したモバイルおよびリモートアクセス導入ガイド(X12.5)(Mobile and Remote Access Through Cisco Expressway Deployment Guide (X12.5))』を参照してください。

4. Expressway-Cのログに次のエラーが表示される： XCP_JABBERD Detail=Unable to connect to host '%IP%', port 7400:(111) Connection refused

Expressway-Eネットワークインターフェイスコントローラ(NIC)が正しく設定されていないと、Extensible Communications Platform(XCP)サーバが更新されない可能性があります。Expressway-Eがこれらの基準を満たしている場合は、次の問題が発生する可能性があります。

1. 単一のNICを使用します。
2. Advanced Networking Option Keyがインストールされている。
3. [Use Dual Network Interfaces]オプションが[Yes] に設定されている。

この問題を修正するには、[Use Dual Network Interfaces]オプションを[No] に変更します。

この問題が発生する理由は、Expressway-Eが誤ったネットワークインターフェイスでXCPセッションをリッスンし、接続が失敗またはタイムアウトするためです。Expressway-Eは、TCPポート7400でXCPセッションをリッスンします。これを確認するには、 netstatコマンドをVCSからルートとして発行します。

5. Expressway-Eサーバのホスト名/ドメイン名が_collab-edge SRVで設定されたものと一致しない

DNSページ設定のExpressway-Eサーバのホスト名/ドメインが**_collab-edge** SRV応答で受信したホスト名/ドメインと一致しない場合、JabberクライアントはExpressway-Eと通信できません。Jabberクライアントは、**get_edge_config**応答のxmppEdgeServer/Address要素を使用して、Expressway-EへのXMPP接続を確立します。

Expressway-EからJabberクライアントへの**get_edge_config**応答でのxmppEdgeServer/Addressの例を次に示します。

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example URL</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

これを回避するには、**_collab-edge** SRVレコードがExpressway-Eのホスト名/ドメイン名と一致していることを確認します。この問題はCisco Bug ID CSCuo83458に記載されており、Cisco Bug ID CSCuo82526で部分的なサポートが追加されています。

6.現在のWebEx Connectサブスクリプションが原因でログインできない

Jabber for Windowsの口グには次のように表示されます。

```
2014-11-22 19:55:39,122 INFO  [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://URL server;
Url: http://example URL server';;;.2014-11-22
19:55:39,122 INFO [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://example URL server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example URL server/cas/FederatedSSO?org=example URL]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://website URL/cas/FederatedSSO?org=example URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

口グインの試行はWebEx Connectにリダイレクトされます。

永続的な解決を行うには、WebExに問い合せてサイトを使用停止にする必要があります。

回避策

短期的には、これらのオプションのいずれかを使用してルックアップから除外できます。

- このパラメータをjabber-config.xmlに追加します。次に、CUCMのTFTPサーバにjabber-config.xmlファイルをアップロードします。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。

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

- アプリケーションの観点から、次を実行します。
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX

  注:2つ目のオプションはモバイルデバイスでは機能しません。

- WEBEXサービスを除外するクリック可能なURLを作成します。
ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

UCサービス検出の詳細と、『Cisco Jabber 12.8のオンプレミス導入』の一部のサービスを除外する方法について説明しています。

7. Expressway-Cサーバに「Configured but with errors」というエラーメッセージが表示される Provisioning server：トラバーサルサーバ情報を待機しています。

[ステータス(Status)] > [ユニファイドコミュニケーション(Unified Communications)]に移動してエラーメッセージが表示された場合、 "Configured but with errors. Provisioning server: Waiting for traversal server info." unified CM登録とIM&Pサービスの場合、Expressway-Cで設定された内部DNSサーバには、Expressway-E用の2つのDNS Aレコードがあります。Expressway-Eに複数のDNS Aレコードが存在する理由としては、該当するユーザがExpressway-Eでスタティックが有効になっているシングルNICからスタティックNATが有効になっているデュアルNICに移動したか、その逆が考えられます。また、内部DNSサーバで適切なDNS Aレコードを削除し忘れた可能性もあります。したがって、Expressway-CでDNSルックアップユーティリティを使用してExpressway-EのFQDNを解決すると、2つのDNS Aレコードが表示されます。

解決方法

Expressway-E NICがスタティックNATを使用する単一のNIC用に設定されている場合：

1. Expressway-Cで設定されたDNSサーバのExpressway-E内部IPアドレスのDNS Aレコードを削除します。
2. Expressway-CとユーザPCのDNSキャッシュをCMD(ipconfig /flushdns)。
3. Expressway-Cサーバをリブートします。

Expressway-E NICが、スタティックNATが有効なデュアルNIC用に設定されている場合：

1. Expressway-Cで設定されたDNSサーバのExpressway-E *外部* IPアドレスのDNS Aレコードを削除します。
2. Expressway-CとユーザPCのDNSキャッシュをCMD(ipconfig /flushdns)。
3. Expressway-Cサーバをリブートします。

8. Microsoft DirectAccessがインストールされました

お客様がJabberクライアントと同じPCでMicrosoft DirectAccessを使用している場合、リモートでログインしようとすると、MRAが中断する可能性があります。DirectAccessは、PCがVPNを使用しているかのように、DNSクエリを強制的に内部ネットワークにトンネリングします。

> **注**:Microsoft DirectAccessは、Jabber over MRAではサポートされていません。トラブルシューティングはベストエフォート型です。DirectAccessの構成は、ネットワーク管理者が行います。

一部のお客様は、Microsoft DirectAccess名前解決ポリシーテーブル内のすべてのDNSレコードをブロックすることで成功しています。これらのレコードはDirectAccessで処理されません（Jabberは、MRAを使用してパブリックDNSを介してこれらのレコードを解決できる必要があります）。

- _cisco-udsのSRVレコード
- SRVレコード(_C)
- _collab-edgeのSRVレコード
- すべてのExpressway Esのレコード

9. ExpresswayのリバースDNSルックアップが失敗する

バージョンX8.8以降、Expressway/VCSでは、ExpE、ExpC、およびすべてのCUCMノードに対して順方向および逆方向のDNSエントリを作成する必要があります。

要件の詳細については、『x8.8リリースノートの前提条件とソフトウェアの依存関係』および『モバイルおよびリモートアクセス用のDNSレコード』を参照してください。

内部DNSレコードが存在しない場合は、reverseDNSLookupを参照するExpresswayログにエラーがある可能性があります。

2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102" ThreadID="139882696623872" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception: exception in reverseDNSLookup: reverse DNS lookup failed for address=x.x.x.x"

Expressway-Cは、Expressway-E IPのPTRレコードを照会する際に1つのFQDNのみを受け取ります。DNSから誤ったFQDNを受信すると、ログに次の行が表示され、失敗します。

2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685" ThreadID="140028119959296" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate verification failed for host=xx.xx.xx.xx, additional info: Invalid Hostname"

登録の問題

ソフトフォンが登録できない、SIP/2.0 405方式が許可されない

Expressway-Cからの診断ログには、 **SIP/2.0 405 Method Not Allowed** Jabberクライアントから送信された登録要求に対する応答メッセージ。これは、Expressway-CとCUCMの間の現在のセッション開始プロトコル(SIP)トランク（ポート5060/5061）が原因である可能性があります。

```
SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
```

```
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
Warning: 399 collabzone "SIP trunk disallows REGISTER"
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

この問題を修正するには、CUCMで設定されている現在のSIPトランクに適用されるSIPトランクセキュリティプロファイルのSIPポートと、CUCMのExpressway-Cネイバーゾーンを、5065などの別のポートに変更します。これについては、このビデオで詳しく説明します。設定の要約を次に示します。

CUCM

1. 5060(5065)以外のリスニングポートを使用して、新しいSIPトランクセキュリティプロファイルを作成します。
2. SIPトランクセキュリティプロファイルに関連付けられたSIPトランクを作成し、Expressway-CのIPアドレス、ポート5060に宛先セットを設定します。

Expressway-C

1. CUCMの設定に一致するように、5060(5065)以外のターゲットポートを使用して、CUCMへのネイバーゾーンを作成します。
2. [Expressway-C **Settings] > [Protocols] > [SIP]**で、Expressway-Cが5060でSIPをリッスンしていることを確認します。

ソフトフォンが登録できない、理由="Unknown domain"

Expressway-Cからの診断ログにEvent="**Registration Rejected" Reason="Unknown domain"** Service="SIP" Src-ip="XXX.XXX.XXX.XXX" Src-port="51601" Protocol="TCP" OR="sip:XXX.XXX.XXX.XXX".

この問題を修正するには、次の点を確認してください。

- 非セキュアなデバイスセキュリティプロファイルを使用しない場合、Jabberクライアントは CUCMで**セキュアなデバイスセキュリティプロファイル**を使用しますか。
- Jabberクライアントがセキュアなデバイスセキュリティプロファイルを使用する場合、はセキュリティプロファイルの名前をFQDN形式で表し、そのFQDN名はExpressway-C証明書にSANとして設定されていますか。
- Jabberクライアントがセキュアなデバイスセキュリティプロファイルを使用している場合は、[System] > [Enterprise Parameters] > [Security Parameters] > [Cluster Security Mode] に移動し、CUCMクラスタがセキュアであることを確認するために[Cluster Security Mode]が1に設定されていることを確認します。値が**0**の場合、管理者は文書化された手順を実行してクラスタを保護する必要があります。

ソフトフォンが登録できない、理由 "Idle countdown expired"

Jabberクライアントが REGISTER メッセージで送信する時間枠内に Expressway-E ログを確認する場合は、 **Idle countdown expired** エラーが発生する可能性があります。

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

このスニペットは、ファイアウォールでポート5061が開いていることを示します。ただし、十分な時間をかけて渡されるアプリケーション層トラフィックがないため、TCP接続は閉じられます。

この状況が発生した場合、Expressway-Eの前にあるファイアウォールでSIPインスペクション/アプリケーションレイヤゲートウェイ(ALG)機能がオンになっている可能性が高くなります。この問題を修正するには、この機能を無効にする必要があります。この方法が不明な場合は、ファイアウォールのベンダーの製品マニュアルを参照してください。

SIPインスペクション/ALGの詳細については、『Cisco Expressway-EおよびExpressway-C基本設定の導入ガイド』の付録4を参照してください。

ファームウェアで設定された電話プロキシが原因でMRAが失敗する

Expressway-Eからの診断ログには、ポート5061でTLSネゴシエーション障害が示されていますが、SSLハンドシェイクはポート8443で成功しました。

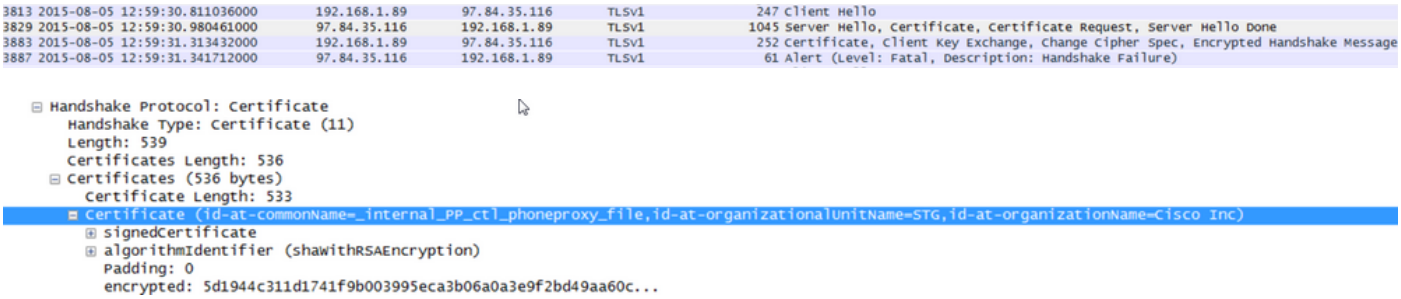
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(67)" Method="::TTSSLErrorOutput" Thread="0x7fae4ddb1700": TTSSL_continueHandshake: Failed to establish SSL connection
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04 15:14:23,535"

Jabberからのログ：

-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert][handlePlatformVerificationResultSynchronously] Verification result : FAILURE reason : [CN_NO_MATCH UNKNOWN]
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handyiron][ssl_state_callback] SSL alert read:fatal:handshake failure
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true, failureReason=eTLSFailure, SSLErrorCode=336151568
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false, failureReason=eFailedToConnect, serverType=ePrimary, role=eNone
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handyiron][secSSLIsConnected] SSL_do_handshake() returned :

SSL_ERROR_SSL.

Jabberからのパケットキャプチャは、Expressway E IPとのSSLネゴシエーションを示していますが、送信された証明書はこのサーバから送信されていません。



FWに電話プロキシが設定されている。

ソリューション：

FWが電話プロキシを実行していることを確認します。これを確認するには、 **show run policy-map** コマンドを実行すると、次のような内容が表示されます。

```
class sec_sip
inspect sip phone-proxy ASA-phone-proxy
```

電話サービスを正常に接続するには、電話プロキシを無効にします。

コール関連の問題

MRA経由でコールする際にメディアが存在しない

シングルNICとデュアルNICの導入でこの問題を引き起こす可能性がある、欠品および不適切な設定の一部を次に示します。

- Expressway-Eの[System] > [Network Interfaces] > [IP]では、スタティックNATは設定されていません。ネットワーク層のNATはファイアウォールで実行する必要がありますが、この設定ではアプリケーション層のIPが変換されます。
- TCP/UDPポートがファイアウォールで開いていません。ポートのリストについては、『Cisco Expressway IPポート使用設定ガイド』を参照してください。

スタティックNATを使用したシングルNICの導入は推奨されません。メディアの問題を防ぐためのいくつかの考慮事項を次に示します。

イッシング

- UCトラバーサルゾーンでは、Expressway-CはExpressway-Eで設定されたパブリックIPアドレスをポイントする必要があります。
- メディアは外部ファイアウォールに「ヘアピン」されるか、または反射する必要があります。Cisco ASAファイアウォールの設定例については、『VCS Expressway TelePresenceデバイス用のASAでのNATリフレクションの設定』を参照してください。

詳細については、『Cisco Expressway-EおよびExpressway-C基本設定導入ガイド』の付録4を参照してください。

MRA経由でPSTNにコールする際にリングバックが発生しない

この問題は、バージョンX8.5より前のExpresswayの制限が原因です。Cisco Bug ID CSCua72781では、Expressway-Cが183 Session Progressまたは180 Ringingで早期のメディアをトラバーサルゾーン経由で転送しない方法について説明しています。バージョンX8.1.xまたはX8.2.xを実行している場合は、バージョンX8.5にアップグレードするか、ここに記載されている回避策を実行できます。

183を180に変換し、着信ダイヤルピアに適用するSIPプロファイルを作成する場合は、Cisco Unified Border Element(CUBE)で回避策を使用できます。以下に、いくつかの例を示します。

```
voice class sip-profiles 11
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"
"SIP/2.0 180 Ringing"
```

その後、**CUCM > CUBE**のSIPプロファイルまたはsip-ua設定モード内のCUBE自体のいずれかで180 Early Mediaを無効にします。

```
disable-early-media 180
```

CUCMおよびIM&Pの問題

CUCMの追加を妨げるASCIIエラー

CUCMをExpressway-Cに追加すると、CUCMを追加できないASCII工ラーが発生します。

Expressway-Cがデータベースに CUCMを追加すると、get関数とlist関数に関連する一連のAXLクエリが実行されます。たとえば、getCallManager、**listCallManager**、**listProcessNode**、**listProcessNodeService**、および**getCCMVersion**などです。**getCallManager**プロセスの実行後、すべてのCUCM Call Manager-trustまたはtomcat-trustを取得するように設定された**ExecuteSQLQuery**によって成功します。

CUCMがクエリを受信し、そのクエリに対して実行すると、CUCMはすべての証明書を報告します。証明書の1つに非ASCII文字が含まれている場合、ExpresswayはWebインターフェイスに次のようなエラーを生成します ascii codec can't decode byte 0xc3 in position 42487: ordinal not in range(128).

この問題は、Cisco Bug ID CSCuo54489で追跡され、バージョンX8.2で解決されています。

セキュアな導入におけるExpressway-CからCUCMへの5061でのアウトバウンドTLS障害

この問題は、CUCMで自己署名証明書を使用し、Tomcat.pem/CallManager.pemが同じサブジェクトを持つ場合に発生します。この問題は、Cisco Bug ID CSCun30200で解決されています。この問題を修正する回避策は、tomcat.pemを削除し、Expressway-CのCUCM設定からTLS検証を無効にすることです。

IM&Pサーバが追加されず、エラーが発生する

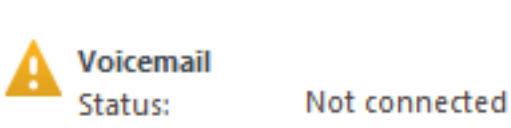
IM&Pサーバを追加すると、Expressway-Cから「This server is not an IM and Presence Server」または「Unable to communicate with .AXL query HTTP error "HTTPError:500'」というメッセー

ジが表示され、IM&Pサーバは追加されません。

IM&Pサーバの追加の一部として、Expressway-CはAXLクエリを使用して、明示的なディレクトリ内のIM&P証明書を検索します。Cisco Bug ID CSCul05131が原因で、証明書はそのストアに存在しないため、誤った エラーが発生します。

その他の問題

Jabberクライアントのボイスメールステータスに「Not connected」と表示される



Jabberクライアントのボイスメールステータスが正常に接続できるようにするには、Expressway-CのHTTP許可リスト内でCisco Unity ConnectionのIPアドレスまたはホスト名を設定する必要があります。

Expressway-Cからこれを実行するには、関連する手順を実行します。

バージョンX8.1およびX8.2の手順

1. [Configuration] > [Unified Communications] > [Configuration] > [Configure HTTP server allow list] をクリックします。
2. [New] > [Enter IP/Hostname] > [Create entry] をクリックします。
3. Jabberクライアントからログアウトし、再度ログインします。

バージョンX8.5の手順

1. [Configuration] > [Unified Communications] > [Unity Connection Servers] をクリックします。
2. [New] > [Enter IP/Hostname, User account credentials] > [Add Address]をクリックします。
3. Jabberクライアントからログアウトし、再度ログインします。

連絡先の写真がExpressway経由でJabberクライアントに表示されない

モバイルおよびリモートアクセスソリューションでは、UDSを利用して連絡先の写真の解決のみを行います。これには、写真を保存できるWebサーバが必要です。設定自体は2倍です。

1. 連絡先の写真を解決するために、クライアントをWebサーバに転送するようにjabber-config.xmlファイルを変更する必要があります。次の設定でこれを実現します。

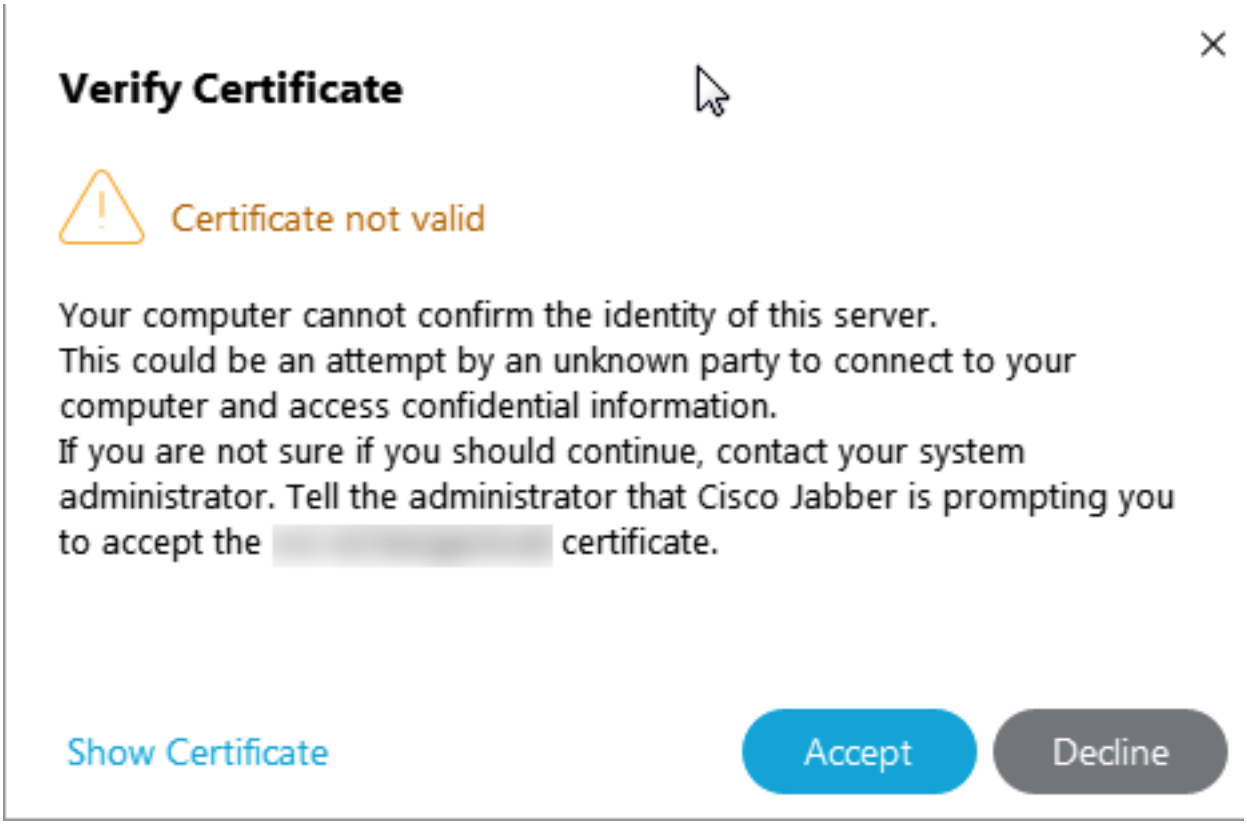
```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%%uid%%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2. Expressway-CのHTTPサーバ許可リストにWebサーバがリストされている必要があります。

   [Configuration] > [Unified Communications] > [Configuration] > [Configure HTTP server allow list] をクリックします。[New] > [Enter IP/Hostname] > [Create entry] をクリックします。Jabberクライアントからログアウトし、再度ログインします。

   注:UDSの連絡先写真の解像度の詳細については、Jabberの連絡先写真のドキュメントを参照してください。

Jabberクライアントがログイン時にExpressway-E証明書を受け入れるように求められる



このエラーメッセージは、クライアントデバイスによって信頼されているパブリックCAによって署名されていないExpressway Edge証明書、またはドメインがサーバ証明書内にSANとして存在しないExpressway Edge証明書に関連している可能性があります。

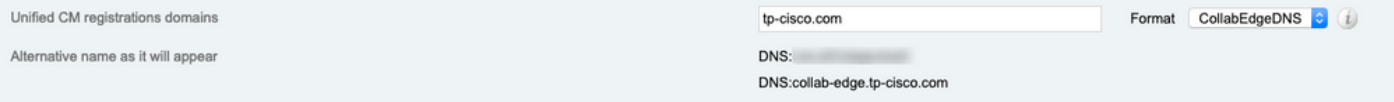
Expresswayの証明書受け入れプロンプトからJabberクライアントを停止するには、次の2つの条件を満たす必要があります。

- Jabberクライアントを実行するデバイス/マシンには、Expressway-E証明書の署名者が証明書信頼ストアにリストされている必要があります。

  注：モバイルデバイスには大きな証明書信頼ストアが含まれているため、パブリック認証局(CA)を使用すると、この操作は簡単に実行できます。

- collab-edgeレコードに使用するUnified CM登録ドメインは、Expressway-E証明書のSAN内に存在する必要があります。ExpresswayサーバのCSRツールでは、Unified CM登録ドメインを

SANとして追加するオプションが提供されます。これは、ドメインがMRA用に設定されている場合にプリロードされます。証明書に署名するCAがドメインをSANとして受け入れない場合は、「CollabEdgeDNS」オプションを使用して、ドメインにプレフィックス「collab-edge」を追加することもできます。



関連情報

- Expresswayでのモバイルおよびリモートアクセスガイド
- 『Cisco Expressway Certificate Creation and Use Deployment Guide』
- ファイアウォールトラバーサル用のCisco TelePresence Video Communication Server(Cisco VCS)IPポートの使用
- 『Deployment and Installation Guide for Cisco Jabber』
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。