

Collaboration スペシャリスト トレーニング v2 - Mobile and Remote Access のトラブルシューティング

最終更新日：2018 年 11 月 2 日

このラボについて

この **Cisco Mobile and Remote Access** のトラブルシューティングのラボには、次のような内容が含まれています。

[要件](#)

[このソリューションについて](#)

[トポロジ](#)

[セッション ユーザ](#)

[はじめに](#)

[シナリオ 1：Mobile and Remote Access のトラブルシューティング](#)

[付録 A：SIP 登録](#)

要件

次の表に、このラボの要件を示します。

表 1. 要件

必須	オプション
<ul style="list-style-type: none"> ● ラップトップ ● Cisco AnyConnect® 	<ul style="list-style-type: none"> ● ルータ (dCloud に登録し、設定済みのもの) ● Cisco Jabber for Windows/Mac

このソリューションについて

Cisco Unified Communications の Mobile and Remote Access (MRA) は、Cisco Collaboration Edge アーキテクチャの中核を成す製品です。MRA によって、Cisco Jabber などのエンドポイントは、そのエンドポイントがエンタープライズ ネットワーク内にない場合でも、Cisco Unified Communications Manager (Unified CM) の登録、コール制御、プロビジョニング、メッセージとプレゼンスといったサービスを利用できます。また、Expressway は、Unified CM 登録にセキュアなファイアウォールトラバーサルと回線側サポートを提供します。

このラボでは、エンタープライズ ネットワークの外部にある Jabber クライアントから Mobile Remote Access にログインできない場合のトラブルシューティングを行います。このラボを受講すると、ソリューションの仕組みをよく理解できるようになるため、将来の設計、実装、トラブルシューティングに役立てることができると期待されます。トラブルシューティングには次の項目があります。

サービス検出

ログイン エラー

電話サービスのエラー

注：このラボには、段階的手順の詳細説明は含まれていません。そのため、実施にあたっては、Cisco Unified Communications を深く理解していることが必要になります。

制約

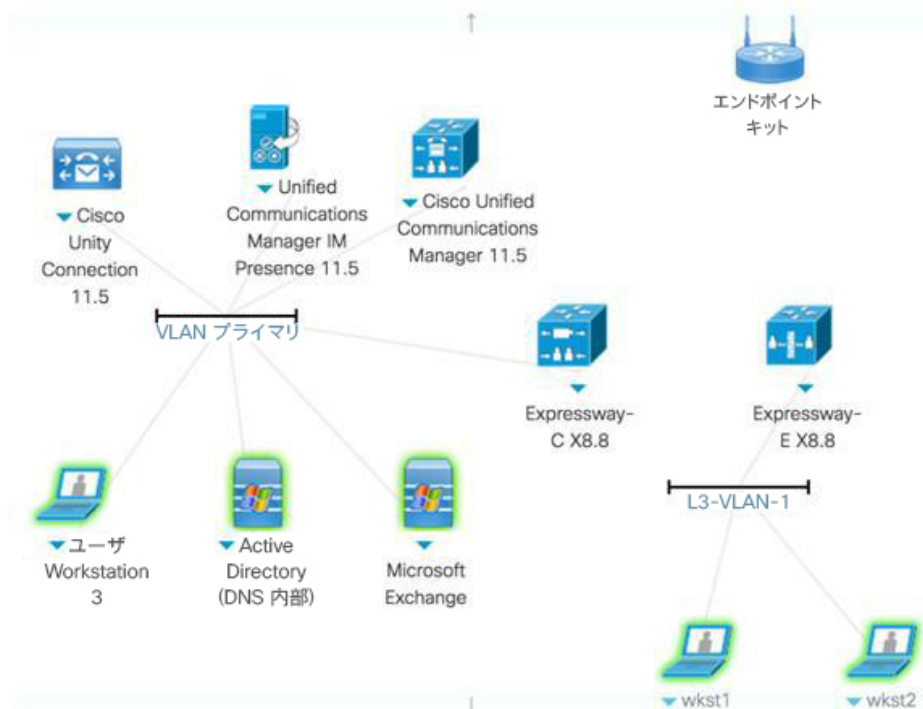
リモート デスクトップの Cisco Jabber for Windows が発信元または発信先であるコールでは、音声とビデオが正確にレンダリングされない場合があります。

正しくセットアップされていれば、ラップトップにインストールされている Cisco Jabber クライアントを使用できます。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ (Topology)] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. トポロジ



セッション ユーザ

表 2. 事前設定済みのユーザ情報

ユーザ名	ユーザ ID	パスワード	エンドポイント デバイス	電子メール/IM	内線番号
Monica Cheng	mcheng	C1sco12345	CSFMCHENG (Jabber for Windows)	mcheng@dcloud.cisco.com	6030
Charles Holland	cholland	C1sco12345	CSFCHOLLAND (Jabber for Windows)	cholland@dcloud.cisco.com	6018

表 3. 接続情報

サーバ	ホスト名	IP アドレス	ユーザ名	パスワード
Unified CM	ucm1	198.18.133.3	administrator	dCloud123!
IM&P	imp1	198.18.133.4	administrator	dCloud123!
Expr-C	v csc	198.18.133.152	admin	dCloud123!
Expr-E	v cse	198.18.1.5	admin	dCloud123!
Active Directory	ad1	198.18.133.1	dcloud\administrator	C1sco12345
Workstation 3	wkst3	198.18.133.38	dcloud\mcheng	C1sco12345
パブリック DNS	N/A	198.18.128.1	N/A	N/A

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dcloud.cisco.com にアクセスして最寄りのロケーションを選択し、Cisco.com アカウントでログインします。
2. ルータを dCloud で初めて使用する場合は、ルータを登録し、設定します。[[手順を見る](#)] [英語]
3. セッションを予約します。[[手順を見る](#)] [英語]
4. 接続をテストします。[[手順を見る](#)] [英語]
5. [マイダッシュボード (My Dashboard)] > [マイセッション (My Sessions)] でセッションのステータスが [アクティブ (Active)] であることを確認します。

注：セッションがアクティブになるまで、最長で 45 分かかることがあります。

6. [表示 (View)] をクリックして、アクティブ セッションを開きます。
7. 最適なパフォーマンスを得るために、Cisco AnyConnect VPN [[手順を見る](#)] [英語] およびラップトップのローカル RDP クライアント [[手順を見る](#)] [英語] を使用してワークステーションに接続します。

Workstation 3 : **198.18.133.38**、ユーザ名 : **dcloud\mcheng**、パスワード : **C1sco12345**

接続後は、自分のラップトップから、Jabber for Windows クライアントを直接利用せずに操作を実行することをお勧めします。Web インターフェイスへのアクセスおよびサーバへの RDP 接続は、Workstation 3 経由で接続するよりも自分のラップトップから実行する方がかなり速くなります。

注 : Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [\[手順を見る\]](#) [英語]。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法では、接続ができない場合や、パフォーマンスが悪い場合があります。

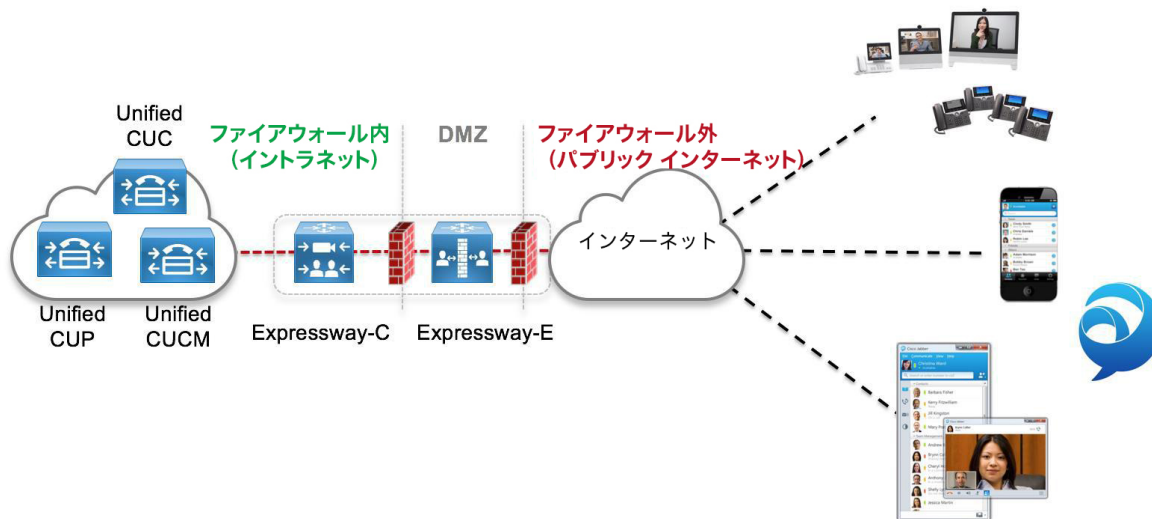
重要 : Cisco UC Manager、Cisco UC Manager IM and Presence、Cisco Expressway-E、Cisco Expressway-C サーバの利用方法を十分理解していることが推奨されます。このラボでは詳細な手順が常に提供されているわけではありません。

シナリオ 1. Mobile and Remote Access のトラブルシューティング

はじめに

ここでは、MRA のログイン、さらに IM&P（インスタント メッセージとプレゼンス）および電話サービスに焦点を当てます。dCloud ポッドの観点から、特に次に示す論理アーキテクチャに注目します。



図 2. 論理アーキテクチャ



ここでは、Workstation 3 を外部ネットワークの Jabber クライアントとして使用します。これをシミュレートするために、外部（「パブリック」）DNS サーバを使用します。

トラブルシューティングの手順

サービス検出

1. **Workstation 3** へのリモート デスクトップ セッションを開始します (198.18.133.38 ユーザ名 : mcheng、パスワード : C1sco12345)。
2. **DNS 設定を確認**します。
3. DNS サーバの設定に利用できるバッチ ファイルがデスクトップに 2 つあることを**確認**します。**Troubleshooting 1.bat**  は、ワークステーションにパブリック DNS サーバを設定します。**Troubleshooting 2.bat**  は、必要に応じて内部 DNS サーバに戻るためのものです。必要に応じて、各ファイルを管理者として実行します (各ファイルを右クリックして選択)。
4. **Troubleshooting 1.bat** ファイルを右クリックして [管理者として実行 (Run as Administrator)] を選択し、パブリック DNS サーバを設定します。
5. **Jabber を再起動**し、ワークステーションへのログインに使用したのと同じクレデンシャルで Jabber に**ログイン**します。内部 DNS サーバを使用している場合はログインできますが、パブリック DNS サーバを使用している場合は**失敗**します。

重要 : DNS サーバを変更する場合は、バッチ ファイルを管理者として実行するよう注意してください。

注 : パブリック DNS サーバを使用する場合は、そのワークステーションのホスト名で内部サーバにアクセスすることはできません。

Jabber では最初に、サービスを提供するサーバを検出する必要があります。ここでは、Jabber はサービス ドメインの DNS サービス レコード (DNS SRV レコード) を使用しています。デフォルトでは、サービス ドメインはクライアントの設定に応じて、ユーザが入力した電子メール アドレスか、Windows の UPN (ユーザ プリンシパル名) から取得されます。ログイン手順は、クライアントがエンタープライズ ネットワーク内にあるかインターネット上にあるかによって異なりますが、最初に、クライアントがエンタープライズ ネットワーク内にあるかどうかを判断する必要があります。Jabber クライアントは常に WebEx サービスの検出を試みます。そして次の 2 つの DNS SRV レコードを使用して、サービスがエンタープライズ ネットワーク内にあるかどうかを判定します。

```
_cisco-uds._tcp.domain.com
```

```
_cuplogin._tcp.domain.com
```

それらのレコードが解決可能である場合、クライアントで所定の手順が開始され、エンタープライズ ネットワーク内に Unified CM と IM&P があることを前提にして、それに直接接続します。レコードが解決不能である場合には、クライアントは Expr-E (MRA) 経由で接続を試みます。ここでは、クライアントが Expr-E 経由で接続する状況に焦点を当てます。Expr-E を検出するために、クライアントはさらに SRV レコードの検索を行います。

```
_collab-edge._tls.domain.com
```

したがって、正確な SRV レコードを保持することが重要になります。導入全体でドメインが 1 つだけである場合は、SRV レコードを作成するのは簡単です。ドメインが複数ある場合は、多少複雑になります。これはスペシャリスト トレーニングであるため、ドメインが複数ある場合のセットアップを取り上げます。主要なドメインとして、次の 2 つがあります。

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 ドメインとも呼ばれる Expr-E のドメイン。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。

Extensible Messaging and Presence Protocol (XMPP) トラフィックで使用される、UC ドメインとも呼ばれる IM and Presence ドメイン。エンド ユーザはこのドメインを使用してログインします。

6. ラボの環境で、これら 2 つのドメインを確認してください。Workstation 1 (198.18.1.36 ユーザ名 : **dcloud\cholland**、パスワード : **C1sco12345**) に対するリモート デスクトップ セッションを確立します。
7. **Firefox** を起動し、[コラボレーション管理リンク (Collaboration Admin Links)] -> [Cisco Expressway-E] メニューを使用して、Expressway-E (**exp-e-1.dcloud.cisco.com/198.18.1.5**) にアクセスします。ユーザ名 : **admin**、パスワード : **dCloud123!** でログインします。
8. **Expr-E** のドメインは、[システム (System)] -> [DNS] の管理インターフェイスから確認できます。パブリック レコードを使用するため、このドメインは各ポッドによって異なります。
9. **IM&P** (**imp1.dcloud.cisco.com/198.18.133.4** ユーザ名 : **administrator**/パスワード : **dCloud123!**) ドメインは、通常ユーザがログインするドメインで、[プレゼンス (Presence)] > [ドメイン (Domains)] でアクセスできる **IM&P の管理** ページで確認できます。ドメインは複数ありますが、ここで注目するのはテスト アカウントで使用するドメインです。これらのドメインをメモします。

図 3. システム管理ドメイン

System Managed Domains (3)	
Domain	In use on Local Cluster
alpha.com	✓
dcloud.cisco.com	✓
uk.dcloud.cisco.com	✓

このシナリオでは、IM&P ドメインは、(すべてのポッドが共有する) パブリック DNS サーバでは使用できない内部ドメインです。たとえば `internal.local` など、企業が内部専用のドメインを持っている場合も同様です。

そのため、Expr-E のドメインである「外部」ドメインを使用して、Expr-E を検出する必要があります。

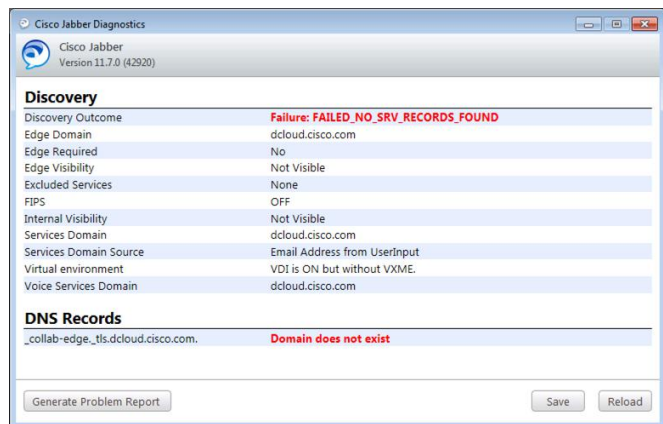
注 : このガイドでは、Expr-E のドメインとして **collabedge-121.dc-01.com** を使用します。ドメインとパブリック IP アドレスは各ポッドによって異なるため、セットアップに関連付けられている正しいドメインと IP アドレスを使用してください。

ユーザが、他のドメインを把握する必要はありません。自分の同一の電子メール アドレス (この事例では、mcheng@dcloud.cisco.com) を使用してログインするだけでかまいません。設定によっては、Jabber が Windows の UPN から自動的にこのドメインを検出できる場合もあります。

10. Jabber クライアントの動作を確認するには、[Cisco Jabber 診断ツール](#) (Ctrl+Shift+D) を使用します。

この場合、クライアントは `cisco-uds` の SRV レコードを解決できません。エンタープライズ ネットワークの外部にあるためそれ自体は問題ありませんが、`collab-edge` レコードも検出できなくなることは問題です。

図 4. Cisco Jabber の診断



クライアントは collab-edge SRV レコードのドメイン部分として dcloud.cisco.com を使用します。これは内部ドメインであり、すべてのポッドが共有するため、外部 DNS サーバはこれを解決できません。

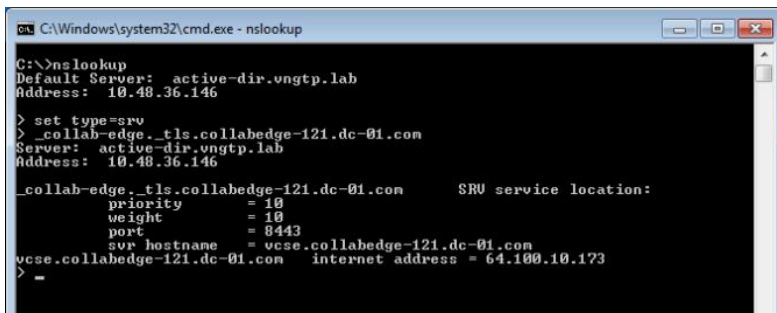
11. **Workstation 1** に接続されている RDP セッションに戻ります。

12. Expr-E サーバのドメインは **collabedge-XXX.dc-0Y.com** です (XXX の部分は、自分の Collab Edge の 3 桁の番号に置き換え、0Y の部分は、自分の DC 番号に置き換えます)。コマンド プロンプト ウィンドウを開き、「nslookup」を使用し、次のコマンドを入力して collab-edge SRV レコードがこのドメインで解決可能であるかどうかを検証します。

```
nslookup.
set type=svr
_collab-edge._tls.collabedge-XXX.dc-0Y.com (Replace XXX with your Collab Edge three digit number and the 0Y with your DC number.)
```

アドレス解決に伴い、(この例では) collabedge-121.dc-01.com を DNS SRV レコードのドメインとして使用するようクライアントに指示する必要があります。

図 5. Nslookup を利用した SRV レコードの確認



```
C:\Windows\system32\cmd.exe - nslookup
C:\>nslookup
Default Server: active-dir.vngtp.lab
Address: 10.48.36.146

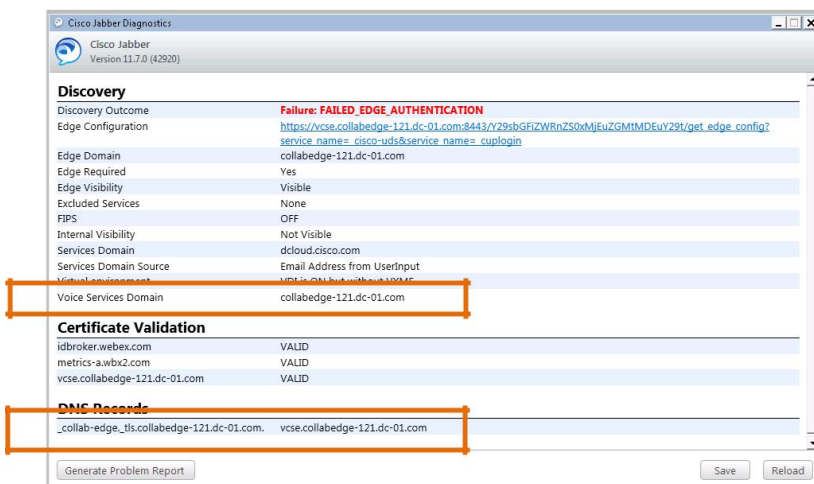
> set type=svr
> _collab-edge._tls.collabedge-121.dc-01.com
Server: active-dir.vngtp.lab
Address: 10.48.36.146

_collab-edge._tls.collabedge-121.dc-01.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = vcse.collabedge-121.dc-01.com
vcse.collabedge-121.dc-01.com internet address = 64.100.10.173
>
```

サービス検出のトラブルシューティング

この問題の解決方法は複数ありますが、以下のページではそのうちの 1 つについて説明します。ここでの目標はログインできるようにすることではなく、Jabber で DNS SRV レコードのドメインとして collabedge-XXX.dc-0Y.com が使用されるようにすることです (XXX の部分は、自分の Collab Edge の 3 桁の番号に置き換え、0Y の部分は、自分の DC 番号に置き換えます)。

図 6. Cisco Jabber の診断 - 正しいドメインの検出



注：エンタープライズ ネットワーク内にいるため、Troubleshooting2.bat を使用して、ワークステーションの DNS サーバを内部 DNS に変更することができます（バッチは必ず管理者として実行してください）。

注：不明な点がある場合は、[この記事](#)をヒントにするか、以降のページを参照して解決方法を確認してください。

サービス検出の解決

DNS SRV レコードの別のドメインをクライアントに指示する場合は、音声サービス ドメインを使用できます。音声サービス ドメインを設定すると、クライアントはこのドメインをサービス ドメインに優先して DNS SRV レコードの検索に使用します。これを設定する方法は複数あります（Jabber が稼働するプラットフォームによっても異なります）。

jabber-config.xml ファイルを使用する

メディア サービス インターフェイス (MSI) 経由で Jabber をインストールする際に、パラメータとして追加する設定 URL を使用して Jabber-bootstrap.properties ファイルを編集する

企業モビリティ管理を使用する

詳細については、[『Planning Guide for Cisco Jabber \(Cisco Jabber プランニング ガイド\)』](#)の「Service Discovery (サービス検出)」の章を参照してください。

このラボでは *jabber-config.xml* ファイルを使用します。

これはシンプルな解決方法ですが、Unified Communications Manager (Unified CM) クラスターの Trivial File Transfer Protocol (TFTP) サーバからファイルをダウンロードするため、まずクライアントを（エンタープライズ ネットワーク内で）オンプレミスで接続する必要があります。つまりこの解決方法は、クライアントが最初にオンプレミスでログインし、音声サービス ドメインを含む jabber-config.xml ファイルを取得できる場合のみ有効です。

- このファイルを TFTP サーバで確認するには、http でファイルにアクセスします（ブラウザによっては、右クリックで [ソースを表示 (View Source)] を選択することが必要な場合があります）：<http://198.18.133.3:6970/jabber-config.xml> (Workstation 1 で Firefox を起動し、[コラボレーションユーザーリンク (Collaboration User Links)] > [Jabber 設定 XML ファイル (Jabber Config XML File)] リンクの順にアクセス)

```
<?xml version="1.0" encoding="utf-8"?>
<config>
<Policies>
  <EnableSIPURIDialling>True</EnableSIPURIDialling>
</Policies>
<Client>
  <enablesavechathistorytoexchange>True</enablesavechathistorytoexchange>
  <InternalExchangeServer>mail1</InternalExchangeServer>
</Client>
<Directory>
  <SipUri>mail</SipUri>
  <UseSIPURIToResolveContacts>>true</UseSIPURIToResolveContacts>
  <BDISipUri>mail</BDISipUri>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BusinessPhone>telephoneNumber</BusinessPhone>
</Directory>
</config>
```

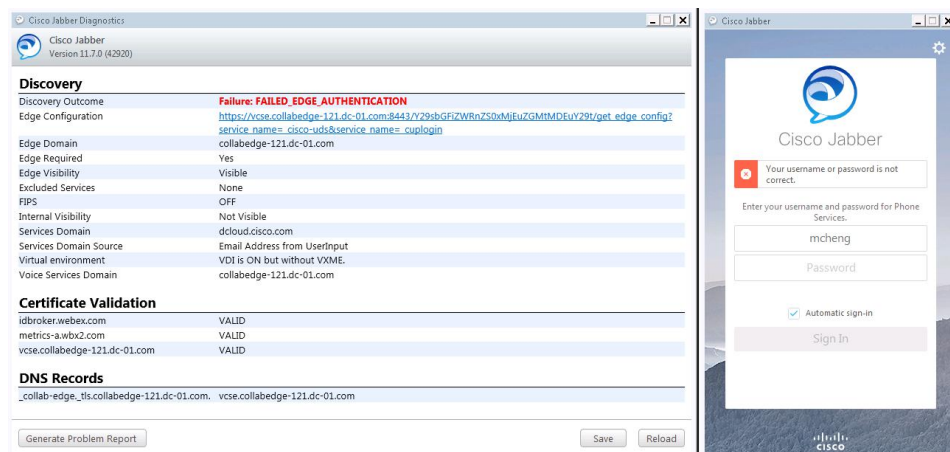
- 現時点で音声サービス ドメインは設定されていないので、それを追加する必要があります。[Jabber 設定ファイル ジェネレータ](#)がツールとして役立ちます。音声サービス ドメインを追加した jabber-config.xml ファイルは次のようになります。

```
<?xml version="1.0" encoding="utf-8"?>
<config>
<Policies>
  <EnableSIPURIDialling>True</EnableSIPURIDialling>
<VoiceServicesDomain>collabedge-121.dc-01.com</VoiceServicesDomain>
</Policies>
<Client>
  <enablesavechathistorytoexchange>True</enablesavechathistorytoexchange>
  <InternalExchangeServer>mail</InternalExchangeServer>
</Client>
<Directory>
  <SipUri>mail</SipUri>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <BDISipUri>mail</BDISipUri>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BusinessPhone>telephoneNumber</BusinessPhone>
</Directory>
</config>
```

注：このラボでは既存の jabber-config ファイルを編集します。そのために必要なのは、VoiceServicesDomain プロパティのみです。

- このラボでは、上記のテキストを新しいメモ帳ファイルにコピーし（または TFTP サーバから保存したコピーを編集し）、jabber-config.xml として保存します。次に [ソフトウェアアップグレード (Software Upgrades)] -> [TFTP ファイルの管理 (TFTP File Management)] にアクセスし、<https://198.18.133.3/cmplatform> (Cisco Unified OS の管理) で [ファイルのアップロード (Upload File)] を選択して、jabber-config.xml を TFTP サーバにアップロードします。
- 次に、デスクトップの **Troubleshooting 2.bat** を使用して Workstation 3 の DNS サーバを内部 DNS サーバ (198.18.133.1) に変更し、ログインします。DNS サーバを内部 DNS サーバに変更することで、Jabber は _cisco-uds SRV レコードを解決し、Unified CM と IM&P に登録できます。登録中に、Jabber は更新された jabber-config.xml ファイルを取得します。エッジを介した次の更新時には、クライアントでは jabber-config.xml ファイルで設定した音声サービスドメインが使用されます。この時点では、設定した音声サービスドメインの _cisco-uds SRV レコードがまだないため、内部ログインも失敗します。
- Troubleshooting1.bat** を使用して DNS サーバをもう一度外部 DNS サーバ (198.18.128.1) に変更し（バッチは必ず管理者として実行してください）、Jabber を再起動後再度ログインして、正常に機能したか確認します。結果は以下のようになります。

図 7. サービス検出の最終結果



- ここではサービスドメインはまだ dcloud.cisco.com (ユーザ入力の電子メール アドレスから取得) ですが、音声サービスドメインは正しく設定され、エッジドメインとして使用されています。エッジとの接続に問題があることを示すエラーが表示されます。次はこれについてトラブルシューティングを行う必要があります。

ログイン エラー

なぜログインに失敗するのか、トラブルシューティングする必要があります。そのためには、Expr-C と Expr-E の両方からのログが必要になります。次の手順に従ってログを収集します。

- 両方の Expressway にログインし、[メンテナンス (Maintenance)] > [診断 (Diagnostics)] > [診断ログ (Diagnostic Logging)] に移動します。
- [ロギング中に tcpdump を採取 (Take tcpdump while logging)] チェックボックスをオンにします。
- [新しいログを開始 (Start new log)] ボタンをクリックします。
- 問題を再現します。

問題を再現する場合は、先に Jabber を終了してキャッシュ情報をクリアし、ログ内の情報をすべてキャプチャできるようにします。[コラボレーション ソリューション アナライザ](#)を使用して問題をトラブルシューティングできます。これは TAC のエンジニアが開発したベータ ツールであり、TAC エンジニアが日常業務で使用しているものです。

- [ロギング停止 (Stop logging)] ボタンをクリックします。
- [ログのダウンロード (Download log)] ボタンを使用して、ログをダウンロードします。

問題を特定して修正します。目的は Jabber にログインできるようになることですが、電話サービスではまだエラーが発生します。解決方法がわからない場合は、次のページの手順に従ってください。

ログイン エラーの解決

- まず**ログを収集**します。
 - Jabber を終了する
 - Expr-C と Expr-E の両方で診断ログを有効にする
 - Jabber を起動してログインを試みる
 - ログを収集する
- [コラボレーション ソリューション アナライザ](#)に Expr-E の**ログをアップロード**します。Expr-E のログから開始するのは、Expr-E が Jabber クライアントからの get_edge_config リクエストの送信先サーバであるためです。
- アップロードしてアナライザがファイルを処理すると、Expressway の設定のサマリーを含むシステム情報の概要と、コールおよび MRA のログイン情報を含むログ概要パネルが表示されます。システム情報から見てみましょう。

図 8. コラボレーション ソリューション アナライザ。警告記号によって、可能性のある障害ポイントをすぐに見つけることができます。

The screenshot shows the 'System information' page with a warning icon. The 'MRA' tab is selected. Under 'EDGE DOMAINS', a warning states 'No Edge Domain found in the configuration'. Below, two traversal zones are listed with their configurations and status.

TRAVERSAL ZONE 2	
Name	VCS-C for MRA
Type	TraversalServer
H323 Port	6001
SIP Port	7001
TLS Verify	vcsc.dcloud.cisco.com
Zone Status	Failed (No peer connected)

TRAVERSAL ZONE 3	
Name	VCS-C for B2B Video Traversal Server
Type	TraversalServer
H323 Port	6004
SIP Port	7004
TLS Verify	vcsc.dcloud.cisco.com
Zone Status	Failed (No peer connected)

At the bottom of the page, there is a link for 'Log overview'.

4. トラバーサルゾーンでエラーが発生すると、Expr-E は Expr-C から MRA 設定（エッジドメインの設定を含む）を取得できず、またこの時点では Expr-E が送信先を認識していないため、MRA に関連するトラフィックも許可されません。Expr-C でゾーン設定を確認すると、予想どおり両方のトラバーサルゾーンが障害発生状態になっています。

図 9. Expr-C の MRA トラバーサルゾーン設定。DNS 解決の失敗。

The screenshot shows the Cisco Expressway-C configuration page for an MRA traversal zone. The configuration is as follows:

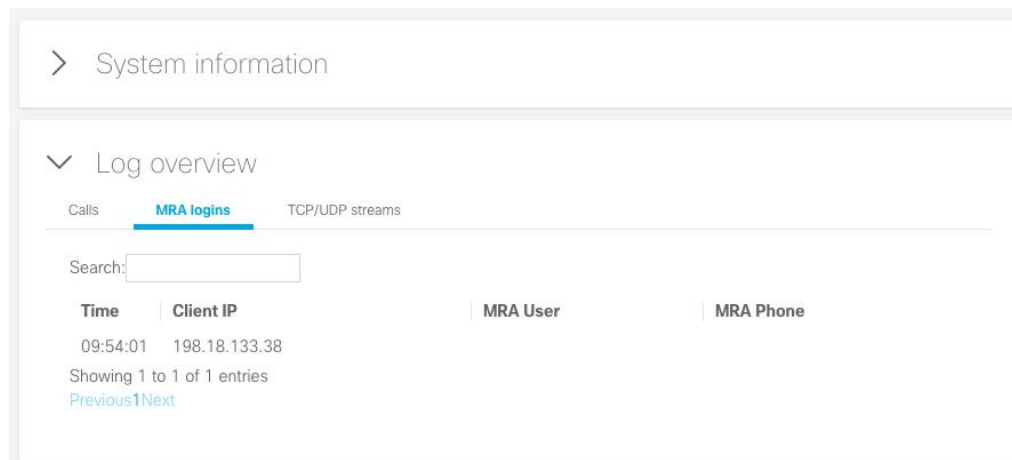
- Configuration:** Name: VCS-E for MRA, Type: Unified Communications Inverse, Top count: 15
- Connection credentials:** Username: cisco, Password: *****
- SIP:** Port: 7001, Accept proxy registrations: Allow, ICE support: Off, Multicast mode: On, SP proxy mode: Off, Preloaded SP routes support: Off, SP parameter preservation: Off
- Authentication:** Authentication policy: Treat as authenticated
- Client settings:** Retry interval: 120
- Location:** Peer 1 address: vcse.collabedge-999.dc-0Y.com

An error message is displayed: "SIP Failed: DNS resolution failed. Check the certificates for the traversal connection."

ここでは検索ルールは不要ですが、Expr-E の FQDN : vcse.collabedge -XXX.dc-0Y.com を修正する必要があります。ラボでは使用しませんが、練習のために B2B トラバーサルゾーンのピアを修正することもできます。ゾーンがアクティブになるまで待ち、手順 1 に従ってログ収集を行ってください。

5. Jabber の動作が変わらないため、Expr-E のログを再度確認します。システム情報に警告は表示されていませんが、[ログの概要 (Log overview)] > [MRA ログイン (MRA logins)] タブに移動すると、検出された MRA ログインがログに表示されています。

図 10. コラボレーション ソリューション アナライザ、ログの概要



6. 任意のログインを選択すると、プロビジョニングされたすべてのメッセージ (https) と SIP 登録メッセージ (存在する場合) が表示されます。

図 11. コラボレーション ソリューション アナライザ - MRA ログインの詳細

MRA Login Details

MRA Login

Time	Leg 1	Leg 2	Source	Destination	XML	Message
09:54:01	→ GET HTTPS		198.18.133.38	198.18.1.5		GET https://oauthcb HTTP/1.1
09:54:01	← HTTP		198.18.1.5	198.18.133.38		HTTP/1.1 503 Service Unavailable
09:54:09	→ GET HTTPS		198.18.133.38	198.18.1.5		GET https://Y29sbGFIZWRnZS0xMjEuZGMtMDEuY29t/get_edge_config?service_name=_cisco-uds&
09:54:09	← HTTP		198.18.1.5	198.18.133.38		HTTP/1.1 403 Forbidden

7. Expr-E は「403 forbidden」を返します。リクエストの太字部分にマウス ポインタを合わせると、リクエストの base64 エンコード部分がデコードされ、リクエスト先のドメインが表示されます。

図 12. コラボレーション ソリューション アナライザ - Base 64 デコード

Time	Leg 1	Leg 2	Source	Destination	XML	Message
09:54:01	→ GET HTTPS		198.18.133.38	198.18.1.5		GET https://oauthcb HTTP/1.1
09:54:01	← HTTP		198.18.1.5	198.18.133.38		HTTP/1.1 503 Service Unavailable
09:54:09	→ GET HTTPS		198.18.133.38	198.18.1.5		GET https://Y29sbGFIZWRnZS0xMjEuZGMtMDEuY29t/get_edge_config?servic
09:54:09	← HTTP		198.18.1.5	198.18.133.38		HTTP/1.1 403 Forbidden

8. このドメインに対する権限がないため、Expr-E では 403 エラーが返されます。Expr-E が権限を持つドメインは、[ステータス (Status)] ([ステータス (Status)] > [Unified Communications]) で確認できます。

図 13. Expr-E - ユニファイド コミュニケーションのステータス

Unified Communications (last updated: 20:22:06 CDT)

Unified Communications status	Enabled
Unified CM registrations	Configured
IM and Presence Service	Configured
XMPP Federation	Not configured (Enable federation on Unified Communications page)
Single Sign-On support	Not configured (Enable on the Unified Communications page)

Activity

Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0

Domains

Name	Services	Associated zones
dcloud.cisco.com	Unified CM registrations, IM and Presence Service	VCS-C for MRA
collabedge-999.dc-01.com	Unified CM registrations, IM and Presence Service	VCS-C for MRA

Zones

Name	SIP status
VCS-C for MRA (vcs.c.dcloud.cisco.com)	Active

このページは、MRA に関連するゾーンのステータスと接続を管理するのに最適であり、Expr-C と Expr-E の両方で使用できます。これらのドメインは Expr-C で設定され、Expr-E に提供されます。これを修正するには、**Expr-C の外部ドメインを修正して、Unified CM の登録と IM and Presence Service に対して有効にする必要があります。**

図 14. Expr-C - 設定されたドメイン

Domains

Saved: Domain collabedge-121.dc-01.com created.

Index	Domain name	Expressway registrations	Unified CM registrations	IM and Presence Service	XMPP Federation	Actions
<input type="checkbox"/>	1 dcloud.cisco.com	On	On	On	Off	View/Edit
<input type="checkbox"/>	2 collabedge-121.dc-01.com	Off	On	On	Off	View/Edit

New Delete Select all Unselect all

9. 修正されたところで、手順 1 に従ってログ収集を繰り返します。

10. ここで別のエラーが発生します。

図 15. Cisco Jabber 診断 - ログイン エラー

Discovery Outcome

Discovery Outcome: **Failure: FAILED_EDGE_CREDENTIALS_NOT_SET**

Edge Configuration: https://vcs.collabedge-121.dc-01.com:8443/129sbGFZWRnZ50MMjEuzGMIMDEuY29t/get_edge_config?service_name=cisco-uds&service_name=cuplogin

Edge Domain: collabedge-121.dc-01.com

Edge Required: Yes

Edge Visibility: Visible

Excluded Services: None

FGS: Off

Internal Visibility: Not Visible

Services Domain: dcloud.cisco.com

Services Domain Source: Email Address from UserInput

Virtual environment: VDI is ON but without VXME

Voice Services Domain: collabedge-121.dc-01.com

Certificate Validation

vcse.collabedge-121.dc-01.com: VALID

DNS Records

_collab-edge_tis.collabedge-121.dc-01.com: vcse.collabedge-121.dc-01.com

Generate Problem Report Save Reload

Cannot find your services automatically. Click advanced settings to set up manually.

mcheng@dcloud.cisco.com

Continue

Advanced settings

11. 前回と同じ一連のログを収集し、[コラボレーション ソリューション アナライザ](#)にアップロードします。これらのログを使用して変更を行うと、Expr-C にアクセスできます。結果を確認してください。

図 16. コラボレーション ソリューション アナライザ - MRA ログインの詳細

Time	Leg 1	Leg 2	Source	Destination	XML	Message
10:13:09	→ GET HTTP		127.0.0.1	198.18.133.152		GET http://vcs_control.collabedge-121.dc-01.com:8443/Y29sbGFIZWRnZS0x
10:13:09	← GET HTTP		198.18.133.152	127.0.0.1		GET /Y29sbGFIZWRnZS0xMjEuZGMtMDEuY29t/get_edge_config?service_nar
10:13:10	→ HTTP		127.0.0.1	198.18.133.152		HTTP/1.1 200 OK
10:13:10	← HTTP		198.18.133.152	127.0.0.1		HTTP/1.1 200 OK

12. ここでは、get_edge_config リクエストが Expr-C に到達し、クライアントに応答が送信されますが、その後変化がありません。応答を詳しく見るには、XML が含まれるメッセージをクリックします。完全なメッセージが判読可能なフォーマットで表示されます。

図 17. コラボレーション ソリューション アナライザ - HTTP 200 OK

```

HTTP/1.1 200 OK
Content-Type: text/xml
Server: CE_C ECS
Set-Cookie:<CONCEALED>
Date: Tue, 30 Aug 2016 10:13:10 GMT
Content-Length: 1020
Age: 1
Connection: keep-alive

<?xml version=" 1.0" ?>
<getEdgeConfigResponse version=" 1.0" >
  <serviceConfig>
    <service>
      <name>_cisco-phone-tftp</name>
      <error>NameError</error>
    </service>
    <service>
      <name>_cuplogin</name>
      <error>NameError</error>
    </service>
    <service>
      <name>_cisco-uds</name>
      <error>NameError</error>
    </service>
  </serviceConfig>
</getEdgeConfigResponse>

```


13. この応答には、クライアントが要求した UDS サービスに関する情報は含まれていません。

```
<service>
<name>_cisco-uds</name>
<error>NameError</error>
</service>
```

14. Expr-C サーバは `get_edge_config` リクエストを受け取ると、リクエスト内のドメインを確認します。この場合は `collabedge-121.dc-01.com` です。DNS SRV レコードを使用して UDS サービスが特定され、次の DNS クエリが実行されます：`_cisco-uds.tcp.collabedge-121.dc-01.com`

15. DNS クエリを見ると、この DNS SRV レコードでエラーが発生することがわかります。

図 18. コラボレーション ソリューション アナライザ - DNS クエリ

Log overview

Calls MRA logins TCP/UDP streams **DNS queries**

Search:

Record type	Query	Response	DNS server
PTR	173.10.100.64.in-addr.arpa	✖ DNS response code: 3 - No such name	198.18.133.1
SRV	_cisco-phone-ftp_tcp.collabedge-121.dc-01.com	✖ DNS response code: 3 - No such name	198.18.133.1
SRV	_cuplogin_tcp.collabedge-121.dc-01.com	✖ DNS response code: 3 - No such name	198.18.133.1
SRV	_cisco-uds_tcp.collabedge-121.dc-01.com	✖ DNS response code: 3 - No such name	198.18.133.1

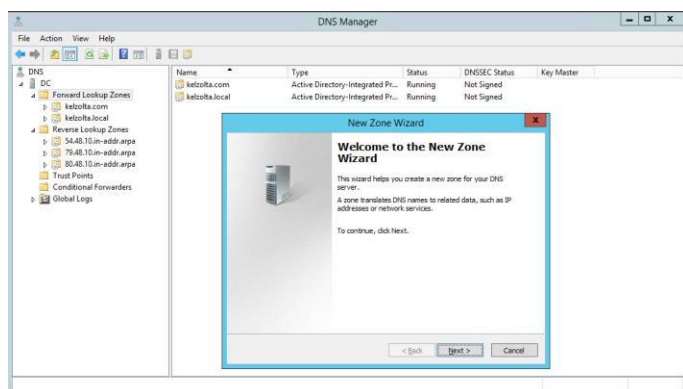
16. 以前参照した記事で説明されているように、Expr-C がこの SRV レコードを解決できることを確認する必要があります。最も簡単な方法は、`collabedge-121.dc-01.com` ドメインの正引きゾーンおよび `64.100.10` ネットワークの逆引きゾーンと以下の DNS レコードを内部 DNS に追加することです。

- `_cisco-uds_tcp.collabedge-121.dc-01.com -> ucm1.dcloud.cisco.com:8443`
- `vcse.collabedge-121.dc-01.com -> 64.100.10.173`
- `64.100.10.173 > vcse.collabedge-121.dc-01.com` の後方参照

17. 内部 DNS サーバ (Active Directory ドメイン コントローラ、198.18.133.1) へのリモート デスクトップ接続を (できれば自分のラップトップから) 開き、DNS Manager を開始します。

18. AD1 サーバで Forward Lookup Zones を右クリックし、[新規ゾーン... (New Zone ...)] オプションを選択します。ウィザードが表示されます。

図 19. DNS Manager の [新規ゾーン ウィザード (New Zone Wizard)]



プライマリ ゾーンの作成を選択して名前を `collabedge-121.dc-01.com` とし、それ以外のすべての設定はデフォルト値のままにします。

19. SRV レコードを作成するには、新しいゾーンを開き、右クリックして [他の新規レコード... (Other New Records ...)] を選択します。

図 20. 新しい SRV レコードの作成

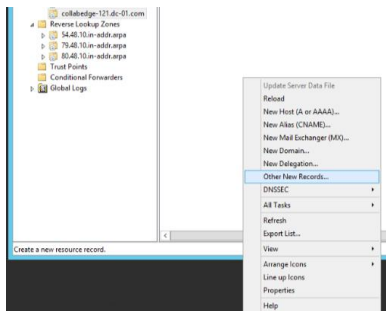
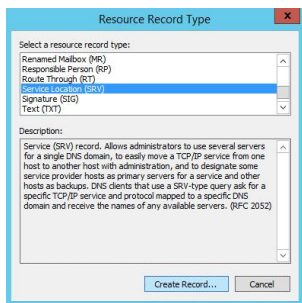
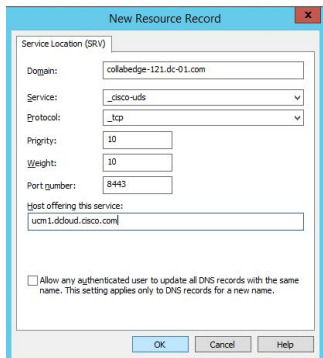


図 21. [リソースレコードタイプ (Resource Record Type)] から [サービスロケーション (SRV) (Service Location (SRV))] を選択



[サービス (Service)] は SRV レコードの最初の部分で、[プロトコル (Protocol)] は 2 つ目の部分です。[優先度 (Priority)] と [重み付け (Weight)] は、このシナリオでは重要ではありません。_cisco-uds (UDS サービス) 用の [ポート番号 (Port number)] は、必ず 8443 にします。[このサービスを提供するホスト (Host offering this service)] が、SRV レコードの宛先になります。ここでは常に完全修飾ホスト名を使用することを強く推奨します。場合によっては完全修飾ホスト名が必須となることもあります。この場合は UCM サーバになります。

図 22. SRV レコードの設定



SRV レコードによって、Microsoft DNS サーバのゾーン内にフォルダ構造が自動的に作成されます。最後の手順が完了したら、[完了 (Done)] をクリックしてウィザードを終了します。

20. 上記に挙げた 2 番目の DNS エントリは必ず必要になります。collabedge-121.dc-01.com のゾーンを内部 DNS サーバに追加すると、DNS サーバがこのゾーンに対するクエリを転送しなくなるからです。標準的な A レコード (ホスト) を追加するほうが、はるかに簡単です。

- a 自分のゾーンのルート フォルダに移動してもう一度右クリックし、[新規ホスト (A または AAAA) ... (New Host (A or AAAA)...)] を選択します。
- b ホスト名を入力します (厳密にホスト名のみ。FQDN は 2 番目の読み取り専用フィールドで自動的に更新されます)。
- c IP アドレスを入力します。
- d パブリック IP のため、DNS サーバは、関連するポインタレコード (PTR) レコードを自身で作成できません。次のステップで、[関連するポインタレコード (PTR) を作成する (Create associated pointer (PTR) record)] をオフにして手動で完了することができます。
- e 設定を終えたら、[ホストの追加 (Add Host)] をクリック後、[完了 (Done)] をクリックします。

図 23. [新規ホスト (New Host)] フォーム

21. 逆引きは有効な方法であり、Expressway X8.8 のリリース ノートに記載されているように、Expressway X8.8 以降では必須になっています。

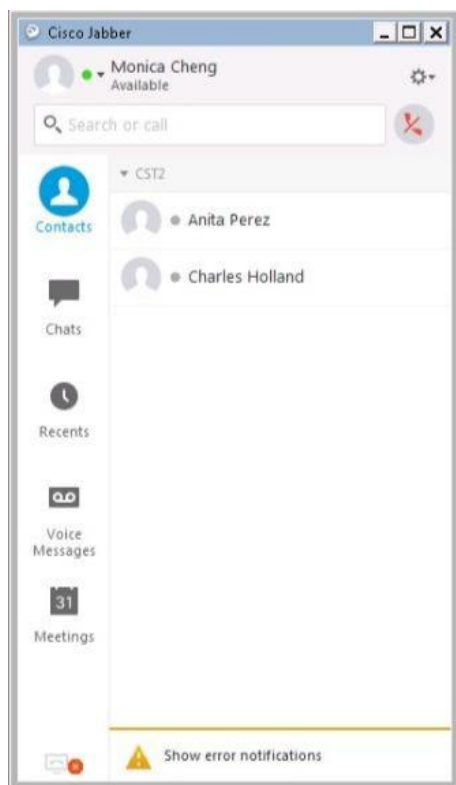
内部 DNS サーバには 64.100.10.x ネットワークの逆引きゾーンはないため、作成する必要があります。逆引きゾーンを新しく作成する方法は、正引きゾーンを作成する方法とほぼ同じです。違うのは、右クリックするフォルダが Reverse Lookup Zones である点です。同様のウィザードを使用し、[ネットワーク ID (Network ID)] フィールドに 64.100.10 と入力して、IPv4 逆引きゾーンを作成します。これで、逆引きゾーン内に 10.100.64.in-addr.arpa という名前のフォルダが作成されます。

- a このフォルダに移動して、右クリックで [新規ポインタ (PTR) ... (New Pointer (PTR) ...)] を選択します。
- b Expressway-E の外部アドレスと FQDN を入力して IP を完了させます (前のステップで作成しているので、参照することもできます)。
- c [OK] を押します。

図 24. PTR レコードの追加

22. これらの変更を行うと Jabber にログイン可能になりますが、電話サービスは機能せず、使用できません。

図 25. Jabber - 電話サービスが無効



電話サービスのエラー

対応が必要な最後の問題は、電話サービスの問題です。これには、ログと[コラボレーション ソリューション アナライザ](#)が有効です。解決方法がわからない場合は、以下のページの手順に従ってください。

電話サービス エラーの解決

1. 前と同じ手順に従ってログを収集します。
 - Jabber を終了する
 - Expr-C と Expr-E の両方で診断ログを有効にする
 - Jabber を起動してログインし、電話サービスでエラーが発止するまで待つ
 - ログを収集する
2. Expr-E のログを[コラボレーション ソリューション アナライザ](#)にアップロードし、SIP 登録の状況を確認します。
3. ユーザに関連付けられている端末を確認します。クライアントは、/cucm-uds/user/mcheng/devices に対して GET リクエストを実行します。それに対する応答には、関連する端末の情報と XML が含まれます。

図 26. ユーザに関連付けられたデバイス

```

HTTP/1.1 200 OK
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00:00 UTC
Set-Cookie:<CONCEALED>
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Type: application/xml
Date: Wed, 31 Aug 2016 10:01:29 GMT
Server:
Age: 0
Content-Length: 152
Connection: keep-alive

<?xml version=" 1.0" ?>
<devices uri=" https://ucm1.dcloud.cisco.com:8443/cucm-uds/user/mcheng/devices" version=" 11.5.1" />

```

4. このラボではすでに CSF 端末がテスト ユーザに関連付けられているため、SIP 登録の確認に移ります。

図 27. コラボレーション ソリューション アナライザ - SIP 登録

Log overview

Calls MRA logins **SIP registrations** TCP/UDP streams DNS queries

Search:

From	To	Call ID	Src IP	Dest IP
6030@ucm1.dcloud.cisco.com	6030@ucm1.dcloud.cisco.com	005056b8-7f450002-0000540b-00001ee9@198.18.133.38	64.100.10.173	198.18.133.152
6030@ucm1.dcloud.cisco.com	6030@ucm1.dcloud.cisco.com	005056b8-7f450003-00006985-00005751@198.18.133.38	64.100.10.173	198.18.133.152
6030@ucm1.dcloud.cisco.com	6030@ucm1.dcloud.cisco.com	005056b8-7f450004-0000401a-00007731@198.18.133.38	64.100.10.173	198.18.133.152
6030@ucm1.dcloud.cisco.com	6030@ucm1.dcloud.cisco.com	005056b8-7f450005-00007f13-00001679@198.18.133.38	64.100.10.173	198.18.133.152

5. MRA ログインを確認すると、HTTPS メッセージに加えて、関連する SIP 登録も表示されています。いずれかを選択すると、Unified CM から [405 メソッドが許可されない (405 Method Not Allowed)] という応答が返されます。

図 28. コラボレーション ソリューション アナライザ - SIP 登録の詳細

SIP signaling

Time	Leg 1	Leg 2	CSeq	Source	Destination
06:32:09	→ REGISTER		102 REGISTER	64.100.10.173	198.18.133.152
06:32:09		→ REGISTER	102 REGISTER	198.18.133.152	198.18.133.3
06:32:09		← 100 TRYING	102 REGISTER	198.18.133.3	198.18.133.152
06:32:09		← 405 METHOD NOT ALLOWED	102 REGISTER	198.18.133.3	198.18.133.152
06:32:09	← 405 METHOD NOT ALLOWED		102 REGISTER	198.18.133.152	64.100.10.173

6. メッセージの詳細は本文に記載されています。

図 29. コラボレーション ソリューション アナライザ - [405 メソッドが許可されない (405 Method Not Allowed)]


```


SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 198.18.133.152:5060;egress-
zone=CEtcpucm1dcloudcisco.com;branch=z9hG4bK62b376eb4a2b5735d15de7b8b63dea2420859.d4022f6a833ad0f73d501fc8e4eee75c;proxy-
call-id=2457a63a-1f9a-4515-930e-e25edd731672;rport,SIP/2.0/TLS 64.100.10.173:7001;egress-
zone=VCSCforMRA;branch=z9hG4bK4391726fc5d96a21c57eb4923b2bc0f92297.b43a29220dbcb7ad8464e73e9feb60c;proxy-call-
id=93804dbb-bef3-40e7-9a4e-33ec5bfe8a56;received=64.100.10.173;rport=7001;ingress-zone=VCSEforMRA,SIP/2.0/TLS
198.18.133.38:59001;branch=z9hG4bK0000473e;received=198.18.133.38;ingress-zone=CollaborationEdgeZone
Call-ID: 005056b8-7f450002-0000540b-00001ee9@198.18.133.38
CSeq: 102 REGISTER
From: <sip:6030@ucm1.dcloud.cisco.com>;tag=005056b87f45000200002d82-00002d73
To: <sip:6030@ucm1.dcloud.cisco.com>;tag=1318307227
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
Server: Cisco-CUCM11.5
Date: Wed, 31 Aug 2016 06:32:09 GMT
Warning: 399 ucm1 "SIP trunk disallows REGISTER"
Content-Length: 0

```

7. Expr-C が、Unified CM に SIP トランクによる SIP 登録を送信します。Unified CM は、SIP トランクでの登録を承認しません。そのことについて Expr-C にアラートが表示され、アラートに関するシステム情報が示されます。

図 30. コラボレーション ソリューション アナライザ - システム情報アラート

System information 

General information  IP Configuration MRA

ALERTS


Severity	Reason
Warning	Unified CM port conflict - There is a port conflict on Unified CM 198.18.133.3 between neighbor zone CUCM Neighbor and Unified Communications

8. このツールが検出した問題については MRA ログインでもアラートが出され、是正措置が指示されます。


図 31. コラボレーション ソリューション アナライザ - MRA ログインのトラブルシューティング


Log overview

Calls **MRA logins** SIP registrations TCP/UDP streams DNS queries

Time	Client IP	MRA User	MRA Phone
06:31:54	198.18.133.38	mcheng	CSFMCHENG 

MRA Login Details

MRA Login **Troubleshooting** 

 MRA registration failed for phone : CSFMCHENG

9. Unified CM は、SIP トランクに関連付けられている TCP 接続経由で SIP 登録を受け取ります。これは Unified CM が、Expr-C への SIP トランクをポート 5060 でリッスンするためです。これとは異なるポートを使用する必要があります。この問題を修正します。
 - a Unified CM で、Expr-C への SIP トランクに適用された SIP トランク セキュリティ プロファイルの着信ポートを、ポート 5560 に変更します。トランクを必ずリセットしてください。
 - b 上記の情報に合わせて、Expr-C で、Unified CM へのネイバー ゾーンのポートを 5560 に変更します。
10. テストを再度実行すると正常に機能します。コラボレーション エンジンに有効な一連のログをアップロードすると、MRA ログインに、HTTPS メッセージと SIP 登録メッセージの両方が含まれていることを確認できます。

これでラボは終わりです。

付録 A SIP 登録の詳細

有効な設定が行われたところで、SIP シグナリングを詳細に見てみましょう。ツールで簡単に確認できます。

ソフトフォン登録

1. クライアントが SIP 登録を Expr-E に送信します。

```
REGISTER sip:ucm1.dcloud.cisco.com SIP/2.0
Via: SIP/2.0/TLS 198.18.133.38:56920;branch=z9hG4bK00004b7c
Call-ID: 005056b8-7f450002-000051fe-0000798f@198.18.133.38
CSeq: 102 REGISTER
Contact: <sip:d2d564d1-6b01-8be7-a7f8-b44b905fc6d6@198.18.133.38:56920;transport=tls>;+sip.instance="urn:uuid:00000000-0000-0000-0000-005056b87f45>";+u.sip!devicename.ccm.cisco.com="CSEFMCHENG";+u.sip!model.ccm.cisco.com="503";video
From: <sip:6030@ucm1.dcloud.cisco.com>;tag=005056b87f45000200003d5f-0000701f
To: <sip:6030@ucm1.dcloud.cisco.com>
Max-Forwards: 70
Route: <sip:vcse.collabedge-121.dc-01.com;transport=tls;lr>, <sip:198.18.133.152:5061;transport=tls;zone-id=2;directed;lr>, <sip:ucm1.dcloud.cisco.com;transport=tcp;lr>
User-Agent: Cisco-CSF
Expires: 3600
Date: Fri, 02 Sep 2016 13:28:08 GMT
Proxy-Authorization: Digest username="mcheng", realm="vcse.collabedge-121.dc-01.com", uri="sip:ucm1.dcloud.cisco.com", response="5fa4d7097f712a5864294f2904d95d48", nonce="ef30e93be9fac7c6c424d13a0938daca77797e8ddaa4360628784682eb9d", opaque="AQAAADohLG338MMdvzJnwlrKIF09Gvb", cnonce="00006dfb", qop=auth, nc=00000001, algorithm=MD5
```

Via ヘッダーは、REGISTER リクエストに対する SIP 応答のパスを決定するために使用されます。

Route ヘッダーは、SIP 登録リクエストのパスを決定するために使用されます。ここでは、クライアントが実際に SIP 登録が従うパスを決定していることを確認できます。

```
sip:vcse.collabedge-121.dc-01.com;transport=tls;lr
```

```
sip:198.18.133.152:5061;transport=tls;zone-id=2;directed;lr
```

```
sip:ucm1.dcloud.cisco.com;transport=tcp;lr
```

最初のルートは Expr-E 自体であり、2 番目のエントリは Expr-C で、最後のエントリは Unified CM です。

2. この登録を確認していくと、次の内容が Expr-E から Expr-C に送信されることを確認できます。

```
REGISTER sip:ucml.dcloud.cisco.com SIP/2.0
Via: SIP/2.0/TLS 64.100.10.173:7001;egress-
zone=VCSCforMRA;branch=z9hG4bK64ed5a54e1c5999788e0d07e9dd44f782863.7d3dec7739d8c538ca3bf47cf0eb14de;prox_y-
call-id=06cd0c4f-0488-4db4-9db4-e3ac8e7a2cdf;rport
Via: SIP/2.0/TLS 198.18.133.38:56920;branch=z9hG4bK00004b7c;received=198.18.133.38;ingress-
zone=CollaborationEdgeZone
Call-ID: 005056b8-7f450002-000051fe-0000798f@198.18.133.38
CSeq: 102 REGISTER
Contact: <sip:d2d564d1-6b01-8be7-a7f8-
b44b905fc6d6@198.18.133.38:56920;transport=tls>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-
005056b87f45>";+u.sip!devicename.ccm.cisco.com="CSFMCHENG";+u.sip!model.ccm.cisco.com="503";video;+u.sip !user
id.ccm.cisco.com="mcheng"
From: <sip:6030@ucml.dcloud.cisco.com>;tag=005056b87f45000200003d5f-0000701f
To: <sip:6030@ucml.dcloud.cisco.com>
Max-Forwards: 15
Route: <sip:ucml.dcloud.cisco.com;transport=tcp;lr>
Path: <sip:64.100.10.173:7001;transport=tls;lr>
Path: <sip:198.18.133.38:56920;transport=tls;apparent;ds;lr>
User-Agent: Cisco-CSF
Expires: 3600
Date: Fri, 02 Sep 2016 13:28:08 GMT
Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-
serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-
config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg P-Asserted-
Identity: <sip:6030@ucml.dcloud.cisco.com>
X-TAATag: 7b0077e8-84e8-4e52-92b5-5bf0cad28284
```

Via ヘッダーにどのように Expr-E が追加され、応答が送信されるかがわかります。Route ヘッダーには、使用するトランスポートを含む Unified CM が示されます。この Route ヘッダーは、Expr-C で自動的に作成された検索ルールに一致します。これはログで確認できます。

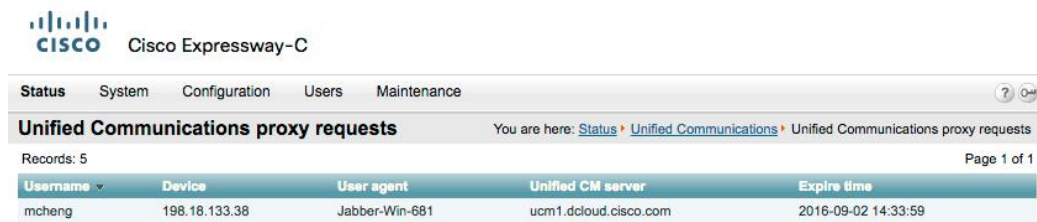
```
Module="network.search" Level="DEBUG": Detail="Considering search rule 'CEtcp-ucml.dcloud.cisco.com'
towards target 'CEtcp-ucml.dcloud.cisco.com' at priority '45' with alias
'ucml.dcloud.cisco.com;transport=tcp;lr'"
```

200 OK 応答は via ヘッダーのパスに従い、Unified CM から Expr-C、Expr-C から Expr-E、そして最終的に Expr-E から Jabber に送信されます。

登録の検証方法

Expr-C で登録を確認することができます。ここでは Jabber デバイスのユーザ名と IP アドレスで検証できます。

図 32. 登録の検証 - Expr-C



The screenshot shows the Cisco Expressway-C interface. At the top, there is a navigation menu with 'Status', 'System', 'Configuration', 'Users', and 'Maintenance'. Below this, the page title is 'Unified Communications proxy requests'. A breadcrumb trail indicates the current location: 'You are here: Status > Unified Communications > Unified Communications proxy requests'. Below the title, it says 'Records: 5' and 'Page 1 of 1'. A table lists the proxy requests with the following columns: Username, Device, User agent, Unified CM server, and Expire time. The table contains one row with the following data: Username: mcheng, Device: 198.18.133.38, User agent: Jabber-Win-681, Unified CM server: ucm1.dcloud.cisco.com, and Expire time: 2016-09-02 14:33:59.

Username	Device	User agent	Unified CM server	Expire time
mcheng	198.18.133.38	Jabber-Win-681	ucm1.dcloud.cisco.com	2016-09-02 14:33:59

Unified CM では、Expr-C の IP アドレスによってデバイスが登録されていることがわかります。

図 33. 登録の検証 - Unified CM



The screenshot shows the Unified CM interface. It displays the 'Phone Type' section with 'Product Type: Cisco Unified Client Services Framework' and 'Device Protocol: SIP'. Below this, the 'Real-time Device Status' section shows 'Registration: Registered with Cisco Unified Communications Manager ucm1.dcloud.cisco.com', 'IPv4 Address: 198.18.133.152', and 'Active Load ID: Jabber_for_Windows-11.7.0.42920'.

Phone Type
Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Real-time Device Status
Registration: Registered with Cisco Unified Communications Manager ucm1.dcloud.cisco.com
IPv4 Address: 198.18.133.152
Active Load ID: Jabber_for_Windows-11.7.0.42920

Jabber 自体の接続ステータスを確認すると、Expressway 経由で接続していることがわかります。

図 34. 登録の検証 - Jabber



The screenshot shows the 'Connection Status' window for Cisco Jabber. It displays 'Cisco Jabber Version 11.7.0 (42920)'. Below this, the 'Softphone' status is shown as 'Connected'. The details include: Protocol: SIP, Address: ucm1.dcloud.cisco.com (CCMCIP - Expressway) (IPv4), Device: CSFMCHENG, and Line: 6030.

Softphone
Status: Connected
Protocol: SIP
Address: ucm1.dcloud.cisco.com (CCMCIP - Expressway) (IPv4)
Device: CSFMCHENG
Line: 6030

© 2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2019 年 1 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
<http://www.cisco.com/jp>

お問い合わせ先