

ExpresswayでのXMPPフェデレーションの設定とトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ1:Expressway EでXMPPフェデレーションを有効にする](#)

[ExpresswayでのXMPP設定の確認](#)

[Expressway CおよびExpressway EでのXMPPフェデレーションのトラブルシューティング](#)

[ステップ2:ダイヤルバックシークレットの設定](#)

[ダイヤルバックシークレットの確認](#)

[ステップ3:セキュリティモードの設定](#)

[セキュリティモードのトラブルシューティング](#)

[一般的な問題:](#)

[症状1:一方向のメッセージング。外部へのインターネットは機能しません。IM&Pステータスがアクティブ](#)

[症状2:フェデレーションが失敗し、CUPのXCPルータがパケットをバウンスしている](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

概要

このドキュメントでは、ExpresswayでのExtensible Messaging and Presence Protocol(XMPP)フェデレーションの設定手順について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

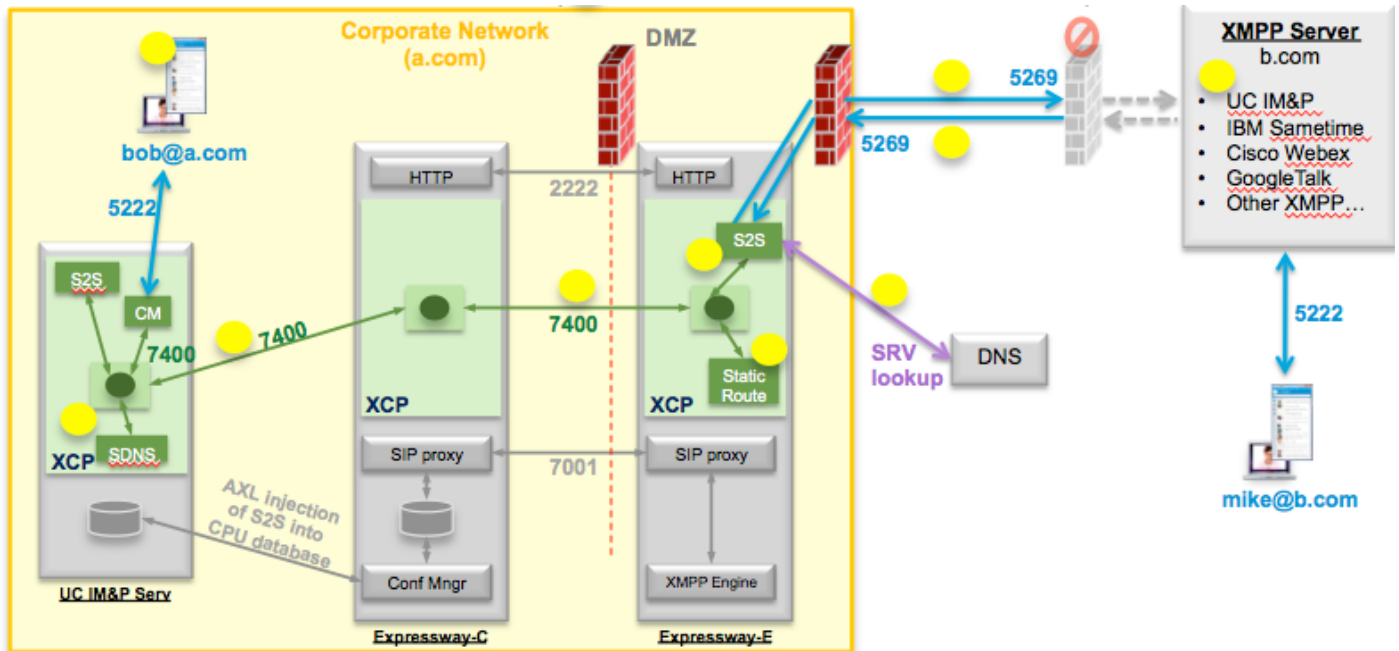
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Expressway X8.2以降
- Unified Call Manager(CM)インスタントメッセージング(IM)およびプレゼンスサービス 9.1.1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。

背景説明

次の図は、高度な通信を示しています。



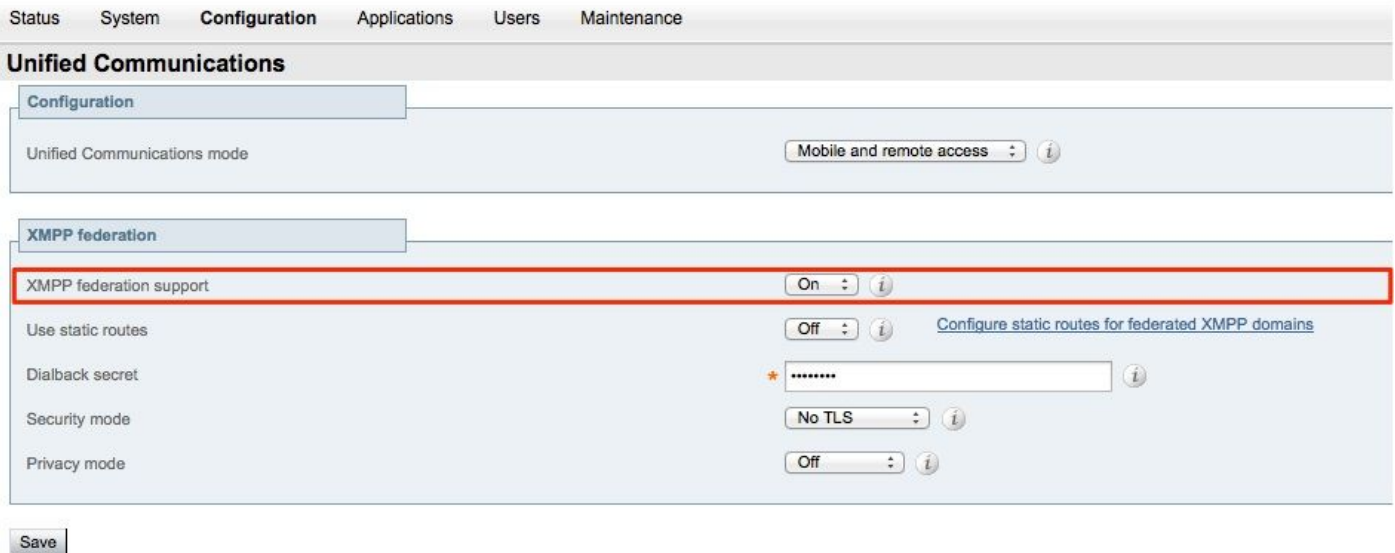
ExpresswayでXMPPフェデレーションを有効にすると、アクティブなサーバからサーバ(S2S)がCisco Unified Presence(CUP)からExpressway Edge(Expressway E)に移動します。このコンポーネントは、フェデレーテッドドメイン間のすべてのXMPP通信を管理します。

- S2Sはポート5269を使用してフェデレーテッドドメインと通信します
- ExpresswayE、C、およびCUPのXCPルータ間の内部XMPPトラフィックは、ポート7400で動作します
- Expressway EからのXMPPプロビジョニング情報は、ポート2222のSSHトンネルを介してExpressway Cに送信されます
- Expressway Cは、AXLポート8443を介して必要なルーティング情報でCUPを更新します

設定

ステップ1:Expressway EでXMPPフェデレーションを有効にする

[Configuration] > [Unified Communication] > XMPPフェデレーションサポート >オン



XMPPフェデレーションを有効にすると、次のように表示されます。

1. Expressway-Eはローカル設定を更新し、この設定をExpressway Core(Expressway C)で複製します。

Expressway Eのログには次のように表示されます。 "Detail="xconfiguration xcpConfiguration is_federation_enabled - changed from: : 0 ~ 1"

2. Expressway-Cは、Expressway E S2SコンポーネントのレルムでCUPデータベースの「xmpp2snodes」テーブルを更新します。

Expressway Cのログには次のように表示されます。 "Module="network.axl" Level="INFO" Action="Send" URL="<https://cups.ciscotac.net:8443/axl/>" Function="executeSQLQuery"

3.パブリックDNSが、フェデレーションが必要なすべてのドメインのXMPPサーバSRVレコードで更新されていることを確認します。

`_xmpp-server._tcp.domain.com (ポート5269)`

ExpresswayでのXMPP設定の確認

ステップ1:CUP Command Line Interface (CLI ; コマンドラインインターフェイス) から次のクエリを実行して、データベースの変更がIM&Pサーバで正常に受け入れられたかどうかを確認します。

```
admin:run sql select * from xmpp2snodes
pkid cp_id
```

```
=====
055c13d9-943d-459d-a3c6-af1d1176936d cm-2_s2scp-1.eft-xwye-a-coluc-com
admin:
```

ステップ2:IM&PサーバでXMPPフェデレーションがオフになっていることを確認します。

[プレゼンス] > [ドメイン間フェデレーション] > [XMPPフェデレーション] > [設定] > [XMPPフェデレーションノードステータス] > [オフ]

Expressway CおよびExpressway EでのXMPPフェデレーションのトラブルシューティング

ステップ 1：デバッグレベルのログを有効にします。

Expressway-E:

[Maintenance] > [Diagnostics] > [Advanced] > [Support Log configuration] > developer.clusterdb.restapi

Expressway-C:

[Maintenance] > [Diagnostics] > [Advanced] > [Support Log configuration] > developer.clusterdb.restapi

[Maintenance] > [Diagnostics] > [Advanced] > [Network Log configuration] > [network.axl]

ステップ2:Expressway-CおよびExpressway-Eで診断ログとTCPダンプを開始します。

ネットワークの問題が疑われる場合は、CLIからIM&P側でパケットキャプチャを実行します。

「utils network capture eth0 file axl_inject.pcap count 1000000 size all」

ステップ3:Expressway-EでXMPPフェデレーションを有効にする

30秒待ってから、「ExpresswayでのXMPP設定の確認」で説明する手順を実行します

ステップ2：ダイヤルバックシークレットの設定

[Configuration] > [Unified Communication] > [Dialback Secret]

Success: Saved

Configuration

Unified Communications mode Mobile and remote access ⓘ

XMPP federation

XMPP federation support On ⓘ

Use static routes Off ⓘ [Configure static routes for federated XMPP domains](#)

Dialback secret * ⓘ

Security mode No TLS ⓘ

Privacy mode Off ⓘ

Save

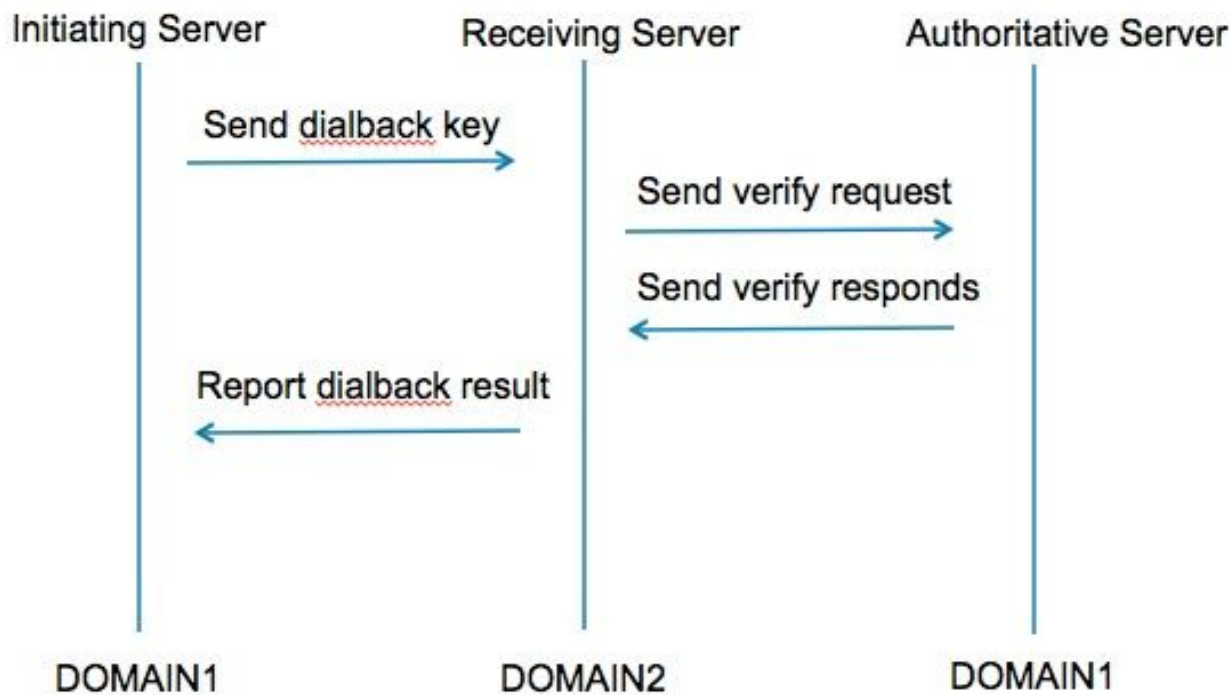
Unified Communications service configuration status

SIP registrations and provisioning on Unified CM	Configured (See Unified Communications status)
IM and Presence services on Unified CM	Configured (See Unified Communications status)
XMPP federation	Configured (See Unified Communications status)

Related tasks

[View XMPP federation activity in the event log](#)

ダイヤルバックはどのように機能しますか。



ステップ1：発信側サーバは、そのダイヤルバック結果が設定されたシークレットに基づいて計算し、受信側サーバに送信します。

ステップ2：受信側サーバは、開始元ドメインの権限のあるサーバでこの結果を検証します。

ステップ3：権威サーバが同じダイヤルバックシークレットを共有するため、結果を検証できます。

ステップ4：検証されると、受信側サーバは開始サーバからのXMPPを受け入れます。

ステップ5：開始サーバが_xmpp-server._tcp.<target domain>に対してルックアップを実行し、受信サーバを見つけます

ステップ6：受信側のサーバが_xmpp-server._tcp.<originning domain>に対してルックアップを実行し、権限のあるサーバを見つけます

ステップ7：権限サーバは、開始サーバと同じにすることができます

ダイヤルバックシークレットの確認

Expresswayが開始サーバである場合、次のデバッグが表示されます。

```
XCP_CM2[12122]:..Level="INFO " CodeLocation="stanza.component.out"
Detail="xcoder=34A9B60C8 sending:<db:result from='coluc.com'
to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:result>"
```

```
XCP_CM2[12122]:..Level="DEBUG" CodeLocation="stream.out" Detail="(00000000-0000-0000-
0000-000000000000, coluc.com:vngtp.lab, OUT) xcoder=34A9B60C8 Scheduling dialback
timeout in 30 secs"
```

```
XCP_CM2[12122]:..Level="INFO " CodeLocation="ConnInfoHistory" Detail="接続状態の変更
: PENDING->CONNECTED:.."
```

Expresswayが受信側サーバである場合、次のデバッグが表示されます。

```
XCP_CM2[22992]:..Level="VBOSE" CodeLocation="stanza.component.in"
Detail="xcoder=05E295A2B received:
<db:result from='coluc.com'
to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:result>"
```

```
XCP_CM2[22992]:..Level="INFO " CodeLocation="Resolver.cpp:128" Detail=
"coluc.com:puny=coluc.com:service=_xmpp-server._tcp:defport=0'のリゾルバ検索を開始していま
す"
```

```
XCP_CM2[22992]:..Level="INFO " CodeLocation="debug" Detail="(e5b18d01-fe24-4290-bba1-
a57788a76468, vngtp.lab:coluc.com, IN)
resolved dialback address for host=coluc.com method=SRV dns-timetals=(TOTAL:0.003157
SRV:0.002885)"
```

```
XCP_CM2[22992]:..Level="INFO " CodeLocation="DBVerify.cpp:270" Detail="(e5b18d01-fe24-
4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
DBVerifyストリームが開いています。Sending db:verify packet:<db:verify from='vngtp.lab'
id='05E295A2B' to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b verify03</db >"
```

```
XCP_CM2[22992]:..Level="INFO " CodeLocation="DBVerify.cpp:282" Detail="(e5b18d01-fe24-
4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
DBVerifyパケット受信<db:verify from='coluc.com' id='05E295A2B' to='vngtp.lab'
```

```
type='valid'>d780f198ac34a dbd795fcdaf8762eaf 52ea9b03</db:verify>
```

Expresswayが正規サーバである場合、このデバッグが表示されます

```
XCP_CM2[5164]:..Level="INFO " CodeLocation="debug" Detail="xcoder=94A9B60C8  
onStreamOpen:  
<stream:stream from='vngtp.lab' id='1327B794B' to='coluc.com' version='1.0' xml:lang='en-  
US.UTF-8' xmlns='jabber:server' xmlns:db='jabber:server:back'  
xmlns:stream='http://etherx.jabber.org/streams'/> 」
```

```
XCP_CM2[5164]:..Level="VBOSE" CodeLocation="stanza.component.in"  
Detail="xcoder=94A9B60C8 received::  
<db:verify from='vngtp.lab' id='05E295A2B'  
to='coluc.com'>d780f198ac34adbdbd795fcdaf8762eaf52ea9b verify03</db >"
```

```
XCP_CM2[5164]:..Level="INFO " CodeLocation="stream.in" Detail="xcoder=94A9B60C8 closing  
stream used for dialback only"
```

ステップ3：セキュリティモードの設定

The screenshot shows the Cisco Expressway-E configuration page for Unified Communications. The 'XMPP federation' section is expanded, and the 'Security mode' dropdown menu is open. The 'Security mode' label is highlighted with a red box, and the dropdown menu options are also highlighted with a red box. The options are: No TLS (selected), TLS required, TLS optional, and No TLS. The 'Save' button is visible at the bottom left.

セキュリティモードのトラブルシューティング

- Wiresharkを使用して
- 機能は、Transport Layer Security(TLS)が必要か、オプションか、TLSなしかを示します
次のパケットキャプチャ証明書は、TLSが必要な場合の例を示しています。

Source	Destination	Protocol	Length	Info
10.48.36.171	10.48.55.113	TCP	74	30353 > xmpp-server [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1119103043 TSecr=0
10.48.55.113	10.48.36.171	TCP	74	xmpp-server > 30353 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=1119100129 TSecr=1119100129
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1119103043 TSecr=1119100129
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	XMPP/XML	254	STREAM < coluc.com
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	XMPP/XML	173	FEATURES
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	XMPP/XML	117	STARTTLS
10.48.55.113	10.48.36.171	XMPP/XML	116	PROCEED
10.48.36.171	10.48.55.113	TCP	298	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	1434	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	1369	[TCP segment of a reassembled PDU]
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=464 Ack=3017 Win=36096 Len=0 TSval=1119100134 TSecr=1119100134
10.48.36.171	10.48.55.113	TCP	640	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	292	[TCP segment of a reassembled PDU]
10.48.36.171	10.48.55.113	TCP	298	[TCP segment of a reassembled PDU]
10.48.55.113	10.48.36.171	TCP	113	[TCP segment of a reassembled PDU]
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3460 Win=41600 Len=0 TSval=1119103110 TSecr=1119100156
10.48.55.113	10.48.36.171	XMPP Protocol		PROCEED [xmlns="urn:iETF:params:xml:ns:xmpp-tls"] xmlns: urn:iETF:params:xml:ns:xmpp-tls

SSLとしてデバッグすると、TLSハンドシェイクが表示されます

Source	Destination	Protocol	Length	Info
10.48.36.171	10.48.55.113	TCP	74	30353 > xmpp-server [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1119103043 TSecr=0
10.48.55.113	10.48.36.171	TCP	74	xmpp-server > 30353 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=1119100129 TSecr=1119100129
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1119103043 TSecr=1119100129
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	TLSv1.2	254	Continuation Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	TLSv1.2	173	Continuation Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	TLSv1.2	117	Continuation Data
10.48.55.113	10.48.36.171	TLSv1.2	116	Continuation Data
10.48.36.171	10.48.55.113	TLSv1.2	275	Client Hello
10.48.55.113	10.48.36.171	TLSv1.2	1434	Server Hello
10.48.55.113	10.48.36.171	TLSv1.2	1369	Certificate, Server Hello Done
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=464 Ack=3017 Win=36096 Len=0 TSval=1119100134 TSecr=1119100134
10.48.36.171	10.48.55.113	TLSv1.2	640	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10.48.55.113	10.48.36.171	TLSv1.2	292	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
10.48.36.171	10.48.55.113	TLSv1.2	298	Application Data
10.48.55.113	10.48.36.171	TLSv1.2	283	Application Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3460 Win=41600 Len=0 TSval=1119103110 TSecr=1119100156
10.48.55.113	10.48.36.171	TLSv1.2	113	Application Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3507 Win=41600 Len=0 TSval=1119103110 TSecr=1119100195
10.48.36.171	10.48.55.113	TLSv1.2	190	Application Data
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=3507 Ack=1394 Win=33408 Len=0 TSval=1119100236 TSecr=1119103110
10.48.55.113	10.48.36.171	TLSv1.2	218	Application Data

一般的な問題:

症状 1: 一方向のメッセージング。外部へのインターネットは機能しません。IM&Pステータスがアクティブ

Expressway-Cのログ:

```
"Function="executeSQLQuery" Status="401" Reason="None"
```

原因 1: Expressway-C側のIM&Pユーザのクレデンシャルが正しくありません。

これは、このURLを実行し、Expressway Cで設定されているクレデンシャルでログインして確認することもできます

[Configuration] > [Unified Communications] > [IM and Presence Servers]

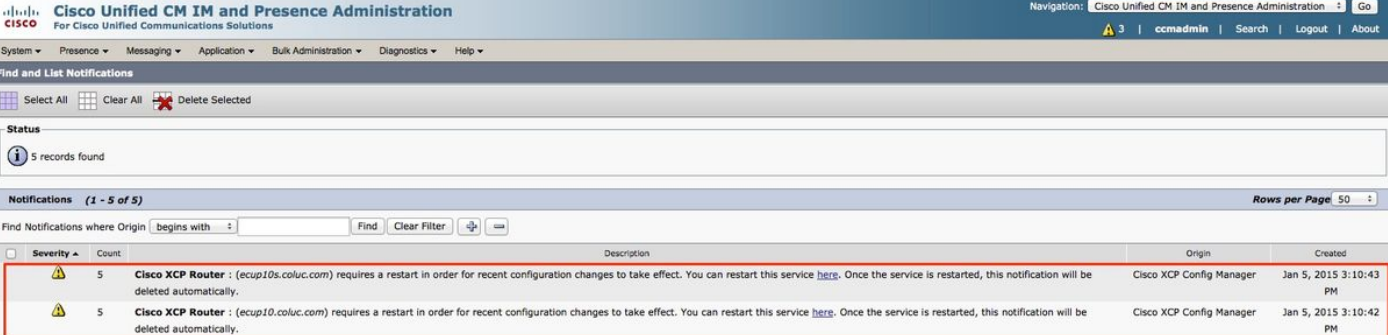
https://cups_address.domain.com:8443/axl

解決策 1 : パスワードの更新、CUPサーバ検出の更新

症状 2 : フェデレーションが失敗し、CUPのXCPルータがパケットをバウンスしている

原因 2 : CUPのXCPルータが再起動されていない

これは、CUP Administrationの[Notifications]ページで確認することができます。



The screenshot shows the Cisco Unified CM IM and Presence Administration web interface. The main content area displays a table of notifications. The table has columns for Severity, Count, Description, Origin, and Created. Two notifications are listed, both with a severity of 5 and a count of 5. The description for both notifications states: "Cisco XCP Router : (ecup10s.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service [here](#). Once the service is restarted, this notification will be deleted automatically." The origin for both is "Cisco XCP Config Manager" and the creation time is "Jan 5, 2015 3:10:43 PM" and "Jan 5, 2015 3:10:42 PM" respectively.

Severity	Count	Description	Origin	Created
5	5	Cisco XCP Router : (ecup10s.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service here . Once the service is restarted, this notification will be deleted automatically.	Cisco XCP Config Manager	Jan 5, 2015 3:10:43 PM
5	5	Cisco XCP Router : (ecup10.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service here . Once the service is restarted, this notification will be deleted automatically.	Cisco XCP Config Manager	Jan 5, 2015 3:10:42 PM

解決策 2 : CUPでXCPルータを再起動する

時には通知が行われませんが、CUPのXCPルータログはまだパケットのバウンスを行っています。XCP Routerサービスを再起動しても解決しない場合は、IM&Pクラスタをリブートします。

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

現在、この設定に関する特定のトラブルシューティング情報ははありません。

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)