在Expressway上配置XMPP聯合併對其進行故障排除

目錄

簡介

本檔案將介紹Expressway上可擴充訊息和狀態通訊協定(XMPP)聯合的設定步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

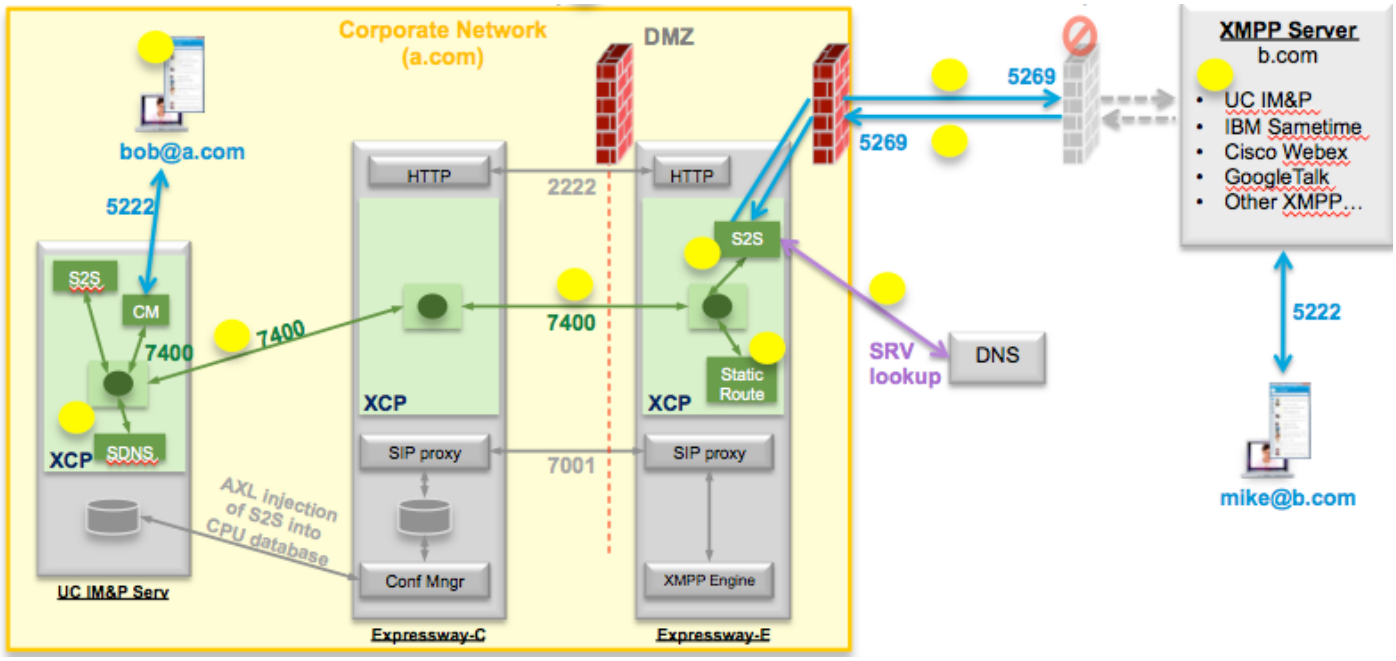
本文中的資訊係根據以下軟體和硬體版本：

- Cisco Expressway X8.2或更高版本
- Unified Call Manager(CM)即時消息(IM)和線上狀態服務9.1.1或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

此圖說明高級通訊：



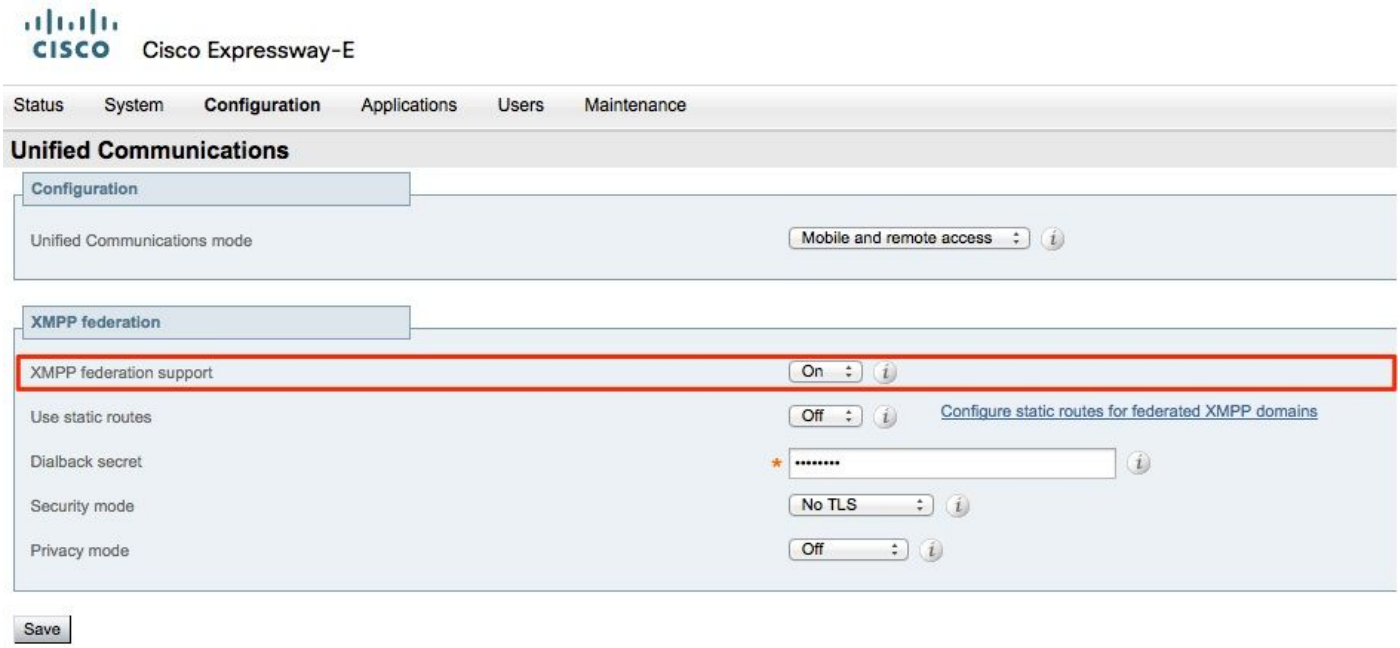
如果在Expressway上啟用XMPP聯合，則活動伺服器到伺服器(S2S)會從Cisco Unified Presence(CUP)移動到Expressway邊緣(Expressway E)。 此元件管理聯合域之間的所有XMPP通訊。

- S2S使用埠5269與聯合域通訊
- ExpresswayE、C和CUP上的XCP路由器之間的內部XMPP流量在埠7400上運行
- 來自Expressway E的XMPP調配資訊通過埠2222上的SSH隧道傳送到Expressway C
- Expressway C通過AXL埠8443使用必要的路由資訊更新CUP

設定

步驟1.在Expressway E上啟用XMPP聯合

配置>統一通訊> XMPP聯合支援 >開啟



啟用XMPP聯合後，將觀察此情況：

1. Expressway-E更新其本地配置，並使用Expressway核心(Expressway C)複製此設定。

Expressway E日誌將顯示： "Detail="xconfiguration xcpConfiguration is_federation_enabled — 更改自：0到：1"

2. Expressway-C使用Expressway E S2S元件領域更新CUP資料庫上的「xmpps2snodes」表。

Expressway C日誌將顯示： "Module="network.axl" Level="INFO" Action="Send" URL="https://cups.ciscotac.net:8443/axl/" Function="executeSQLQuery"

3.確保使用需要與其聯合的所有域的XMPP伺服器SRV記錄更新公共DNS。

埠5269上的_xmpp-server._tcp.domain.com

檢驗Expressway上的XMPP配置

步驟1.通過從CUP命令列介面(CLI)運行此查詢，驗證IM&P伺服器是否成功接受了資料庫更改：

admin：運行sql select * from xmpps2snodes
pkid cp_id
==== ====
055c13d9-943d-459d-a3c6-af1d1176936d cm-2_s2scp-1.eft-xwye-a-coluc-com
admin:

步驟2.驗證IM&P伺服器上的XMPP聯合是否已關閉：

Presence > Inter-Domain Federation > XMPP Federation > Settings > XMPP Federation Node Status > Off

排除Expressway C和Expressway E上的XMPP聯合故障

步驟1..啟用DEBUG級別日誌：

在Expressway-E上：

維護>診斷>高級>支援日誌配置> developer.clusterdb.restapi

在Expressway-C上：

維護>診斷>高級>支援日誌配置> developer.clusterdb.restapi

維護>診斷>高級>網路日誌配置> network.axl

步驟2.在Expressway-C和Expressway-E上啟動診斷日誌和TCP轉儲：

如果懷疑存在網路問題，請從CLI在IM&P端執行資料包捕獲：

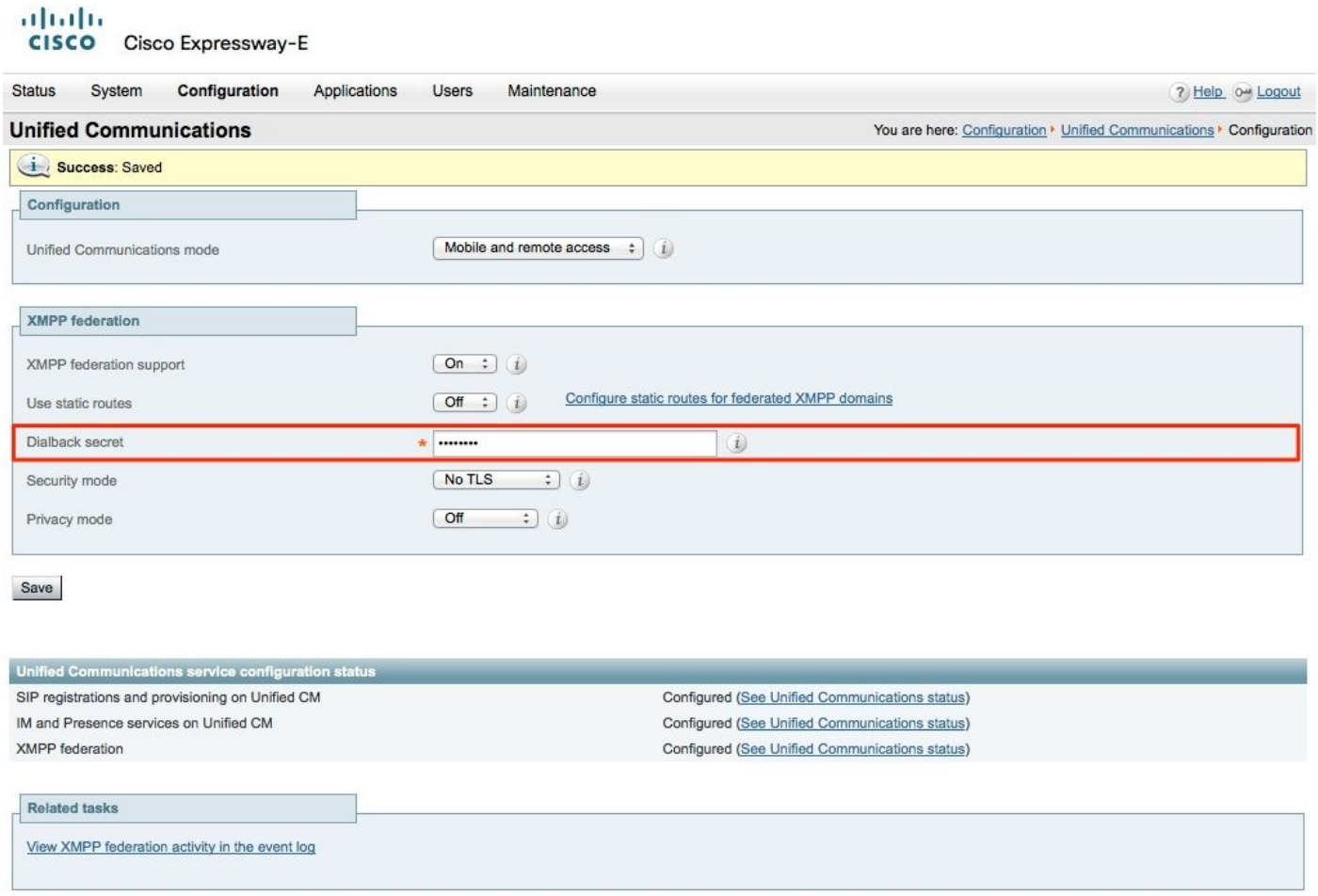
"utils network capture eth0 file axl_inject.pcap count 1000000 size all"

步驟3.在Expressway-E上啟用XMPP聯合

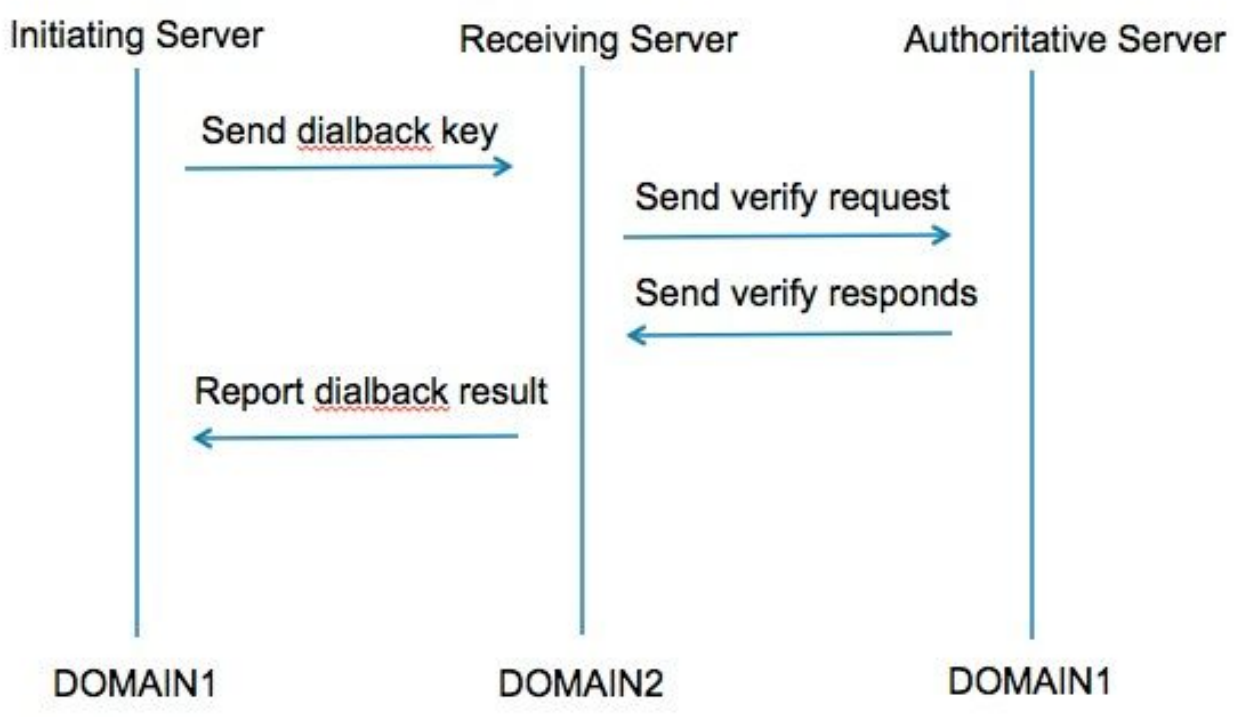
等待30秒，然後完成「檢驗Expressway上的XMPP配置」中所述的步驟

步驟2.配置回撥密碼

Configuration > Unified Communication > Dialback Secret



回撥如何工作？



步驟1.發起伺服器根據配置的金鑰計算其回撥結果，並傳送給接收伺服器。

步驟2.接收伺服器將與發起域的授權伺服器驗證此結果。

步驟3.由於授權伺服器共用相同的回撥金鑰，因此能夠驗證結果。

步驟4.驗證後，接收伺服器將接受來自發起伺服器的XMPP。

步驟5.發起伺服器對_xmpp-server._tcp.<目標域>執行查詢以查詢接收伺服器

步驟6.接收伺服器對_xmpp-server._tcp.<原始域>執行查詢以查詢授權伺服器

步驟7.授權伺服器可以與發起伺服器相同

驗證回撥密碼

Expressway在啟動伺服器時顯示此調試：

XCP_CM2[12122]:..Level="INFO " CodeLocation="stanza.component.out" Detail="xcoder=34A9B60C8傳送：<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在30秒內安排回撥超時。"

XCP_CM2[12122]:..Level="INFO " CodeLocation="ConnInfoHistory" Detail="連線狀態更改：PENDING->CONNECTED:...

Expressway作為接收伺服器時顯示此調試:

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

XCP_CM2[22992]:..Level="INFO " CodeLocation="Resolver.cpp:128" Detail=
"開始為'coluc.com:puny=coluc.com:service=_xmpp-server._tcp:defport=0'查詢解析程式"

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-timings=(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流已開啟。傳送db：驗證資料包：<db:verify from='vngtp.lab' id='05E295A2B'
to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"

XCP_CM2[22992]:..Level="INFO " CodeLocation="DBVerify.cpp:282" Detail="(e5b18d01-fe24-4290-bba1-a57788a76468, vngtp.lab:coluc.com,IN)
DBVerify收到資料包<db:verify from='coluc.com' id='05E295A2B' to='vngtp.lab'
type='valid'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>

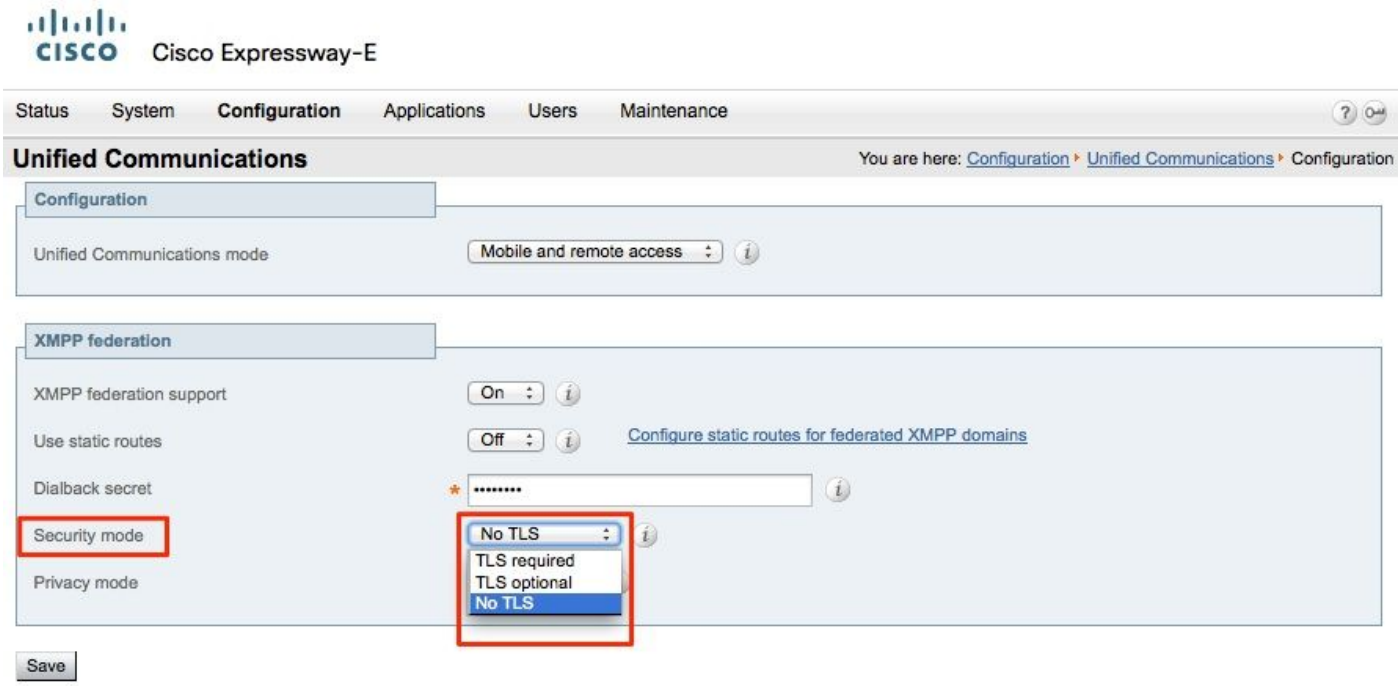
Expressway作為授權伺服器時顯示此調試

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:dialback'
xmlns:stream='http://etherx.jabber.org/streams'/>"

XCP_CM2[5164]:..Level="VBOSE" CodeLocation="stanza.component.in"
Detail="xcoder=94A9B60C8已接收：
<db:verify from='vngtp.lab' id='05E295A2B'
to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"

XCP_CM2[5164]:..Level="INFO " CodeLocation="stream.in" Detail="xcoder=94A9B60C8結束流僅用於回撥"

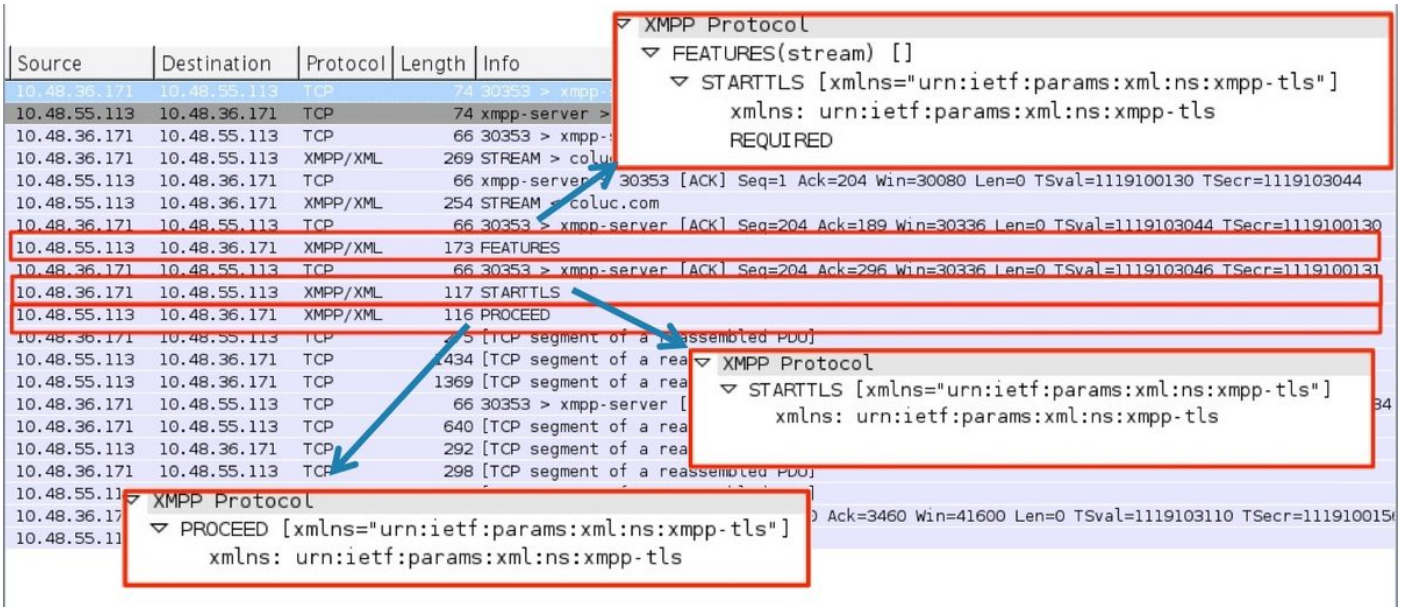
步驟3.配置安全模式



安全模式故障排除

- Wireshark可用於排除故障
- 功能將顯示傳輸層安全性(TLS)是必需的，是可選的，還是不需要TLS

此資料包捕獲摘錄顯示了何時需要TLS的示例：



當調試為SSL時，您將看到TLS握手

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 W
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=111910012
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
10.48.36.171	10.48.55.113	TLSv1.2	269	Continuation Data
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=1119103049 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

常見問題：

症狀1:單向報文傳送。外部網際網路不起作用。IM&P狀態為活動狀態

在Expressway-C日誌上：

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

原因1: Expressway-C端的IM&P使用者憑據錯誤。

也可以通過運行此URL並使用在Expressway C上配置的憑證登入來驗證這一點

Configuration > Unified Communications > IM and Presence Servers

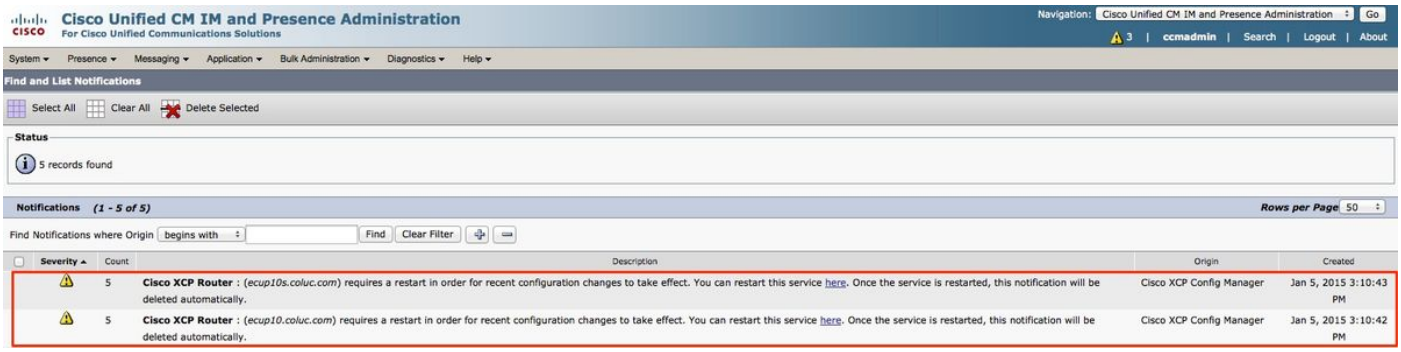
https://cups_address.domain.com:8443/axl

解決方案1 :更新密碼，刷新CUP伺服器發現

症狀2:聯合失敗，CUP上的XCP路由器正在退回資料包

原因二:CUP上的XCP路由器尚未重新啟動

這可以在CUP **Administration**的**Notifications**頁面下驗證。



解決方案2:在CUP上重新啟動XCP路由器

有時不會發出通知，但CUP上的XCP路由器日誌仍會彈跳資料包。 如果重新啟動XCP路由器服務不能解決此問題，則重新啟動IM&P群集可以解決此問題。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 技術支援與文件 - Cisco Systems