在Expressway上配置XMPP联合并排除故障

目录

简介

本文档介绍Expressway上可扩展消息传送和在线状态协议(XMPP)联合的配置步骤。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

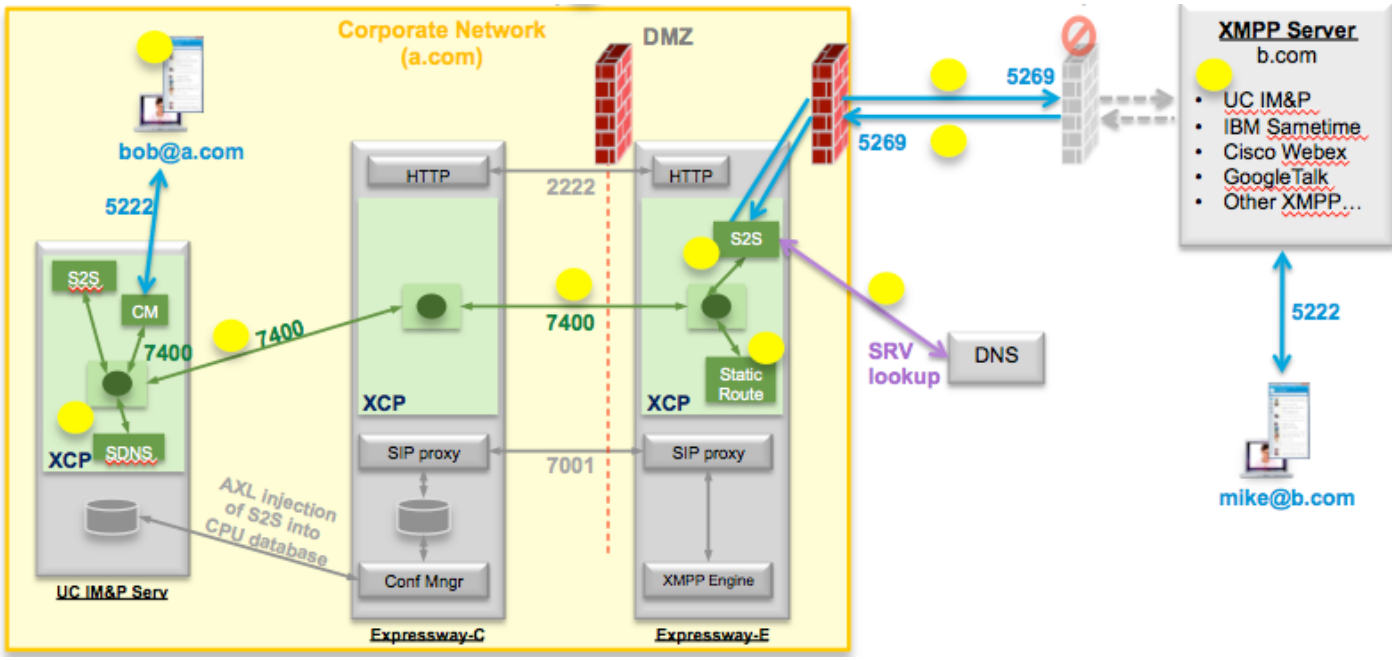
本文档中的信息基于以下软件和硬件版本：

- Cisco Expressway X8.2或更高版本
- Unified Call Manager(CM)即时消息(IM)和在线状态服务9.1.1或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

下图说明了高级通信：



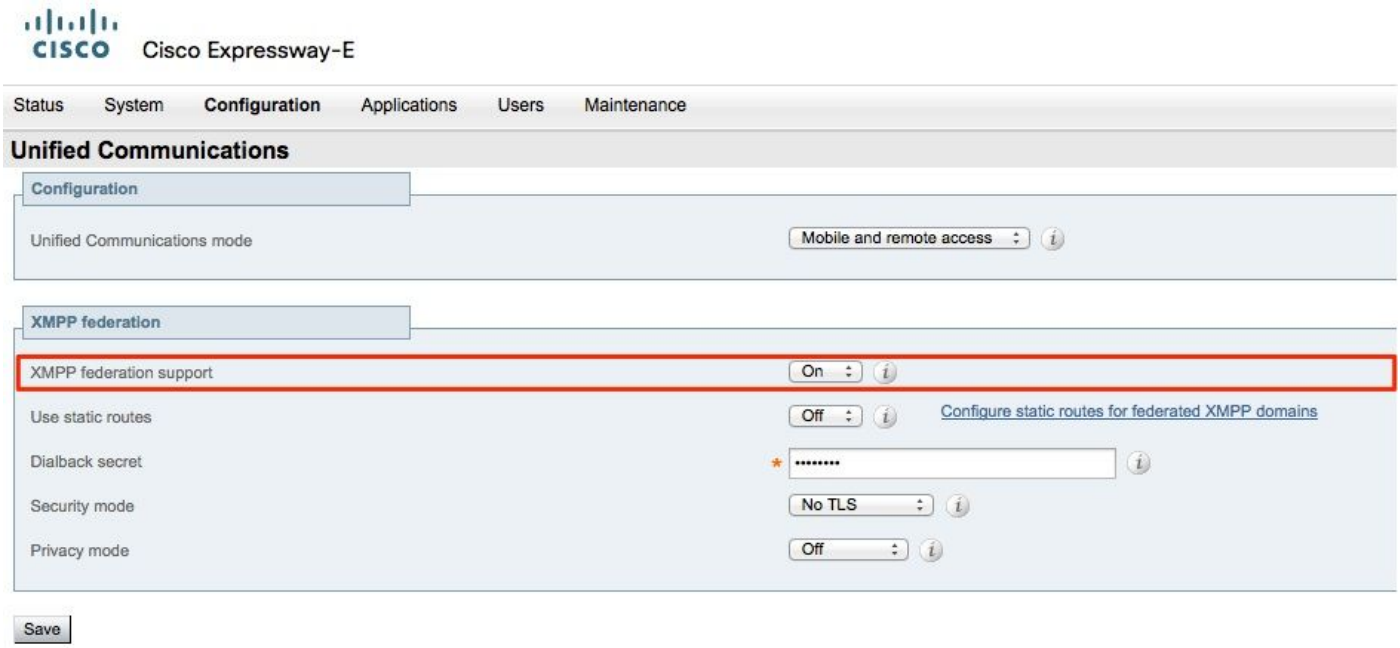
如果在Expressway上启用XMPP联合，则活动服务器到服务器(S2S)从Cisco Unified Presence(CUP)移动到Expressway边缘(Expressway E)。 此组件管理联合域之间的所有XMPP通信。

- S2S使用端口5269与联合域通信
- ExpresswayE、C和CUP上的XCP路由器之间的内部XMPP流量在端口7400上运行
- 来自Expressway E的XMPP调配信息通过端口2222上的SSH隧道发送到Expressway C
- Expressway C通过AXL端口8443使用必要的路由信息更新CUP

配置

步骤1.在Expressway E上启用XMPP联合

Configuration > Unified Communication > XMPP联合支持 >开



启用XMPP联合后，将观察到以下情况：

1. Expressway-E更新其本地配置，并将此设置复制到Expressway核心(Expressway C)。

Expressway E日志将显示： "Detail="xconfiguration xcpConfiguration is_federation_enabled — 更改自：0到：1"

2. Expressway-C使用Expressway E S2S组件领域更新CUP数据库上的“xmpps2snodes”表。

Expressway C日志将显示： "Module="network.axl" Level="INFO" Action="Send" URL="https://cups.ciscotac.net:8443/axl/" Function="executeSQLQuery"

3.确保使用XMPP服务器SRV记录更新公共DNS，以便所有需要联合的域都能使用这些记录。

_xmpp-server._tcp.domain.com（端口5269）

验证Expressway上的XMPP配置

步骤1.通过从CUP命令行界面(CLI)运行此查询，验证IM&P服务器是否成功接受了数据库更改：

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

步骤2.验证IM&P服务器上的XMPP联合关闭：

在线状态>域间联合> XMPP联合>设置> XMPP联合节点状态>关闭

排除Expressway C和Expressway E上的XMPP联合故障

步骤1:.启用DEBUG级别日志：

在Expressway-E上：

维护>诊断>高级>支持日志配置> developer.clusterdb.restapi

在Expressway-C上：

维护>诊断>高级>支持日志配置> developer.clusterdb.restapi

维护>诊断>高级>网络日志配置> network.axl

步骤2.在Expressway-C和Expressway-E上启动诊断日志和TCP转储：

如果怀疑存在网络问题，请从CLI在IM&P端执行数据包捕获：

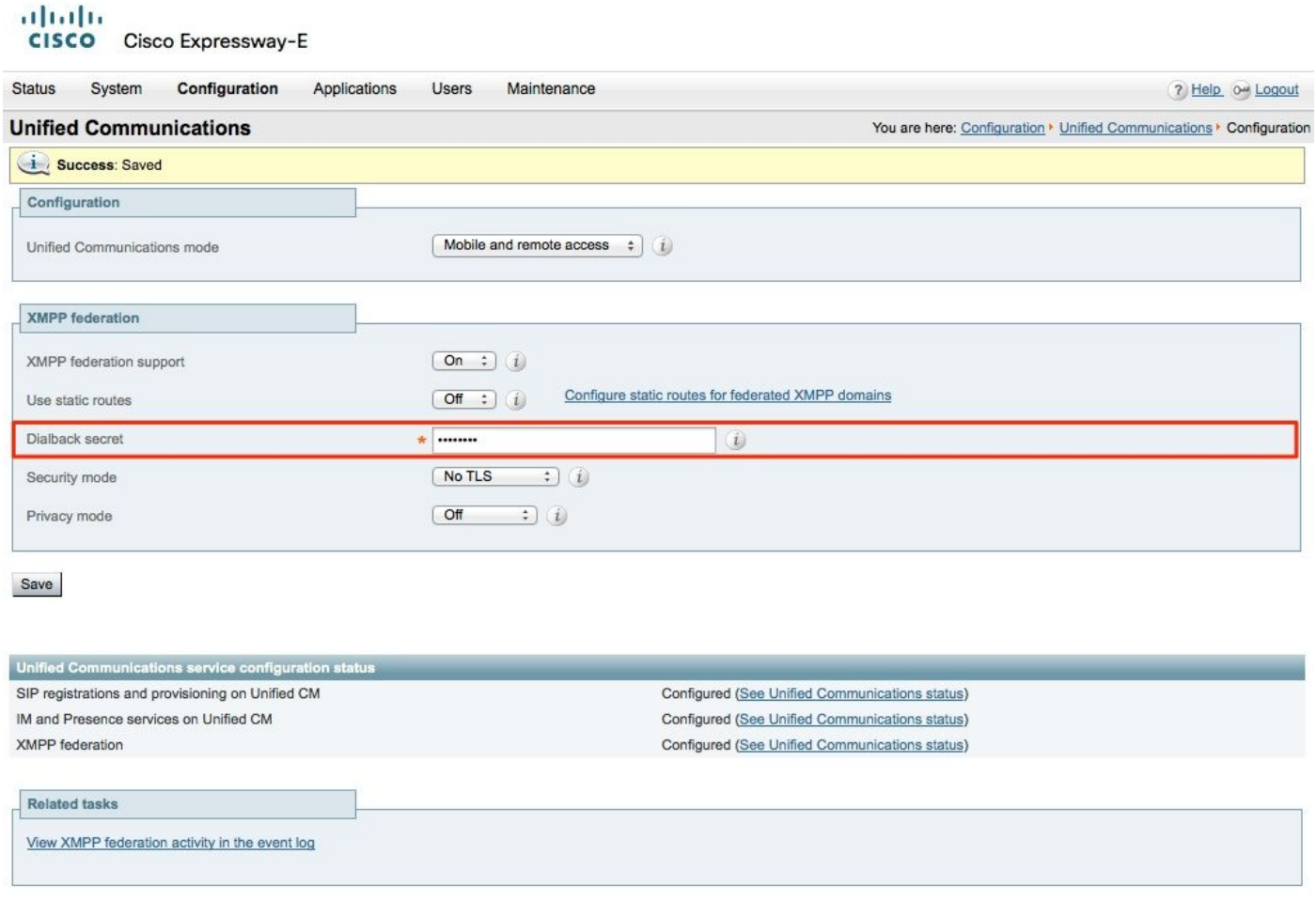
"utils network capture eth0 file axl_inject.pcap count 1000000 size all"

步骤3.在Expressway-E上启用XMPP联合

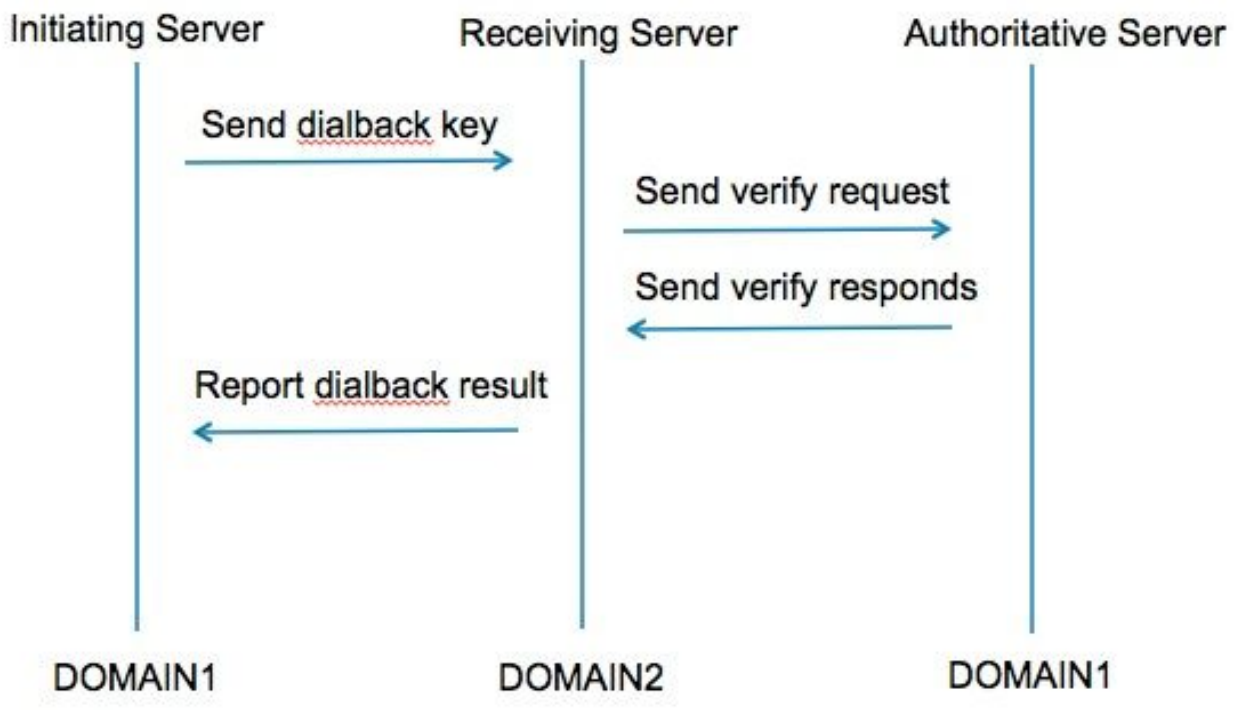
等待30秒，然后完成“验证Expressway上的XMPP配置”下描述的步骤

步骤2.配置回拨密钥

Configuration > Unified Communication > Dialback Secret



拨回如何工作？



步骤1.发起方服务器根据配置其回拨结果的密钥进行计算，并发送到接收服务器。

步骤2.接收服务器将从发起域向授权服务器验证此结果。

步骤3.由于授权服务器共享相同的拨回密钥，因此它能够验证结果。

步骤4.验证后，接收服务器将接受来自发起服务器的XMPP。

步骤5.发起服务器对_xmpp-server._tcp.<target domain>执行查找以查找接收服务器

步骤6.接收服务器对_xmpp-server._tcp.<orginating domain>执行查找以查找授权服务器

步骤7.授权服务器可以与发起服务器相同

验证回拨密钥

当Expressway是发起服务器时，Expressway显示此调试：

XCP_CM2[12122]:..Level="INFO " CodeLocation="stanza.component.out" Detail="xcoder=34A9B60C8发送：<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调度30秒内的回拨超时。"

XCP_CM2[12122]:..Level="INFO " CodeLocation="ConnInfoHistory" Detail="连接状态更改：PENDING->CONNECTED:...

当Expressway是接收服务器时，它显示此调试:

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

XCP_CM2[22992]:..Level="INFO " CodeLocation="Resolver.cpp:128" Detail=
"正在启动'coluc.com:puny=coluc.com:service=_xmpp-server._tcp:defport=0'的解析器查找"

XCP_CM2[22992]:..Level="INFO " CodeLocation="debug" Detail="(e5b18d01-fe24-4290-bba1-a57788a76468, vngtp.lab:coluc.com， IN)
已解析的主机的回拨地址=coluc.com方法=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流是打开的。正在发送db:verify数据包：<db:verify from='vngtp.lab' id='05E295A2B'
to='coluc.com'>d780f198ac34a6db795fcdaf8762ea9b03</db:verify>"

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

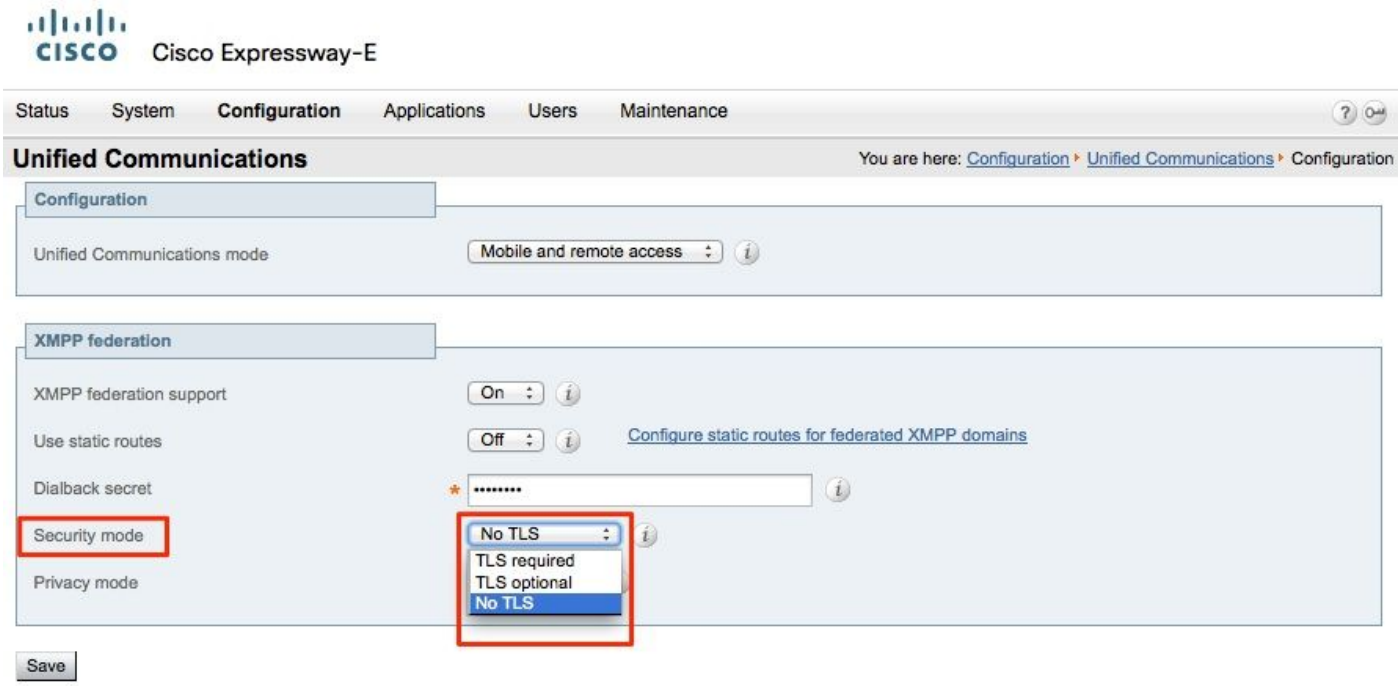
当Expressway是授权服务器时，Expressway显示此调试

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已收到：
<db:verify from='vngtp.lab' id='05E295A2B'
to='coluc.com'>d780f198ac34a6db795fcdaf8762ea9b03</db:verify>"

XCP_CM2[5164]:..Level="INFO " CodeLocation="stream.in" Detail="xcoder=94A9B60C8关闭流仅用于拨回"

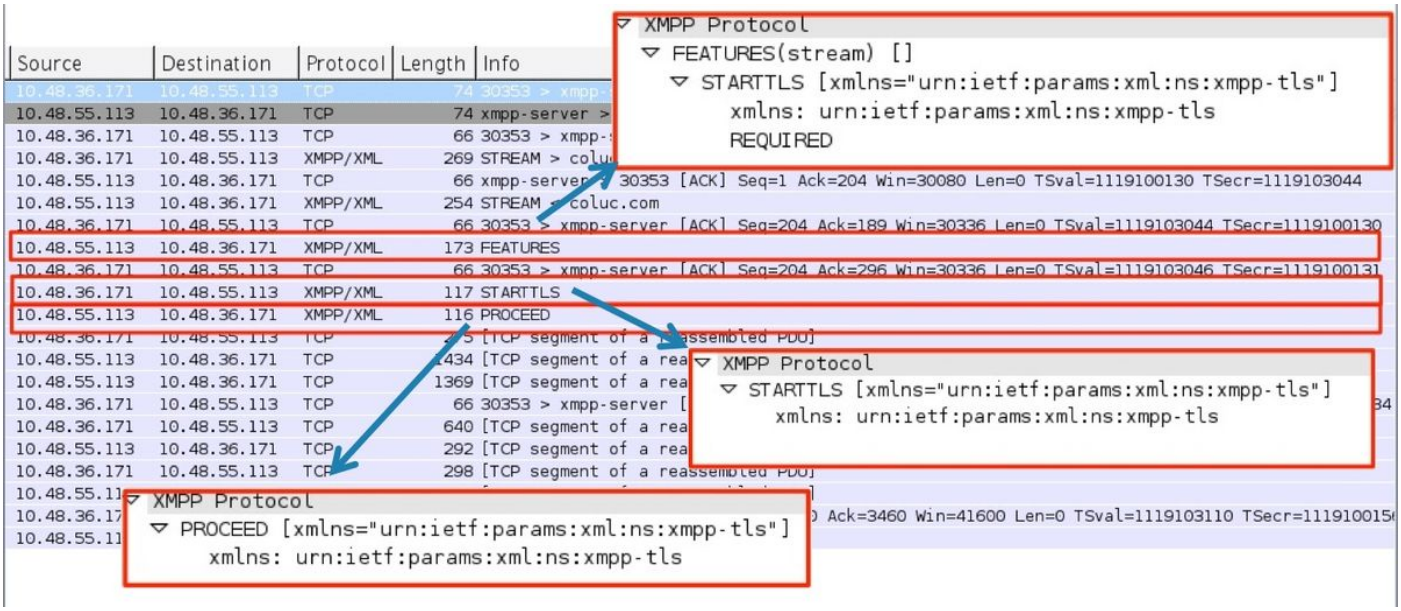
步骤3.配置安全模式



安全模式故障排除

- Wireshark可用于排除故障
- 功能将显示是否需要传输层安全(TLS)、可选或无TLS

本数据包捕获节目显示了何时需要TLS的示例：



当调试为SSL时，您会看到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

常见问题:

症状 1:单向消息。外部的Internet不起作用。IM&P状态为活动

在Expressway-C日志上：

"Function="executeSQLQuery"状态="401"原因="无"

原因 1：Expressway-C端IM&P用户的凭据错误。

这也可以通过运行此URL并使用Expressway C上配置的凭证登录来验证

Configuration > Unified Communications > IM and Presence Servers

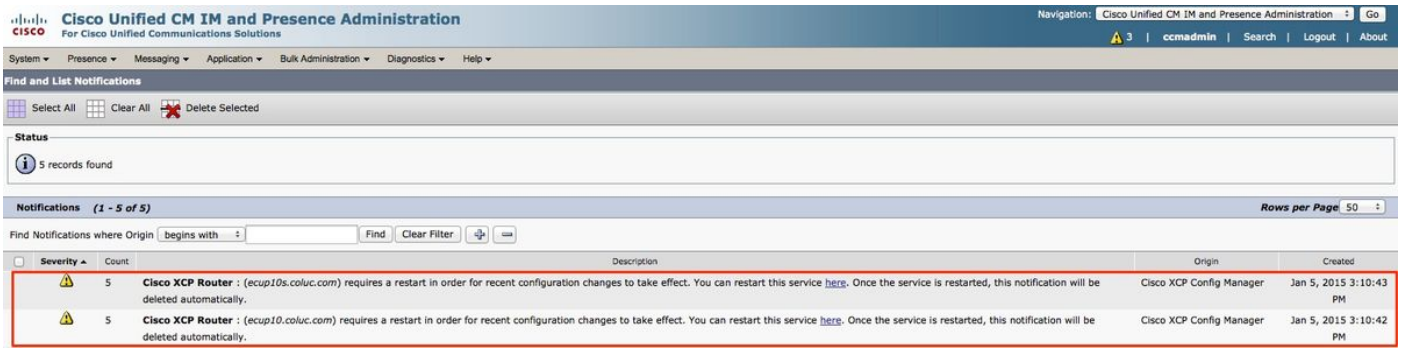
https://cups_address.domain.com:8443/axl

解决方案 1：更新密码，刷新CUP服务器发现

症状 2:联合失败，CUP上的XCP路由器正在反弹数据包

原因 2：CUP上的XCP路由器尚未重新启动

这可以在“通知”页**面下**的CUP**管理**中验证。



解决方案 2：在CUP上重新启动XCP路由器

有时不会发出通知，但CUP上的XCP路由器日志仍在弹跳数据包。 如果重新启动XCP路由器服务无法解决此问题，则重新启动IM&P集群会解决此问题。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems