

配置Expressway上的CMS WebRTC或Web应用代理

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置步骤](#)

[步骤1:将CMS WB集成到Expressway-C](#)

[第二步：启用TURN on the Expressway-E and Add the Authentication Credential to the Local Authentication Database](#)

[第三步：更改Expressway-E的管理端口](#)

[第四步：将Expressway-E添加为TURN服务器，用于在CMS服务器上进行媒体NAT穿越](#)

[验证](#)

[步骤1:在 Expressway C 上，检查 WB 是否已正确集成](#)

[第二步：验证TURN服务器已添加到CMS服务器](#)

[第三步：验证正在进行的呼叫期间的TURN中继使用情况](#)

[故障排除](#)

[外部 WebRTC 客户端已连接，但无介质（由于 ICE 失败）](#)

[外部 WebRTC 客户端上没有“加入呼叫”选项](#)

[在连接到 cospace 时，外部 WebRTC 客户端（在加载介质过程中）卡住了，随后被重定向到 WB 初始页面](#)

[外部 WebRTC 客户端无法加入 cospace 并收到警告（无法连接，请稍候重试）](#)

[相关信息](#)

简介

本文档介绍通过 Expressway 配置思科会议服务器 (CMS) WebRTC 并对其故障排除的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Expressway X12.6.1及更高版本（由于Exp TURN行为发生变化，x12.6.1及更高版本只能与CMS 2.9.2或更高版本配合使用）
- CMS 服务器 2.9.3 及更高版本
- 网络地址转换 (NAT)


- 在NAT周围使用中继(TURN)遍历
- 用于NAT的会话遍历实用程序(STUN)
- 域名系统 (DNS)

配置前提条件：

- 必须在Expressway上启用和配置与移动和远程访问(MRA)相关的基本设置 (UC遍历区域、SSH隧道)，请点击[此处](#)获取MRA指南。
- 对于CMS 2.9.x - WebBridge(WB)、在CMS上配置并启用的XMPP和CallBridge，请参阅[配置指南](#)
- 在 Expressway E 上安装 TURN 选项密钥。
- 从公共互联网到 Expressway E 的公共 IP 地址的防火墙上开启 TCP 端口 443。
- 从公共Internet到Expressway E的公共IP地址在防火墙上打开的TCP和UDP端口 3478 (TURN请求)。
 - 仅当CMS API中的“turnservers”将tcpPortNumberOverride设置为3478时才需要TCP 3478。
- 防火墙上打开的UDP端口3478 (TURN请求)从CMS到Expressway E的专用IP地址 (如果在Expressway E上使用双NIC)。
 - CMS 2.9.2及更低版本向Exp E发送绑定请求，而2.9.3则向Exp E发送分配请求
- Webbridge加入URL的外部DNS记录，可解析为Expressway-E的面向公众的IP地址。
- 可解析为Webbridge服务器IP地址的加入URL的内部DNS记录。
- 如果运行X12.5.2或更低版本，请确保外部防火墙允许Expressway-E的公共IP地址进行NAT反射，[点击](#)此处 (例如配置)。从X12.5.3开始，独立Expressway不再需要此功能。
- 使用端口443进行TURN时，您仍需要打开外部防火墙上介质的UDP端口3478。

 注意：启用TCP端口443时，Expressway无法再对TCP端口3478做出响应。

 注意：用于Jabber访客服务的Expressway对不能用于CMS WebRTC代理服务。

 注：如果从早期版本升级到3.0或更高版本，请参阅[Cisco Meeting Server 2.9到3.0 \(及以后 \) 平稳升级指南](#)

使用的组件

本文档不限于特定的软件和硬件版本，但必须满足最低软件版本要求。

- CMS 应用编程接口 (API)
- Expressway
- CMS 服务器

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

WebRTC代理支持已从X8.9.2版本添加到Expressway，使外部用户能够浏览到Cisco Meeting Server Web Bridge。

外部客户端和访客可以通过受支持的浏览器管理或加入会议，无需任何软件。 [点击此处获取受支持的浏览器列表。](#)

截至2021年2月5日，以下是CMS 3.1.1支持的浏览器：

Table 2: Cisco Meeting Server web app tested on browsers and versions

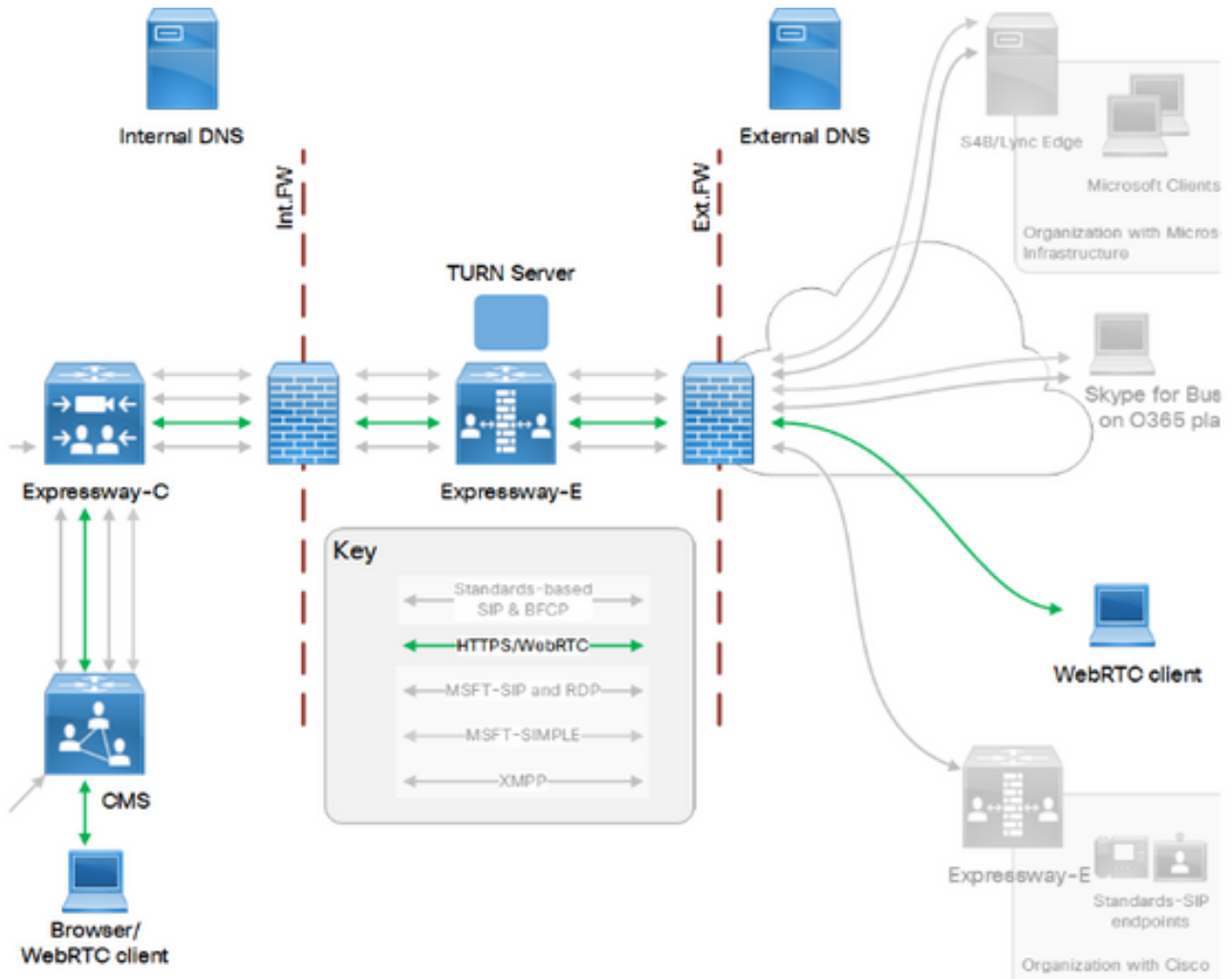
Browsers	Versions
Google Chrome (Windows, macOS and Android)	85
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	88
Apple Safari for macOS	13.0 and 14.0
Apple Safari for iOS	iOS versions: 13.0 and 14.0
Yandex (Windows)	20.8 and 20.11

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

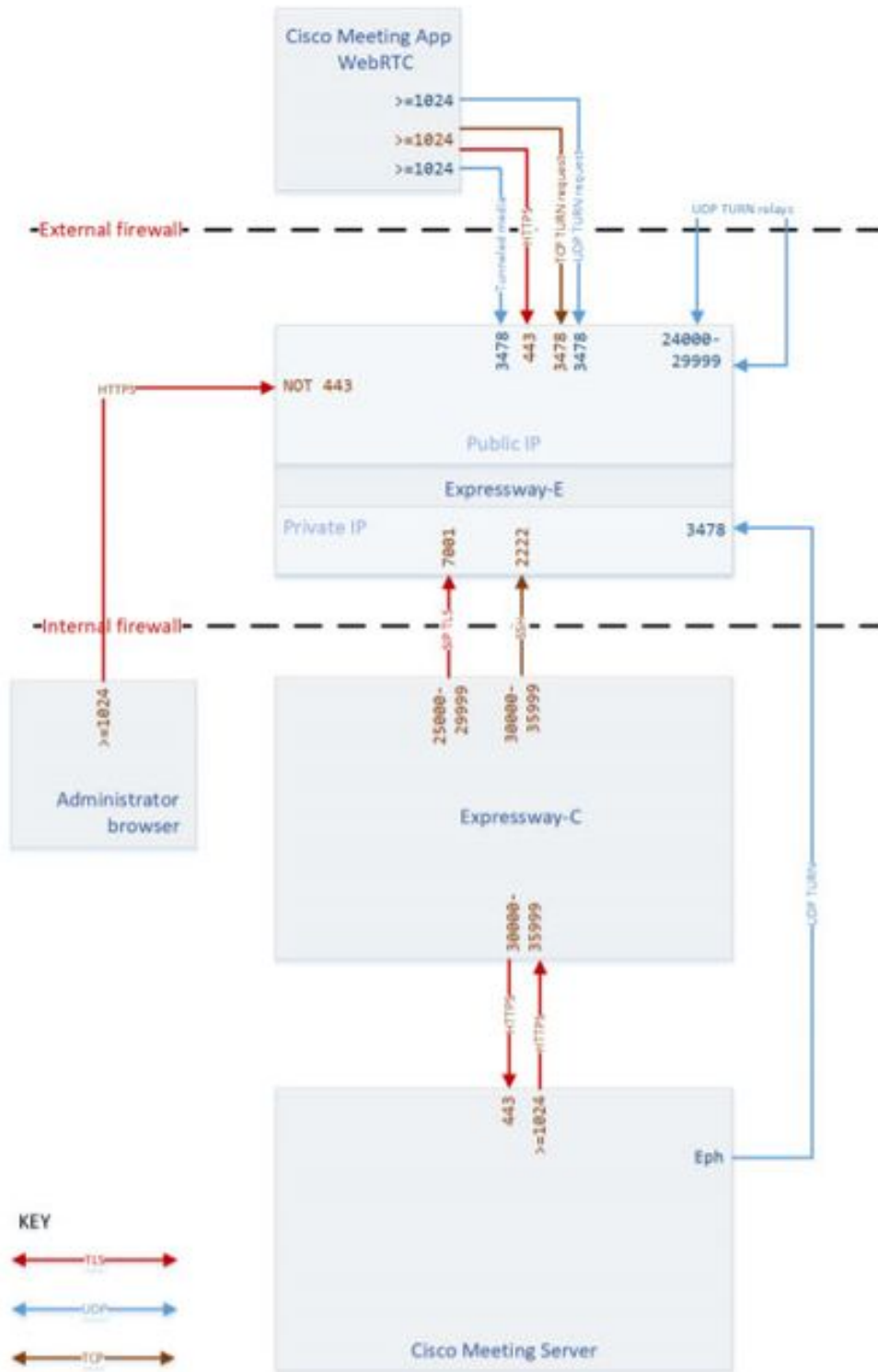
配置


网络图



此图像提供适用于CMS WebRTC的Web代理连接流的示例：(来自Exp IP端口使用配置指南)。

Web Proxy for Cisco Meeting Server Connections



 注意：运行X12.5.2或更早版本时，您必须配置外部防火墙以允许Expressway-E和公共IP地址的NAT反射（防火墙通常不信任具有相同源和目标IP地址的数据包）。从X12.5.3开始，独立Expressway不再需要此功能。

配置步骤

步骤1:将CMS WB集成到Expressway-C

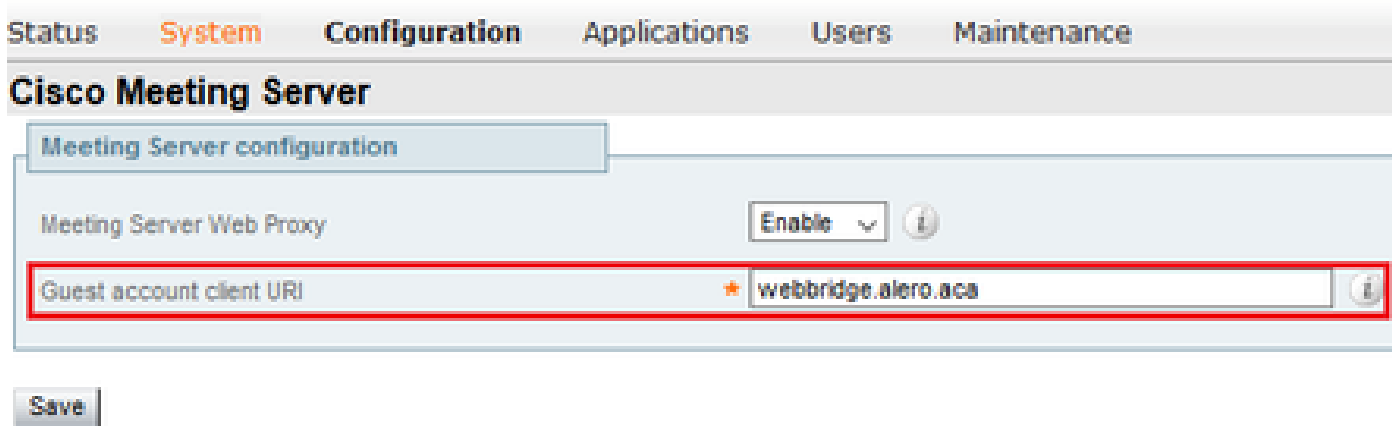
a.导航到配置>统一通信>思科会议服务器。

b.启用会议服务器Web代理。

c.在Guest account client URI字段中输入加入URL。

d.单击Save。

e.将CMS加入URL添加至Expressway-E服务器证书作为主题备用名称(SAN)。请参阅[Cisco VCS证书创建和使用部署指南](#)。





第二步：启用TURN on the Expressway-E and Add the Authentication Credential to the Local Authentication Database

a.导航到Configuration > Traversal > TURN。

b.启用TURN服务，从off到on。

c.选择Configure TURN client credentials on local database并添加凭据（用户名和密码）。

 注：如果您有一个Expressway-Es集群，并且它们都用作TURN服务器，请确保在所有节点上启用它。您必须通过API配置两个单独的turnServer实例，并将它们指向集群中的每个Expressway-E服务器（根据步骤4中所示的配置过程，该过程显示一个Expressway-E服务器的进程；第二个turnServer的配置类似，仅使用各自的IP地址和其他Expressway-E服务器的车削凭证）。

 注意：TCP/HTTPS流量可以在高速公路前面使用网络负载均衡器，但TURN媒体仍必须从客户端进入TURN服务器公共IP。TURN媒体不能通过网络负载均衡器

第三步：更改Expressway-E的管理端口

此步骤是必需的，因为webrtc连接在TCP 443上进入，但Exp 12.7引入了可用于443的新专用管理接口(DMI)。

a. 导航到 System > Administration。

b. 在 Web 服务器配置下，从下拉选项将 Web 管理员端口更改为 445，然后单击保存。

c. 在用于 WebRTC 代理服务的所有 Expressway-E 上重复步骤 3a 到 3b。

 注意：思科建议更改管理端口，因为 WebRTC 客户端使用 443。如果 WebRTC 浏览器尝试访问端口 80，Expressway E 会将连接重定向至端口 443。

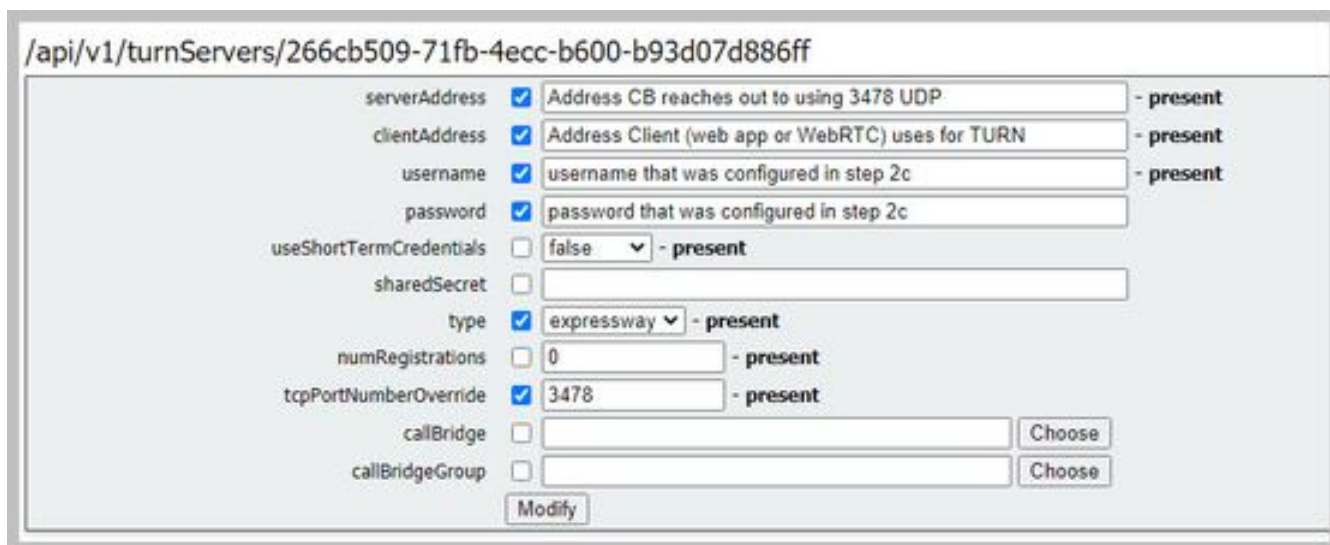
第四步：将 Expressway-E 添加为 TURN 服务器，用于在 CMS 服务器上进行媒体 NAT 穿越

在 CMS 2.9.x 版本中，使用 Configuration —> API 菜单添加翻转服务器：

- serverAddress：(Expressway 的专用 IP 地址)
- clientAddress：(Expressway 的公有 IP 地址)
- 类型：(expressway)
- 用户名：(如步骤 2c 中所配置)
- 密码：(如步骤 2c 中所配置)
- tcpPortNumberOverride:3478

d. 对要用于 TURN 的每个 Expressway E 服务器重复步骤 4c

此映像提供配置步骤的示例：



serverAddress	<input checked="" type="checkbox"/>	Address CB reaches out to using 3478 UDP	- present
clientAddress	<input checked="" type="checkbox"/>	Address Client (web app or WebRTC) uses for TURN	- present
username	<input checked="" type="checkbox"/>	username that was configured in step 2c	- present
password	<input checked="" type="checkbox"/>	password that was configured in step 2c	
useShortTermCredentials	<input type="checkbox"/>	false	- present
sharedSecret	<input type="checkbox"/>		
type	<input checked="" type="checkbox"/>	expressway	- present
numRegistrations	<input type="checkbox"/>	0	- present
tcpPortNumberOverride	<input checked="" type="checkbox"/>	3478	- present
callBridge	<input type="checkbox"/>		Choose
callBridgeGroup	<input type="checkbox"/>		Choose

Modify

验证

使用本部分可确认配置能否正常运行。

步骤 1: 在 Expressway C 上，检查 WB 是否已正确集成

a. 导航到配置 > 统一通信 > 思科会议服务器。您必须看到 WB 的 IP 地址：

Status **System** Configuration Applications Users Maintenance

Cisco Meeting Server You are here: >

Meeting Server configuration

Meeting Server Web Proxy Enable ⓘ

Guest account client URI * ⓘ


Save

Guest account client URI resolved to the following targets

Name	Address
webbridge.alero.aca	10.48.36.5

b. 导航到配置>统一通信> HTTP允许列表>自动添加规则。检查是否已将此项添加到规则：

Meeting Server web bridges	https	443	Prefix	/	GET, POST, PUT, HEAD, DELETE
Meeting Server web bridges	wss	443	Prefix	/	GET, POST, PUT, HEAD, DELETE

 注：在发现的节点中不会找到WB，因为规则仅允许将HTTPS流量代理到WB，而不一定用于统一通信。

c. 检查WB FQDN的安全外壳(SSH)隧道是否已在Expressway-C上构建到Expressway-E，并且处于活动状态。导航到状态>统一通信>统一通信SSH隧道状态。您必须看到WB的FQDN，并且目标必须为Expressway-E。

Status System Configuration Applications Users Maintenance

Unified Communications SSH tunnels status You are here: Status > Unified Communications > Unifi

Target	Domain	Status	Peer
vcs-e.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e.alero.local	alero.lab	Active	10.48.36.247
vcs-e.alero.local	alero.local	Active	10.48.36.247
vcs-e2.alero.local	alero.lab	Active	10.48.36.247
vcs-e2.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e2.alero.local	alero.local	Active	10.48.36.247

第二步：验证TURN服务器已添加到CMS服务器

在CMS API菜单中，查找轮换服务器，然后点击每个服务器。在每个对象中，都有一个链接用于检查状态：

Related objects: [/api/v1/turnServers](#)
[/api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff/status](#)

Table view XML view

Object configuration	
serverAddress	10.0.0.36
clientAddress	175.12.5.1
numRegistrations	0
username	cmsturn
useShortTermCredentials	false
type	expressway
tcpPortNumberOverride	3478

输出显示 TURN 服务器的相关信息，包括往返时间 (RTT) (以毫秒 Ms 计)。此信息对于最适合使用的 TURN 服务器的 CB 选择十分重要。

第三步：验证正在进行的呼叫期间的TURN中继使用情况

使用WebRTC客户端进行实时呼叫时，您可以查看Expressway上的TURN媒体中继状态。导航到 Status > TURN relay usage，然后选择view。

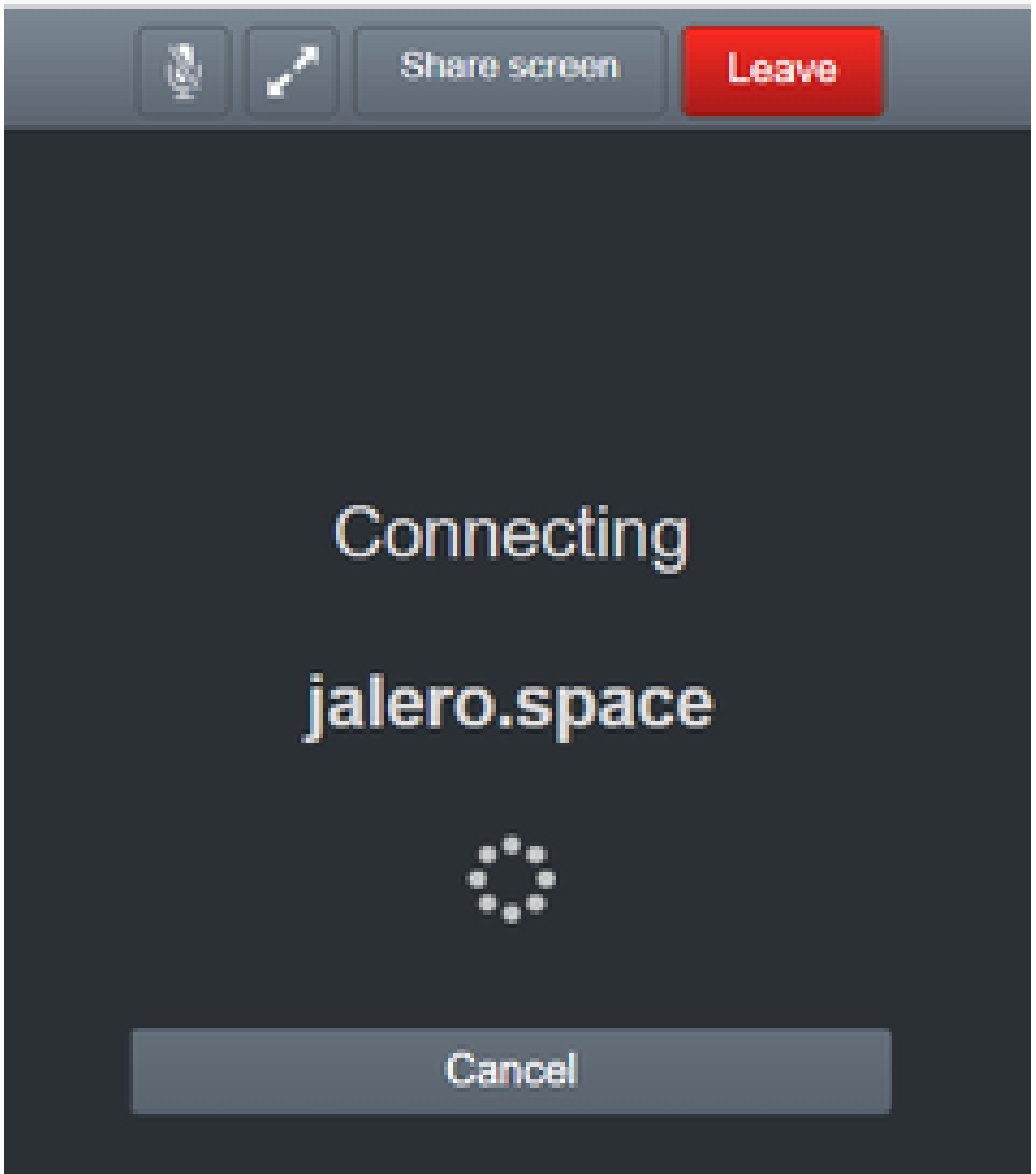
故障排除

有用的工具：

- 来自浏览器的HAR文件([如何在Chrome或Firefox中生成HAR文件](#))
- WebRTC内部转储从浏览器 — chrome://webrtc-internals或edge://webrtc-internals — 在尝试加入时立即创建转储。
- 浏览器控制台日志也非常有用。
- 从客户端、Exp E、Exp C和CMS捕获Wireshark。
- Exp E network.http.trafficserver调试有助于进行websocket故障排除。

外部 WebRTC 客户端已连接，但无介质 (由于 ICE 失败)

在此场景中，RTC客户端能够将呼叫ID解析为jalero.space，但当您输入您的姓名并选择加入呼叫时，客户端将显示Connecting，如下图所示：



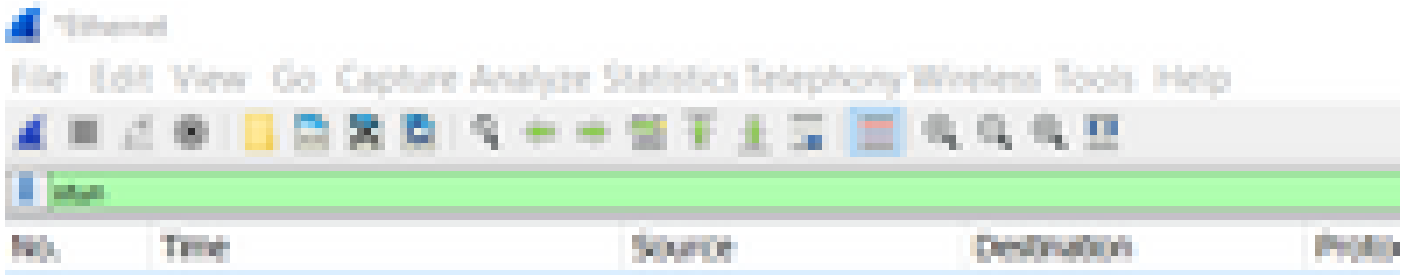
约 30 秒后，会重定向至初始 WB 页面。

要排除故障，请完成以下步骤：

- 当您尝试进行呼叫时，请在 RTC 客户端上启动 Wireshark，当出现故障时，请停止捕捉。
- 出现问题后，检查 CMS 事件日志：

在 CMS WebAdmin 上导航到 Logs > Event logs。

- 使用stun过滤Wireshark跟踪。请参阅以下示例：



在Wireshark跟踪中，您会看到客户端向端口3478上的Expressway-E TURN服务器发送配置了凭证的Allocate Request:

```
1329    2017-04-15 10:26:42.108282    10.55.157.229    10.48.36.248    STUN    186
    Allocate Request UDP user: expturncreds realm: TANDBERG with nonce
```

服务器回应分配错误：

```
1363    2017-04-15 10:26:42.214119    10.48.36.248    10.55.157.229    STUN    254
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 431
    (*Unknown error code*) Integrity Check Failure
```

或

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401
    (Unauthorized) Unauthorized
```

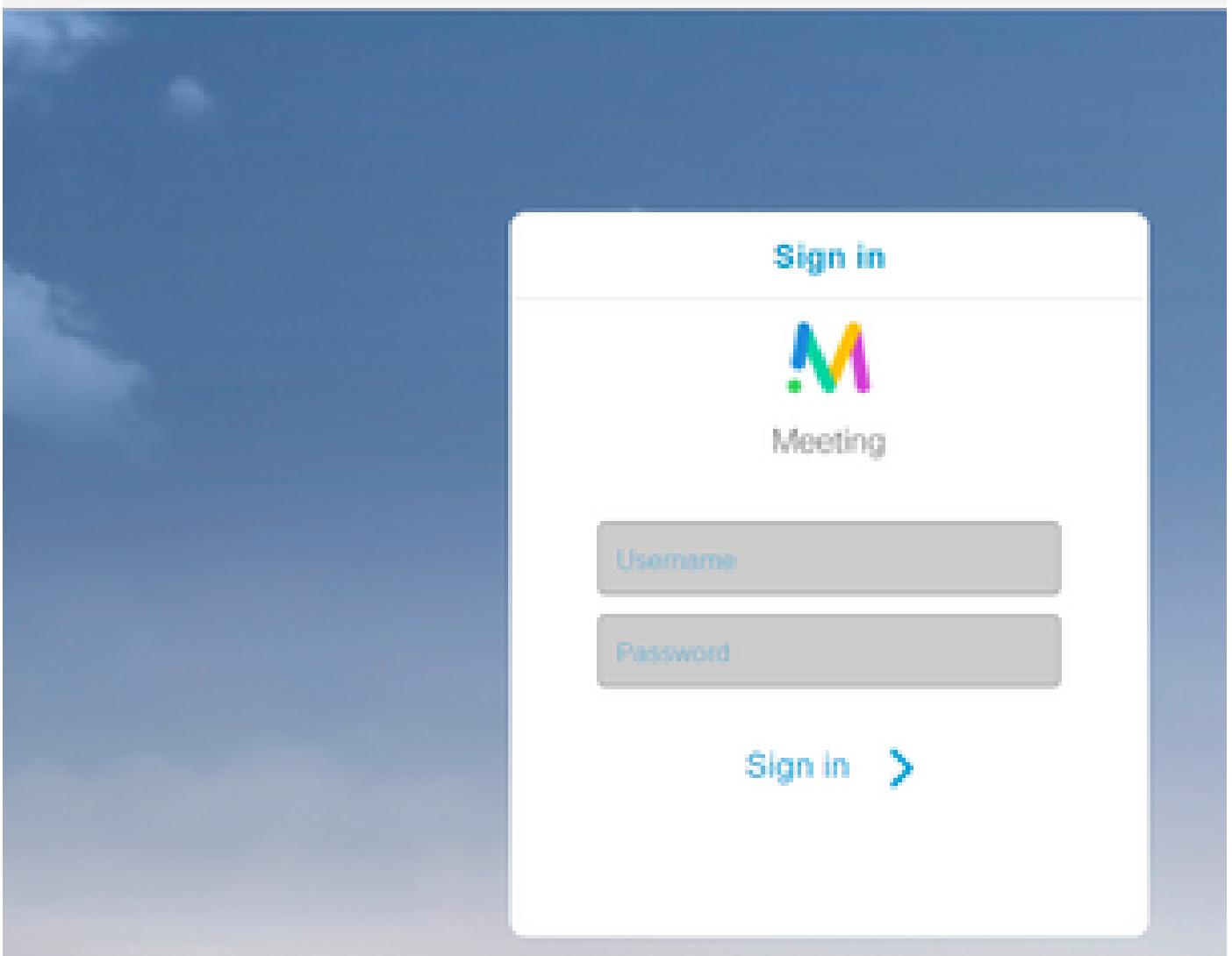
在CMS日志中，显示此日志消息：

```
2017-04-15    10:34:56.536    Warning    call 7: ICE failure 4 (unauthorized - check credentials)
```

解决方案：

检查CMS上配置的TURN凭证，并确保其与Expressway-E本地身份验证数据库上配置的凭证匹配。

外部 WebRTC 客户端上没有“加入呼叫”选项



这会显示在 Callbridge 状态 > 一般页面中：

```
2017-04-15 12:09:06.647 Web bridge connection to "webbridge.alero.aca" failed (DNS failure)
2017-04-15 12:10:11.634 Warning web bridge link 2: name resolution for "webbridge.alero.aca" f
2017-04-15 11:55:50.835 Info failed to establish connection to web bridge link 2 (unknown erro
```

解决方案：

- 确保Callbridge可以将Join URL解析为Webbridge FQDN (Callbridge不能将此解析为 Expressway-E的IP地址)。
- 使用命令dns flush，通过命令行界面(CLI)刷新Callbridge上的DNS缓存。
- 确保WB信任Callbridge服务器证书 (而不是颁发者)。

在连接到 cospace 时，外部 WebRTC 客户端 (在加载介质过程中) 卡住了，随后被重定向到 WB 初始页面

解决方案：

- 确保CMS可以为CB域解析内部网络上的_xmpp-client SRV记录，并确保WebRTC连接可以在内部工作。
- 尝试连接外部客户端时，收集客户端上的Wireshark捕获和诊断日志记录（包括Expressway-E上的tcpdump）：

导航到维护>诊断>诊断日志记录，确保在选择开始新日志之前，已选中Take tcpdump while logging（如本图所示）：



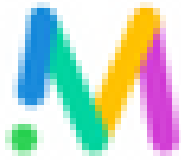
注意：在重现失败的呼叫之前，请确保客户端设备上的Wireshark捕获和Expressway-E上的日志记录已启动。在重现失败的呼叫后，停止 Expressway E 上的日志记录和客户端上的捕获，并下载日志记录和捕获的数据。

- 解压缩/解压缩从Expressway-E下载的日志捆绑包，并打开在面向公共的接口上获取的.pcap文件。
- 使用stun过滤两个数据包捕获：
 - 然后查找从外部客户端到Expressway E公有IP地址的绑定请求，右键单击并选择Follow > UDP Stream。
 - 通常，来自客户端的绑定请求的目标端口在24000-29999范围内，即Expressway-E上的TURN中继端口范围。
- 如果客户端未收到对绑定请求的响应，请检查请求是否到达Expressway E的捕获。
- 如果请求已到达且 Expressway E 回复了客户端，请检查外部 FW 是否允许出站 UDP 流量。
- 如果请求未到达，请检查防火墙，确保之前列出的端口范围未被阻止。
- 如果Expressway-E部署了启用静态NAT模式的双网络接口控制器(DUAL-NIC)，并且为X12.5.2或更低版本，请确保您的外部FW上支持并配置了NAT反射。从X12.5.3开始，独立Expressway不再需要此功能。

外部 WebRTC 客户端无法加入 cospace 并收到警告（无法连接，请稍候重试）

在这种情况下，RTC客户端能够将呼叫ID解析为jalero.space，但当您输入您的姓名并选择加入呼叫时，会立即显示警告无法连接 — 稍后重试：

jalero.space



Meeting

Unable to connect - try again later

External RTC client

Join call



Or sign in and join

解决方案：

检查 CMS 是否能够始终在内部网络上解析 CB 域的 _xmpp-client SRV 记录。

相关信息

- [VCS/Expressway IP 端口使用指南](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。