

配置使用Expressway的CMS WebRTC或Web應用代理

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[配置步驟](#)

[步驟 1.將CMS WB整合到Expressway-C](#)

[步驟 2.啟用TURN on the Expressway-E and Add the Authentication Credential to the Local Authentication Database](#)

[步驟 3.更改Expressway-E的管理埠](#)

[步驟 4.將Expressway-E新增為TURN伺服器，用於在CMS伺服器上進行媒體NAT穿越](#)

[驗證](#)

[步驟 1.在Expressway-C上，檢查WB是否正確整合](#)

[步驟 2.驗證是否已將TURN伺服器新增到CMS伺服器](#)

[步驟 3.驗證正在進行的呼叫期間的TURN中繼使用情況](#)

[疑難排解](#)

[外部WebRTC客戶端連線，但沒有介質（由於ICE故障）](#)

[外部WebRTC客戶端未獲取加入呼叫選項](#)

[在連線到Cospace時，外部WebRTC客戶端停滯（在載入媒體上），然後重定向到WB初始頁面](#)

[外部WebRTC客戶端無法加入Cospace並收到警告（無法連線—請稍後重試）](#)

[相關資訊](#)

簡介

本文檔介紹通過Expressway配置Cisco Meeting Server(CMS)WebRTC和對其進行故障排除的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Expressway X12.6.1及更高版本（x12.6.1及更高版本只能與CMS 2.9.2或更高版本配合使用，這是因為Exp TURN行為發生了變化）
- CMS伺服器2.9.3及更高版本


- 網路位址轉譯(NAT)
- 使用NAT中繼(TURN)遍歷
- 適用於NAT的作業階段穿越公用程式(STUN)
- 網域名稱系統(DNS)

配置先決條件：

- 必須在Expressway上啟用和配置與移動和遠端訪問(MRA)相關的基本設定 (UC遍歷區域、SSH隧道)，請單[擊此處](#)獲取MRA指南。
- 對於CMS 2.9.x - WebBridge(WB)、在CMS上配置並啟用的XMPP和CallBridge，請參閱[配置指南](#)
- TURN選項鍵安裝在Expressway-E上。
- 從公共Internet到Expressway E的公共IP地址在防火牆上開啟的TCP埠443。
- 從公共Internet到Expressway E的公共IP地址在防火牆上開啟的TCP和UDP埠3478 (TURN請求)。
 - 僅當CMS API中的「turnservers」將tcpPortNumberOverride設定為3478時，才需要TCP 3478。
- 在防火牆上開啟的UDP埠3478 (TURN請求) 從CMS連線到Expressway-E的專用IP地址 (如果在Expressway-E上使用雙NIC)。
 - CMS 2.9.2及更低版本向Exp E傳送繫結請求，而2.9.3之後傳送分配請求
- Webbridge的加入URL的外部DNS記錄，可解析為Expressway-E的面向公眾的IP地址。
- 可解析為Webbridge伺服器的IP地址的加入URL的內部DNS記錄。
- 如果運行X12.5.2或更低版本，請確保外部防火牆上允許Expressway-E的公共IP地址進行NAT反射，[按一下此處](#)進行配置示例。從X12.5.3開始，獨立Expressway不再需要此功能。
- 將埠443用於TURN時，仍需要為外部防火牆上的媒體開啟UDP埠3478。

 注意：啟用TCP埠443後，Expressway將無法在TCP埠3478上做出響應。

 註：用於Jabber Guest服務的Expressway對不能用於CMS WebRTC代理服務。

 註：如果從先前版本升級到3.0或更高版本，請參閱[從Cisco Meeting Server 2.9順利升級到3.0 \(及以後 \) 的指南](#)

採用元件

本檔案所述內容不限於特定軟體和硬體版本，但必須滿足最低軟體版本要求。

- CMS應用程式介面(API)
- Expressway
- CMS伺服器

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

已將WebRTC代理支援從X8.9.2版新增到Expressway，使外部使用者能夠瀏覽到Cisco Meeting Server Web Bridge。

外部客戶端和訪客無需受支援的瀏覽器之外的任何軟體即可管理或加入空間。[按一下此處](#)檢視支援的瀏覽器清單。

截至2021年2月5日，以下是CMS 3.1.1支援的瀏覽器：

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

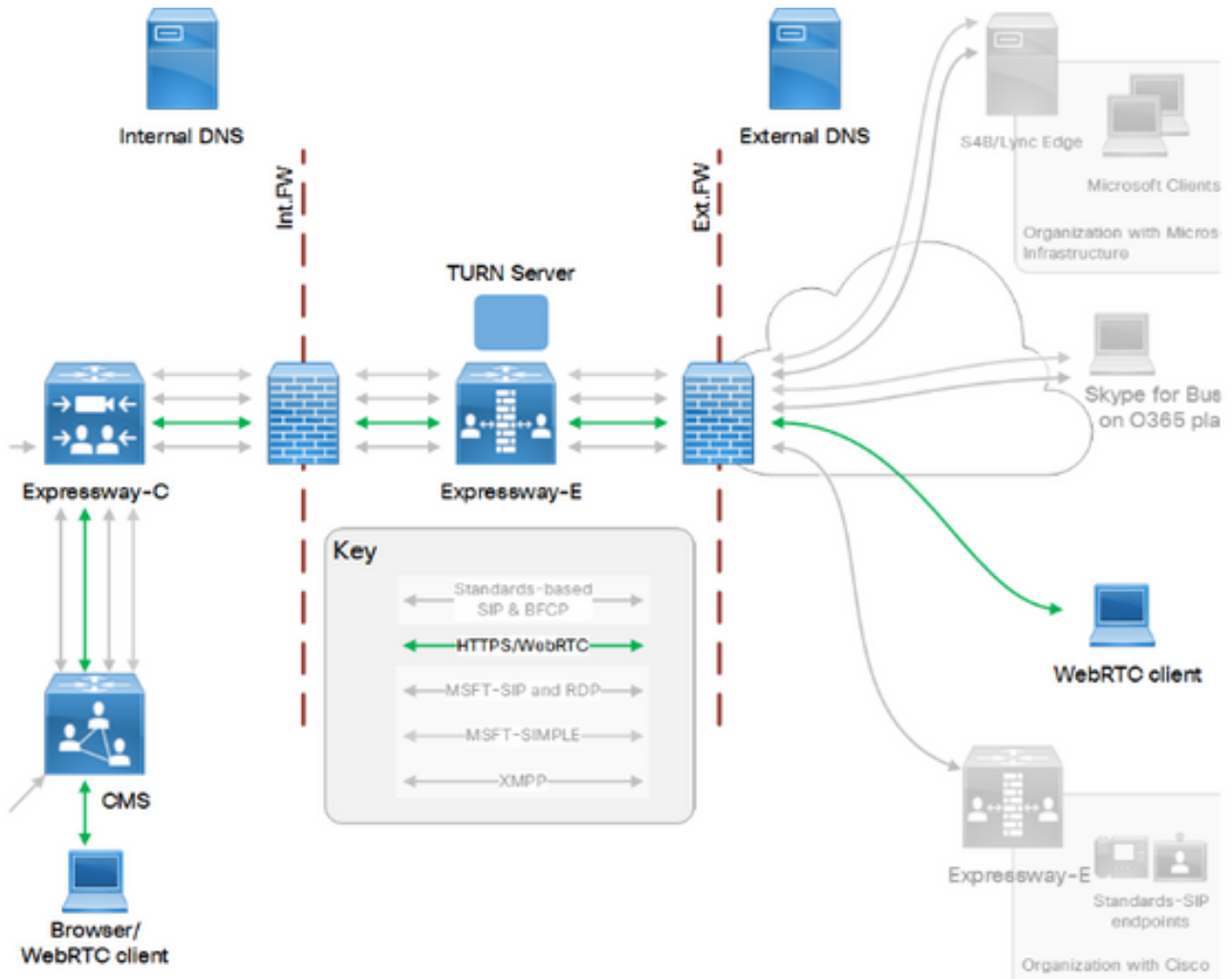
Browsers	Versions
Google Chrome (Windows, macOS and Android)	85
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	88
Apple Safari for macOS	13.0 and 14.0
Apple Safari for iOS	iOS versions: 13.0 and 14.0
Yandex (Windows)	20.8 and 20.11

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.

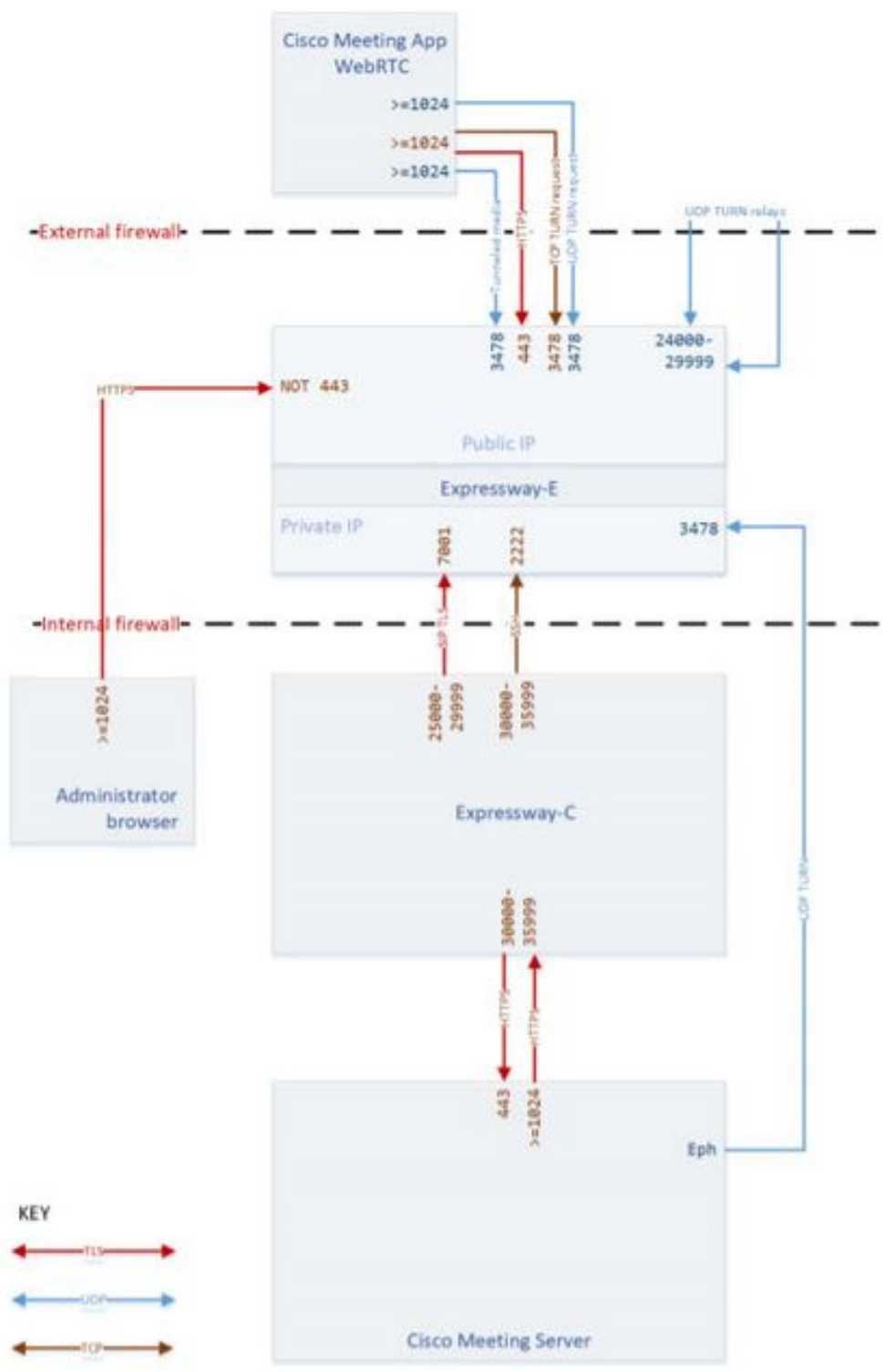
設定

網路圖表



此圖提供用於CMS WebRTC的Web代理的連線流示例：(來自Exp IP埠使用配置指南)。

Web Proxy for Cisco Meeting Server Connections



註：運行X12.5.2或更低版本時，必須配置外部防火牆，以允許Expressway-E和公共IP地址進行NAT反射（防火牆通常不信任具有相同源和目標IP地址的資料包）。從X12.5.3開始，獨立Expressway不再需要此功能。

配置步驟

步驟 1.將CMS WB整合到Expressway-C

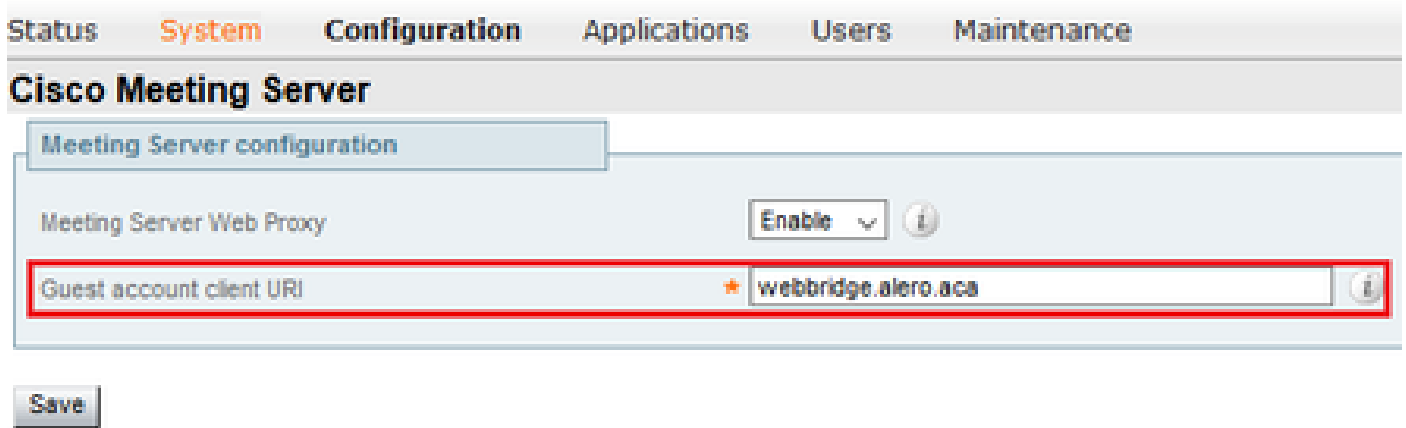
a.導航至Configuration > Unified Communication > Cisco Meeting Server。

b.啟用會議伺服器Web代理。

c.在Guest account client URI欄位中輸入加入URL。

d.按一下Save。

e.將CMS加入URL作為主體替代名稱(SAN)新增到Expressway-E伺服器證書中。請參閱[Cisco VCS證書建立和使用部署指南](#)。




The screenshot shows the 'Cisco Meeting Server' configuration page. The 'Meeting Server configuration' section is active. The 'Meeting Server Web Proxy' is set to 'Enable'. The 'Guest account client URI' field is highlighted with a red box and contains the value 'webbridge.alero.aca'. A 'Save' button is visible at the bottom left.


步驟 2.啟用TURN on the Expressway-E and Add the Authentication Credential to the Local Authentication Database

a.導航到Configuration > Traversal > TURN。

b.啟用TURN services，從off到on。

c.選擇Configure TURN client credentials on local database並新增憑據（使用者名稱和密碼）。

 註：如果您有一個Expressway-Es群集，並且它們都用作TURN伺服器，請確保在所有節點上啟用該群集。必須通過API配置兩個單獨的turnServer例項，並將它們指向群集中的每個Expressway-E伺服器（根據步驟4中所示的配置過程，該過程顯示一個Expressway-E伺服器的進程；第二個turnServer的配置類似，僅使用另一個Expressway-E伺服器各自的IP地址和車削憑證）。

 注意：TCP/HTTPS流量可以在高速公路前使用網路負載均衡器，但TURN媒體仍必須從客戶端轉到伺服器公共IP。TURN媒體不能通過網路負載均衡器


步驟 3.更改Expressway-E的管理埠

此步驟是必需的，因為webrtc連線在TCP 443上進入，但是Exp 12.7引入了可用於443的新專用管理介面(DMI)。

a.定位至系統>管理。

b.在Web伺服器組態下，從下拉選項將Web管理員連線埠變更為445，然後按一下Save。

c.在用於WebRTC代理服務的所有Expressway-Es上重複步驟3a到3b。

 注意：思科建議更改管理埠，因為WebRTC客戶端使用443。如果WebRTC瀏覽器嘗試訪問埠80,Expressway-E會將連線重定向到443。

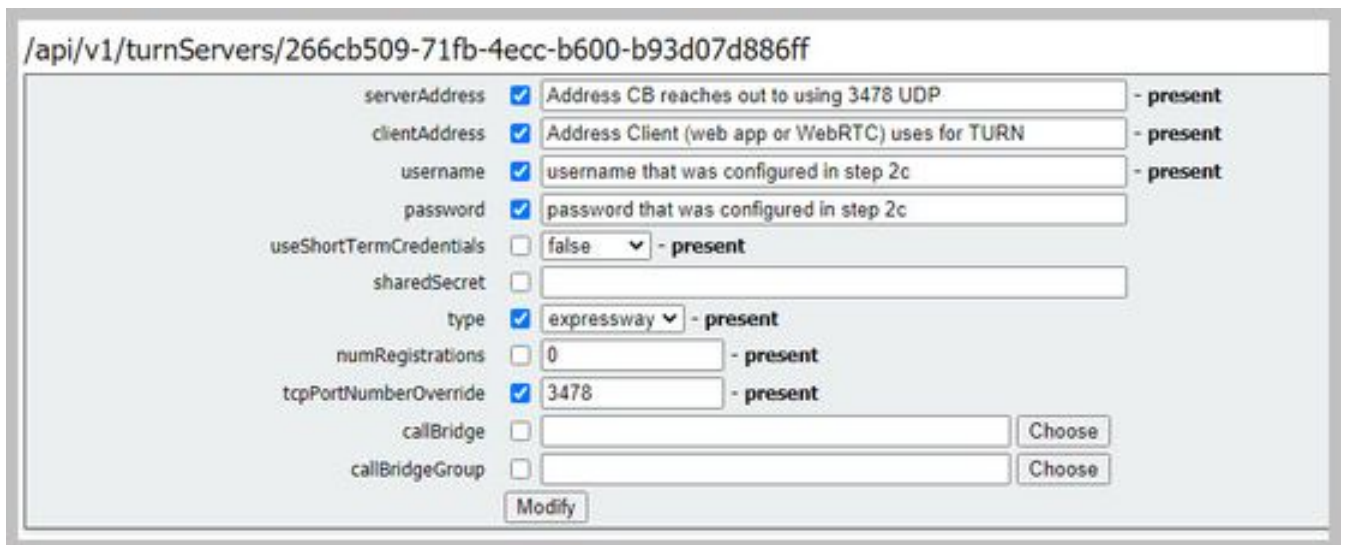
步驟 4.將Expressway-E新增為TURN伺服器，用於在CMS伺服器上進行媒體NAT穿越

在CMS 2.9.x中，使用Configuration —> API選單新增翻轉伺服器：

- serverAddress：(Expressway的專用IP地址)
- clientAddress：(Expressway的公共IP地址)
- 型別：(expressway)
- 使用者名稱：(如步驟2c中所配置)
- 密碼：(如步驟2c中所配置)
- tcpPortNumberOverride:3478

d.對要用於TURN的每個Expressway-E伺服器重複步驟4c

此圖提供設定步驟的範例：



驗證

使用本節內容，確認您的組態是否正常運作。

步驟 1.在Expressway-C上，檢查WB是否正確整合

a.導航至Configuration > Unified Communication > Cisco Meeting Server。您必須看到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 *

Guest account client URI resolved to the following targets	
Name	Address
webbridge.alero.aca	10.48.36.5

b. 導航到 Configuration > Unified Communication > HTTP allow list > Automatically added rules。檢查是否已將以下內容新增到規則：

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

 註：在發現的節點中不會找到WB，因為規則僅允許代理到WB的HTTPS流量，而不一定用於統一通訊。

c. 檢查WB FQDN的安全外殼(SSH)隧道是否已在Expressway-C上構建到Expressway-E，並且是否處於活動狀態。導航至 Status > Unified Communications > Unified Communications SSH tunnels status。您必須看到WB的FQDN，並且目標必須為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

步驟 2. 驗證是否已將TURN伺服器新增到CMS伺服器

在CMS API選單中，查詢輪換伺服器，然後按一下每個伺服器。在每個對象中，都有一個連結用於檢查狀態：

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

輸出會顯示包含與TURN伺服器相關的來回時間(RTT)(以毫秒(Ms)為單位)的資訊。此資訊對選擇要使用的最佳TURN伺服器的CB選擇非常重要。

步驟 3. 驗證正在進行的呼叫期間的TURN中繼使用情況

使用WebRTC客戶端進行即時呼叫時，您可以在Expressway上檢視TURN媒體中繼狀態。導覽至 Status > TURN relay usage，然後選擇view。

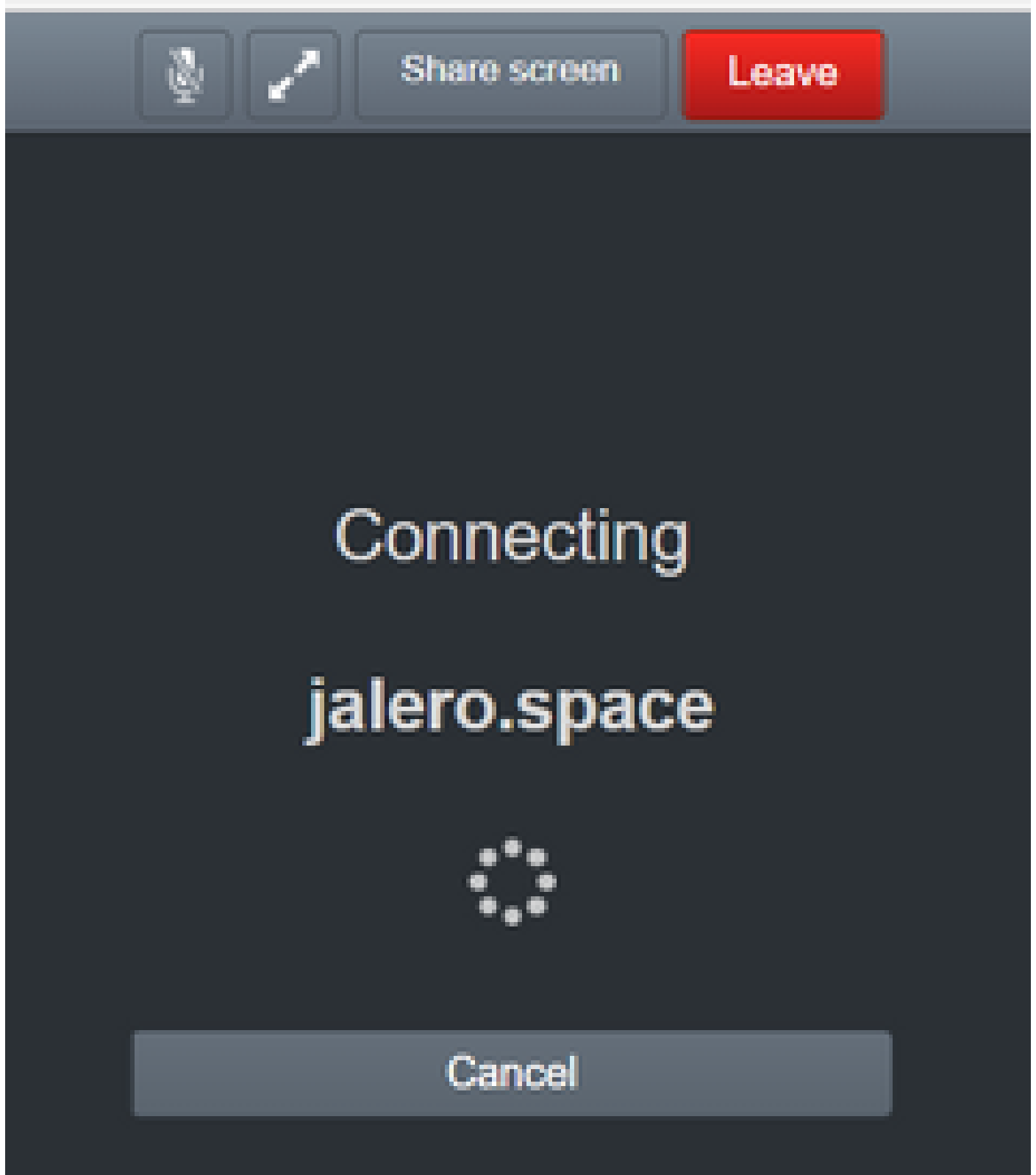
疑難排解

有用的工具：

- 來自瀏覽器的HAR文件([如何在Chrome或Firefox中生成HAR檔案](#))
- WebRTC internals dump from browser - chrome://webrtc-internals或edge://webrtc-internals — 嘗試加入後立即建立轉儲。
- 瀏覽器控制檯日誌也很有用。
- 從客戶端、Exp E、Exp C和CMS捕獲Wireshark。
- Exp E network.http.trafficserver debugs幫助進行websocket故障排除。

外部WebRTC客戶端連線，但沒有介質（由於ICE故障）

在此場景中，RTC客戶端能夠將呼叫ID解析為jalero.space，但當您輸入您的姓名並選擇加入呼叫時，客戶端將顯示Connecting，如下圖所示：



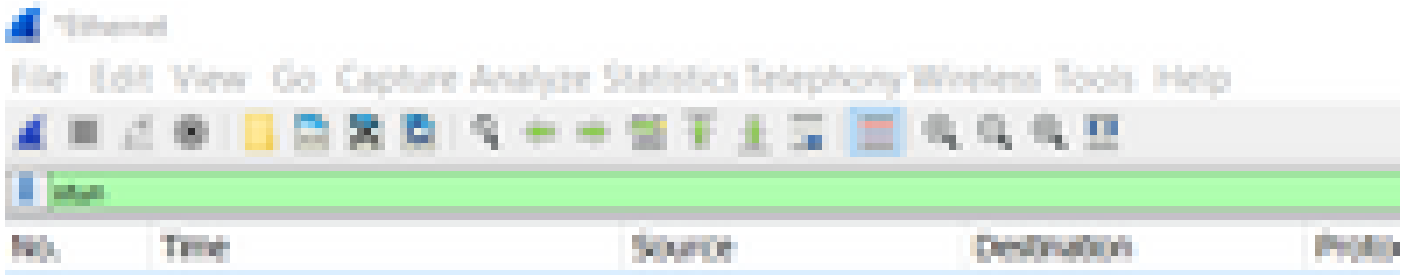
約30秒後，系統會將它重新導向至初始WEB頁面。

若要疑難排解，請完成以下步驟：

- 嘗試呼叫時在RTC客戶端上啟動wireshark，失敗時停止捕獲。
- 發生問題後，檢查CMS事件日誌：

在CMS WebAdmin上導航到Logs > Event logs。

- 使用stun過濾Wireshark跟蹤。請參閱以下範例：



在Wireshark跟蹤中，您看到客戶端向埠3478上的Expressway-E TURN伺服器傳送帶有已配置憑據的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
```

伺服器以Allocate Error回覆：

```
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
```

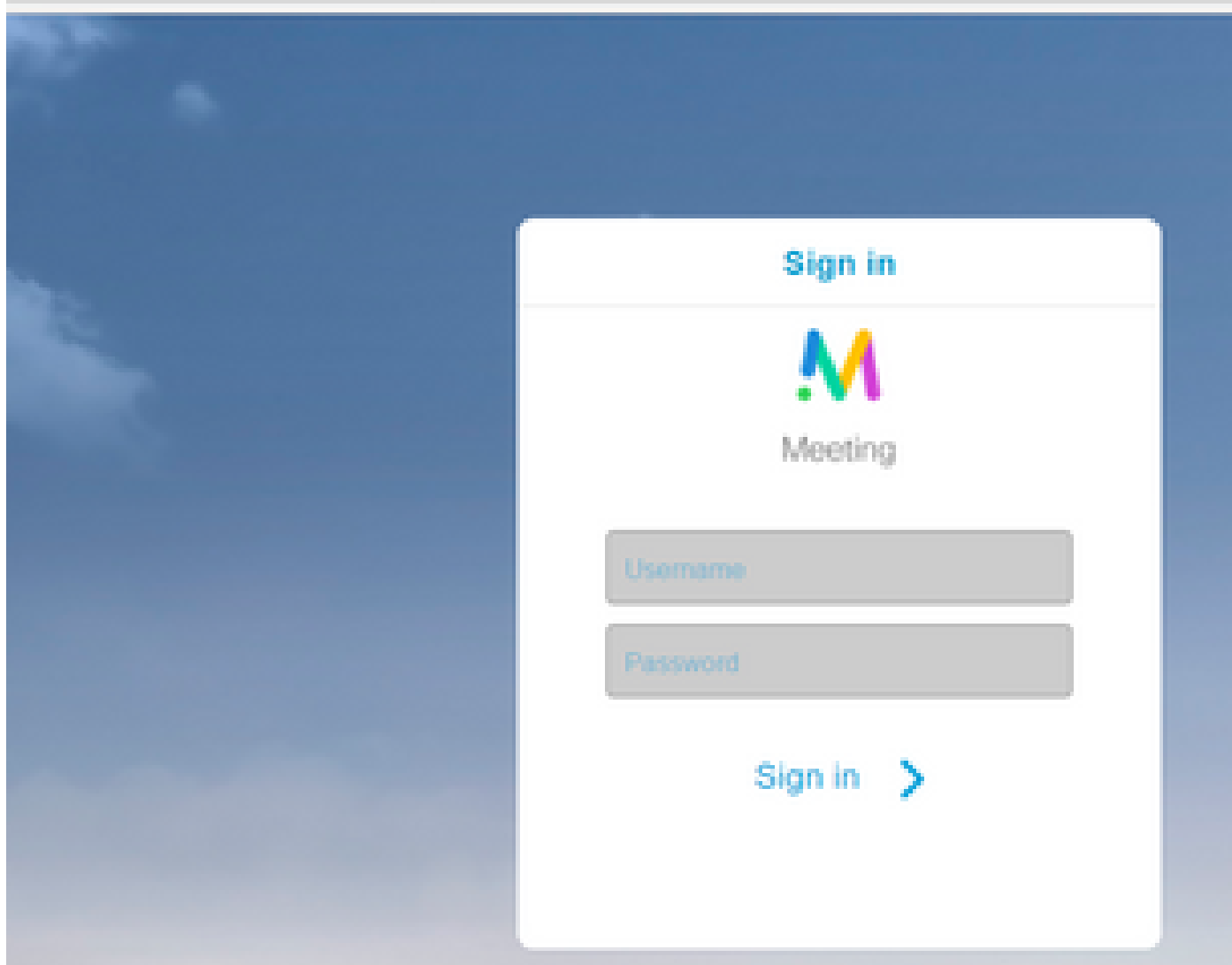
在CMS日誌中，將顯示以下日誌消息：

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

解決方案：

檢查CMS上配置的TURN憑證，並確保其與Expressway-E本地身份驗證資料庫上配置的憑證相匹配。

外部WebRTC客戶端未獲取加入呼叫選項



在Callbridge Status > General頁上，將顯示以下內容：

```
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
```

解決方案：

- 確保Callbridge可以將加入URL解析為Webbridge FQDN (Callbridge不能將此解析為 Expressway-E的IP地址)。
- 使用命令`dns flush`，通過命令列介面(CLI)刷新Callbridge上的DNS快取。
- 確保WB信任Callbridge伺服器證書 (而不是頒發者)。


在連線到Cospace時，外部WebRTC客戶端停滯 (在載入媒體上)，然後重定向到WB初始頁面

解決方案：

- 確保CMS可以解析CB域的內部網路上的_xmpp-client SRV記錄，並確保WebRTC連線可在內部工作。
- 嘗試與外部客戶端連線時，收集客戶端上的Wireshark捕獲和診斷日誌記錄（包括Expressway-E上的tcpdump）：

導覽至Maintenance > Diagnostics > Diagnostic logging，確保在選擇Start new log之前已選中Take tcpdump while logging，如下圖所示：



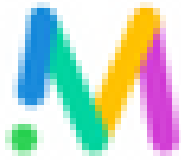
 注意：在重現失敗的呼叫之前，確保客戶端裝置上的Wireshark捕獲和Expressway-E上的日誌記錄已啟動。當出現故障呼叫時，停止並下載Expressway-E上的日誌記錄以及客戶端上的捕獲。

- 解壓縮/解壓縮從Expressway-E下載的日誌捆綁包，並開啟面向公共的介面上獲取的.pcap檔案。
- 使用stun過濾兩個封包擷取：
 - 然後查詢從外部客戶端到Expressway-E公共IP地址的繫結請求，按一下右鍵並選擇Follow > UDP Stream。
 - 通常，來自客戶端的繫結請求的目的埠在24000-29999範圍內，即Expressway-E上的TURN中繼埠範圍。
- 如果客戶端未收到對繫結請求的響應，請檢查請求是否到達Expressway E的捕獲。
- 如果請求到達，並且Expressway-E正在回覆客戶端，請檢查外部FW是否允許出站UDP流量。
- 如果請求沒有到達，請檢查防火牆以確保之前列出的埠範圍沒有被阻止。
- 如果Expressway-E部署了啟用靜態NAT模式的雙網路介面控制器(DUAL-NIC)，並且部署了X12.5.2或更低版本，請確保外部防火牆上支援並配置了NAT反射。從X12.5.3開始，獨立Expressway不再需要此功能。

外部WebRTC客戶端無法加入Cospace並收到警告（無法連線 — 請稍後重試）

在此情況中，RTC客戶端能夠將呼叫ID解析為jalero.space，但當您輸入您的姓名並選擇加入呼叫時，會立即顯示警告Unable to connect - try later:

jalero.space



Meeting

Unable to connect - try again later

External RTC client

Join call



Or sign in and join

解決方案：

檢查內部網路上的CMS是否始終能夠解析CB域的_xmpp-client SRV記錄。

相關資訊

- [VCS/Expressway IP埠使用指南](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。