

Configurer CMS WebRTC ou le proxy Web App sur Expressway

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration Steps](#)

[Étape 1. Intégration de CMS WB à Expressway-C](#)

[Étape 2. Activez TURN sur l'Expressway-E et ajoutez les informations d'authentification à la base de données d'authentification locale](#)

[Étape 3. Modifier le port d'administration de l'Expressway-E](#)

[Étape 4. Ajoutez l'Expressway-E en tant que serveur\(s\) TURN pour la traversée NAT média sur le serveur CMS](#)

[Vérifier](#)

[Étape 1. Dans Expressway-C, vérifiez que le WB est correctement intégré](#)

[Étape 2. Vérifiez que le serveur TURN a été ajouté au serveur CMS](#)

[Étape 3. Vérifier l'utilisation du relais TURN pendant l'appel en cours](#)

[Dépannage](#)

[Le client WebRTC externe se connecte, mais sans support \(en raison de l'échec ICE\)](#)

[Le client WebRTC externe n'a pas accès à l'option pour participer à l'appel \(Join Call\).](#)

[Le client WebRTC externe est resté bloqué \(en chargement des médias\) lors de la connexion à l'espace partagé. Il est ensuite redirigé vers la page initiale WB.](#)

[Il est impossible pour le client WebRTC de se joindre à l'espace partagé et il reçoit un avertissement lui indiquant que la connexion est impossible et qu'il devra réessayer plus tard \(Unable to connect - try again later\).](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour configurer, vérifier et dépanner WebRTC du serveur de réunion Cisco (CMS) par l'intermédiaire d'Expressway.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :


- Expressway X12.6.1 et versions ultérieures (x12.6.1 et versions ultérieures ne peuvent


fonctionner qu'avec CMS 2.9.2 ou versions ultérieures en raison de changements dans le comportement d'Exp TURN)


- Serveur CMS 2.9.3 et versions ultérieures
- Traduction d'adresses réseau (NAT)
- Traversée à l'aide de relais (TURN) autour de la NAT
- Utilitaires de traversée de session (STUN) pour NAT
- Système de noms de domaine (DNS)

Prérequis pour la configuration :

- Les paramètres de base relatifs à l'accès mobile et distant (MRA) (zone de traversée UC, tunnels SSH) doivent déjà être activés et configurés sur l'Expressway, [cliquez ici](#) pour les guides MRA.
- Pour CMS 2.9.x - WebBridge (WB), XMPP et CallBridge configurés et activés sur CMS, consultez le [guide de configuration](#)
- La touche d'option du protocole TURN est installée sur l'Expressway-E.
- Le Port 443 TCP est ouvert sur le pare-feu de l'Internet public à l'adresse IP publique de l'Expressway-E.
- Le Port 3478 TCP et UDP (requêtes du protocole TURN) est ouvert sur le pare-feu de l'Internet public à l'adresse IP publique de l'Expressway-E.
 - TCP 3478 n'est nécessaire que si « turn servers » dans l'API CMS a tcpPortNumberOverride défini sur 3478.
- Port UDP 3478 (requêtes TURN) ouvert sur le pare-feu à partir de CMS vers l'adresse IP privée de l'Expressway-E (si vous utilisez la carte réseau double sur l'Expressway-E).
 - CMS 2.9.2 et versions antérieures envoie des requêtes de liaison à l'Exp E, tandis que 2.9.3 et versions ultérieures envoie des requêtes d'allocation
- Enregistrements DNS externes pour l'URL de jonction de webbridge, pouvant être résolus en adresse IP publique de l'Expressway-E.
- Enregistrement DNS interne pour l'URL de jointure pouvant être résolu en adresse IP du serveur de pont Web.
- Si vous exécutez X12.5.2 ou une version antérieure, assurez-vous que la réflexion NAT est autorisée sur le pare-feu externe pour l'adresse IP publique d'Expressway-E, [cliquez ici](#) pour un exemple de configuration. À partir de X12.5.3, ce n'est plus nécessaire pour un Expressway autonome.
- Lorsque vous utilisez le port 443 pour TURN, vous devez toujours ouvrir le port UDP 3478 pour les supports sur le pare-feu externe.

 Attention : lorsque le port TCP 443 est activé, l'Expressway ne peut plus répondre sur le port TCP 3478.

 Remarque : la paire Expressway utilisée pour les services Jabber Guest ne peut pas être utilisée pour les services proxy WebRTC de CMS.

 Remarque : si vous effectuez une mise à niveau vers la version 3.0 ou ultérieure à partir de versions précédentes, reportez-vous au [Guide de mise à niveau en douceur de Cisco](#)

Composants utilisés

Ce document n'est pas limité à des versions logicielles et matérielles spécifiques, mais les exigences minimales en matière de version logicielle doivent être satisfaites.

- interface de programmation d'application (API) de CMS
- Expressway
- Serveur CMS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La prise en charge du proxy WebRTC a été ajoutée à Expressway à partir de la version X8.9.2, ce qui permet aux utilisateurs hors site de naviguer vers un pont Web Cisco Meeting Server.

Les clients externes et les invités peuvent gérer des espaces ou s'y joindre sans avoir besoin d'autre logiciel, à part un navigateur pris en charge. [Cliquez ici pour obtenir la liste des navigateurs pris en charge.](#)

À partir du 5 février 2021, voici les navigateurs pris en charge pour CMS 3.1.1 :

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

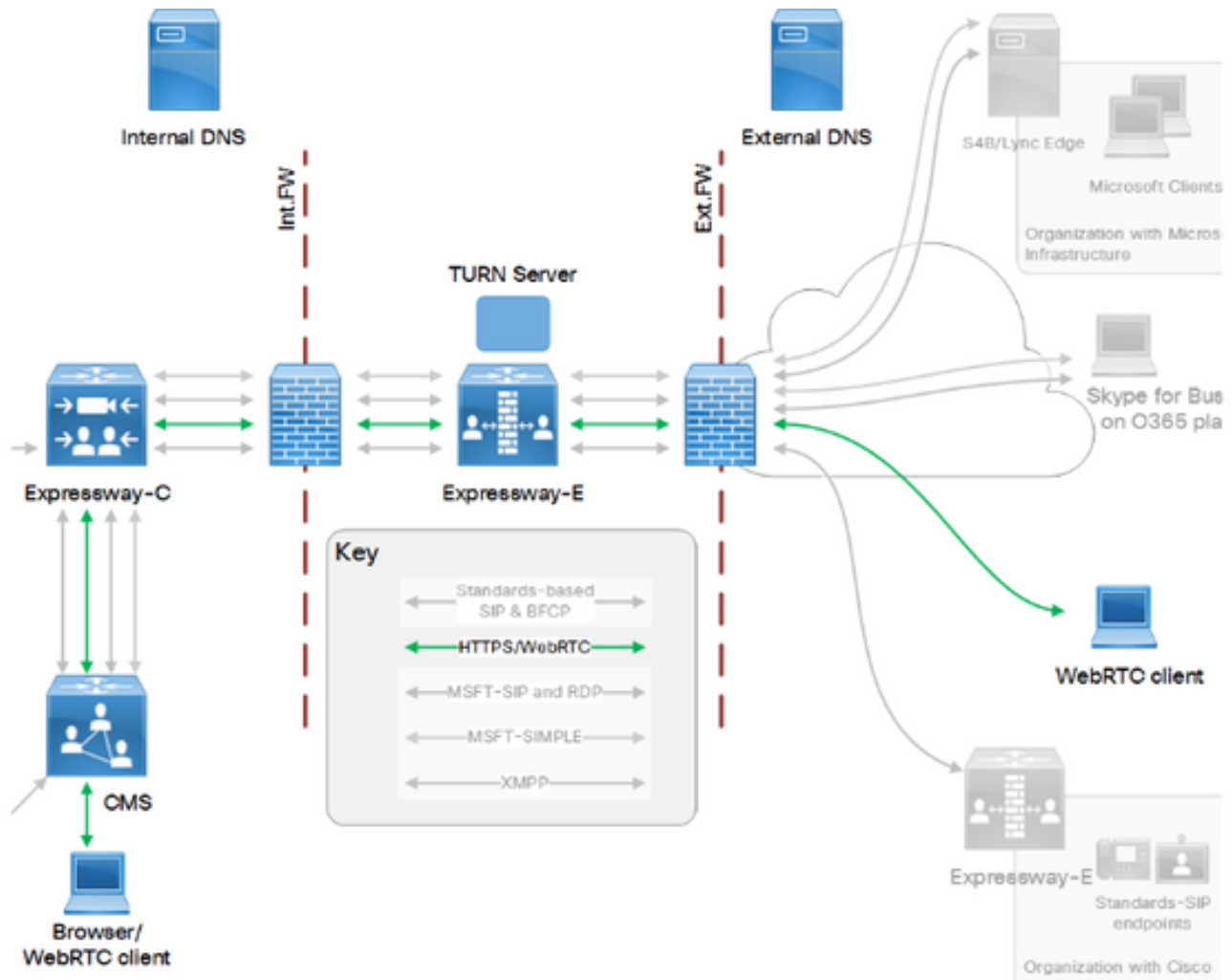
Browsers	Versions
Google Chrome (Windows, macOS and Android)	86
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	86
Apple Safari for macOS	13.x and 14.0
Apple Safari for iOS	iOS versions: 13.x and 14.0
Yandex (Windows)	20.8 and 20.11

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.

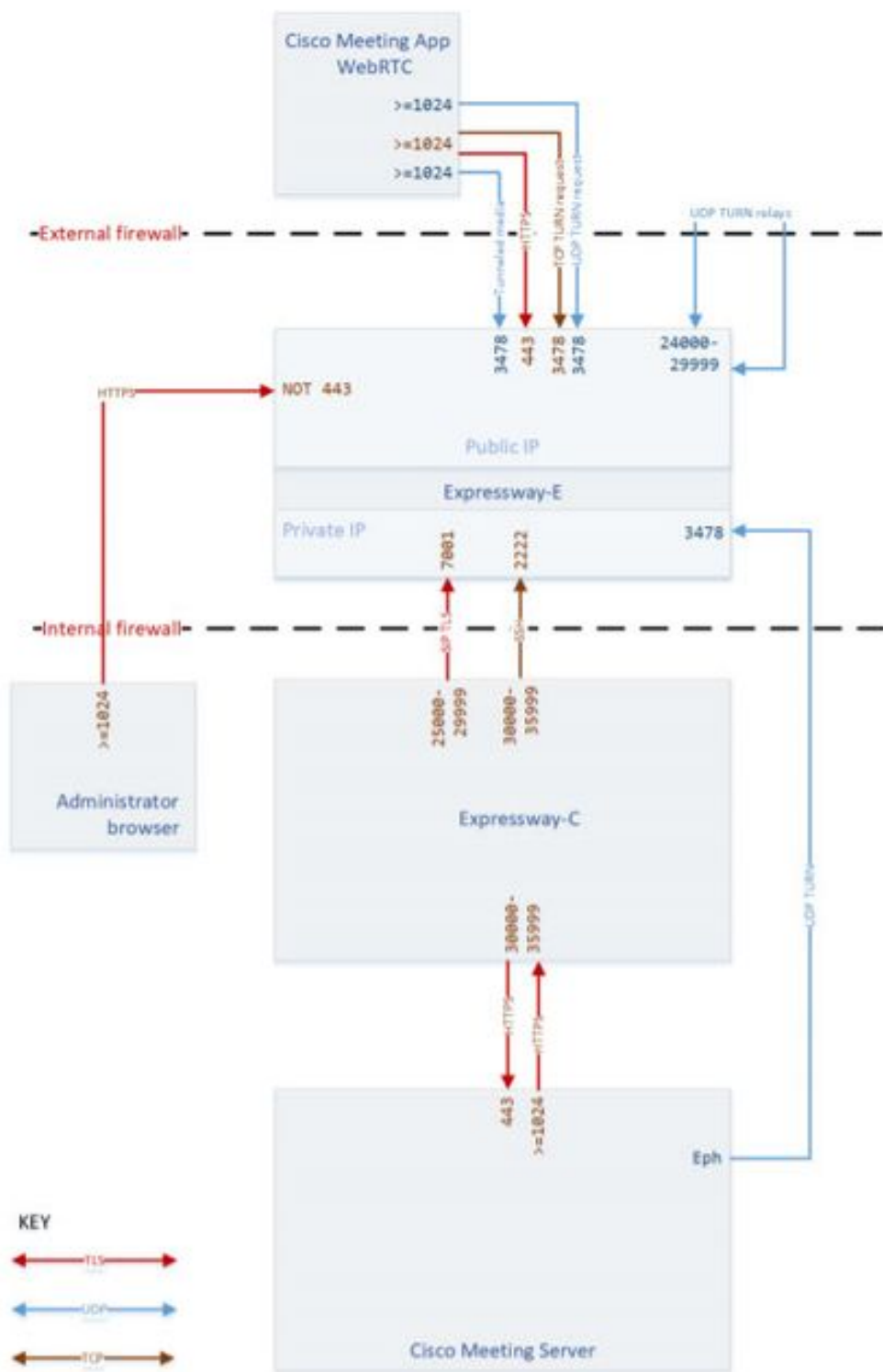
Configurer

Diagramme du réseau



Cette image fournit un exemple du flux de connexions du proxy Web pour CMS WebRTC : (à partir du [guide de configuration](#) Exp IP port Usage).

Web Proxy for Cisco Meeting Server Connections

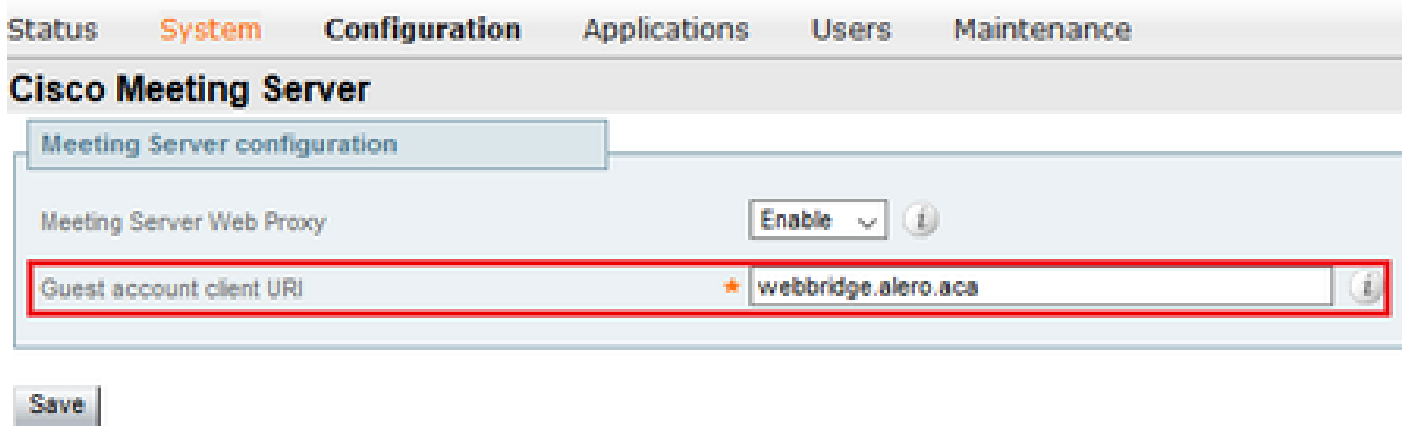


Remarque : lorsque vous exécutez X12.5.2 ou une version antérieure, vous devez configurer votre pare-feu externe pour permettre la réflexion NAT pour l'adresse IP publique Expressway-E (les pare-feu ne font généralement pas confiance aux paquets qui ont la même adresse IP source et de destination). À partir de X12.5.3, ce n'est plus nécessaire pour un Expressway autonome.

Configuration Steps

Étape 1. Intégration de CMS WB à Expressway-C


- a. Accédez à Configuration > Unified Communication > Cisco Meeting Server.
- b. Activez le proxy Web du serveur de téléconférence.
- c. Saisissez l'URL de connexion dans le champ URI du client du compte invité.
- d. Cliquez sur Enregistrer.
- e. Ajoutez l'URL de connexion CMS au certificat du serveur Expressway-E en tant que nom alternatif du sujet (SAN). Reportez-vous au [Guide de déploiement de création et d'utilisation de certificats Cisco VCS](#).





The screenshot shows the 'Cisco Meeting Server' configuration page. At the top, there are tabs for 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'Configuration' tab is selected. Below the tabs, there is a section for 'Meeting Server configuration'. Under this section, there is a 'Meeting Server Web Proxy' dropdown menu set to 'Enable'. Below that, there is a text input field for 'Guest account client URI' which contains the value 'webbridge.alero.aca'. A red box highlights this field. At the bottom left of the configuration area, there is a 'Save' button.

Étape 2. Activez TURN sur l'Expressway-E et ajoutez les informations d'authentification à la base de données d'authentification locale

- a. Accédez à Configuration > Traversal > TURN.
- b. Activez les services TURN, de off à on.
- c. Choisissez Configure TURN client credentials on local database et ajoutez les informations d'identification (nom d'utilisateur et mot de passe).

 Remarque : si vous avez un cluster d'Expressway-Es et qu'ils doivent tous être utilisés comme serveurs TURN, assurez-vous de l'activer sur tous les noeuds. Vous devez configurer deux instances turnServer distinctes sur l'API et les diriger vers chacun des serveurs Expressway-E du cluster (selon le processus de configuration indiqué à l'étape 4, qui montre le processus pour un serveur Expressway-E ; la configuration du second turnServer serait similaire, en utilisant uniquement les adresses IP respectives et les identifiants de tour pour l'autre serveur Expressway-E).

 Remarque : vous pouvez utiliser un équilibreur de charge réseau devant vos autoroutes pour

 le trafic TCP/HTTPS, mais le support TURN doit toujours passer de l'adresse IP publique du client aux serveurs TURN. Le support TURN ne doit pas passer par l'équilibreur de charge réseau


Étape 3. Modifier le port d'administration de l'Expressway-E

Cette étape est nécessaire car les connexions webrtc sont disponibles sur TCP 443, mais Exp 12.7 a introduit une nouvelle interface de gestion dédiée (DMI) qui peut être utilisée pour 443.

a. Accédez à Système > Administration.

b. Sous Web server configuration, remplacez le port d'administrateur Web par 445 dans les options de la liste déroulante, puis cliquez sur Save.

c. Répétez les étapes 3a à 3b sur tous les Expressway-E utilisés pour les services proxy WebRTC.

 Remarque : Cisco recommande de modifier le port d'administration, car les clients WebRTC utilisent 443. Si le navigateur WebRTC tente d'accéder au port 80, l'Expressway-E redirige la connexion vers 443.

Étape 4. Ajoutez l'Expressway-E en tant que serveur(s) TURN pour la traversée NAT média sur le serveur CMS

Dans CMS 2.9.x et les versions ultérieures, utilisez le menu Configuration —>API pour ajouter des serveurs tour :

- serverAddress : (adresse IP privée d'Expressway)
- clientAddress : (adresse IP publique d'Expressway)
- type : (expressway)
- nom d'utilisateur : (tel que configuré à l'étape 2c)
- mot de passe : (tel que configuré à l'étape 2c)
- tcpPortNumberOverride : 3478

d. Répétez l'étape 4c pour chaque serveur Expressway-E à utiliser pour TURN

Cette image fournit un exemple des étapes de configuration :

/api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff

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

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Dans Expressway-C, vérifiez que le WB est correctement intégré

a. Accédez à Configuration > Unified Communication > Cisco Meeting Server. Vous devez voir l'adresse IP du WB :

Status **System** Configuration Applications Users Maintenance

Cisco Meeting Server

You are here: >

Meeting Server configuration

Meeting Server Web Proxy ⓘ


Guest account client URI ⓘ

Guest account client URI resolved to the following targets

Name	Address
webbridge.alero.aca	10.48.36.5

b. Accédez à Configuration > Unified Communication > HTTP allow list > Automatically added rules. Vérifiez qu'il a été ajouté aux règles :

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

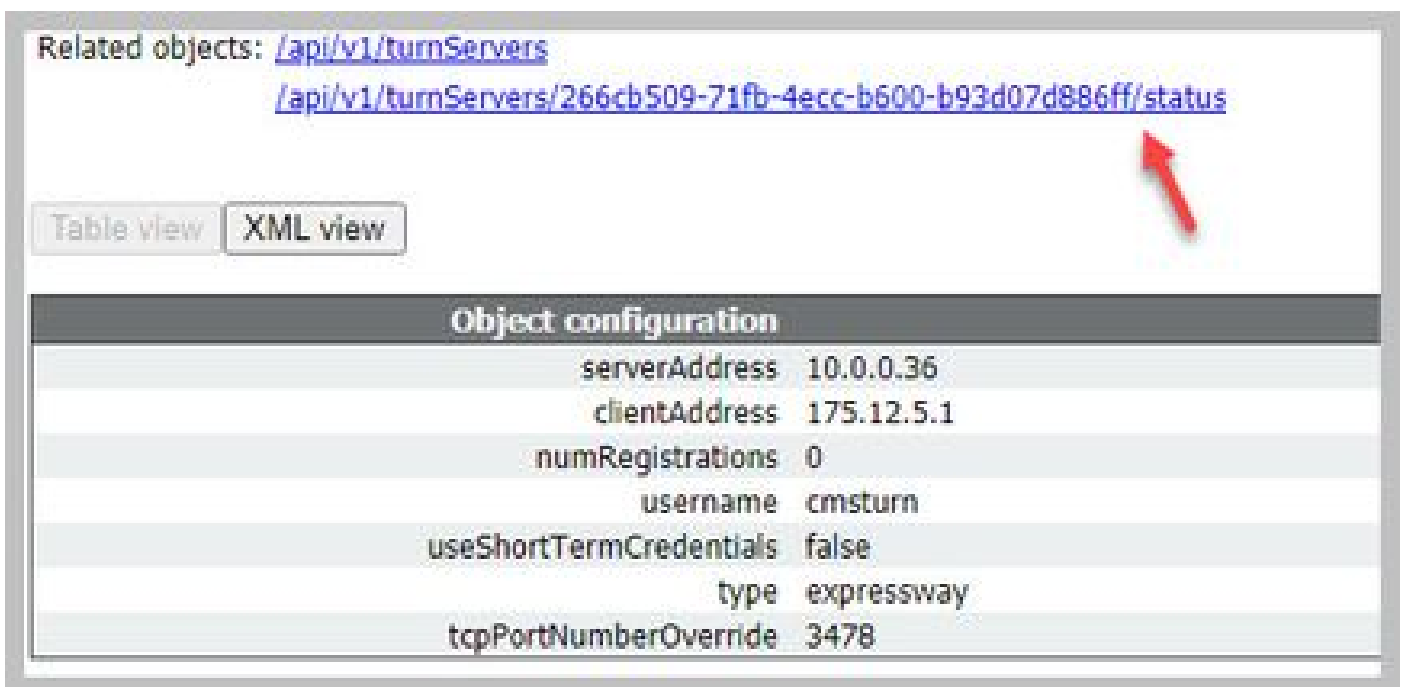
 Remarque : il n'est pas prévu de trouver le WB dans les noeuds détectés, car les règles sont simplement d'autoriser le proxy du trafic HTTPS vers le WB, et pas nécessairement pour la communication unifiée.

c. Vérifiez que le tunnel Secure Shell (SSH) pour le FQDN WB a été construit sur Expressway-C vers l'Expressway-E et qu'il est actif. Accédez à Status > Unified Communications > Unified Communications SSH tunnels status. Vous devez voir le nom de domaine complet du WB et la cible doit être l'Expressway-E.

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

Étape 2. Vérifiez que le serveur TURN a été ajouté au serveur CMS

Dans le menu CMS API, recherchez les serveurs tour, puis cliquez sur chacun d'eux. Dans chaque objet, il y a un lien pour vérifier l'état :



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

Cela produira de l'information, dont la durée totale aller-retour (RTT) en millisecondes (Ms) qui est associée au serveur du protocole TURN. Cette information est importante dans la sélection de CB pour ce qui concerne le meilleur serveur du protocole TURN à utiliser.

Étape 3. Vérifier l'utilisation du relais TURN pendant l'appel en cours

Lors d'un appel en direct effectué avec le client WebRTC, vous pouvez afficher l'état du relais multimédia TURN sur l'Expressway. Accédez à Status > TURN relay usage, puis choisissez view.

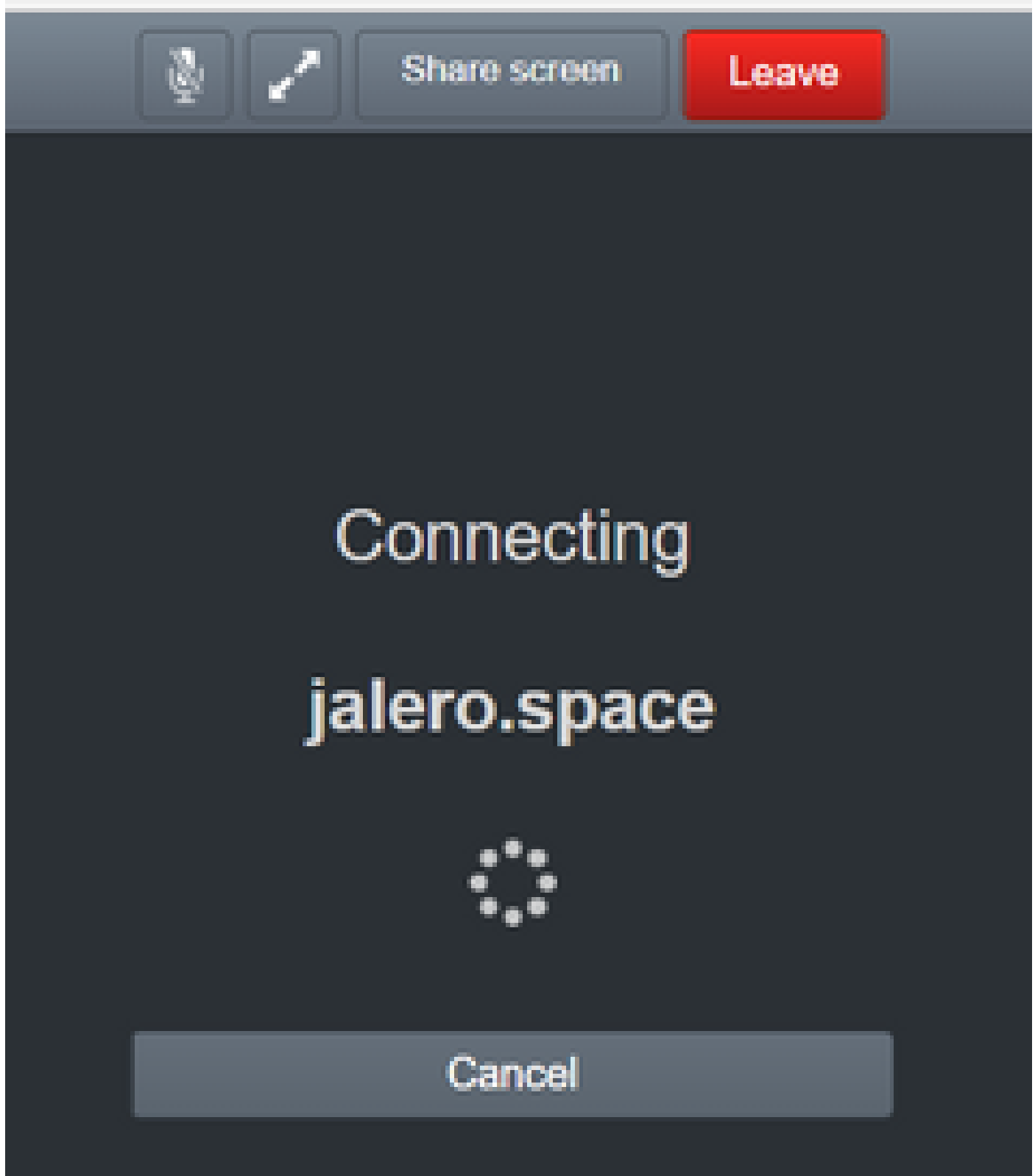
Dépannage

Outils utiles :

- Fichier HAR à partir de navigateurs ([Comment générer un fichier HAR dans Chrome ou Firefox](#))
- WebRTC internal dump from browser - chrome://webrtc-internals ou edge://webrtc-internals - Create dump dès que Join est tenté.
- Les journaux de la console du navigateur peuvent également être utiles.
- Capture Wireshark à partir du client, Exp E, Exp C et CMS.
- Les débogages network.http.traffic.server d'Exp E aident au dépannage des interfaces de connexion Web.

Le client WebRTC externe se connecte, mais sans support (en raison de l'échec ICE)

Dans ce scénario, le client RTC est capable de résoudre l'ID d'appel en jalero.space, mais quand vous entrez votre nom et sélectionnez Join call, le client affiche Connecting, comme illustré dans cette image :



Après environ 30 secondes, il est redirigé vers la page de WB initiale.

Afin de dépanner, complétez ces étapes :

- Lancez Wireshark sur le client RTC lorsque vous tentez d'établir un appel et lorsque la défaillance se produit, arrêtez la capture.
- Une fois que le problème se produit, consultez les journaux d'événements CMS:

Accédez à Logs > Event logs sur le CMS WebAdmin.

- Filtrez les traces Wireshark à l'aide de stun. Reportez-vous à l'exemple suivant :



Dans le traces Wireshark, vous verrez que le client envoie Allocate Request et les renseignements d'authentification configurés au serveur TURN Expressway-E ACTIVATION sur le port 3478 :

```
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
```

Le serveur répond avec Allocate Error :

```
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
```

ou

```
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
```

Dans les journaux CMS, ce message de journal s'affiche :

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

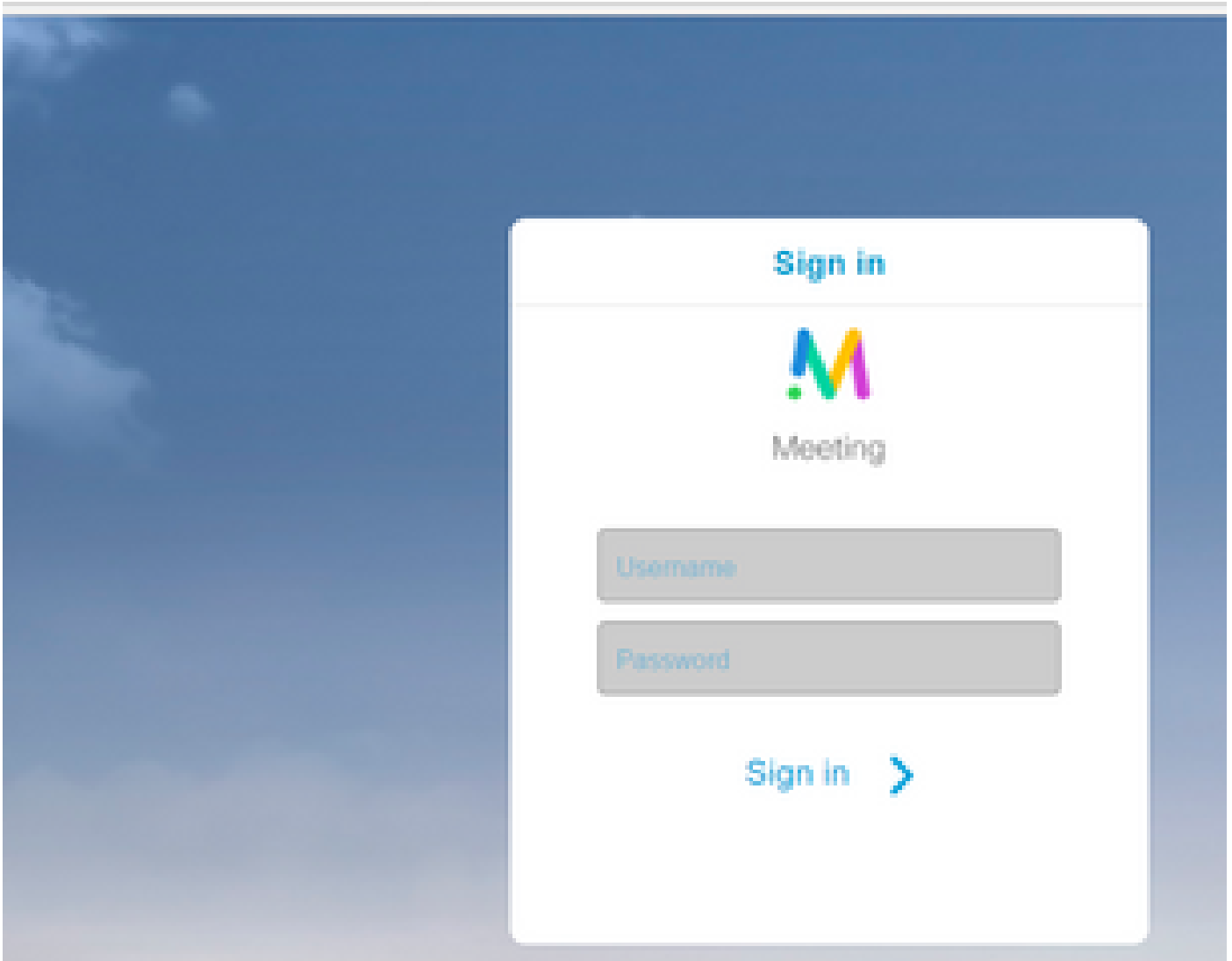
Solution :

Vérifiez les informations d'identification TURN configurées sur le CMS et assurez-vous qu'elles correspondent à celles configurées sur la base de données d'authentification locale

d'Expressway-E.

Le client WebRTC externe n'a pas accès à l'option pour participer à l'appel (Join Call).

⚠ Not secure | <https://webbridge.alero.aca>



Dans la page Callbridge Status > Generalpage, l'information suivante s'affiche :

```
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
```

Solution :

- Assurez-vous que le Callbridge peut résoudre l'URL de jonction au nom de domaine complet du webbridge (le Callbridge ne doit pas résoudre ce problème à l'adresse IP de l'Expressway-E).
- Videz le cache DNS sur Callbridge, via l'interface de ligne de commande (CLI), avec la commande `dns flush`.

- Assurez-vous que le WB approuve le certificat du serveur Callbridge (et non l'émetteur).

Le client WebRTC externe est resté bloqué (en chargement des médias) lors de la connexion à l'espace partagé. Il est ensuite redirigé vers la page initiale WB.

Solution :

- Assurez-vous que CMS peut résoudre l'enregistrement SRV _xmpp-client sur le réseau interne pour le domaine CB, et assurez-vous que les connexions WebRTC fonctionnent en interne.
- Collectez une capture Wireshark sur le client et une journalisation de diagnostic incluant tcpdump sur l'Expressway-E lors de la tentative de connexion avec le client externe :

Accédez à Maintenance > Diagnostics > Diagnostic logging et assurez-vous que Take tcpdump while logging est coché, comme illustré dans cette image, avant de sélectionner Start new log :



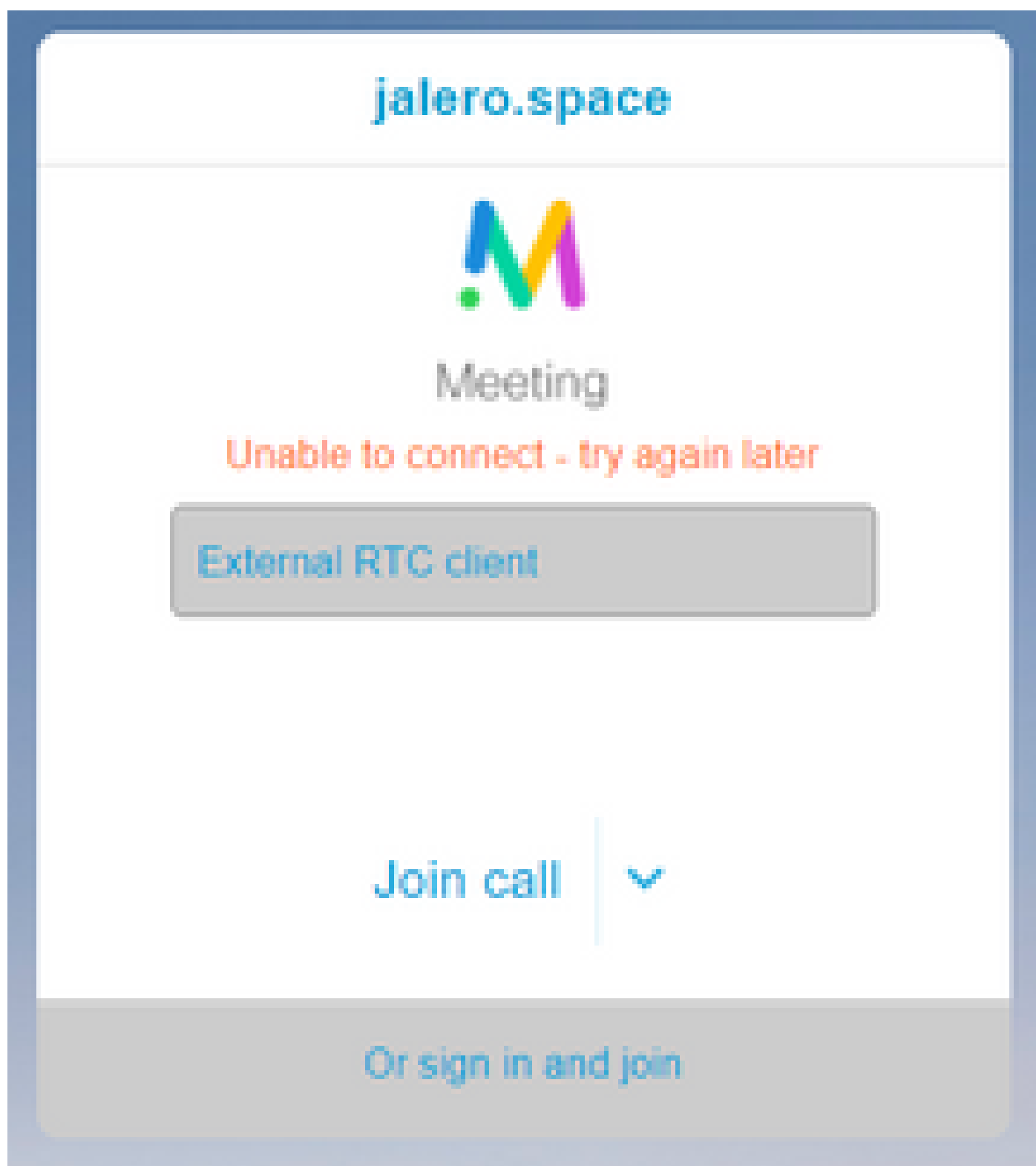
Remarque : assurez-vous que la capture Wireshark sur le périphérique du client et la connexion sur l'Expressway-E sont démarrées avant de reproduire l'appel défaillant. Lorsque l'appel qui a échoué est reproduit, arrêtez et téléchargez la journalisation sur l'Expressway-E ainsi que la capture sur le client.

- Extrayez/décompressez le lot de journaux téléchargé depuis l'Expressway-E et ouvrez le fichier .pcap pris sur l'interface publique.
- Filtrer sur les deux captures de paquets avec étourdissement :
 - Recherchez ensuite la demande de liaison du client externe à l'adresse IP publique d'Expressway-E, cliquez avec le bouton droit et sélectionnez Follow > UDP Stream.
 - Habituellement, le port de destination de la requête de liaison du client serait dans la plage de 24000-29999, qui est la plage de ports de relais TURN sur l'Expressway-E.
- Si aucune réponse aux requêtes de liaison n'est reçue du côté du client, vérifiez la capture de l'Expressway-E si les requêtes arrivent.
- Si les demandes arrivent et que l'Expressway-E répond au client, vérifiez si le transfert externe (External FW) permet le trafic UDP sortant.
- Si les requêtes n'arrivent pas, vérifiez le FW pour vous assurer que la plage de ports précédemment indiquée n'est pas bloquée.
- Si l'Expressway-E est déployé avec un contrôleur d'interface réseau double (DUAL-NIC) avec le mode NAT statique activé et est X12.5.2 ou antérieure, assurez-vous que la réflexion NAT est prise en charge et configurée sur votre FW externe. À partir de X12.5.3, cela n'est

plus nécessaire pour un Expressway autonome.

Il est impossible pour le client WebRTC de se joindre à l'espace partagé et il reçoit un avertissement lui indiquant que la connexion est impossible et qu'il devra réessayer plus tard (Unable to connect - try again later).

Dans ce scénario, le client RTC peut résoudre l'ID d'appel en jalero.space, mais lorsque vous entrez votre nom et sélectionnez Join call, l'avertissement Unable to connect - try again later s'affiche immédiatement :



Solution :

Vérifiez que CMS, sur le réseau interne, est en mesure de toujours résoudre l'enregistrement SRV _xmpp client pour le domaine CB.

Informations connexes

- [Guide d'utilisation du port IP pour VCS/Expressway](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.