

Soutenir la continuité de l'activité pendant la pandémie COVID-19 - Ressources de la solution d'accès mobile et à distance

Contenu

[Introduction](#)

[Taille](#)

[Configuration](#)

[Dépannage](#)

Introduction

Ce document décrit comment dimensionner, configurer et dépanner une solution d'accès mobile et distant (MRA) via Cisco Expressway.

Taille

La [note d'application de l'évolutivité MRA](#) résume comment optimiser la capacité existante dans les déploiements Cisco MRA et inclut des conseils sur la manière d'évaluer la capacité supplémentaire.

En outre, les informations de dimensionnement de Cisco Expressway sont disponibles dans [l'architecture préférée pour les déploiements sur site d'entreprise Cisco Collaboration 12.x, CVD](#), tableaux 9-8 et 9-9.

Configuration

- [L'accès mobile et à distance via Cisco Expressway Deployment Guide \(X12.5\)](#) et [la configuration de base MRA Expressway](#) (vidéo) fournissent des instructions détaillées sur la configuration de la solution MRA.
- La configuration requise pour le pare-feu se trouve dans [Cisco Expressway IP Port Usage](#).
- Certains déploiements peuvent avoir des domaines internes et externes différents. Reportez-vous à [Configurer l'accès mobile et distant via Expressway/VCS dans un déploiement multidomaine](#) pour plus d'informations sur la configuration de MRA.

Dépannage

Si la connexion Jabber sur MRA échoue, procédez comme suit afin de résoudre le problème :

Étape 1. Exécutez [Collaboration Solutions Analyzer](#) (CSA) avec un ensemble d'informations d'identification de test.

CSA est une suite d'outils pour votre solution de collaboration. CSA vous aide lors des différentes

phases du cycle de vie d'une solution de collaboration, et en particulier pour MRA, le validateur Collaboration Edge (CollabEdge) réduit considérablement le temps nécessaire au dépannage de la solution.

CollabEdge validator est un outil qui valide les déploiements MRA en simulant un processus de connexion client. Plusieurs contrôles sont effectués :

- Validation des entrées DNS (Public Domain Name System)
- Contrôles de connectivité externes
- Certificats SSL Expressway-E (Exp-E)
- Contrôles de flux d'applications liés à Unified Communications Manager (UCM) et IM & Presence Server (IM&P) Services de données utilisateur (UDS)eXtensible Messaging and Presence Protocol (XMPP)Enregistrement du protocole SIP (Session Initiation Protocol)

Entrée

Au minimum, l'outil nécessite un domaine pour vérifier la configuration DNS, la détection Exp-E, la connectivité et les certificats SSL Exp-E. Si un nom d'utilisateur et un mot de passe de test sont fournis, l'outil pourra récupérer la configuration de l'utilisateur et du périphérique à partir d'UCM, tenter de s'authentifier contre IM&P et enregistrer un périphérique associé. Si vous disposez d'un déploiement uniquement sur un téléphone, cochez la case et les chèques IM&P seront ignorés.

 Fill in below details

Edge domain	tp.ciscotac.net	 
Username	hocao	 
Password	 
<input type="checkbox"/>	Phone only deployment	

Validate MRA deployment

Exemple de sortie

La première chose qui s'affiche est une vue d'ensemble de la tentative de connexion qui donne une vue d'ensemble de ce qui fonctionne et de ce qui échoue. Exemple :

Solution overview

The dashboard shows two main sections: 'Edge domain' and 'Host analysis'. 'Edge domain' has 'DNS' and 'WebEx' both with green checkmarks. 'Host analysis' has a table with five columns: 'Hostname', 'TCP connectivity', 'SSL certificate', 'MRA login', and 'Softphone'. The 'Hostname' row shows 'ewaye.ciscotac.net' with green checkmarks in all other columns.

Hostname	TCP connectivity	SSL certificate	MRA login	Softphone
ewaye.ciscotac.net	✓	✓	✓	✓

Lorsque quelque chose ne fonctionne pas, il est immédiatement visible dans la section qu'il échoue. Vous trouverez plus de détails dans les sections spécifiques de ce document.

Solution overview

The dashboard shows the same two main sections. 'Edge domain' remains successful. 'Host analysis' shows 'MRA login' with a red 'x' and 'Softphone' with a question mark icon.

Hostname	TCP connectivity	SSL certificate	MRA login	Softphone
ewaye.ciscotac.net	✓	✓	✗	?

Validation du domaine Edge

Dans la validation du domaine Edge, tous les détails sont affichés en ce qui concerne les enregistrements DNS. Cliquez sur le point d'interrogation afin d'afficher plus de détails sur la vérification.

Edge domain

The page is split into two panels: 'DNS configuration' and 'WebEx configuration'. 'DNS configuration' has a table of DNS records. 'WebEx configuration' shows a message that the domain is not enabled for WebEx authentication.

Host	Priority	Weight	Port	IP address
✓ _collab-edge._tls.tp.ciscotac.net				
✓ ewaye.ciscotac.net	0	0	8443	173.38.154.85
✓ _cuplogin._tcp.tp.ciscotac.net				
Not resolvable.				
✓ _cisco-uds._tcp.tp.ciscotac.net				
Not resolvable.				

Contrôles de connectivité externe et de certificat SSL Exp-E

Cette section présente des détails sur la connectivité et les vérifications de certificats Exp-E pour chaque hôte détecté avec les enregistrements DNS. Le point d'interrogation est également disponible ici pour obtenir plus de détails sur les contrôles effectués et pourquoi.

Edge hosts

TCP connectivity ?

Host	8443	5222	5061
ewaye.ciscotac.net	✓	✓	✓

SSL certificate ?

Host	Valid	SAN	IP phone trust	Client auth	Server auth
ewaye.ciscotac.net View	✓	✓	✓	✓	✓

Cliquez sur **Affichage** en regard du nom d'hôte afin d'ouvrir la vue détaillée du certificat et de disposer de tous les détails de la chaîne complète.

SSL certificate

ewaye.tp.ciscotac.net

×

Certificate chain

Full chain available



- ▼ CN: Go Daddy Root Certificate Authority - G2
 - ▼ CN: Go Daddy Secure Certificate Authority - G2
- CN: ewaye.ciscotac.net**

Summary

CN: ewaye.ciscotac.net

Subject: OU=Domain Control Validated, CN=ewaye.ciscotac.net

Issuer:

C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

Detail

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 13402504543026767831 (0xb9ff42df53ab67d7)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

Validity

Not Before: Aug 18 13:44:01 2017 GMT

Not After : Mar 21 16:19:00 2019 GMT

Subject: OU=Domain Control Validated, CN=ewaye.ciscotac.net

Serveurs Edge



Cette section présente les détails de la configuration Edge. Ceci est fait pour chaque Exp-E découvert par DNS.

Tested edge servers



✓ [ewaye.ciscotac.net](#)

Single sign-on (SSO)

-  Domain [tp.ciscotac.net](#) is not enabled for SSO.
-  OAuth token with refresh is not enabled.

Edge configuration

- ✓ Successfully retrieved edge config. 
- ✓ Found `_cisco-uds` SRV record in edge config: [colcmpub.ciscotac.net:8443](#) [colcmsub.ciscotac.net:8443](#)
- ✓ Found user home cluster: [192.168.0.50:8443](#)
- ✓ Found SIP edge server: [ewaye.ciscotac.net:5061](#)
- ✓ Found XMPP edge server: [ewaye.ciscotac.net:5222](#)
- ✓ Found HTTP edge server: [ewaye.ciscotac.net:8443](#)

Le contenu complet de la réponse peut également être développé.

Edge configuration

- ✓ Successfully retrieved edge config. 

Details

Edge config XML:

```
<?xml version='1.0' encoding='UTF-8'?>
<getEdgeConfigResponse version="1.0">
  <serviceConfig>
    <service>
      <name>_cisco-uds</name>
      <server>
        <priority>0</priority>
        <weight>0</weight>
        <port>8443</port>
        <address>colcmpub.ciscotac.net</address>
      </server>
    </service>
  </serviceConfig>
</getEdgeConfigResponse>
</xml>
```

Serveurs UDS

Pour chaque serveur Edge qui peut être sélectionné, les serveurs UDS retournés dans `get_edge_config` sont testés un par un jusqu'à ce qu'un serveur fonctionnel soit trouvé ou que tous échouent.

Tested UDS servers



✓ colcmpub.ciscotac.net



UCM user and device configuration

- ✓ Found Cluster user
- ✓ Found UCM version **11.5.1**
- ✓ Successfully retrieved user configuration. ▾
- ✓ Found users full name: **Hoai Trung Cao**
- ✓ Successfully retrieved jabber-config.xml. ▾
- ✓ No Voice Services Domain in jabber-config.xml or domain matches.

Serveurs IM&P

Pour chaque serveur Edge qui peut être sélectionné dans la section Serveurs Edge, les serveurs IM&P (extraits du profil de service) sont testés un par un jusqu'à ce qu'un serveur fonctionnel soit trouvé ou que tous échouent.



IM&Presence



IM&P user's configuration

- ✓ Found user's UDS service profile URLs in user config. ▾
- ✓ Successfully retrieved user's UDS service profile. ▾
- ✓ Found IM&P server(s). ▾

colimp.ciscotac.net

- ✓ Successfully retrieved session key.
- ✓ Successfully retrieved IM&P user configuration. ▾
- ✓ Successfully retrieved one-time password.
- ✓ Successfully logged in to IM&P.

Enregistrement du téléphone logiciel

Pour chaque serveur Edge qui peut être sélectionné dans la section Serveurs Edge, l'enregistrement du téléphone logiciel est testé. Le type de téléphone logiciel testé dépend des périphériques associés à l'utilisateur et suivez la liste de priorités ci-dessous : CSF, BOT, TCT, TAB. Pour le serveur Edge sélectionné, les serveurs Exp-C (retournés par `get_edge_config`) et Unified CM (configurés dans le groupe CUCM) sont testés jusqu'à ce qu'une combinaison fonctionne ou que tous échouent.

Softphone registration



User's device configuration

- ✓ SIPS port is opened
- ✓ Successfully retrieved device configuration file from UCM. ✓
- ✓ Found user's devices. ✓
- ✓ Found user's device to register: [csfhocao](#)
- ✓ Device Configuration ✓
- ✓ Device's DN: [5010](#)
- ✓ Found Call Manager Group ✓

Tested Expressway-C paths

- ✓ [192.168.0.20](#)

Tested CUCM servers

- ✓ [colcmsub.ciscotac.net](#)

- ✓ Successfully registered CSF softphone to CUCM.

Étape 2. Une fois que vous avez déterminé où le processus de connexion échoue, utilisez [Collaboration Edge Most Common Issues](#) afin de voir s'il correspond à l'un des problèmes connus.

Référez-vous à [Configurer et dépanner des certificats MRA \(Collaboration Edge\)](#) ou [Installer un certificat de serveur sur un Expressway](#) (vidéo) si vous trouvez un problème de certificat via CSA.

Si vous utilisez un contrôleur d'interface réseau (NIC) unique avec la traduction d'adresses réseau statique (NAT) sur Exp-E et que vous utilisez un dispositif de sécurité adaptatif (ASA), consultez [Configurer la réflexion NAT sur l'ASA pour les périphériques VCS Expressway TelePresence](#) afin de vous assurer que la réflexion NAT est correctement configurée.

Étape 3. Si vous n'avez pas pu résoudre votre problème, ouvrez un dossier du centre d'assistance technique (TAC) avec les journaux d'Expressway et un rapport de problème.

- [Téléchargement des journaux de diagnostic et des captures de paquets Expressway](#) (vidéo)
- [Obtention du rapport de problème Jabber Desktop](#) (vidéo)