

Supporto della continuità aziendale durante la pandemia di COVID-19 - Risorse per soluzioni di accesso remoto e mobile

Sommario

[Introduzione](#)

[Dimensioni](#)

[Configurazione](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come dimensionare, configurare e risolvere i problemi relativi a una soluzione MRA (Mobile and Remote Access) tramite Cisco Expressway.

Dimensioni

La [nota sull'applicazione per la scalabilità MRA](#) riassume come ottimizzare la capacità esistente nelle implementazioni Cisco MRA e include indicazioni su come valutare la capacità aggiuntiva.

Inoltre, le informazioni sul dimensionamento di Cisco Expressway sono disponibili in [Architettura preferita per le implementazioni on-premises aziendali di Cisco Collaboration 12.x, CVD](#), tabelle 9-8 e 9-9.

Configurazione

- [Accesso mobile e remoto tramite Cisco Expressway Deployment Guide \(X12.5\)](#) e [Expressway MRA Basic Configuration](#) (video) forniscono istruzioni dettagliate sulla configurazione della soluzione MRA.
- I requisiti del firewall sono disponibili nell'[utilizzo della porta IP di Cisco Expressway](#).
- Alcune distribuzioni possono avere domini interni ed esterni diversi. Per informazioni su come configurare l'Autorità registrazione integrità, vedere [Configurare l'accesso remoto e mobile tramite Expressway/VCS in una distribuzione multidominio](#).

Risoluzione dei problemi

Se l'accesso a Jabber tramite MRA non riesce, completare i seguenti passaggi per risolvere il problema:

Passaggio 1. Eseguire [Collaboration Solutions Analyzer](#) (CSA) con un set di credenziali di test.

CSA è una suite di strumenti per le soluzioni di collaborazione. CSA aiuta durante le diverse fasi del ciclo di vita di una soluzione di collaborazione, in particolare per MRA, Collaboration Edge

(CollabEdge) validator riduce drasticamente il tempo necessario per risolvere i problemi della soluzione.

CollabEdge Convalida è uno strumento che convalida le distribuzioni MRA simulando un processo di accesso client. Sono stati eseguiti diversi controlli:

- Convalida voce DNS (Public Domain Name System)
- Controlli connettività esterna
- Certificati SSL Expressway-E (Exp-E)
- Controlli del flusso di applicazioni correlati a Unified Communications Manager (UCM) e a IM & Presence server (IM&P) UDS (User Data Services) Protocollo XMPP (Extensible Messaging and Presence Protocol) Registrazione SIP (Session Initiation Protocol)

Ingresso

Lo strumento richiede almeno un dominio per controllare la configurazione DNS, l'individuazione Exp-E, la connettività e i certificati SSL Exp-E. Se vengono forniti un nome utente e una password di prova, lo strumento sarà in grado di recuperare la configurazione dell'utente e del dispositivo da UCM, tentare l'autenticazione tramite IM&P e registrare un dispositivo associato. Se si dispone di una distribuzione solo telefonica, selezionare la casella di controllo e i controlli IM&P verranno ignorati.

 Fill in below details

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

Validate MRA deployment

Output di esempio

La prima cosa che viene visualizzata è una panoramica del tentativo di accesso che fornisce una panoramica di ciò che funziona e di ciò che non funziona. Un esempio di funzionamento corretto di tutto:

Solution overview

Edge domain

DNS ✓

WebEx ✓

Host analysis

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

Quando un problema si verifica, viene immediatamente visualizzato nella sezione in cui si verifica. Per ulteriori informazioni, consultare le sezioni specifiche di questo documento.

Solution overview

Edge domain

DNS ✓

WebEx ✓

Host analysis

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

Convalida dominio Edge

Nella convalida del dominio Edge vengono visualizzati tutti i dettagli relativi ai record DNS. Fare clic sul punto interrogativo per visualizzare ulteriori dettagli sul controllo.

Edge domain

DNS configuration

✓ **_collab-edge._tls.tp.ciscotac.net**

Host	Priority	Weight	Port	IP address
✓ 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.

WebEx configuration

✓ Domain [tp.ciscotac.net](#) is not enabled for WebEx authentication.

Controlli connettività esterna e certificato SSL Exp-E

In questa sezione vengono illustrati i dettagli relativi alla connettività e ai controlli dei certificati Exp-E per ogni host individuato con i record DNS. Il punto interrogativo è disponibile anche qui per ulteriori dettagli su quali controlli vengono effettuati e perché.

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	✓	✓	✓	✓	✓

Fare clic su **Visualizza** accanto a nome host per aprire la visualizzazione dei dettagli del certificato e rendere disponibili tutti i dettagli dell'intera catena.

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

Server perimetrali

Questa sezione mostra i dettagli di configurazione di Edge. Questa operazione viene eseguita per ogni Exp-E individuato dal 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](#)

Il contenuto completo della risposta può essere ampliato.

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>
```

Server UDS

Per ogni server perimetrale che è possibile selezionare, i server UDS restituiti in `get_edge_config` vengono testati singolarmente fino a quando non ne viene individuato uno funzionante o tutti funzionano correttamente.

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.

Server IM&P

Per ogni server perimetrale che è possibile selezionare nella sezione Server perimetrali, i server IM&P (recuperati dal profilo del servizio) vengono testati uno per uno fino a quando non viene rilevato un server funzionante o tutti non funzionano.



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.

Registrazione Softphone

Per ogni server perimetrale che può essere selezionato nella sezione Server perimetrali, viene verificata la registrazione del softphone. Il tipo di softphone testato dipende dai dispositivi associati all'utente e segue questo elenco con priorità: CSF, BOT, TCT, TAB. Per il server perimetrale selezionato, i server Exp-C (restituiti da `get_edge_config`) e il server Unified CM (configurato nel gruppo CUCM) vengono testati finché una combinazione non funziona o finché tutti non funzionano.

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.

Passaggio 2. Dopo aver individuato la posizione in cui si è verificato l'errore di login, utilizzare [Collaboration Edge Most Common Issues](#) per verificare se corrisponde a uno dei problemi noti.

Se si riscontra un problema di certificato tramite CSA, fare riferimento a [Configurazione e risoluzione dei problemi dei certificati MRA \(Collaboration Edge\)](#) o [Installazione di un certificato server in Expressway](#) (video).

Se si usa un singolo Network Interface Controller (NIC) con NAT (Network Address Translation) statico su Exp-E e si usa un'appliance ASA (Adaptive Security Appliance), vedere [Configurare la riflessione NAT sull'appliance ASA per i dispositivi VCS Expressway TelePresence](#) per assicurarsi che la riflessione NAT sia configurata correttamente.

Passaggio 3. Se non è stato possibile risolvere il problema, aprire una richiesta TAC (Technical Assistance Center) con i registri di Expressway e la segnalazione di un problema.

- [Download di registri diagnostici e acquisizioni pacchetti Expressway](#) (video)
- [Recupero del Report di problema di Jabber Desktop](#) (video)