

COVID-19 대유행의 비즈니스 연속성 지원 - 모바일 및 원격 액세스 솔루션 리소스

목차

[소개](#)

[크기](#)

[구성](#)

[문제 해결](#)

소개

이 문서에서는 Cisco Expressway를 통해 MRA(Mobile and Remote Access) 솔루션의 크기 조정, 구성 및 문제 해결 방법에 대해 설명합니다.

크기

MRA [Scale Application Note](#)에는 Cisco MRA 구축에서 기존 용량을 최적화하는 방법이 요약되어 있으며 추가 용량을 평가하는 방법에 대한 지침이 포함되어 있습니다.

또한 Cisco Expressway 크기 조정 정보는 [Preferred Architecture for Cisco Collaboration 12.x Enterprise On-Premises Deployments, CVD](#), 표 9-8 및 9-9에서 확인할 수 있습니다.

구성

- [Cisco Expressway 구축 설명서\(X12.5\)](#) 및 [Expressway MRA 기본 구성\(비디오\)](#)을 통한 모바일 및 원격 액세스는 MRA 솔루션 구성 방법에 대한 단계별 지침을 제공합니다.
- 방화벽 요구 사항은 [Cisco Expressway IP Port Usage](#)에서 확인할 수 있습니다.
- 일부 구축에는 서로 다른 내부 및 외부 도메인이 있을 수 있습니다. MRA를 구성하는 방법에 대한 자세한 내용은 [다중 도메인 구축에서 Expressway/VCS를 통한 모바일 및 원격 액세스 구성](#)을 참조하십시오.

문제 해결

MRA를 통해 Jabber에 로그인하는 데 실패하면 다음 단계를 완료하여 문제를 해결합니다.

1단계. 테스트 인증서 세트와 함께 CSA([Collaboration Solutions Analyzer](#))를 실행합니다.

CSA는 협업 솔루션을 위한 도구 모음입니다. CSA는 협업 솔루션 라이프사이클의 여러 단계, 특히 MRA를 위해 Collaboration Edge(CollabEdge) 검증기를 사용하면 솔루션 문제 해결에 필요한 시간을 크게 줄일 수 있습니다.

CollabEdge 검증기는 클라이언트 로그인 프로세스를 시뮬레이션하여 MRA 구축을 검증하는 도구입니다. 몇 가지 확인이 완료되었습니다.

- DNS(Public Domain Name System) 항목 유효성 검사
- 외부 연결 검사
- Expressway-E(Exp-E) SSL 인증서
- UCM(Unified Communications Manager) 및 IM & Presence 서버(IM&P) 관련 애플리케이션 흐름 확인 사용자 데이터 서비스(UDS)XMPP(Extensible Messaging and Presence Protocol)SIP(Session Initiation Protocol) 등록

입력

최소한 DNS 구성, Exp-E 검색, 연결 및 Exp-E SSL 인증서를 확인하기 위한 도메인이 필요합니다. 테스트 사용자 이름 및 비밀번호가 제공된 경우 이 툴은 UCM에서 사용자 및 디바이스 컨피그레이션을 검색하고 IM&P에 대해 인증을 시도하며 연결된 디바이스를 등록할 수 있습니다. 전화 전용 구축이 있는 경우 확인란을 선택하면 IM&P 검사를 건너뛴니다.

Fill in below details



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

Validate MRA deployment

샘플 출력

첫 번째로 표시되는 내용은 로그인 시도 개요로, 작동 방식 및 실패 사항에 대한 개요를 제공합니다. 모든 것이 올바르게 작동하는 경우의 예:

Solution overview

<div style="background-color: #fff; padding: 5px; border: 1px solid #ccc;"> <p> Edge domain</p> <p>DNS ✓</p> <p>WebEx ✓</p> </div>	<div style="background-color: #fff; padding: 5px; border: 1px solid #ccc;"> <p> Host analysis</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>Hostname</th> <th>TCP connectivity</th> <th>SSL certificate</th> <th>MRA login</th> <th>Softphone</th> </tr> </thead> <tbody> <tr> <td>ewaye.ciscotac.net</td> <td>✓</td> <td>✓</td> <td>✓</td> <td>✓</td> </tr> </tbody> </table> </div>	Hostname	TCP connectivity	SSL certificate	MRA login	Softphone	ewaye.ciscotac.net	✓	✓	✓	✓
Hostname	TCP connectivity	SSL certificate	MRA login	Softphone							
ewaye.ciscotac.net	✓	✓	✓	✓							

문제가 해결되지 않으면 오류가 발생한 섹션에 즉시 표시됩니다. 자세한 내용은 이 문서의 특정 섹션에서 확인할 수 있습니다.

Solution overview

Edge domain

DNS ✓

WebEx ✓

Host analysis

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

에지 도메인 검증

Edge 도메인 검증에서 DNS 레코드와 관련된 모든 세부사항이 표시됩니다.체크에 대한 자세한 내용을 표시하려면 물음표를 클릭합니다.

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.

외부 연결 및 Exp-E SSL 인증서 검사

이 섹션에서는 DNS 레코드로 검색된 각 호스트에 대한 연결 및 Exp-E 인증서 검사에 대한 세부 정보를 보여줍니다.여기서 확인 사항 및 그 이유에 대한 자세한 내용을 보려면 물음표를 참조하십시오.

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	✓	✓	✓	✓

인증서 세부 정보 보기를 열고 전체 체인에 대한 모든 세부 정보를 사용할 수 있도록 하려면 호스트 이름 옆에 있는 **View**를 클릭합니다.

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

에지 서버


이 섹션에서는 Edge 컨피그레이션 세부사항을 보여줍니다. 이는 DNS에서 검색한 모든 Exp-E에 대해 수행됩니다.

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](#)

응답의 전체 내용도 확장할 수 있습니다.

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>
```

UDS 서버

선택할 수 있는 각 Edge 서버에 대해 `get_edge_config`에서 반환된 UDS 서버는 작동하는 서버가 검색되거나 모두 실패할 때까지 하나씩 테스트됩니다.

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.

IM&P 서버

Edge Servers(에지 서버) 섹션에서 선택할 수 있는 각 Edge 서버에 대해 IM&P 서버(서비스 프로파일에서 가져옴)는 작동하는 서버를 찾거나 모두 실패할 때까지 하나씩 테스트됩니다.



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.

소프트폰 등록

Edge 서버 섹션에서 선택할 수 있는 각 Edge 서버에 대해 소프트폰 등록이 테스트됩니다. 테스트된 소프트폰 유형은 사용자와 연결된 디바이스에 따라 다르며 다음 우선 순위 목록을 따릅니다. CSF, BOT, TCT, TAB. 선택한 에지 서버의 경우, CUCM 그룹에 구성된 대로 Exp-C 서버 (get_edge_config에 의해 반환됨)와 Unified CM 서버(CUCM 그룹에 구성됨)는 조합이 작동하거나 모든 서버가 실패할 때까지 테스트됩니다.

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.

2단계. 로그인 프로세스 실패 위치를 확인한 후 [Collaboration Edge Most Common Issues](#)를 사용하여 알려진 문제 중 하나와 일치하는지 확인합니다.

CSA를 통해 인증서 문제를 발견한 경우 [MRA\(Collaboration Edge\) 인증서 구성 및 문제 해결 또는 Expressway](#)(비디오)에 서버 인증서 설치를 참조하십시오.

Exp-E에서 고정 NAT(Network Address Translation)가 있는 단일 NIC(Network Interface Controller)를 사용하고 ASA(Adaptive Security Appliance)를 사용하는 경우 NAT 리플렉션이 올바르게 구성되었는지 확인하려면 VCS Expressway TelePresence [디바이스에 대한 ASA의 NAT 리플렉션 구성](#)을 참조하십시오.

3단계. 문제를 해결할 수 없는 경우 Expressway 로그와 문제 보고서를 사용하여 TAC(Technical Assistance Center) 케이스를 여십시오.

- [Expressway 진단 로그 및 패킷 캡처 다운로드](#)(비디오)
- [Jabber Desktop 문제 보고서 받기](#)(비디오)