Collaboration Edge의 가장 일반적인 문제 해결

목차

소개

이 문서에서는 구축 단계에서 고객이 직면하는 가장 일반적인 Collaboration Edge 문제를 해결하는

방법을 설명합니다.

배경 정보

MRA(Mobile & Remote Access)는 VPN(Virtual Private Network-less) Jabber 기능을 위한 구축 솔루션입니다. 이 솔루션을 통해 최종 사용자는 전 세계 어디서나 내부 엔터프라이즈 리소스에 연결할 수 있습니다. 이 가이드는 Collaboration Edge 솔루션을 트러블슈팅하는 엔지니어가 구축 과정에서 고객이 직면하는 가장 일반적인 문제를 신속하게 파악하고 해결할 수 있도록 돕기 위해 작성되었습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM(Cisco Unified Communications Manager)
- Cisco Expressway 코어
- Cisco Expressway 에지
- Cisco IM and Presence(IM&P)
- Windows용 Cisco Jabber
- MAC용 Cisco Jabber
- Android용 Cisco Jabber
- iOS용 Cisco Jabber
- 보안 인증서
- DNS(Domain Name System)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Expressway 버전 X8.1.1 이상
- CUCM Release 9.1(2)SU1 이상 및 IM&P Version 9.1(1) 이상
- Cisco Jabber 버전 9.7 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

로그인 문제

Jabber에서 MRA를 통해 로그인할 수 없음

이 증상은 다양한 문제로 인해 발생할 수 있으며, 그 중 일부는 여기에 요약되어 있습니다.

1. SRV(Collaboration Edge Service Record)가 생성되지 않았거나 포트 8443에 연결할 수 없음

Jabber 클라이언트가 MRA에 성공적으로 로그인하려면 특정 협업 에지 SRV 레코드를 생성하고 외

부에서 액세스할 수 있어야 합니다. Jabber 클라이언트가 처음 시작되면 DNS SRV 쿼리를 만듭니다.

1. **_cisco-uds**: 이 SRV 레코드는 CUCM 서버를 사용할 수 있는지 확인하는 데 사용됩니다.

2. **_cuplogin**: 이 SRV 레코드는 IM&P 서버를 사용할 수 있는지 확인하는 데 사용됩니다.

3. **_collab-edge**: 이 SRV 레코드는 MRA를 사용할 수 있는지 확인하는 데 사용됩니다.

Jabber 클라이언트가 시작되고 **_cisco-uds** 및**_cuplogin에** 대한 SRV 응답을 받지 못하고**_collab-edge에 대한 응답을 받지 못하는** 경우 **이 응답을 사용하여 SRV 응답에 나열된 Expressway-E에 연결을 시도합니다.**

_collab-edge SRV 레코드는 포트 8443을 사용하는 Expressway-E의 FQDN(정규화된 도메인 이름)을 **가리킵니다**. **_collab-edge SRV**가 생성되지 않았거나 외부에서 사용할 수 없거나, 사용 가능하지만 포트 8443에 연결할 수 없으면 Jabber 클라이언트가 로그인하지 못합니다.

_collab-edge SRV 레코드가 확인 가능한지 그리고 CSA(Collaboration Solutions Analyzer)의 SRV 검사기를 사용하여 TCP 포트 8443에 연결할 수 있는지 확인할 수 있습니다.

포트 8443에 연결할 수 없는 경우 보안 디바이스(방화벽)에서 포트를 차단하거나 Exp-E에서 GW(Default Gateway) 또는 고정 경로의 컨피그레이션이 잘못되었기 때문일 수 있습니다.

2. VCS Expressway에서 사용할 수 없거나 사용 가능한 인증서가 없습니다.

Jabber 클라이언트가 **_collab-edge**에 대한 응답을 받은 다음 포트 8443을 통해 TLS(Transport Layer Security)를 사용하여 Expressway에 연결하여 Expressway에서 인증서를 검색하여 Jabber 클라이언트와 Expressway 간의 통신을 위한 TLS를 설정합니다.

Expressway에 Expressway의 FQDN 또는 도메인을 포함하는 유효한 서명 인증서가 없으면 이 작업이 실패하고 Jabber 클라이언트가 로그인하지 못합니다.

이 문제가 발생하면 Expressway에서 CSR(Certificate Signing Request) 툴을 사용합니다. 이 툴에는 Expressway의 FQDN이 주체 대체 이름(SAN)으로 자동으로 포함됩니다.

> **참고**: MRA를 사용하려면 Expressway-C와 Expressway-E 사이, Expressway-E와 외부 엔드포인트 사이의 보안 통신이 필요합니다.

Expressway 인증서 요구 사항 기능별 다음 표는 MRA 구축 가이드에서 확인할 수 있습니다.

Table 1. CSR Alternative Name Element and Unified Communications Features

Add These Items as Subject Alternative Names	When Generating a CSR for These Purposes			
	Mobile and Remote Sccess	Jabber guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence Service chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	

3. 에지 구성에 UDS 서버가 없습니다.

Jabber 클라이언트가 Expressway-E와의 보안 연결을 성공적으로 설정한 후 에지 컨피그레이션(get_**edge_config**)을 요청합니다. 이 에지 컨피그레이션에는 **_cuplogin** 및**_cisco-uds에** 대한 SRV **레코드가 포함되어 있습니다**. 에지 컨피그레이션에서 **_cisco-uds** SRV 레코드가 반환되지 않으면 Jabber 클라이언트가 로그인을 진행할 수 없습니다.

이 문제를 해결하려면 **_cisco-uds SRV 레코드**가 내부에서 생성되었으며 Expressway-C에서 확인할 수 있는지 확인합니다.

DNS SRV 레코드에 대한 자세한 내용은 X8.11용 MRA 구축 가이드에서 확인할 수 있습니다.

이는 듀얼 도메인에 있는 경우에도 흔히 나타나는 증상입니다. 듀얼 도메인에서 실행하고 Jabber 클라이언트가 UDS(사용자 데이터 서비스)를 반환하지 않는 경우 _cisco-uds SRV 레코드가 외부 도메인의 내부 DNS에 생성되었는지 확인해야 합니다.

> **참고**: Expressway 버전 X12.5 이후에는 더 이상 내부 DNS에 _cisco-UDS SRV 레코드를 추가할 필요가 없습니다. 이 개선 사항에 대한 자세한 내용은 Cisco Expressway 구축 가이드를 통한 모바일 및 원격 액세스(X12.5)를 참조하십시오.

4. Expressway-C 로그에 이 오류가 표시됩니다. XCP_JABBERD Detail=호스트 '%IP%'에 연결할 수 없습니다. 포트 7400:(111) 연결이 거부되었습니다.

Expressway-E NIC(Network Interface Controller)가 잘못 구성된 경우 이로 인해 XCP(Extensible Communications Platform) 서버가 업데이트되지 않을 수 있습니다. Expressway-E가 이러한 기준을 충족하는 경우 다음과 같은 문제가 발생할 수 있습니다.

1. 단일 NIC 사용.
2. 고급 네트워킹 옵션 키가 설치되어 있습니다.
3. Use Dual Network Interfaces(이중 네트워크 인터페이스 사용) 옵션이 **Yes(예)**로 설정되어 있습니다.

이 문제를 해결하려면 Use Dual Network Interfaces(이중 네트워크 인터페이스 사용) 옵션을 **No(아니요)**로 변경합니다.

이 문제가 발생하는 이유는 Expressway-E가 잘못된 네트워크 인터페이스에서 XCP 세션을 수신 대기하므로 연결이 실패/시간 초과되기 때문입니다. Expressway-E는 TCP 포트 7400에서 XCP 세션을 수신 대기합니다. 다음을 사용하면 이를 확인할 수 있습니다. netstatVCS에서 루트로 제공하는 명령입니다

5. Expressway-E 서버 호스트 이름/도메인 이름이 _collab-edge SRV에 구성된 것과 일치하지 않습니다.

DNS 페이지 컨피그레이션의 Expressway-E 서버 호스트 이름/도메인이 **_collab-edge SRV 응답**에서 받은 것과 일치하지 않으면 Jabber 클라이언트가 Expressway-E와 통신할 수 없습니다. Jabber 클라이언트는 **get_edge_config 응답**에서 xmppEdgeServer/Address 요소를 사용하여 Expressway-E에 대한 XMPP 연결을 설정합니다.

다음은 Expressway-E에서 Jabber 클라이언트로 보내는 **get_edge_config 응답**에서 xmppEdgeServer/Address가 표시되는 예입니다.

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example URL</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

이를 방지하려면 _collab-**edge SRV 레코드가** Expressway-E 호스트 이름/도메인 이름과 일치하는지 확인합니다. Cisco 버그 ID CSCuo83458이 이 항목에 등록되었으며 Cisco 버그 ID CSCuo82526에 대한 일부 지원이 추가되었습니다.

6. 현재 WebEx Connect 구독으로 인해 로그인할 수 없습니다.

Windows용 Jabber 로그는 다음을 보여줍니다.

```
2014-11-22 19:55:39,122 INFO  [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://URL server;
Url: http://example URL server';;;.2014-11-22
19:55:39,122 INFO [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://example URL server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example URL server/cas/FederatedSSO?org=example URL]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://website URL/cas/FederatedSSO?org=example URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

로그인 시도는 WebEx Connect로 전달됩니다.

영구적인 해결을 위해서는 WebEx에 연락하여 사이트를 서비스 해제해야 합니다.

해결 방법

단기적으로는 이러한 옵션 중 하나를 사용하여 조회에서 제외할 수 있습니다.

- jabber-config.xml에 이 매개변수를 추가합니다. 그런 다음 jabber-config.xml 파일을 CUCM의 TFTP 서버에 업로드합니다. 먼저 클라이언트가 내부적으로 로그인해야 합니다.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
<Policies>
<ServiceDiscoveryExcludedServices>WEBEX<
/ServiceDiscoveryExcludedServices>
</Policies>
</config>
```

- 애플리케이션 관점에서 다음을 실행합니다.
  msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX

  참고: 두 번째 옵션은 모바일 디바이스에서는 작동하지 않습니다.

- WEBEX 서비스를 제외하는 클릭 가능한 URL을 생성합니다.
  ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

UC 서비스 검색에 대한 자세한 내용과 Cisco Jabber 12.8용 온프레미스 구축에서 일부 서비스를 제외하는 방법을 확인할 수 있습니다.

7. Expressway-C 서버에 "구성되었지만 오류가 있습니다. 프로비저닝 서버: 접근 서버 정보를 기다리는 중입니다."

Status(상태) > Unified Communications로 이동하고 오류 메시지가 표시되면 "Configured but with errors. Provisioning server: Waiting for traversal server info." unified CM 등록 및 IM&P 서비스의 경우 Expressway-C에 구성된 내부 DNS 서버에는 Expressway-E에 대한 DNS A 레코드 2개가 있습니다. Expressway-E에 대한 여러 DNS A 레코드의 원인은 영향을 받는 사용자가 Expressway-E에서 고정 NAT가 활성화된 단일 NIC에서 고정 NAT가 활성화된 듀얼 NIC로 이동하거나 그 반대로 이동했을 수 있으며 내부 DNS 서버에서 해당 DNS A 레코드를 삭제하지 않았기 때문입니다. 따라서 Expressway-C에서 DNS 조회 유틸리티를 사용하고 Expressway-E FQDN을 확인할 때 DNS A 레코드 두 개가 표시됩니다.

솔루션

Expressway-E NIC가 고정 NAT를 사용하는 단일 NIC에 대해 구성된 경우

1. Expressway-C에 구성된 DNS 서버에서 Expressway-E 내부 IP 주소에 대한 DNS A 레코드를 삭제합니다.
2. CMD를 통해 Expressway-C 및 사용자 PC의 DNS 캐시 플러시(ipconfig /flushdns).
3. Expressway-C 서버를 재부팅합니다.

고정 NAT가 활성화된 듀얼 NIC에 대해 Expressway-E NIC가 구성된 경우

1. Expressway-C에 구성된 DNS 서버에서 Expressway-E *외부* IP 주소에 대한 DNS A 레코드를 삭제합니다.
2. CMD를 통해 Expressway-C 및 사용자 PC의 DNS 캐시 플러시(ipconfig /flushdns).
3. Expressway-C 서버를 재부팅합니다.

8. 설치된 Microsoft DirectAccess

고객이 Jabber 클라이언트와 동일한 PC에서 Microsoft DirectAccess를 사용하는 경우, 원격으로 로그인을 시도하면 MRA가 중단될 수 있습니다. DirectAccess는 PC가 VPN을 사용한 것처럼 DNS 쿼

리를 내부 네트워크로 터널링하도록 강제합니다.

> **참고**: Microsoft DirectAccess는 Jabber over MRA에서 지원되지 않습니다. 모든 트러블슈팅은 최선의 노력입니다. DirectAccess의 구성은 네트워크 관리자의 책임입니다.

일부 고객은 Microsoft DirectAccess 이름 확인 정책 테이블에서 모든 DNS 레코드를 차단하여 성공을 거뒀습니다. 이러한 레코드는 DirectAccess에서 처리되지 않습니다(Jabber는 MRA를 사용하는 공용 DNS를 통해 이러한 레코드를 확인할 수 있어야 함).

- _cisco-uds에 대한 SRV 레코드
- SRV 레코드(_C)
- _collab-edge에 대한 SRV 레코드
- 모든 Expressway Es에 대한 레코드

9. Expressway Reverse DNS 조회 실패

버전 X8.8부터 Expressway/VCS는 ExpE, ExpC 및 모든 CUCM 노드에 대해 전달 및 역방향 DNS 항목을 생성해야 합니다.

전체 요구 사항에 대해서는 x8.8 릴리스 노트의 전제 조건 및 소프트웨어 종속성 및 모바일 및 원격 액세스를 위한 DNS 레코드를 참조하십시오.

내부 DNS 레코드가 없는 경우 reverseDNSLookup을 참조하는 Expressway 로그에 오류가 있을 수 있습니다.

2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102" ThreadID="139882696623872" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception: exception in reverseDNSLookup: reverse DNS lookup failed for address=x.x.x.x"

Expressway-C는 Expressway-E IP에 대한 PTR 레코드를 쿼리할 때 하나의 FQDN만 수신합니다. DNS에서 잘못된 FQDN을 수신하는 경우 로그에 이 행이 표시되고 실패합니다.

2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685" ThreadID="140028119959296" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate verification failed for host=xx.xx.xx.xx, additional info: Invalid Hostname"

등록 문제

소프트폰이 등록할 수 없습니다. SIP/2.0 405 메서드가 허용되지 않습니다.

Expressway-C의 진단 로그에는 **SIP/2.0 405 Method Not Allowed** Jabber 클라이언트에서 보낸 등록 요청에 대한 응답 메시지입니다. 포트 5060/5061이 있는 Expressway-C와 CUCM 간의 현재 SIP(Session Initiation Protocol) 트렁크 때문일 수 있습니다.

```
SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
```

```
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
Warning: 399 collabzone "SIP trunk disallows REGISTER"
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

이 문제를 해결하려면 CUCM에 구성된 현재 SIP 트렁크 및 CUCM의 Expressway-C 네이버 영역에 적용되는 SIP 트렁크 보안 프로필의 SIP 포트를 5065와 같은 다른 포트로 변경합니다. 이에 대해서는 이 비디오에서 자세히 설명합니다. 구성 요약은 다음과 같습니다.

CUCM

1. 5060(5065)이 아닌 수신 대기 포트로 새 SIP 트렁크 보안 프로필을 생성합니다.
2. SIP 트렁크 보안 프로파일과 연결된 SIP 트렁크를 생성하고 Expressway-C IP 주소, 포트 5060으로 대상을 설정합니다.

고속도로 C

1. CUCM 컨피그레이션과 일치하도록 대상 포트가 5060(5065)이 아닌 CUCM에 대한 인접 영역을 생성합니다.
2. Expressway-C Settings(Expressway-C **설정) > Protocols(프로토콜) > SIP**에서 Expressway-C가 5060에서 SIP를 계속 수신하는지 확인합니다.

소프트폰을 등록할 수 없습니다. 이유="Unknown domain"

Expressway-C의 진단 로그에 Event=가 표시됩니다.**"Registration Rejected" Reason="Unknown domain"** Service="SIP" Src-ip="XXX.XXX.XXX.XXX" Src-port="51601" Protocol="TCP" AOR="sip:XXX.XXX.XXX.XXX".

이 문제를 해결하려면 다음 사항을 확인하십시오.

- Jabber 클라이언트는 비보안 **디바이스 보안 프로파일**을 사용하지 않으려는 경우 CUCM에서 보안 디바이스 보안 프로파일을 사용합니까?

- Jabber 클라이언트가 보안 디바이스 보안 프로파일을 사용하는 경우, 보안 프로파일의 이름이 FQDN 형식이고 Expressway-C 인증서에 SAN으로 구성된 FQDN 이름입니까?

- Jabber 클라이언트가 보안 디바이스 보안 프로파일을 사용하는 경우 **System > Enterprise Parameters > Security Parameters > Cluster Security Mode**로 이동하고 클러스터 보안 모드가 1로 설정되어 있는지 확인하여 CUCM 클러스터가 보호되었는지 확인합니다. 값이 **0인** 경우 관리자는 클러스터 보안을 위해 문서화된 절차를 거쳐야 합니다.

소프트폰을 등록할 수 없습니다. 이유 "Idle countdown expired"

Jabber 클라이언트가 REGISTER 메시지에서 보내는 기간 동안 Expressway-E 로그를 검토할 때 **Idle countdown expired** 코드 조각에 표시된 것과 같은 오류입니다.

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

이 코드 조각은 방화벽에서 포트 5061이 열려 있음을 나타냅니다. 그러나 충분한 시간 내에 전달되는 애플리케이션 레이어 트래픽이 없으므로 TCP 연결이 닫힙니다.

이러한 상황이 발생하면 Expressway-E 앞의 방화벽에서 SIP 검사/ALG(Application Layer Gateway) 기능이 켜져 있을 가능성이 높습니다. 이 문제를 해결하려면 이 기능을 비활성화해야 합니다. 이 방법을 잘 모르는 경우 방화벽 공급업체 제품 설명서를 참조하십시오.

SIP Inspection/ALG에 대한 자세한 내용은 Cisco Expressway-E 및 Expressway-C-Basic Configuration DeploymentGuide의 부록 4를 참조하십시오.

펌웨어에 구성된 전화 프록시로 인해 MRA 실패

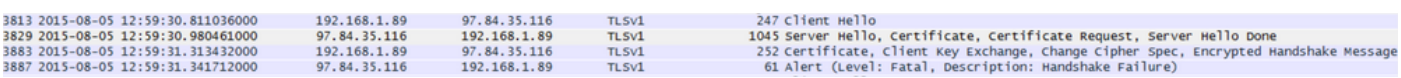
Expressway-E의 진단 로그에 포트 5061에서 TLS 협상 실패가 표시되지만 SSL 핸드셰이크가 포트 8443에서 성공했습니다.

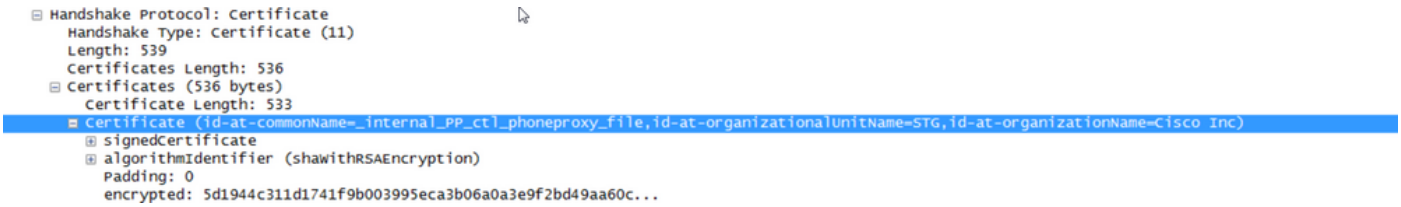
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(67)" Method="::TTSSLErrorOutput" Thread="0x7fae4ddb1700": TTSSL_continueHandshake: Failed to establish SSL connection
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04 15:14:23,535"

Jabber의 로그:

-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert][handlePlatformVerificationResultSynchronously] Verification result : FAILURE reason : [CN_NO_MATCH UNKNOWN]
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handyiron][ssl_state_callback] SSL alert read:fatal:handshake failure
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true, failureReason=eTLSFailure, SSLErrorCode=336151568
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false, failureReason=eFailedToConnect, serverType=ePrimary, role=eNone
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handyiron][secSSLIsConnected] SSL_do_handshake() returned : SSL_ERROR_SSL.

Jabber의 패킷 캡처는 Expressway E IP와의 SSL 협상을 표시하지만 전송된 인증서는 이 서버에서 가져오지 않습니다.





FW에 전화 프록시가 구성되어 있습니다.

해결책:

FW에서 Phone Proxy를 실행하는지 확인합니다. 이를 확인하려면 **show run policy-map** 명령을 실행하면 다음과 비슷한 내용이 표시됩니다.

```
class sec_sip
inspect sip phone-proxy ASA-phone-proxy
```

전화 서비스에 대한 전화 프록시를 사용하지 않도록 설정합니다.

통화 - 관련 문제

MRA를 통해 전화를 걸 때 미디어 없음

다음은 단일 및 듀얼 NIC 구축에서 이 문제를 일으킬 수 있는 구성 부재 및 잘못된 구성 중 일부입니다.

- 고정 NAT는 Expressway-E의 System(시스템) > Network Interfaces(네트워크 인터페이스) > IP에서 구성되지 않습니다. 네트워크 레이어의 NAT는 방화벽에서 수행해야 하지만, 이 설정은 애플리케이션 레이어의 IP를 변환합니다.
- TCP/UDP 포트가 방화벽에 열려 있지 않습니다. 포트 목록은 Cisco Expressway IP Port Usage 컨피그레이션 가이드를 참조하십시오

고정 NAT 구축을 사용하는 단일 NIC는 권장되지 않습니다. 다음은 미디어 문제를 방지하기 위한 몇 가지 고려 사항입니다.

방출

- UC 접근 영역에서 Expressway-C는 Expressway-E에 구성된 공용 IP 주소를 가리켜야 합니다.
- 미디어는 "헤어핀"하거나 외부 방화벽에 반영해야 합니다. Cisco ASA 방화벽의 컨피그레이션 예는 Configure NAT Reflection On The ASA For The VCS Expressway TelePresence Devices에서 찾을 수 있습니다.

이에 대한 자세한 내용은 Cisco Expressway-E 및 Expressway-C Basic Configuration Deployment Guide의 부록 4를 참조하십시오.

MRA를 PSTN으로 호출할 때 링백 없음

이 문제는 X8.5 이전 버전의 Expressway에 대한 제한 때문입니다. Cisco 버그 ID CSCua72781은 Expressway-C가 183 Session Progress 또는 180 Ringing의 초기 미디어를 접근 영역에 전달하지 않는 방법을 설명합니다. 버전 X8.1.x 또는 X8.2.x를 실행하는 경우 버전 X8.5로 업그레이드하거나 여기에 나열된 해결 방법을 수행할 수 있습니다.

183을 180으로 전환하고 수신 다이얼 피어에 적용하는 SIP 프로필을 만드는 경우 CUBE(Cisco Unified Border Element)에서 해결 방법을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
voice class sip-profiles 11
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"
"SIP/2.0 180 Ringing"
```

그런 다음 CUCM **> CUBE**의 SIP 프로파일 또는 sip-ua 컨피그레이션 모드 내의 CUBE 자체에서 180 Early Media를 비활성화합니다.

```
disable-early-media 180
```

CUCM 및 IM&P 문제

CUCM을 추가하지 못하게 하는 ASCII 오류

Expressway-C에 CUCM을 추가하면 CUCM을 추가할 수 없는 ASCII 오류가 발생합니다.

Expressway-C가 데이터베이스에 CUCM을 추가하면 get 및 list 함수와 관련된 일련의 AXL 쿼리를 통해 실행됩니다. 이러한 기능의 예로는 getCallManager, **listCallManager**, **listProcessNode**, **listProcessNodeService** 및 getCCMVersion을 들 **수 있습니다.** getCallManager **프로세스**가 실행된 후 모든 CUCM Call Manager-trust 또는 tomcat-trust를 검색하도록 설정된 ExecuteSQLQuery에 의해 성공합니다.

CUCM이 쿼리를 받아 실행하면 CUCM은 모든 인증서를 다시 보고합니다. 인증서 중 하나에 비 ASCII 문자가 포함된 경우 Expressway는 다음과 유사한 오류를 웹 인터페이스에 생성합니다 ascii codec can't decode byte 0xc3 in position 42487: ordinal not in range(128).

이 문제는 Cisco 버그 ID CSCuo54489로 추적되며 버전 X8.2에서 해결됩니다.

보안 구축의 Expressway-C에서 CUCM으로 5061의 아웃바운드 TLS 실패

이 문제는 CUCM 및 Tomcat.pem/CallManager.pem의 자체 서명 인증서를 사용할 때 동일한 주제가 있을 때 발생합니다. 이 문제는 Cisco 버그 ID CSCun30200으로 해결됩니다. 이 문제를 해결하기 위한 해결 방법은 tomcat.pem을 삭제하고 Expressway-C의 CUCM 컨피그레이션에서 TLS Verify를 비활성화하는 것입니다.

IM&P 서버가 추가되지 않았고 오류가 발생했습니다.

IM&P 서버를 추가하면 Expressway-C에서 "이 서버가 IM and Presence 서버가 아닙니다." 또는 "HTTP 오류 "HTTPError:500" .AXL 쿼리 HTTP와 통신할 수 없습니다."라고 보고하므로 IM&P 서버가 추가되지 않습니다.

IM&P 서버를 추가하는 과정에서 Expressway-C는 AXL 쿼리를 사용하여 명시적 디렉토리에서 IM&P 인증서를 찾습니다. Cisco 버그 ID CSCul05131로 인해 인증서가 해당 저장소에 없으므로 잘못된 오류가 발생합니다.

기타 문제

Jabber 클라이언트의 음성 메일 상태가 "연결 안 됨"으로 표시됨

Jabber 클라이언트 음성 메일 상태가 성공적으로 연결되도록 하려면 Expressway-C의 HTTP 허용 목록 내에서 Cisco Unity Connection IP 주소 또는 호스트 이름을 구성해야 합니다.

Expressway-C에서 이 작업을 완료하려면 다음 절차를 수행합니다.

버전 X8.1 및 X8.2의 절차

1. Configuration(**컨피그레이션) > Unified Communications > Configuration(컨피그레이션) > Configure HTTP server allow list(HTTP 서버 허용 목록 구성)를 클릭합니다**.
2. New(**새로 만들기) > Enter IP/Hostname(IP/호스트 이름 입력) > Create entry(항목 생성)를 클릭합니다**.
3. Jabber 클라이언트에서 로그아웃한 다음 다시 로그인합니다.

버전 X8.5 절차

1. Configuration(**컨피그레이션) > Unified Communications > Unity Connection Servers(Unity 연결 서버)를 클릭합니다**.
2. New(**새로 만들기) > Enter IP/Hostname(IP/호스트 이름 입력), User account credentials(사용자 계정 자격 증명) > Add Address(주소 추가)를 클릭합니다**.
3. Jabber 클라이언트에서 로그아웃한 다음 다시 로그인합니다.

연락처 사진이 Expressway를 통해 Jabber 클라이언트에 표시되지 않음

모바일 및 원격 액세스 솔루션은 연락처 사진 확인을 위해 UDS만 사용합니다. 이 경우 사진을 저장할 수 있는 웹 서버가 있어야 합니다. 구성 자체가 두 배입니다.

1. Jabber-config.xml 파일을 수정하여 클라이언트를 연락처 사진 확인을 위해 웹 서버에 연결해야 합니다. 여기서 구성하면 이러한 결과가 생성됩니다.

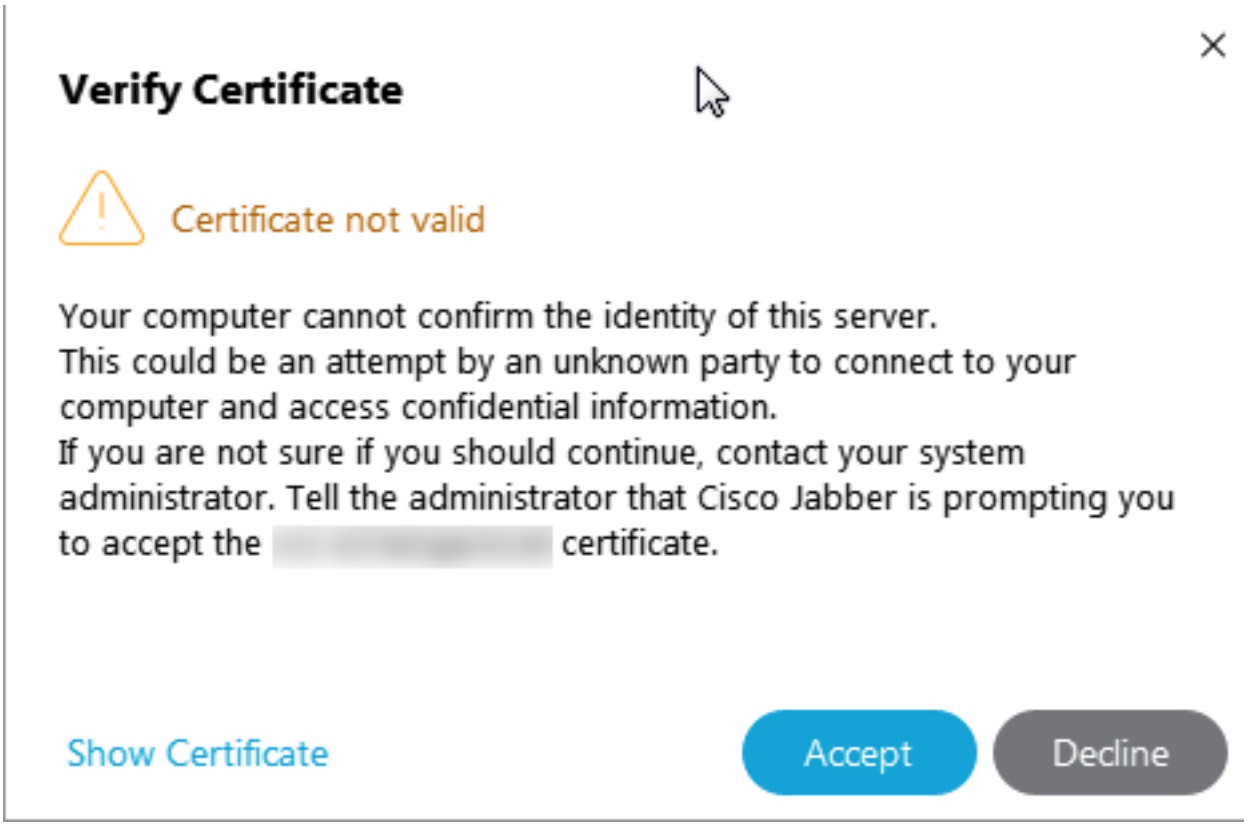
```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%%uid%%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2. Expressway-C는 HTTP 서버 허용 목록에 웹 서버가 나열되어 있어야 합니다.

   Configuration(**컨피그레이션) > Unified Communications > Configuration(컨피그레이션) > Configure HTTP server allow list(HTTP 서버 허용 목록 구성)를 클릭합니다**.New(**새로 만들기) > Enter IP/Hostname(IP/호스트 이름 입력) > Create entry(항목 생성)를 클릭합니다**.Jabber 클라이언트에서 로그아웃한 다음 다시 로그인합니다.

   참고: UDS 연락처 사진 확인에 대한 자세한 내용은 Jabber 연락처 사진 설명서를 참조하십시오.

Jabber 클라이언트는 로그인하는 동안 Expressway-E 인증서를 수락하라는 프롬프트가 표시됩니다



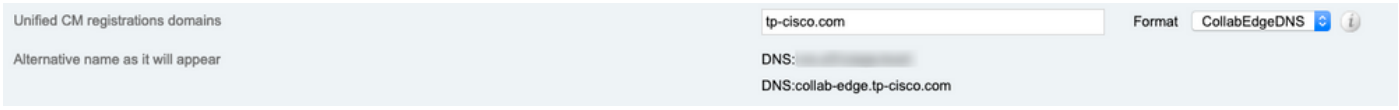
이 오류 메시지는 클라이언트 디바이스에서 신뢰하는 공용 CA에서 서명하지 않은 Expressway Edge 인증서 또는 도메인이 서버 인증서에 SAN으로 없는 것과 관련이 있습니다.

Expressway 인증서 수락 프롬프트에서 Jabber 클라이언트를 중지하려면 아래 나열된 두 가지 기준을 충족해야 합니다.

- Jabber 클라이언트를 실행하는 디바이스/시스템에는 Expressway-E 인증서의 서명자가 인증서 신뢰 저장소에 나열되어 있어야 합니다.

  참고: 이 작업은 모바일 디바이스에 대규모 인증서 신뢰 저장소가 있으므로 공용 인증 기관을 사용하는 경우 쉽게 수행할 수 있습니다.

- 협업 에지 레코드에 사용되는 Unified CM 등록 도메인이 Expressway-E 인증서의 SAN 내에 있어야 합니다. Expressway 서버의 CSR 도구는 Unified CM 등록 도메인을 SAN으로 추가하는 옵션을 제공하며, 도메인이 MRA용으로 구성된 경우 미리 로드됩니다. 인증서를 서명한 CA가 도메인을 SAN으로 승인하지 않을 경우 "CollabEdgeDNS" 옵션을 사용하여 접두사 "collab-edge"를 도메인에 추가할 수도 있습니다.



관련 정보

- [Expressway를 통한 모바일 및 원격 액세스 가이드]

- Cisco Expressway 인증서 생성 및 사용 구축 설명서
- 방화벽 통과를 위한 Cisco TelePresence Video Communication Server(Cisco VCS) IP 포트 사용
- Cisco Jabber 구축 및 설치 설명서
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.