Collaboration Edge - meest voorkomende problemen oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met de Collaboration Edge-problemen die klanten tijdens de implementatiefase het meest ondervinden.

Achtergrondinformatie

Mobile & Remote Access (MRA) is een implementatieoplossing voor Virtual Private Network-less (VPN) Jabber-mogelijkheden. Met deze oplossing kunnen eindgebruikers verbinding maken met interne bedrijfsresources van overal ter wereld. Deze handleiding is geschreven om engineers die problemen oplossen met de Collaboration Edge-oplossing de mogelijkheid te geven om snel de meest voorkomende problemen te identificeren en op te lossen die klanten tijdens de implementatiezin tegenkomen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM)
- Cisco Expressway Core
- Cisco Expressway Edge
- Cisco IM en aanwezigheid (IM&P)
- Cisco Jabber voor Windows
- Cisco Jabber voor MAC
- Cisco Jabber voor Android
- Cisco Jabber voor iOS
- Beveiligingscertificaten
- Domain Name System (DNS)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Expressway versie X8.1.1 of hoger
- CUCM release 9.1(2)SU1 of hoger en IM&P versie 9.1(1) of hoger
- Cisco Jabber versie 9.7 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Problemen met inloggen

Jabber kan niet inloggen via MRA

Dit symptoom kan worden veroorzaakt door een breed scala aan problemen, waarvan enkele hier worden geschetst.

1. Collaboration Edge Service Record (SRV) niet gemaakt en/of poort 8443 onbereikbaar

Om een Jabber-client met succes te kunnen inloggen met MRA, moet er een specifiek collaboration edge SRV-bestand worden gemaakt en extern toegankelijk zijn. Wanneer een Jabber-client in eerste instantie is gestart, worden DNS-SRV-vragen gesteld:

1. **_cisco-uds**: Deze SRV-record wordt gebruikt om te bepalen of een CUCM-server beschikbaar is.

2. **_cuplogin**: Deze SRV record wordt gebruikt om te bepalen of een IM&P server beschikbaar is.

3. **_collab-edge**: Deze SRV-record wordt gebruikt om te bepalen of MRA beschikbaar is.

Als de Jabber-client is gestart en geen SRV-antwoord ontvangt voor **_cisco-uds** en **_cuplogin** en **wel** een antwoord ontvangt voor **_collab-edge**, dan gebruikt de client dit antwoord om te proberen contact op te nemen met de Expressway-E die in het SRV-antwoord wordt vermeld.

Het SRV**_collab-edge** record verwijst naar de Fully Qualified Domain Name (FQDN) van Expressway-E met poort **8443**. Als de **_collab-edge** SRV niet is gemaakt, of niet extern beschikbaar is, of als het wel beschikbaar is, maar poort 8443 niet bereikbaar is, dan kan de Jabber-client niet inloggen.

U kunt bevestigen of de **_collab-edge** SRV-record oplosbaar is en TCP-poort 8443 bereikbaar is met de SRV Checker in Collaboration Solutions Analyzer (CSA).

Als poort 8443 niet bereikbaar is, is dit mogelijk omdat een beveiligingsapparaat (firewall) de poort blokkeert of omdat de standaardgateway (GW) of statische routes in de Exp-E niet goed zijn geconfigureerd.

2. Onaanvaardbaar of geen beschikbaar certificaat op VCS Express

Nadat de Jabber client een antwoord heeft ontvangen voor **_collab-edge**, neemt het vervolgens contact op met Expressway met Transport Layer Security (TLS) via poort 8443 om te proberen het certificaat van Expressway op te halen om TLS in te stellen voor communicatie tussen de Jabber client en Expressway.

Als Expressway geen geldig ondertekend certificaat heeft dat FQDN of domein van Expressway bevat, dan mislukt dit en kan de Jabber-client niet inloggen.

Als dit probleem zich voordoet, gebruikt u de tool Certificaatondertekeningsaanvraag (CSR) op Expressway, die automatisch de FQDN van Expressway als Onderwerp Alternatieve Naam (SAN) bevat.

> **Opmerking**: MRA vereist beveiligde communicatie tussen Expressway-C en Expressway-E, en tussen Expressway-E en externe eindpunten.

De volgende tabel met de Expressway-certificaatvereisten per functie vindt u in de MRA-implementatiegids:

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. Geen UDS-servers gevonden in Edge Configuration

Nadat de Jabber client met succes een veilige verbinding met Expressway-E tot stand heeft gebracht, vraagt hij om zijn randconfiguratie (**get_edge_config**). Deze randconfiguratie bevat de SRV-records voor **_cuplogin** en **_cisco-uds**. Als de SRV**_cisco-uds** records niet worden teruggegeven in de randconfiguratie, dan kan de Jabber-client niet verder gaan met inloggen.

Om dit op te lossen, zorg ervoor dat **_cisco-uds** SRV records intern worden gemaakt en oplosbaar door Expressway-C.

Meer informatie over de DNS SRV-records vindt u in de MRA-implementatiegids voor X8.11.

Dit is ook een veelvoorkomend symptoom als je in een duaal domein bent. Als u in een duaal domein draait en vindt dat de Jabber-client niet teruggestuurd wordt naar een User Data Service (UDS), moet u bevestigen dat de _cisco-uds SRV-records in de interne DNS met het externe domein worden gemaakt.

> **Opmerking**: na Expressway versie X12.5 is het niet langer een vereiste om een _cisco-UDS SRV record toe te voegen aan de interne DNS. Raadpleeg de Implementatiegids voor mobiele en externe toegang via Cisco Expressway (X12.5) voor meer informatie over deze verbetering.

4. Expressway-C logbestanden tonen deze fout: XCP_JABBERD Detail=Cannot to connect to host '%IP%', poort 7400:(11) Verbinding geweigerd

Als Expressway-E Network Interface Controller (NIC) niet correct is geconfigureerd, kan dit ervoor zorgen dat de XCP-server (Extensible Communications Platform) niet wordt bijgewerkt. Als Expressway-E aan deze criteria voldoet, kom je waarschijnlijk dit probleem tegen:

1. Gebruikt één NIC.
2. Er wordt een geavanceerde netwerkoptietoets geïnstalleerd.
3. De optie Dubbele netwerkinterfaces gebruiken is op **Ja** ingesteld.

Om dit probleem te verhelpen, wijzigt u de optie Dubbele netwerkinterfaces gebruiken in **Nee**.

Dit is een probleem omdat Expressway-E luistert naar de XCP-sessie op de verkeerde netwerkinterface, waardoor de verbinding mislukt/uitvalt. Expressway-E luistert op TCP-poort 7400 voor de XCP-sessie. U kunt dit controleren als u de netstatopdracht vanuit de VCS als root.

5. Expressway-E Server Hostname/Domain Name komt niet overeen met wat is geconfigureerd in de _collab-edge SRV

Als de Expressway-E Server hostnaam/domein in de DNS-paginaconfiguratie niet overeenkomt met wat werd ontvangen in het **_collab-edge** SRV antwoord, kan de Jabber client niet communiceren met Expressway-E. De Jabber-client gebruikt het element xmppEdgeServer/Address in de reactie **get_edge_config** om de XMPP-verbinding met Expressway-E tot stand te brengen.

Dit is een voorbeeld van hoe de xmppEdgeServer/Address eruit ziet in de reactie **get_edge_config** van Expressway-E op de Jabber-client:

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

Om dit te voorkomen, zorg ervoor dat de SRV**_collab-edge** record overeenkomt met de Expressway-E hostnaam/domeinnaam. Cisco bug-id CSCuo83458 is voor dit bestand ingediend en gedeeltelijke ondersteuning is toegevoegd aan Cisco bug-id CSCuo82526.

6. Kan niet inloggen vanwege een huidig Webex Connect-abonnement

De logboeken van Jabber voor Windows tonen dit:

```
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]
```

De inlogpogingen worden geleid naar Webex Connect.

Voor een permanente oplossing dient u contact op te nemen met Webex om de website te laten ontmantelen.

Tijdelijke oplossing

Op korte termijn, kunt u één van deze opties gebruiken om het van de raadpleging uit te sluiten.

- Voeg deze parameter toe aan jabber-config.xml. Upload vervolgens het bestand jabber-config.xml naar de TFTP-server op CUCM. Het vereist dat de client eerst intern inlogt.

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

- Vanuit een toepassingsperspectief, stel dit in werking:
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX

  Opmerking: de tweede optie werkt niet voor mobiele apparaten.

- Maak een aanpasbare URL die de WEBEX-service uitsluit:
ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

U kunt meer informatie vinden over de UC-servicedetectie en over de manier waarop u bepaalde services kunt uitsluiten in On-Premises Implementation voor Cisco Jabber 12.8.

7. De Expressway-C Server toont de foutmelding "Configureer maar met fouten. Provisioning server: wachten op informatie over de transversale server."

Als u naar Status > Unified Communications navigeert en de foutmelding ziet, "Configured but with errors. Provisioning server: Waiting for traversal server info." voor Unified CM-registraties en IM&P-service beschikken de interne DNS-server(s) die op Expressway-C zijn geconfigureerd over twee DNS A-records voor Expressway-E. De reden achter meerdere DNS A-records voor de Expressway-E kan zijn dat de betrokken gebruiker is verplaatst van één NIC met statische NAT ingeschakeld op de Expressway-E naar dual-NIC met statische NAT ingeschakeld, of vice versa, en is vergeten de juiste DNS A-record in de interne DNS-server(s) te verwijderen. Daarom, wanneer u het DNS lookup nut in Expressway-C gebruikt en Expressway-E FQDN oplost, merkt u twee DNS A-records op.

Oplossing

Als de Expressway-E NIC is geconfigureerd voor één NIC met statische NAT:

1. Verwijdert de DNS A-record voor het interne IP-adres van Expressway-E in de DNS-server(s) die in Expressway-C zijn geconfigureerd.
2. Spoel het DNS-cachegeheugen in Expressway-C en de gebruikers-pc via CMD (ipconfig /flushdns).
3. Start de Expressway-C server opnieuw op.

Als de Expressway-E NIC is geconfigureerd voor dubbele NIC met statische NAT ingeschakeld:

1. Verwijdert de DNS A-record voor het *externe* IP-adres van Expressway-E in de DNS-server(s) die in Expressway-C zijn geconfigureerd.
2. Spoel het DNS-cachegeheugen in de Expressway-C en de gebruikers-PC via CMD (ipconfig /flushdns).
3. Start de Expressway-C server opnieuw op.,

8. Microsoft Direct Access geïnstalleerd

Als de klant Microsoft DirectAccess op dezelfde pc gebruikt als de Jabber-client, wanneer u probeert op afstand in te loggen, kan dit MRA verbreken. DirectAccess dwingt DNS-vragen om in het interne netwerk te worden getunneld alsof de pc een VPN gebruikte.

> **Opmerking**: Microsoft DirectAccess wordt niet ondersteund met Jabber via MRA. Om het even welke het oplossen van problemen is beste poging. De netwerkbeheerder is verantwoordelijk voor de configuratie van DirectAccess.

Sommige klanten hebben succes gehad door alle DNS-records in de Microsoft DirectAccess Name Resolution Policy Table te blokkeren. Deze records worden niet door DirectAccess verwerkt (Jabber moet deze via openbare DNS met MRA kunnen oplossen):

- SRV-record voor _cisco-uds
- SRV-record voor _cuplogin
- SRV-record voor _collab-edge
- Een record voor alle snelweg Es

9. Expressway-mislukking van omgekeerde DNS-raadplegingen

Beginnend in Versie X8.8, vereist Expressway/VCS voorwaartse en omgekeerde DNS ingangen die voor ExpE, ExpC, en alle knopen CUCM moeten worden tot stand gebracht.

Zie Voorwaarden en softwareafhankelijkheden in de x8.8 Releaseopmerkingen en DNS-records voor mobiele en externe toegang voor alle vereisten.

Als er geen interne DNS-records aanwezig zijn, is er een mogelijke fout in Expressway-logbestanden die verwijzen naar reverseDNSLookup:

```
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-C ontvangt slechts één FQDN bij het opvragen van de PTR-record voor Expressway-E IP. Als het een onjuiste FQDN van DNS ontvangt, toont het deze lijn in de logboeken en ontbreekt:

```
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"
```

Registratieproblemen

Softphone kan niet worden geregistreerd, SIP/2.0 405 methode niet toegestaan

Een diagnostisch logboek van Expressway-C toont een **SIP/2.0 405 Method Not Allowed** bericht in antwoord op de registratieaanvraag die door de Jabber-client is verzonden. Dit is waarschijnlijk te wijten aan een huidige Session Initiation Protocol (SIP) trunk tussen Expressway-C en CUCM met poort 5060/5061.

```
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
```

Om deze kwestie te corrigeren, wijzigt u de SIP-poort op het SIP Trunk-beveiligingsprofiel dat wordt toegepast op de huidige SIP-trunk die in CUCM is geconfigureerd en de Expressway-C-buurzone voor CUCM in een andere poort zoals 5065. Dit wordt verder uitgelegd in deze video. Hier is een configuratiesamenvatting:

CUCM

1. Maak een nieuw SIP Trunk-beveiligingsprofiel met een luisterpoort anders dan 5060 (5065).
2. Maak een SIP Trunk die is gekoppeld aan het SIP Trunk-beveiligingsprofiel en de bestemming die is ingesteld op het IP-adres van Expressway-C, poort 5060.

Autoweg-C

1. Maak een buurzone naar CUCM(s) met een doelpoort anders dan 5060 (5065) om aan de CUCM-configuratie te voldoen.
2. In de **Instellingen** Expressway-C **> Protocollen > SIP**, zorgt u ervoor dat Expressway-C nog steeds op 5060 naar SIP luistert.

Softphone kan niet worden geregistreerd, reden="Unknown domain"

Een diagnostisch logboek van Expressway-C toont Event="**Registration Rejected" Reason="Unknown domain**" Service="SIP" SRC-ip="XXX.XXX.XXX.XXX" SRC-port="51601" Protocol="TCP" AOR="SIP:XXX.XXX.XXX.XXX"

Controleer deze punten om dit probleem op te lossen:

- Gebruikt de Jabber-client een **Beveiligingsprofiel voor een beveiligd apparaat** in CUCM als het niet de bedoeling is een niet-beveiligd Beveiligingsprofiel voor een apparaat te gebruiken?

- Als de Jabber-clients een beveiligd profiel voor apparaatbeveiliging gebruiken, is de naam van het beveiligingsprofiel in FQDN-indeling en is die FQDN-naam ingesteld op het Expressway-C-certificaat als een SAN?

- Als de Jabber-clients een beveiligd beveiligingsprofiel voor een apparaat gebruiken, navigeer dan naar **System > Enterprise Parameters > Security Parameters > Cluster Security Mode** en

controleer of de Cluster Security Mode is ingesteld op 1 om te verifiëren dat het CUCM-cluster is beveiligd. Als de waarde **0** is, moet de beheerder de gedocumenteerde procedure doorlopen om het cluster te beveiligen.

Softphone kan niet worden geregistreerd, reden "Idle countdown expired"

Wanneer u de Expressway-E-logbestanden bekijkt tijdens de tijdlijn die de Jabber-client in een REGISTER-bericht verstuurt, zoekt u naar een **Idle countdown expired** fout zoals aangegeven in het codefragment hier.

```
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"
```

Dit fragment geeft aan dat de firewall poort 5061 open heeft. Er is echter geen verkeer op de toepassingslaag dat in voldoende tijd wordt doorgegeven, zodat de TCP-verbinding wordt gesloten.

Als u deze situatie tegenkomt, is er een hoge mate van waarschijnlijkheid dat de firewall voor Expressway-E de functionaliteit SIP Inspection/Application Layer Gateway (ALG) heeft ingeschakeld. Om dit probleem op te lossen, moet u deze functionaliteit uitschakelen. Als u niet zeker weet hoe u dit moet doen, raadpleegt u de productdocumentatie van uw firewallverkoper.

Voor meer informatie over SIP Inspectie/ALG kunt u Bijlage 4 van de Implementatiegids voor configuratie van Cisco Expressway-E en Expressway-C-Basic raadplegen.

MRA faalt vanwege telefoonproxy geconfigureerd in firmware

Een diagnostisch log van de Expressway-E toont een TLS-onderhandeling fout in poort 5061, maar de SSL-handdruk is geslaagd in poort 8443.

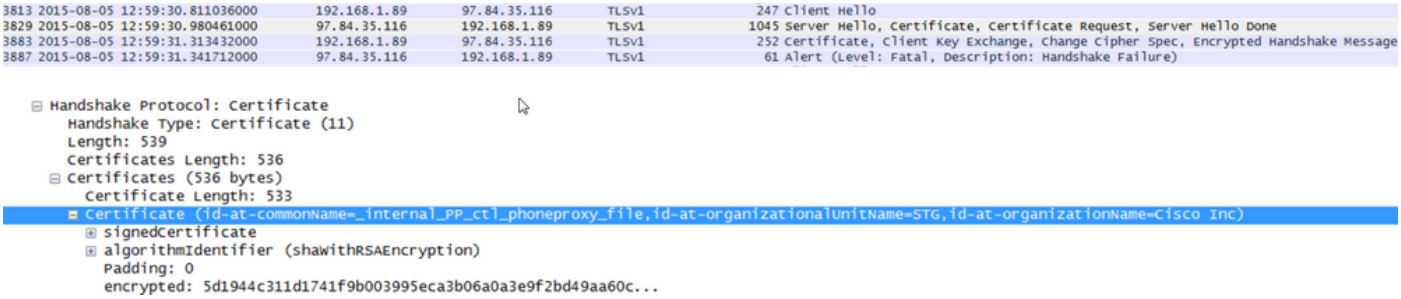
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646" 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"

Logs vanaf Jabber:

-- 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.

De pakketopname van Jabber toont een SSL-onderhandeling met Expressway E IP; het verzonden certificaat komt echter niet van deze server:



De FW heeft een telefoonproxy geconfigureerd.

Oplossing:

Bevestig dat de FW Phone Proxy uitvoert. Om dat te controleren, voert u de **show run policy-map** commando en het toont je iets gelijkaardigs:

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

Schakel telefoonproxy uit voor telefoonservices die succesvol verbinding moeten maken.

Gespreksgerelateerde problemen

Geen media wanneer u via MRA belt

Dit zijn enkele van de afwezige en onjuiste configuraties die dit probleem kunnen veroorzaken in enkele en dubbele NIC-implementaties:

- Statische NAT is niet geconfigureerd in Expressway-E onder System > Network Interfaces > IP. NAT op de netwerklaag moet nog steeds worden uitgevoerd in de firewall, maar deze instelling vertaalt het IP op de toepassingslaag.
- TCP/UDP-poorten zijn niet geopend in de firewall. Raadpleeg voor een lijst met poorten de Configuratiehandleiding voor IP-poortgebruik van Cisco Expressway

Enkelvoudige NIC met statische NAT-implementaties wordt niet aanbevolen. Hier zijn enkele overwegingen om mediaproblemen te voorkomen:

ontbreken

- In de UC-traverse zone moet Expressway-C verwijzen naar het openbare IP-adres dat in Expressway-E is geconfigureerd.
- Media moeten "haarspeld" of reflecteren in de externe firewall. Een configuratievoorbeeld met

een Cisco ASA-firewall kunt u vinden in Configure NAT Reflection on the ASA for the VCS Expressway TelePresence Devices.

Meer informatie over dit onderwerp is te vinden in Bijlage 4 van de implementatiegids voor Cisco Expressway-E en Expressway-C Basic Configuration.

Geen terugbellen wanneer u via MRA naar PSTN belt

Dit probleem is te wijten aan een beperking op Expressways voorafgaand aan Versie X8.5. Cisco bug-id CSC72781 beschrijft hoe Expressway-C geen vroege media doorstuurt in 183 Session Progress of 180 Ringing over de traversale zone. Als u de versies X8.1.x of X8.2.x uitvoert, kunt u upgraden naar Versie X8.5 of als alternatief de hier genoemde tijdelijke oplossing uitvoeren.

Het is mogelijk om een tijdelijke oplossing te gebruiken op het Cisco Unified Border Element (CUBE) als u een SIP-profiel maakt waarmee de 183 wordt omgezet in een 180-profiel en dit op de inkomende dial-peer toepast. Voorbeeld:

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

Daarna zouden ze 180 vroege media uitschakelen op ofwel het SIP-profiel van de **CUCM > CUBE** of de CUBE zelf binnen de sip-ua configuratiemodus.

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

Problemen met CUCM en IM&P

ASCII-fout die toevoeging van CUCM voorkomt

Wanneer u CUCM aan Expressway-C toevoegt, stuit u op een ASCII-fout die de toevoeging van CUCM voorkomt.

Wanneer Expressway-C CUCM aan zijn database toevoegt, doorloopt het een reeks AXL-vragen die betrekking hebben op get en list functies. Voorbeelden hiervan zijn getCallManager, **listCallManager**, **listProcessNode**, **listProcessNodeService** en **getCCMVersion**. Nadat het **getCallManager** proces is uitgevoerd, wordt het gevolgd door een **ExecuteSQLQuery** die is ingesteld om alle CUCM Call Manager-trust of tomcat-trusts op te halen.

Nadat CUCM de query heeft ontvangen en deze uitvoert, rapporteert CUCM vervolgens alle certificaten terug. Als een van de certificaten een niet-ASCII teken bevat, genereert Expressway een fout in de webinterface die vergelijkbaar is met ascii codec can't decode byte 0xc3 in position 42487: ordinal not in range(128).

Dit probleem wordt gevolgd met Cisco bug-id CSCuo5489 en wordt opgelost in versie X8.2.

Uitgaande TLS-fouten op 5061 van Expressway-C naar CUCM in beveiligde implementaties

Dit probleem doet zich voor wanneer u zelfondertekende certificaten gebruikt op CUCM en Tomcat.pem/CallManager.pem hebben hetzelfde onderwerp. Het probleem wordt aangepakt met

Cisco bug-id CSCun30200. De tijdelijke oplossing om het probleem te corrigeren is het verwijderen van de tomcat.pem en het uitschakelen van TLS verify uit de CUCM-configuratie op Expressway-C.

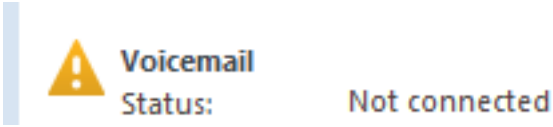
IM&P-server niet toegevoegd en fouten aangetroffen

Wanneer u een IM&P-server toevoegt, meldt Expressway-C: "Deze server is geen IM en Presence Server" of "Kan niet communiceren met .AXL query HTTP-fout "HTTPError:500"", wat ertoe leidt dat de IM&P-server niet wordt toegevoegd.

Als onderdeel van de toevoeging van een IM&P-server gebruikt Expressway-C een AXL-query om de IM&P-certificaten te zoeken in een expliciete map. Wegens Cisco-bug-id CSCul05131 bevinden de certificaten zich niet in die winkel; daarom wordt u geconfronteerd met de valse fout.

Diverse kwesties

Voicemail status op Jabber client toont "geen verbinding"



Om de Jabber-client voicemail-status succesvol te verbinden, moet u het Cisco Unity Connection IP-adres of de hostnaam configureren in de lijst met toegestane HTTP-adressen op Expressway-C.

Om dit van Expressway-C te voltooien, voer de relevante procedure uit:

Procedure voor de versies X8.1 en X8.2

1. Klik op **Configuration > Unified Communications > Configuration > Configure HTTP-server sta lijst toe**.
2. Klik op **Nieuw > Voer IP/Hostname in > Voer een nieuw adres in**.
3. Log uit van de Jabber client en log vervolgens terug in.

Procedure voor versie X8.5

1. Klik op **Configuration > Unified Communications > Unity Connection servers**.
2. Klik op **Nieuw > IP/hostnaam, gebruikersaccountreferenties invoeren > Adres toevoegen**.
3. Log uit van de Jabber client en log vervolgens terug in.

Contact Foto's verschijnen niet op Jabber clients via expressways

De Mobile & Remote Access-oplossing maakt alleen gebruik van UDS voor contactfotoresolutie. Dit vereist dat u een webserver beschikbaar hebt om de foto's op te slaan. De configuratie zelf is tweevoudig.

1. Het bestand jabber-config.xml moet worden aangepast om de clients naar de webserver te sturen voor het oplossen van de foto. De configuratie hier bereikt dit.

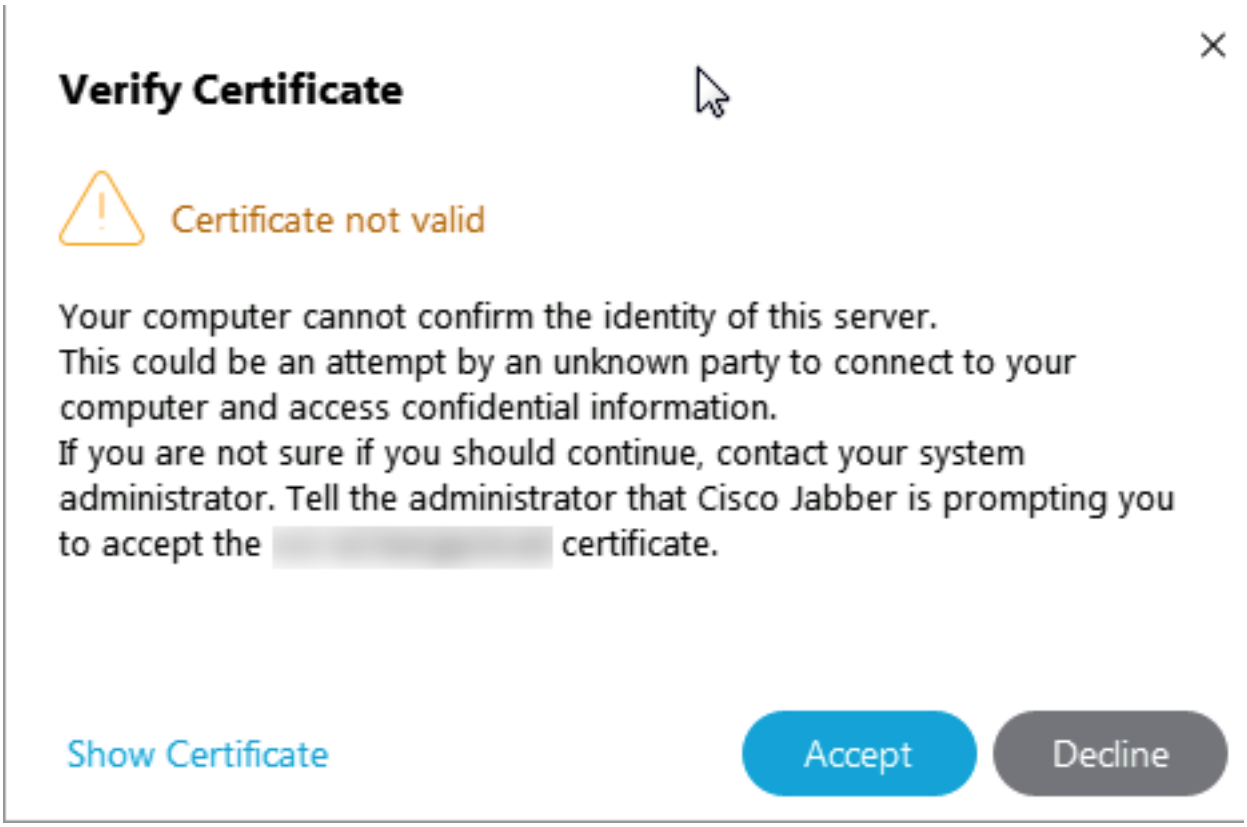
```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%%uid%%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2. Expressway-C moet de webserver hebben die vermeld staat in de HTTP-server Allow List.

   Klik op **Configuration > Unified Communications > Configuration > Configure HTTP-server sta lijst toe**.Klik op **Nieuw > Voer IP/Hostname in > Voer een nieuw adres in**.Log uit van de Jabber client en log vervolgens terug in.

   Opmerking: Raadpleeg voor meer informatie over de UDS Contact Photo-resolutie de Jabber Contact Photo Documentation.

Jabber-clients worden gevraagd om het Expressway-E-certificaat tijdens het inloggen te accepteren



Deze foutmelding kan gerelateerd zijn aan het Expressway Edge-certificaat dat niet is ondertekend door een openbare CA die wordt vertrouwd door het clientapparaat of dat het domein afwezig is als SAN in het servercertificaat.

Om de Jabber client te stoppen met de Expressway certificaatacceptatieprompt, moet u voldoen aan de twee onderstaande criteria:

- Het apparaat/de machine dat de Jabber-client uitvoert, moet de ondertekenaar van het

Expressway-E-certificaat hebben in het bijbehorende certificaatvertrouwensarchief.

Opmerking: dit is eenvoudig te realiseren als u een openbaar certificaat gebruikt omdat mobiele apparaten een grote certificaat trust store bevatten.

- Het Unified CM registratiedomein dat voor de collab-edge record wordt gebruikt, moet in het SAN van het Expressway-E-certificaat aanwezig zijn. CSR tool in de Expressway server geeft u de optie om het Unified CM registratiedomein als een SAN toe te voegen, het is vooraf geladen als het domein is geconfigureerd voor MRA. Als de CA die het certificaat ondertekent een domein niet als SAN accepteert, kunt u ook de optie "CollabEdgeDNS" gebruiken, die het prefix "collab-edge" aan het domein toevoegt:

Gerelateerde informatie

- Gids voor mobiele en externe toegang via expressways
- Implementatiegids voor Cisco Expressway-certificaat maken en gebruiken
- Cisco TelePresence Video Communication Server (Cisco VCS) IP-poortgebruik voor firewalltransmissie
- Implementatie- en installatiehandleiding voor Cisco Jabber
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.