Risoluzione dei problemi più comuni di Collaboration Edge

Sommario

Introduzione

Questo documento descrive come risolvere i problemi più comuni di Collaboration Edge che si verificano durante la fase di distribuzione.

Premesse

Mobile & Remote Access (MRA) è una soluzione di installazione per la funzionalità Jabber VPN (Virtual Private Network-less). Questa soluzione consente agli utenti finali di connettersi alle risorse aziendali interne da qualsiasi parte del mondo. Questa guida è stata redatta per consentire ai tecnici che si occupano della risoluzione dei problemi relativi alla soluzione Collaboration Edge di identificare e risolvere rapidamente i problemi più comuni che si verificano durante la fase di distribuzione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM)
- Cisco Expressway Core
- Cisco Expressway Edge
- Cisco IM e Presence (IM&P)
- Cisco Jabber per Windows
- Cisco Jabber per MAC
- Cisco Jabber per Android
- Cisco Jabber per iOS®
- Certificati di protezione
- Domain Name System (DNS)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Expressway versione X8.1.1 o successiva
- CUCM release 9.1(2)SU1 o successive e IM&P versione 9.1(1) o successive
- Cisco Jabber versione 9.7 o successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problemi di accesso

Jabber non riesce ad accedere tramite MRA

Questo sintomo può essere causato da un'ampia gamma di problemi, alcuni dei quali sono descritti qui.

1. Record del servizio Collaboration Edge (SRV) non creato e/o porta 8443 non raggiungibile

Affinché un client Jabber possa eseguire correttamente il login con MRA, è necessario creare un record SRV del perimetro di collaborazione specifico e renderlo accessibile esternamente. Quando un client Jabber viene avviato inizialmente, esegue query DNS SRV:

1. _cisco-uds: questo record SRV viene utilizzato per determinare se è disponibile un server CUCM.

2. _cuplogin: questo record SRV viene utilizzato per determinare se è disponibile un server IM&P.

3. _collab-edge: questo record SRV viene utilizzato per determinare se è disponibile l'Autorità registrazione integrità.

Se il client Jabber viene avviato e non riceve una risposta SRV per _cisco-uds e _cuplogin e non riceve una risposta per _collab-edge, utilizza questa risposta per tentare di contattare l'Expressway-E elencato nella risposta SRV.

Il record SRV _collab-edge punta al nome di dominio completo (FQDN) di Expressway-E con porta 8443. Se l'SRV _collab-edge non è stato creato, non è disponibile esternamente o è disponibile, ma la porta 8443 non è raggiungibile, il client Jabber non riesce ad eseguire il login.

È possibile verificare se il record SRV _collab-edge è risolvibile e la porta TCP 8443 raggiungibile con SRV Checker in Collaboration Solutions Analyzer (CSA).

Se la porta 8443 non è raggiungibile, è possibile che un dispositivo di sicurezza (firewall) blocchi la porta o che una configurazione errata del gateway predefinito (GW) o delle route statiche in Exp-E.

2. Certificato non accettabile o non disponibile in VCS Expressway

Dopo aver ricevuto una risposta per _collab-edge, il client Jabber contatta Expressway con Transport Layer Security (TLS) sulla porta 8443 per tentare di recuperare il certificato da Expressway per impostare TLS per la comunicazione tra il client Jabber ed Expressway.

Se Expressway non dispone di un certificato firmato valido che contiene il nome di dominio completo (FQDN) o il dominio di Expressway, l'operazione non riuscirà e il client Jabber non riuscirà ad eseguire l'accesso.

Se si verifica questo problema, utilizzare lo strumento Richiesta di firma del certificato (CSR) in Expressway, che include automaticamente il nome di dominio completo (FQDN) di Expressway come nome alternativo del soggetto (SAN).

Nota: l'MRA richiede una comunicazione sicura tra Expressway-C ed Expressway-E e tra Expressway-E ed endpoint esterni.

La tabella seguente con i requisiti dei certificati Expressway per funzionalità è disponibile nella Guida alla distribuzione di MRA:

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. Nessun server UDS trovato nella configurazione Edge

Quando il client Jabber stabilisce una connessione protetta con Expressway-E, richiede la configurazione del perimetro (get_edge_config). Questa configurazione edge contiene i record SRV per _cuplogin e _cisco-uds. Se i record SRV _cisco-uds non vengono restituiti nella configurazione perimetrale, il client Jabber non è in grado di procedere con l'accesso.

Per risolvere questo problema, verificare che i record SRV _cisco-uds siano stati creati internamente e che possano essere risolti da Expressway-C.

Per ulteriori informazioni sui record DNS SRV, vedere la Guida alla distribuzione di MRA per X8.11.

Questo è un sintomo comune anche se si è in un dominio doppio. Se si esegue in un dominio doppio e si rileva che il client Jabber non ha restituito alcun UDS (User Data Service), è necessario confermare che i record SRV _cisco-uds sono stati creati nel DNS interno con il dominio esterno.

Nota: dopo Expressway versione X12.5, non è più necessario aggiungere un record _cisco-UDS SRV al DNS interno. Per ulteriori informazioni su questo miglioramento, vedere la Guida alla distribuzione di Mobile and Remote Access Through Cisco Expressway (X12.5).

---

4. Registri Expressway-C mostrano questo errore: XCP_JABBERD Detail=Unable to connect to host '%IP%', port 7400:(111) Connection Refused

Se il controller NIC (Network Interface Controller) Expressway-E non è configurato correttamente, il server Extensible Communications Platform (XCP) potrebbe non essere aggiornato. Se Expressway-E soddisfa questi criteri, probabilmente si verificherà questo problema:

1. Utilizza una singola scheda NIC.
2. È installato il tasto Opzioni di rete avanzate.
3. L'opzione Usa interfacce di rete doppie è impostata su Sì.

Per risolvere il problema, modificare l'opzione Use Dual Network Interfaces (Usa interfacce di rete doppie) in No.

Il motivo di questo problema è che Expressway-E è in ascolto della sessione XCP sull'interfaccia di rete errata, il che provoca un errore o un timeout della connessione. Expressway-E resta in ascolto sulla porta TCP 7400 per la sessione XCP. Per verificare questa condizione, usare il comando netstat dal software VCS come root.

5. Il nome host/nome di dominio del server Expressway-E non corrisponde alla configurazione in _collab-edge SRV

Se il nome host/dominio del server Expressway-E nella configurazione della pagina DNS non corrisponde a quanto ricevuto nella risposta SRV _collab-edge, il client Jabber non è in grado di comunicare con Expressway-E. Il client Jabber utilizza l'elemento xmppEdgeServer/Address nella risposta get_edge_config per stabilire la connessione XMPP a Expressway-E.

Questo è un esempio di come appare xmppEdgeServer/Address nella risposta get_edge_config da Expressway-E al client Jabber:

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

Per evitare questo problema, verificare che il record SRV _collab-edge corrisponda al nome host/dominio Expressway-E. per questo è stato archiviato l'ID bug Cisco CSCuo83458 ed è stato aggiunto il supporto parziale all'ID bug Cisco CSCuo82526.

6. Impossibile eseguire l'accesso a causa di una sottoscrizione di connessione WebEx corrente

Nei log di Jabber per Windows viene visualizzato quanto segue:

```
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]
```

I tentativi di accesso vengono indirizzati a WebEx Connect.

Per una risoluzione permanente, è necessario contattare WebEx per ottenere la rimozione delle autorizzazioni dal sito.

Soluzione alternativa

Nel breve periodo, è possibile utilizzare una di queste opzioni per escluderla dalla ricerca.

- Aggiungere questo parametro a jabber-config.xml. Quindi caricare il file jabber-config.xml sul server TFTP su CUCM. È necessario che il client esegua prima l'accesso interno.

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

- Dal punto di vista dell'applicazione, eseguire quanto segue: msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX

Nota: la seconda opzione non funziona per i dispositivi mobili.

- Creare un URL selezionabile che escluda il servizio WEBEX: ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

Per ulteriori informazioni sull'individuazione dei servizi UC e su come escludere alcuni servizi, vedere Implementazione locale per Cisco Jabber 12.8.

7. Il server Expressway-C visualizza il messaggio di errore: "Configurato ma con errori. Provisioning server: in attesa di informazioni sul server traversal."

Se si seleziona Stato > Unified Communications e viene visualizzato il messaggio di errore "Configurato ma con errori". Server di provisioning: in attesa di informazioni sul server di attraversamento." per le registrazioni di Unified CM e il servizio IM&P, i server DNS interni configurati in Expressway-C dispongono di due record A DNS per Expressway-E. Il motivo alla base di più record A DNS per Expressway-E potrebbe essere che l'utente interessato si è spostato da una singola NIC con NAT statico abilitato su Expressway-E a una doppia NIC con NAT statico abilitato o viceversa e ha dimenticato di eliminare il record A DNS appropriato nei server DNS interni. Pertanto, quando si utilizza l'utilità di ricerca DNS in Expressway-C e si risolve l'FQDN di Expressway-E, si notano due record A DNS.

Soluzione

Se la scheda di interfaccia di rete Expressway-E è configurata per una singola scheda di interfaccia di rete con NAT statico:

1. Eliminare il record A DNS per l'indirizzo IP interno Expressway-E nei server DNS configurati in Expressway-C.
2. Scaricare la cache DNS in Expressway-C e nel PC utente tramite CMD (ipconfig /flushdns).
3. Riavviare il server Expressway-C.

Se la scheda di interfaccia di rete Expressway-E è configurata per una scheda di interfaccia di rete doppia con NAT statico abilitato:

1. Eliminare il record A DNS per l'indirizzo IP esterno Expressway-E nei server DNS configurati in Expressway-C.
2. Scaricare la cache DNS in Expressway-C e il PC utente tramite CMD (ipconfig /flushdns).
3. Riavviare il server Expressway-C.,

8. Microsoft DirectAccess installato

Se si utilizza Microsoft DirectAccess sullo stesso PC del client Jabber, quando si tenta di eseguire l'accesso in remoto, è possibile che l'MRA venga interrotto. DirectAccess impone l'accesso tramite tunneling delle query DNS alla rete interna come se il PC utilizzasse una VPN.

Nota: Microsoft DirectAccess non è supportato con Jabber su MRA. La risoluzione dei problemi è la cosa migliore. La configurazione di DirectAccess è di responsabilità dell'amministratore di rete.

In alcuni casi è possibile bloccare tutti i record DNS nella tabella dei criteri di risoluzione dei nomi di Microsoft DirectAccess. Questi record non vengono elaborati da DirectAccess (Jabber deve essere in grado di risolverli tramite DNS pubblico con MRA):

- Record SRV per _cisco-uds
- Record SRV per _cuplogin

- Record SRV per _collab-edge
- Record per tutti i tipi di Expressway

9. Ricerche DNS inverse Expressway non riuscite

A partire dalla versione X8.8, Expressway/VCS richiede la creazione di voci DNS forward e reverse per ExpE, ExpC e tutti i nodi CUCM.

Per i requisiti completi, vedere Prerequisiti e dipendenze software nelle note sulla versione x8.8 e nei record DNS per l'accesso remoto e mobile.

Se non sono presenti record DNS interni, è possibile che nei registri Expressway sia presente un errore che fa riferimento a 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 riceve un solo FQDN quando esegue una query sul record PTR per l'indirizzo IP Expressway-E. Se riceve un FQDN errato dal DNS, visualizza questa riga nei registri e ha esito negativo:

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"

Problemi di registrazione

Softphone non è in grado di eseguire la registrazione, SIP/2.0 405 Metodo non consentito

Un log di diagnostica da Expressway-C mostra un messaggio SIP/2.0 405 Method Not Allowed in risposta alla richiesta di registrazione inviata dal client Jabber. Ciò è probabilmente dovuto a un trunk SIP (Session Initiation Protocol) corrente tra Expressway-C e CUCM con porta 5060/5061.

<#root>

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
```

Per risolvere il problema, modificare la porta SIP sul profilo di sicurezza trunk SIP applicato al trunk SIP corrente configurato in CUCM e alla zona adiacente Expressway-C per CUCM su una porta diversa, ad esempio 5065. Questa condizione viene spiegata più avanti in questo video. Di seguito è riportato un riepilogo della configurazione:

CUCM

1. Creare un nuovo profilo di sicurezza trunk SIP con una porta di attesa diversa da 5060 (5065).
2. Creare un trunk SIP associato al profilo di sicurezza trunk SIP e alla destinazione impostata sull'indirizzo IP Expressway-C, porta 5060.

Expressway-C

1. Creare una zona adiacente per CUCM con una porta di destinazione diversa da 5060 (5065) per corrispondere alla configurazione CUCM.
2. In Impostazioni Expressway-C > Protocolli > SIP, assicurarsi che Expressway-C sia ancora in ascolto su 5060 per SIP.

Softphone non può essere registrato, Motivo="Dominio sconosciuto"

In un log di diagnostica da Expressway-C viene visualizzato 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".

Per risolvere il problema, controllare i seguenti punti:

- Il client Jabber utilizza un profilo di sicurezza del dispositivo sicuro in CUCM quando non si intende utilizzare un profilo di sicurezza del dispositivo non sicuro?

- Se i client Jabber utilizzano un profilo di sicurezza del dispositivo protetto, il nome del profilo di sicurezza è in formato FQDN e tale nome FQDN è configurato nel certificato Expressway-C come SAN?

- Se i client Jabber utilizzano un profilo di sicurezza del dispositivo protetto, passare a Sistema > Parametri aziendali > Parametri di sicurezza > Modalità di sicurezza cluster e verificare che la modalità di sicurezza del cluster sia impostata su 1 per verificare che il cluster CUCM sia stato protetto. Se il valore è 0, l'amministratore deve eseguire la procedura documentata per proteggere il cluster.

Impossibile registrare Softphone. Motivo: "Conto alla rovescia inattivo scaduto"

Quando si esaminano i log di Expressway-E durante l'intervallo di tempo inviato dal client Jabber in un messaggio REGISTER, cercare un errore "Inattività conto alla rovescia scaduto" come indicato nel frammento di codice qui.

<#root>

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**

"

Questo frammento indica che il firewall non ha la porta 5061 aperta. Tuttavia, non vi è traffico a livello di applicazione che viene trasmesso in un periodo di tempo sufficiente per cui la connessione TCP viene chiusa.

In questo caso, è molto probabile che il firewall davanti a Expressway-E disponga della funzionalità SIP Inspection/Application Layer Gateway (ALG) attivata. Per risolvere il problema, è necessario disattivare questa funzionalità. In caso di dubbi su come eseguire questa operazione, fare riferimento alla documentazione del fornitore del firewall.

Per ulteriori informazioni su SIP Inspection/ALG, fare riferimento all'Appendice 4 della Guida alla configurazione di base di Cisco Expressway-E ed Expressway-C.

Errore dell'MRA a causa del proxy telefonico configurato nel firmware

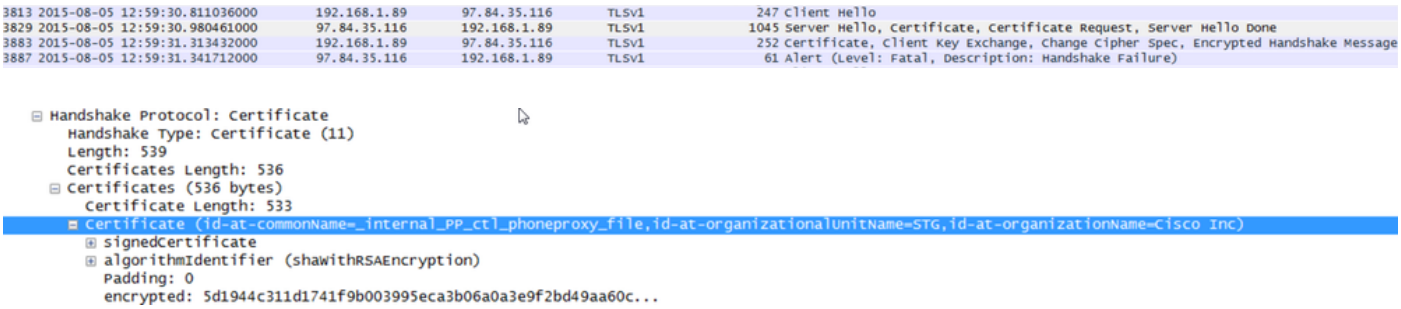
Un log di diagnostica da Expressway-E mostra un errore di negoziazione TLS nella porta 5061, tuttavia l'handshake SSL è riuscito nella porta 8443.

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"

Registri da 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.

L'acquisizione del pacchetto da Jabber mostra una negoziazione SSL con l'indirizzo IP di Expressway E; tuttavia il certificato inviato non proviene da questo server:



Il firmware dispone di un proxy telefonico configurato.

Soluzione:

Confermare che il firmware esegua il proxy telefonico. Per verificare questa condizione, immettere il **show run policy-map** comando che visualizzerà un risultato simile al seguente:

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

Disabilita il proxy telefonico per i servizi telefonici per la connessione.

Problemi correlati alle chiamate

Nessun supporto quando si chiama tramite MRA

Di seguito sono riportate alcune delle configurazioni errate o assenti che possono causare il problema nelle distribuzioni con una o due schede NIC:

- NAT statico non configurato in Expressway-E in Sistema > Interfacce di rete > IP. NAT a livello di rete deve ancora essere eseguito nel firewall, ma questa impostazione traduce l'IP a livello di applicazione.
- Le porte TCP/UDP non sono aperte nel firewall. Per un elenco delle porte, fare riferimento alla Cisco Expressway IP Port Usage Configuration Guide.

Non è consigliabile utilizzare una singola scheda NIC con distribuzioni NAT statiche. Ecco alcune considerazioni per evitare problemi relativi ai supporti:

- Nella zona di attraversamento UC, Expressway-C deve puntare all'indirizzo IP pubblico configurato in Expressway-E.
- I supporti devono essere "hairpin" o riflettere nel firewall esterno. Un esempio di configurazione con un Cisco ASA Firewall è disponibile in Configurazione della riflessione NAT sull'appliance ASA per i dispositivi VCS Expressway TelePresence.

Per ulteriori informazioni su questo argomento, consultare l'Appendice 4 della Guida alla configurazione di base di Cisco Expressway-E ed Expressway-C.

Nessuna richiamata quando l'MRA viene chiamato su PSTN

Questo problema è dovuto a una limitazione di Expressways precedente alla versione X8.5. L'ID bug Cisco CSCua72781 descrive come Expressway-C non inoltra i file multimediali in anticipo nell'avanzamento della sessione 183 o nel ring 180 attraverso la zona trasversale. Se si eseguono le versioni X8.1.x o X8.2.x, è possibile eseguire l'aggiornamento alla versione X8.5 oppure eseguire la soluzione alternativa indicata di seguito.

È possibile utilizzare una soluzione per Cisco Unified Border Element (CUBE) se si crea un profilo SIP che trasforma il 183 in un 180 e lo applica alla connessione peer in ingresso. Ad esempio:

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

In seguito, disabilitavano 180 Early Media sul profilo SIP di CUCM > CUBE o sul CUBE stesso nella modalità di configurazione sip-ua.

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

Problemi CUCM e IM&P

Errore ASCII che impedisce l'aggiunta di CUCM

Quando si aggiunge CUCM a Expressway-C, si verifica un errore ASCII che impedisce l'aggiunta di CUCM.

Quando Expressway-C aggiunge CUCM al proprio database, esegue una serie di query AXL relative alle funzioni get ed list. Esempi di questi includono getCallManager, listCallManager, listProcessNode, listProcessNodeService, e getCCMVersion. Dopo l'esecuzione del processo getCallManager, un set ExecuteSQLQuery riesce a recuperare tutte le attendibilità del gestore delle chiamate CUCM o tutte le attendibilità del gestore delle chiamate CUCM.

Una volta che CUCM riceve la query ed esegue su di essa, CUCM restituisce tutti i propri certificati. Se uno dei certificati contiene un carattere non ASCII, Expressway genera un errore nell'interfaccia Web simile a "ascii codec cannot decode byte 0xc3 in position 42487: ordinal not in range(128)".

Il problema viene rilevato con l'ID bug Cisco CSCuo54489 e risolto nella versione X8.2.

Errori TLS in uscita su 5061 da Expressway-C a CUCM in implementazioni sicure

Questo problema si verifica quando si utilizzano certificati autofirmati in CUCM e Tomcat.pem/CallManager.pem hanno lo stesso oggetto. Il problema è stato risolto con l'ID bug Cisco CSCun30200. Per risolvere il problema, eliminare tomcat.pem e disabilitare la verifica TLS dalla configurazione CUCM su Expressway-C.

Server IM&P non aggiunto e rilevati errori

Quando si aggiunge un server IM&P, Expressway-C segnala "Questo server non è un server IM e Presence" o "Impossibile comunicare con l'errore HTTP query .AXL "HTTPError:500"", che determina la mancata aggiunta del server IM&P.

Nell'ambito dell'aggiunta di un server IM&P, Expressway-C utilizza una query AXL per cercare i certificati IM&P in una directory esplicita. A causa dell'ID bug Cisco CSCul05131, i certificati non sono presenti in tale archivio; è stato quindi rilevato il falso errore.

Problemi vari

Stato Voicemail sul client Jabber indica "Non connesso"

Per configurare lo stato Voicemail del client Jabber in modo che la connessione abbia esito positivo, è necessario configurare l'indirizzo IP o il nome host di Cisco Unity Connection all'interno dell'elenco degli indirizzi HTTP consentiti in Expressway-C.

Per completare questa operazione da Expressway-C, eseguire la procedura appropriata:

Procedura per le versioni X8.1 e X8.2

1. Fare clic su Configurazione > Comunicazioni unificate > Configurazione > Configura elenco server HTTP consentiti.
2. Fare clic su New > Enter IP/Hostname > Create entry (Nuovo > Immettere IP/nome host > Crea voce).
3. Uscire dal client Jabber, quindi accedere nuovamente.

Procedura per la versione X8.5

1. Fare clic su Configurazione > Unified Communications > Unity Connection Server.
2. Fare clic su Nuovo > Immettere IP/Nome host, Credenziali account utente > Aggiungi indirizzo.
3. Uscire dal client Jabber, quindi accedere nuovamente.

Le foto dei contatti non vengono visualizzate sui client Jabber tramite Expressways

La soluzione Mobile & Remote Access utilizza UDS solo per la risoluzione delle foto dei contatti. È quindi necessario disporre di un server Web per l'archiviazione delle foto. La configurazione stessa è duplice.

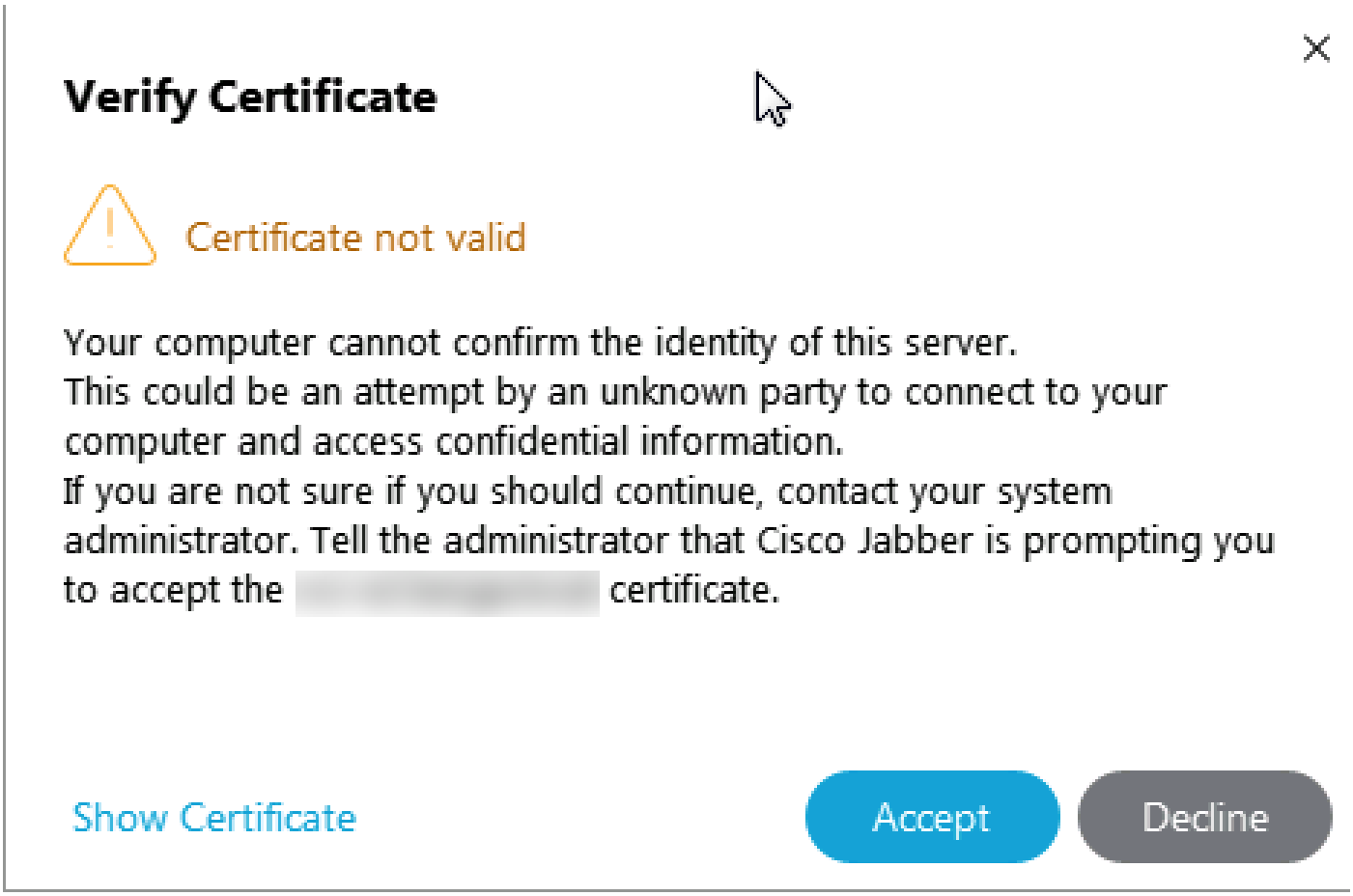
1. È necessario modificare il file jabber-config.xml per indirizzare i client al server Web per la risoluzione delle foto dei contatti. A tale scopo, è necessario eseguire la configurazione descritta di seguito.

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

2. 1. Fare clic su Configurazione > Comunicazioni unificate > Configurazione > Configura elenco server HTTP consentiti.
   2. Fare clic su New > Enter IP/Hostname > Create entry (Nuovo > Immettere IP/nome host > Crea voce).
   3. Uscire dal client Jabber, quindi accedere nuovamente.Expressway-C deve avere il server Web elencato nell'elenco degli indirizzi consentiti del server HTTP.

Nota: per ulteriori informazioni sulla risoluzione delle foto a contatto con UDS, consultare la documentazione della foto a contatto di Jabber.

I client Jabber devono accettare il certificato Expressway-E durante l'accesso



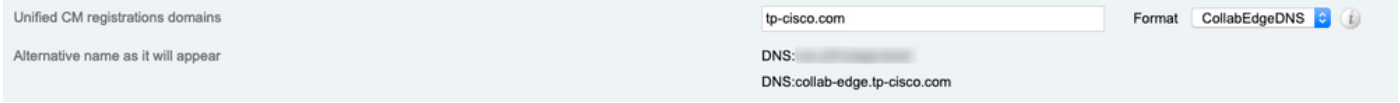
Questo messaggio di errore può essere correlato al certificato Expressway Edge non firmato da una CA pubblica considerata attendibile dal dispositivo client o che il dominio non è presente come SAN nel certificato server.

Per arrestare il client Jabber dalla richiesta di accettazione del certificato di Expressway, è necessario soddisfare i due criteri elencati di seguito:

- Per il dispositivo/computer che esegue il client Jabber il firmatario del certificato Expressway-E deve essere elencato nel relativo archivio certificati attendibili.

> Nota: questa operazione può essere eseguita facilmente se si utilizza un'autorità di certificazione pubblica, in quanto i dispositivi mobili contengono un archivio certificati attendibili di grandi dimensioni.

- Il dominio di registrazione Unified CM utilizzato per il record del margine del laboratorio deve essere presente nella SAN del certificato Expressway-E. Lo strumento CSR nel server Expressway consente di aggiungere il dominio di registrazione CM unificato come SAN. Se il dominio è configurato per MRA, viene precaricato. Se la CA che firma il certificato non accetta un dominio come SAN, è possibile utilizzare anche l'opzione "CollabEdgeDNS", che aggiunge il prefisso "collab-edge" al dominio:



Informazioni correlate

- Guida all'accesso remoto e mobile su Expressways
- Guida alla creazione e all'utilizzo dei certificati Cisco Expressway
- Cisco TelePresence Video Communication Server (Cisco VCS) - Utilizzo della porta IP per il attraversamento del firewall
- Guida all'installazione e alla distribuzione di Cisco Jabber
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).