Résolution des problèmes les plus courants liés à Collaboration Edge

Table des matières

Introduction

Ce document décrit comment résoudre les problèmes les plus courants rencontrés par la périphérie de la collaboration au cours de la phase de déploiement.

Informations générales

Mobile & Remote Access (MRA) est une solution de déploiement pour la fonctionnalité Jabber VPN (Virtual Private Network-less). Cette solution permet aux utilisateurs finaux de se connecter aux ressources internes de l'entreprise où qu'ils se trouvent dans le monde. Ce guide a été rédigé pour permettre aux ingénieurs chargés du dépannage de la solution Collaboration Edge d'identifier et de résoudre rapidement les problèmes les plus courants rencontrés au cours de la phrase de déploiement.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Cisco Expressway Core
- Cisco Expressway Edge
- Cisco IM and Presence (IM&P)
- Cisco Jabber pour Windows
- Cisco Jabber pour MAC
- Cisco Jabber pour Android
- Cisco Jabber pour iOS®
- Certificats de sécurité
- Système de noms de domaine (DNS)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Expressway version X8.1.1 ou ultérieure
- CUCM version 9.1(2)SU1 ou ultérieure et IM&P version 9.1(1) ou ultérieure
- Cisco Jabber version 9.7 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problèmes de connexion

Jabber ne parvient pas à se connecter via MRA

Ce symptôme peut être causé par un large éventail de problèmes, dont quelques-uns sont décrits ici.

1. Enregistrement de service de périphérie de collaboration (SRV) non créé et/ou port 8443 inaccessible

Pour qu'un client Jabber puisse se connecter avec succès avec MRA, un enregistrement SRV de périphérie de collaboration spécifique doit être créé et accessible en externe. Lors du démarrage initial d'un client Jabber, celui-ci émet des requêtes DNS SRV :

1. _cisco-uds : cet enregistrement SRV est utilisé afin de déterminer si un serveur CUCM est disponible.

2. _cuplogin : Cet enregistrement SRV est utilisé afin de déterminer si un serveur IM&P est disponible.

3. _collab-edge : cet enregistrement SRV est utilisé afin de déterminer si MRA est disponible.

Si le client Jabber est démarré et ne reçoit pas de réponse SRV pour _cisco-uds et _cuplogin et ne reçoit pas de réponse pour _collab-edge, il utilise alors cette réponse pour essayer de contacter l'Expressway-E répertorié dans la réponse SRV.

L'enregistrement _collab-edge SRV pointe vers le nom de domaine complet (FQDN) d'Expressway-E avec le port 8443. Si le SRV _collab-edge n'est pas créé, ou n'est pas disponible en externe, ou s'il est disponible, mais que le port 8443 n'est pas accessible, alors le client Jabber ne parvient pas à se connecter.

Vous pouvez vérifier si l'enregistrement SRV _collab-edge peut être résolu et si le port TCP 8443 peut être atteint à l'aide du vérificateur SRV dans Collaboration Solutions Analyzer (CSA).

Si le port 8443 n'est pas accessible, c'est peut-être parce qu'un périphérique de sécurité (pare-feu) bloque le port ou une mauvaise configuration de la passerelle par défaut (GW) ou des routes statiques dans l'Exp-E.

2. Certificat inacceptable ou non disponible sur VCS Expressway

Une fois que le client Jabber a reçu une réponse pour _collab-edge, il contacte alors Expressway avec TLS (Transport Layer Security) sur le port 8443 pour essayer de récupérer le certificat d'Expressway pour configurer TLS pour la communication entre le client Jabber et Expressway.

Si Expressway n'a pas de certificat signé valide qui contient le nom de domaine complet ou le domaine d'Expressway, cela échoue et le client Jabber ne parvient pas à se connecter.

Si ce problème se produit, utilisez l'outil de demande de signature de certificat (CSR) sur Expressway, qui inclut automatiquement le nom de domaine complet d'Expressway comme nom

alternatif de sujet (SAN).

Remarque : l'ARM nécessite une communication sécurisée entre Expressway-C et Expressway-E, ainsi qu'entre Expressway-E et les terminaux externes.

Le tableau suivant avec les exigences de certificat d'Expressway par fonctionnalité se trouve dans le Guide de déploiement 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. Aucun serveur UDS trouvé dans la configuration de périphérie

Une fois que le client Jabber a établi avec succès une connexion sécurisée avec Expressway-E, il demande sa configuration de périphérie (get_edge_config). Cette configuration de périphérie contient les enregistrements SRV pour _cuplogin et _cisco-uds. Si les enregistrements _cisco-uds SRV ne sont pas retournés dans la configuration de périphérie, alors le client Jabber ne peut pas continuer avec la connexion.

Afin de corriger cela, assurez-vous que les enregistrements _cisco-uds SRV sont créés en interne et peuvent être résolus par Expressway-C.

Pour plus d'informations sur les enregistrements DNS SRV, consultez le Guide de déploiement MRA pour X8.11.

C'est également un symptôme courant si vous êtes dans un domaine double. Si vous exécutez dans un domaine double et que vous constatez que le client Jabber n'est retourné par aucun service de données utilisateur (UDS), vous devez confirmer que les enregistrements SRV _cisco-uds sont créés dans le DNS interne avec le domaine externe.

Remarque : après la version X12.5 d'Expressway, il n'est plus nécessaire d'ajouter un enregistrement SRV _cisco-UDS au DNS interne. Pour plus d'informations sur cette amélioration, consultez le Guide de déploiement de l'accès mobile et distant via Cisco Expressway (X12.5).

---

4. Les journaux d'Expressway-C affichent cette erreur : XCP_JABBERD Detail=Impossible de se connecter à l'hôte « %IP% », connexion au port 7400:(111) refusée

Si le contrôleur d'interface réseau (NIC) Expressway-E n'est pas correctement configuré, le serveur XCP (Extensible Communications Platform) peut ne pas être mis à jour. Si Expressway-E répond à ces critères, vous risquez de rencontrer le problème suivant :

1. Utilise une seule carte réseau.
2. La touche d'option de mise en réseau avancée est installée.
3. L'option Use Dual Network Interfaces est définie sur Yes.

Afin de corriger ce problème, changez l'option Use Dual Network Interfaces en No.

Ce problème est dû au fait qu'Expressway-E écoute la session XCP sur la mauvaise interface réseau, ce qui entraîne l'échec/le dépassement du délai de connexion. Expressway-E écoute la session XCP sur le port TCP 7400. Vous pouvez le vérifier si vous utilisez la commande netstat du VCS comme racine.

5. Le nom d'hôte/de domaine du serveur Expressway-E ne correspond pas à ce qui est configuré dans le SRV _collab-edge

Si le nom d'hôte/domaine du serveur Expressway-E dans la configuration de la page DNS ne correspond pas à ce qui a été reçu dans la réponse SRV _collab-edge, le client Jabber ne peut pas communiquer avec Expressway-E. Le client Jabber utilise l'élément xmppEdgeServer/Address dans la réponse get_edge_config pour établir la connexion XMPP à Expressway-E.

Voici un exemple de ce à quoi ressemble xmppEdgeServer/Address dans la réponse get_edge_config d'Expressway-E au client Jabber :

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

Afin d'éviter cela, assurez-vous que l'enregistrement _collab-edge SRV correspond au nom d'hôte/nom de domaine Expressway-E. L'ID de bogue Cisco CSCuo83458 a été classé pour cela et une prise en charge partielle a été ajoutée sur l'ID de bogue Cisco CSCuo82526.

6. Impossible de se connecter en raison d'un abonnement WebEx Connect actuel

Les journaux Jabber pour Windows affichent ceci :

```
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]
```

Les tentatives de connexion sont dirigées vers WebEx Connect.

Pour obtenir une résolution permanente, vous devez contacter WebEx afin de mettre le site hors service.

Solution de contournement

À court terme, vous pouvez utiliser l'une de ces options pour l'exclure de la recherche.

- Ajoutez ce paramètre au fichier jabber-config.xml. Téléchargez ensuite le fichier jabber-config.xml sur le serveur TFTP de CUCM. Il nécessite que le client se connecte d'abord en interne.

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

- Du point de vue de l'application, exécutez ceci :
  msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX

Remarque : la deuxième option ne fonctionne pas pour les appareils mobiles.

- Créez une URL cliquable qui exclut le service WEBEX :
  ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

Vous trouverez plus de détails sur la découverte de services UC et sur la façon d'exclure certains services dans Déploiement sur site pour Cisco Jabber 12.8.

7. Le serveur Expressway-C affiche le message d'erreur suivant : « Configured but with errors ». Provisioning server : attente des informations du serveur de traversée."

Si vous naviguez vers Status > Unified Communications et voyez le message d'erreur, "Configured but with errors. Provisioning server : Waiting for traversal server info." Pour les enregistrements Unified CM et le service IM&P, le ou les serveurs DNS internes configurés sur l'Expressway-C ont deux enregistrements DNS A pour l'Expressway-E. La raison derrière plusieurs enregistrements DNS A pour l'Expressway-E pourrait être que l'utilisateur affecté est passé d'une carte réseau unique avec la NAT statique activée sur l'Expressway-E à une carte réseau double avec la NAT statique activée, ou vice versa, et a oublié de supprimer l'enregistrement DNS A approprié dans le(s) serveur(s) DNS interne(s). Par conséquent, lorsque vous utilisez l'utilitaire de recherche DNS dans l'Expressway-C et résolvez le nom de domaine complet de l'Expressway-E, vous remarquez deux enregistrements DNS A.

Solution

Si la carte réseau Expressway-E est configurée pour une seule carte réseau avec NAT statique :

1. Supprimez l'enregistrement DNS A pour l'adresse IP interne d'Expressway-E dans le ou les serveurs DNS configurés dans l'Expressway-C.
2. Videz le cache DNS dans l'Expressway-C et le PC utilisateur via CMD (ipconfig /flushdns).
3. Redémarrez le serveur Expressway-C.

Si la carte réseau Expressway-E est configurée pour une carte réseau double avec la fonction NAT statique activée :

1. Supprimez l'enregistrement DNS A pour l'adresse IP externe Expressway-E dans le ou les serveurs DNS configurés dans l'Expressway-C.
2. Videz le cache DNS de l'Expressway-C et du PC utilisateur via CMD (ipconfig /flushdns).
3. Redémarrez le serveur Expressway-C.,

8. Microsoft DirectAccess installé

Si vous utilisez Microsoft DirectAccess sur le même PC que le client Jabber, lorsque vous tentez de vous connecter à distance, cela peut interrompre l'ARM. DirectAccess force les requêtes DNS à être tunnellisées vers le réseau interne comme si le PC utilisait un VPN.

Remarque : Microsoft DirectAccess n'est pas pris en charge avec Jabber sur MRA. Tout dépannage est le meilleur effort. La configuration de DirectAccess relève de la responsabilité de l'administrateur réseau.

Vous pouvez parfois bloquer tous les enregistrements DNS dans la table de stratégie de résolution de noms Microsoft DirectAccess. Ces enregistrements ne sont pas traités par DirectAccess (Jabber doit être en mesure de les résoudre via un DNS public avec MRA) :

- Enregistrement SRV pour _cisco-uds
- Enregistrement SRV pour _cuplogin

- Enregistrement SRV pour _collab-edge
- Un record pour tous les Expressway Es

9. Échec des recherches DNS inversées d'Expressway

À partir de la version X8.8, Expressway/VCS nécessite la création d'entrées DNS avant et arrière pour ExpE, ExpC et tous les noeuds CUCM.

Pour connaître la configuration requise, reportez-vous à Prerequisites and Software Dependencies in the x8.8 Release Notes and DNS Records for Mobile and Remote Access.

Si les enregistrements DNS internes ne sont pas présents, il y a une erreur possible dans les journaux Expressway qui font référence à 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 ne reçoit qu'un seul nom de domaine complet lors de l'interrogation de l'enregistrement PTR pour l'adresse IP d'Expressway-E. S'il reçoit un nom de domaine complet incorrect du DNS, il affiche cette ligne dans les journaux et échoue :

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"

Problèmes d'enregistrement

Le téléphone logiciel ne peut pas s'enregistrer, méthode SIP/2.0 405 non autorisée

Un journal de diagnostic d'Expressway-C affiche un message SIP/2.0 405 Method Not Allowed en réponse à la demande d'enregistrement envoyée par le client Jabber. Cela est probablement dû à une liaison SIP (Session Initiation Protocol) actuelle entre Expressway-C et CUCM avec le port 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
```

Afin de corriger ce problème, changez le port SIP sur le profil de sécurité de la ligne principale SIP qui est appliqué à la ligne principale SIP actuelle configurée dans CUCM et la zone voisine d'Expressway-C pour CUCM vers un port différent tel que 5065. Ceci est expliqué plus en détail dans cette vidéo. Voici un résumé de la configuration :

CUCM

1. Créez un nouveau profil de sécurité de ligne principale SIP avec un port d'écoute autre que 5060 (5065).
2. Créez une ligne principale SIP associée au profil de sécurité de ligne principale SIP et à la destination définie sur l'adresse IP Expressway-C, port 5060.

Expressway-C

1. Créez une zone voisine vers CUCM(s) avec un port cible autre que 5060 (5065) pour correspondre à la configuration CUCM.
2. Dans Expressway-C Settings > Protocols > SIP, assurez-vous que Expressway-C écoute toujours le SIP sur 5060.

Le téléphone logiciel ne peut pas s'enregistrer, raison="Domaine inconnu"

Un journal de diagnostic d'Expressway-C indique 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".

Afin de corriger ce problème, vérifiez ces points :

- Le client Jabber utilise-t-il un profil de sécurité de périphérique sécurisé dans CUCM lorsque l'intention n'est pas d'utiliser un profil de sécurité de périphérique non sécurisé ?

- Si les clients Jabber utilisent un profil de sécurité de périphérique sécurisé, le nom du profil de sécurité est-il au format FQDN et ce nom est-il configuré sur le certificat Expressway-C en tant que SAN ?

- Si les clients Jabber utilisent un profil de sécurité de périphérique sécurisé, accédez à System > Enterprise Parameters > Security Parameters > Cluster Security Mode et vérifiez que le Cluster Security Mode est défini sur 1 afin de vérifier que le cluster CUCM a été sécurisé. Si la valeur est 0, l'administrateur doit suivre la procédure documentée pour sécuriser le cluster.

Le téléphone logiciel ne peut pas s'enregistrer, raison "Le compte à rebours inactif a expiré"

Lorsque vous examinez les journaux Expressway-E pendant la période que le client Jabber envoie dans un message REGISTER, recherchez une erreur "Idle countdown expiré" comme indiqué dans l'extrait de code ici.

<#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

"

Cet extrait indique que le port 5061 du pare-feu est ouvert ; cependant, aucun trafic de couche application n'est transmis suffisamment longtemps pour que la connexion TCP se ferme.

Si vous rencontrez cette situation, il est fort probable que la fonctionnalité SIP Inspection/Application Layer Gateway (ALG) soit activée sur le pare-feu situé en face d'Expressway-E. Afin de résoudre ce problème, vous devez désactiver cette fonctionnalité. Si vous ne savez pas comment procéder, reportez-vous à la documentation produit de votre fournisseur de pare-feu.

Pour plus d'informations sur SIP Inspection/ALG, vous pouvez consulter l'Annexe 4 du Guide de déploiement de configuration de base de Cisco Expressway-E et Expressway-C.

Échec de MRA en raison de la configuration du proxy téléphonique dans le micrologiciel

Un journal de diagnostic de l'Expressway-E indique un échec de négociation TLS sur le port 5061, mais la connexion SSL a réussi sur le port 8443.

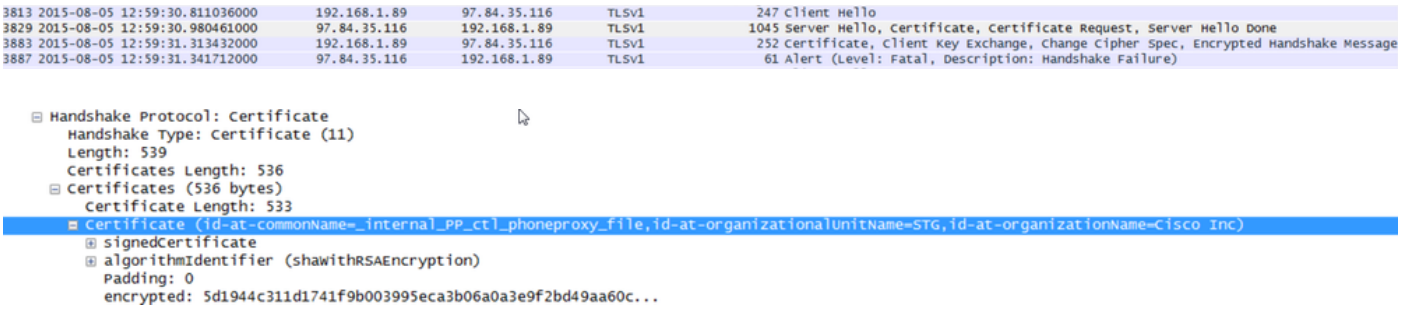
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646"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

Journaux de 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.

La capture de paquets à partir de Jabber montre une négociation SSL avec l'IP Expressway E ;

cependant le certificat envoyé ne provient pas de ce serveur :



Le proxy téléphonique du pare-feu est configuré.

Solution :

Vérifiez que le pare-feu exécute le proxy téléphonique. Afin de vérifier cela, entrez la commande, **show run policy-map** et elle vous montre quelque chose de similaire à :

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

Désactivez le proxy téléphonique pour que les services téléphoniques se connectent correctement.

Problèmes liés aux appels

Aucun média lorsque vous appelez via MRA

Voici quelques-unes des configurations absentes et incorrectes qui peuvent causer ce problème dans les déploiements de carte réseau simple et double :

- La fonction NAT statique n'est pas configurée dans l'Expressway-E sous System > Network Interfaces > IP. La NAT au niveau de la couche réseau doit toujours être effectuée dans le pare-feu, mais ce paramètre traduit l'IP au niveau de la couche application.
- Les ports TCP/UDP ne sont pas ouverts dans le pare-feu. Pour obtenir la liste des ports, reportez-vous au Guide de configuration de l'utilisation des ports IP de Cisco Expressway.

Une carte réseau unique avec des déploiements NAT statiques n'est pas recommandée. Voici quelques considérations pour éviter les problèmes de support :

- Dans la zone de traversée UC, Expressway-C doit pointer vers l'adresse IP publique configurée dans l'Expressway-E.
- Le support doit être « hairpin » ou refléter dans le pare-feu externe. Un exemple de configuration avec un pare-feu Cisco ASA est disponible dans Configurer la réflexion NAT sur l'ASA pour les périphériques de téléprésence VCS Expressway.

Pour plus d'informations à ce sujet, reportez-vous à l'Annexe 4 du Guide de déploiement de la configuration de base de Cisco Expressway-E et Expressway-C.

Pas de retour d'appel lorsque Call Over MRA vers PSTN

Ce problème est dû à une limitation sur Expressways antérieure à la version X8.5. Le bogue Cisco CSCua72781 décrit comment Expressway-C ne transfère pas les premiers supports dans 183 Session Progress ou 180 Ringing à travers la zone de traversée. Si vous exécutez les versions X8.1.x ou X8.2.x, vous pouvez effectuer une mise à niveau vers la version X8.5 ou effectuer la solution de contournement indiquée ici.

Il est possible d'utiliser une solution de contournement sur Cisco Unified Border Element (CUBE) si vous créez un profil SIP qui transforme le 183 en un 180 et l'applique sur le terminal de numérotation dial-peer entrant. Exemple :

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

Ensuite, ils désactivent 180 Early Media sur le profil SIP de CUCM > CUBE ou sur le CUBE lui-même dans le mode de configuration sip-ua.

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

Problèmes CUCM et IM&P

Erreur ASCII qui empêche l'ajout de CUCM

Lorsque vous ajoutez CUCM à Expressway-C, vous rencontrez une erreur ASCII qui empêche l'ajout de CUCM.

Lorsque Expressway-C ajoute CUCM à sa base de données, il exécute une série de requêtes AXL relatives aux fonctions get et list. Par exemple, getCallManager, listCallManager, listProcessNode, listProcessNodeService et getCCMVersion. Une fois que le processus getCallManager est exécuté, il est remplacé par un jeu ExecuteSQLQuery pour récupérer toutes les approbations de CUCM Call Manager ou tomcat.

Une fois que CUCM reçoit la requête et l'exécute, CUCM renvoie tous ses certificats. Si l'un des certificats contient un caractère non-ASCII, Expressway génère une erreur dans l'interface Web semblable à "le codec ascii ne peut pas décoder l'octet 0xc3 à la position 42487 : ordinal not in range(128)".

Ce problème est suivi avec l'ID de bogue Cisco CSCuo5489 et est résolu dans la version X8.2.

Défaillances TLS sortantes sur 5061 d'Expressway-C vers CUCM dans des déploiements sécurisés

Ce problème se produit lorsque vous utilisez des certificats auto-signés sur CUCM et que Tomcat.pem/CallManager.pem ont le même objet. Le problème est résolu avec l'ID de bogue Cisco CSCun30200. La solution de contournement pour corriger le problème est de supprimer tomcat.pem et de désactiver la vérification TLS de la configuration CUCM sur Expressway-C.

Serveur IM&P non ajouté et erreurs rencontrées

Lorsque vous ajoutez un serveur IM&P, Expressway-C signale « Ce serveur n'est pas un serveur IM&P » ou « Impossible de communiquer avec l'erreur HTTP de requête .AXL « HTTPError : 500 », ce qui a pour conséquence de ne pas ajouter le serveur IM&P.

Dans le cadre de l'ajout d'un serveur IM&P, Expressway-C utilise une requête AXL pour rechercher les certificats IM&P dans un répertoire explicite. En raison de l'ID de bogue Cisco CSCul05131, les certificats ne sont pas dans ce magasin ; par conséquent, vous rencontrez l'erreur false.

Problèmes divers

L'état de la messagerie vocale sur le client Jabber indique « Non connecté »

Pour que l'état de la messagerie vocale du client Jabber se connecte correctement, vous devez configurer l'adresse IP ou le nom d'hôte de Cisco Unity Connection dans la liste d'autorisation HTTP sur Expressway-C.

Afin de compléter ceci à partir d'Expressway-C, effectuez la procédure appropriée :

Procédure pour les versions X8.1 et X8.2

1. Cliquez sur Configuration > Unified Communications > Configuration > Configure HTTP server allow list.
2. Cliquez sur New > Enter IP/Hostname > Create entry.
3. Déconnectez-vous du client Jabber, puis reconnectez-vous.

Procédure pour la version X8.5

1. Cliquez sur Configuration > Unified Communications > Unity Connection Servers.
2. Cliquez sur New > Enter IP/Hostname, User account credentials > Add Address.
3. Déconnectez-vous du client Jabber, puis reconnectez-vous.

Les photos de contact n'apparaissent pas sur les clients Jabber via Expressways

La solution Mobile & Remote Access utilise uniquement UDS pour la résolution des photos de contact. Pour cela, vous devez disposer d'un serveur Web pour stocker les photos. La configuration elle-même est double.

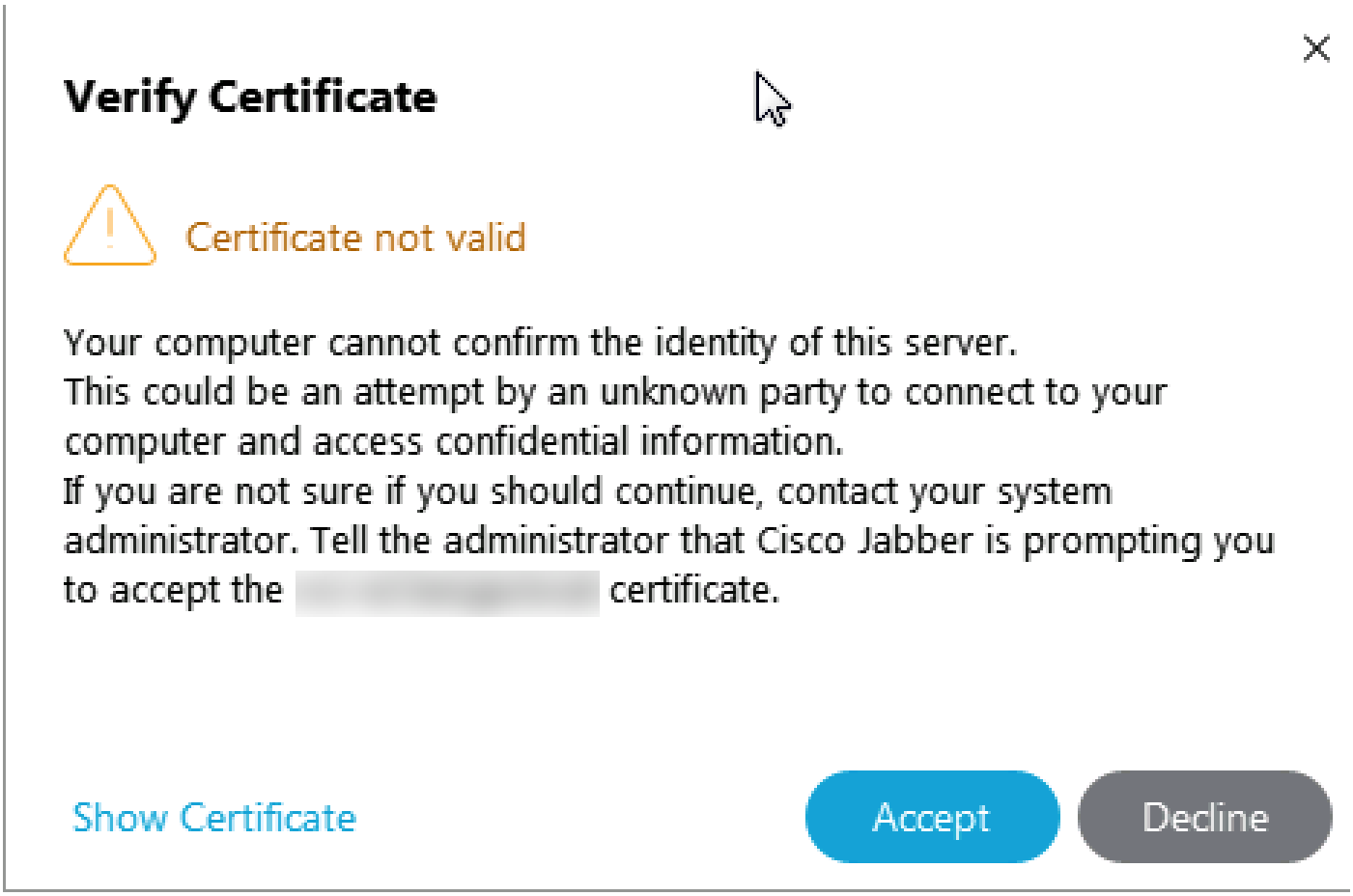
1. Le fichier jabber-config.xml doit être modifié pour diriger les clients vers le serveur Web pour la résolution de la photo du contact. La configuration ici permet d'atteindre cet objectif.

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

2. 1. Cliquez sur Configuration > Unified Communications > Configuration > Configure HTTP server allow list.
   2. Cliquez sur New > Enter IP/Hostname > Create entry.
   3. Déconnectez-vous du client Jabber, puis reconnectez-vous.Le serveur Web d'Expressway-C doit figurer dans la liste verte des serveurs HTTP.

Remarque : pour plus d'informations sur la résolution de la photo de contact UDS, reportez-vous à la documentation de la photo de contact Jabber.

Les clients Jabber sont invités à accepter le certificat Expressway-E lors de la connexion



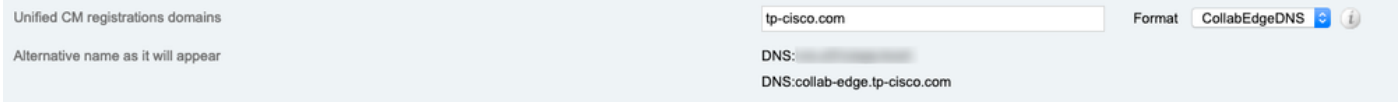
Ce message d'erreur peut être lié au certificat Expressway Edge non signé par une autorité de certification publique qui est approuvée par le périphérique client ou que le domaine est absent en tant que SAN dans le certificat du serveur.

Pour arrêter le client Jabber à l'invite d'acceptation du certificat Expressway, vous devez remplir les deux critères suivants :

- Le périphérique/l'ordinateur qui exécute le client Jabber doit avoir le signataire du certificat Expressway-E répertorié dans son magasin de certificats de confiance.

> Remarque : cette opération est facile si vous utilisez une autorité de certification publique, car les appareils mobiles contiennent un grand magasin de certificats de confiance.

- Le domaine d'enregistrement Unified CM utilisé pour l'enregistrement de périphérie de collaboration doit être présent dans le SAN du certificat Expressway-E. L'outil CSR du serveur Expressway vous donne la possibilité d'ajouter le domaine d'enregistrement Unified CM en tant que SAN, il est préchargé si le domaine est configuré pour MRA. Si l'autorité de certification qui signe le certificat n'accepte pas un domaine en tant que SAN, vous pouvez également utiliser l'option « CollabEdgeDNS », qui ajoute le préfixe « collab-edge » au domaine :



Informations connexes

- Guide d'accès mobile et à distance sur Expressways
- Guide de déploiement de création et d’utilisation de certificats Cisco Expressway
- Utilisation des ports IP du serveur Cisco TelePresence Video Communication Server (Cisco VCS) pour la traversée du pare-feu
- Guide de déploiement et d'installation de Cisco Jabber
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.