Périphérie de Collaboration la plupart des problèmes courants

Contenu

Introduction

Le mobile et l'Accès à distance (MRA) est une solution de déploiement pour la capacité sans réseau privée virtuelle du Jabber (VPN). Cette solution permet à des utilisateurs finaux pour se connecter aux ressources de l'entreprise internes à partir de n'importe où dans le monde. Ce guide a été écrit pour donner les ingénieurs qui dépannent la solution de périphérie de Collaboration la capacité pour les identifier rapidement et résoudre la plupart des problèmes courants les clients font face pendant l'expression de déploiement.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Noyau de Cisco Expressway
- Périphérie de Cisco Expressway
- Cisco IM et présence (IM&P)
- Cisco Jabber pour Windows
- Cisco Jabber pour Mac
- Cisco Jabber pour Android
- Cisco Jabber pour l'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 :

- Version X8.1.1 d'Expressway ou plus tard
- Version 9.1(2)SU1 CUCM ou plus tard et version 9.1(1) ou ultérieures IM&P
- Version 9.7 ou ultérieures de Cisco Jabber

Questions de procédure de connexion

Jabber incapable de se connecter par MRA

Ce symptôme peut sont provoqué par par un large éventail de questions, quelques uns dont sont tracés les grandes lignes ici.

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

Pour qu'un client de Jabber puisse ouvrir une session avec succès avec MRA, un enregistrement SRV spécifique de périphérie de Collaboration doit être créé et accessible extérieurement. Quand

un client de Jabber est au commencement commencé, il fait des requêtes des DN 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 de Jabber est commencé et ne reçoit pas de réponse SRV pour les **_cisco-uds** et le **_cuplogin** et reçoit une réponse pour le **_collab-edge**, alors il emploie cette réponse pour essayer d'entrer en contact avec Expressway-e répertorié dans la réponse SRV.

L'enregistrement SRV de **_collab-edge** devrait indiquer le nom de domaine complet (FQDN) d'Expressway-e avec le port **8443**. Si le **_collab-edge** SRV n'est pas créé, ou n'est pas extérieurement disponible, ou si c'est disponible, mais le port 8443 n'est pas accessible, alors le client de Jabber n'ouvre pas une session.

Vous pouvez confirmer si l'enregistrement SRV de **_collab-edge** est résoluble et le port TCP 8443 accessible utilisant le contrôleur SRV dans l'analyseur de solutions de Collaboration (CSA).

Si le port 8443 n'est pas accessible, ceci pourrait être dû à un périphérique de sécurité (Pare-feu) bloquant le port ou une mauvaise configuration des artères de la passerelle par défaut (gw) ou de la charge statique dans l'exp-e.

2. Certificat inacceptable ou aucun disponible sur le VCS Expressway

Après que le client de Jabber ait reçu une réponse pour le **_collab-edge**, il entre en contact avec alors Expressway avec le Transport Layer Security (TLS) au-dessus du port 8443 pour essayer de récupérer le certificat d'Expressway pour installer le TLS pour la transmission entre le client de Jabber et Expressway.

Si Expressway n'a pas un certificat signé valide qui contient le FQDN ou le domaine d'Expressway, alors ceci échoue et le client de Jabber n'ouvre pas une session.

Si cette question se produit, le client devrait utiliser l'outil de la demande de signature de certificat (CSR) sur Expressway, qui inclut automatiquement le FQDN d'Expressway comme nom alternatif soumis (SAN).

> Remarque: MRA exige la communication protégée entre Expressway-C et Expressway-e, et entre Expressway-e et les points finaux externes.

La prochaine table avec les conditions requises de certificat d'Expressway par la caractéristique peut être trouvée du 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 serveurs UDS trouvés dans la configuration de périphérie

Après que le client de Jabber établisse 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 le **_cuplogin** et les **_cisco-uds**. Si les enregistrements SRV de **_cisco-uds** ne sont pas renvoyés dans la configuration de périphérie, alors le client de Jabber ne peut pas procéder à la procédure de connexion.

Afin de réparer ceci, assurez-vous que des enregistrements SRV de **_cisco-uds** sont créés intérieurement et résoluble par Expressway-C.

Plus d'informations sur les enregistrements SRV de DN peuvent être trouvées du guide de déploiement MRA pour X8.11.

C'est également un symptôme commun si vous êtes dans un double domaine. Si vous vous exécutez dans un double domaine et trouvez le client de Jabber n'est pas retourné n'importe quel service de données d'utilisateur (UDS), vous devez confirmer que les enregistrements SRV de _cisco-uds sont créés dans les DN internes avec le domaine externe.

> Remarque: Après la version X12.5 d'Expressway, ce n'est plus une condition requise d'ajouter un enregistrement SRV de _cisco-UDS aux DN internes. Pour plus d'informations sur cette amélioration, voyez le mobile et l'Accès à distance par le guide de déploiement de Cisco Expressway (X12.5).

4. Les logs d'Expressway-C affichent cette erreur : XCP_JABBERD Detail= " incapable de se connecter pour héberger « %IP% », connexion du port 7400:(111) refusée »

Si le contrôleur d'interface réseau d'Expressway-e (NIC) est inexactement configuré, ceci peut rendre le serveur extensible de la plate-forme de transmissions (XCP) mis à jour. Si Expressway-e répond à ces critères, alors vous rencontrerez probablement cette question :

1. Utilise un NIC simple.
2. La touche option avancée de réseau est installée.
3. La double option d'interfaces réseau d'utilisation est placée à **oui**.

Afin de corriger ce problème, changez la double option d'interfaces réseau d'utilisation à **non.**

La raison que c'est un problème est parce qu'Expressway-e écoute la session XCP sur l'interface réseau fausse, qui entraîne échouer de connexion pour/délai d'attente. Expressway-e écoute sur

le port TCP 7400 la session XCP. Vous pouvez vérifier ceci si vous utilisez`netstat` la commande du VCS comme racine.

5. L'adresse Internet/nom de domaine de serveur d'Expressway-e n'apparie pas ce qui est configuré dans le _collab-edge SRV

Si l'adresse Internet/domaine de serveur d'Expressway-e dans la configuration de page de DN n'apparie pas ce qui a été reçu dans la réponse du **_collab-edge** SRV, le client de Jabber ne peut pas communiquer avec Expressway-e. Le client de Jabber emploie le xmppEdgeServer/élément d'adresse en réponse de **get_edge_config** pour établir la connexion XMPP à Expressway-e.

C'est un exemple de ce que ressemble au xmppEdgeServer/adresse dans la réponse de **get_edge_config d'**Expressway-e au client de Jabber :

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

Afin d'éviter ceci, assurez-vous que l'enregistrement SRV de **_collab-edge** apparie l'adresse Internet/nom de domaine d'Expressway-e. L'ID de bogue Cisco CSCuo83458 a été classé pour ceci et le support partiel a été ajouté sur l'ID de bogue Cisco CSCuo82526.

6. Incapable d'ouvrir une session en raison d'un abonnement existant de WebEx Connect

Le Jabber pour des logs de 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://loginp.webexconnect.com;
Url: http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com';;;.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://loginp.webexconnect.com/cas/FederatedSSO?org=example.com2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]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://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]
success: [true] configStoreName: [LocalFileConfigStore]
```

Les tentatives de procédure de connexion sont dirigées vers le WebEx Connect.

Pour une résolution permanente, vous devez entrer en contact avec le WebEx afin de faire désarmer le site.

Solution de contournement

Àcourt terme, vous pouvez utiliser une de ces options de l'exclure de la consultation.

- Ajoutez ce paramètre au jabber-config.xml. Téléchargez alors le fichier jabber-config.xml au serveur TFTP sur CUCM. Il exige que le client ouvre une session intérieurement d'abord.

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

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

  Remarque: La deuxième option ne fonctionne pas pour des périphériques mobiles.

- Créez un URL clickable qui exclura le service de WEBEX :
  ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX

Vous pouvez trouver plus de détails au sujet de la détection de service UC et comment exclure quelques services dans le déploiement de Sur-sites pour le Cisco Jabber 12.8.

7. Le serveur d'Expressway-C affiche le message d'erreur : « Configuré mais avec des erreurs. Serveur de mise en service : Attendre les informations du serveur de traversée. »

Si vous naviguez vers l'état > des transmissions unifiées et voyez le message d'erreur, "Configured but with errors. Provisioning server: Waiting for traversal server info." pour des enregistrements d'Unified CM et le service IM&P, les serveurs de DN internes configurés sur Expressway-C ayez deux enregistrements des DN A pour Expressway-e. La raison derrière de plusieurs enregistrements des DN A pour Expressway-e a pu être l'utilisateur affecté déplacé du NIC simple avec NAT statique activé sur Expressway-e au double-NIC avec activée NAT statique, ou vice versa, et a oublié de supprimer l'enregistrement approprié des DN A dans les serveurs de DN internes. Par conséquent, quand vous utilisez l'utilitaire de consultation de DN dans Expressway-C et résolvez le FQDN d'Expressway-e, vous noterez deux enregistrements des DN A.

Solution

Si le NIC d'Expressway-e est configuré pour un NIC simple avec NAT statique :

1. Supprimez les DN un enregistrement pour Expressway-e l'adresse IP qu'interne dans les serveurs de DN a configuré dans Expressway-C.
2. Videz le cache DNS dans Expressway-C et le PC de l'utilisateur par l'intermédiaire du CMD (ipconfig /flushdns).
3. Redémarrez le serveur d'Expressway-C.

Si le NIC d'Expressway-e est configuré pour le double NIC avec NAT statique activé :

1. Supprimez les DN un enregistrement pour Expressway-e l'adresse IP qu'*externe* dans les serveurs de DN a configuré dans Expressway-C.
2. Videz le cache DNS dans Expressway-C et le PC de l'utilisateur par l'intermédiaire du CMD (ipconfig /flushdns).
3. Redémarrez le serveur d'Expressway-C.

8. Microsoft DirectAccess a installé

Le client pourrait utiliser Microsoft DirectAccess sur le même PC que le client de Jabber. Quand vous tentez d'ouvrir une session à distance, ceci peut interrompre MRA. DirectAccess forcera des requêtes DNS à percer un tunnel dedans au réseau interne comme si le PC utilisait un VPN.

> Remarque: Microsoft DirectAccess n'est pas pris en charge avec le Jabber au-dessus de MRA. N'importe quel dépannage est meilleur effort. La configuration de DirectAccess est la responsabilité de l'administrateur réseau.

Quelques clients ont eu le succès en bloquant tous les enregistrements DNS dans le Tableau de stratégie de résolution de noms de Microsoft DirectAccess. Ces enregistrements ne devraient pas être traités par DirectAccess (le Jabber doit pouvoir résoudre ces derniers par l'intermédiaire des DN publics en utilisant MRA) :

- Enregistrement SRV pour des _cisco-uds
- Enregistrement SRV pour le _cuplogin
- Enregistrement SRV pour le _collab-edge
- Un enregistrement pour tout l'Expressway es

9. Les consultations de DN d'inverse d'Expressway échoue

Commençant dans la version X8.8, Expressway/VCS exige en avant et des entrées DNS inverses à créer pour ExpE, ExpC, et tous les Noeuds CUCM.

Pour de pleines conditions requises, voir des conditions préalables et les dépendances de logiciel dans les notes de mise à jour x8.8 et les enregistrements DNS pour le mobile et l'Accès à distance.

Si les enregistrements DNS internes ne sont pas présents, vous pourriez voir une erreur dans les logs d'Expressway qui se rapportent au 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 devrait seulement recevoir un FQDN en questionnant l'enregistrement PTR pour l'IP d'Expressway-e. S'il reçoit un FQDN incorrect des DN, il affichera cette ligne dans les logs et échouera :

```
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
host.example.com"
```

Questions d'enregistrement

Le téléphone IP ne peut pas s'enregistrer, la méthode SIP/2.0 405 non permise

Un log diagnostique d'Expressway-C affiche **SIP/2.0 405 Method Not Allowed** un message en réponse à la demande d'enregistrement envoyée par le client de Jabber. C'est vraisemblablement dû à un joncteur réseau d'Initiation Protocol de session existante (SIP) entre Expressway-C et CUCM utilisant le port 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
```

Afin de corriger cette question, changez le port de SIP sur le profil de Sécurité de joncteur réseau de SIP qui est appliqué au

joncteur réseau existant de SIP configuré dans CUCM et à la zone voisine d'Expressway-C pour CUCM à un port différent tel que 5065. Ceci est expliqué plus loin dans ce vidéo. Voici un résumé de configuration :

CUCM

1. Créez un nouveau profil de Sécurité de joncteur réseau de SIP avec un port en mode écoute autre que 5060 (5065).
2. Créez un joncteur réseau de SIP associé au profil et à la destination de Sécurité de joncteur réseau de SIP réglés à l'adresse IP d'Expressway-C, le port 5060.

Expressway-C

1. Créez une zone voisine à CUCM avec un port de destination autre que 5060 (5065) pour apparier la configuration CUCM.
2. Dans des **configurations > des protocoles > le SIP d'**Expressway-C, assurez-vous qu'Expressway-C écoute toujours sur 5060 le SIP.

Le téléphone IP ne peut pas s'enregistrer, Reason="Unknown domain"

Un log diagnostique Expressway-C sip du ""**Registration Rejected" Reason="Unknown domain"** TCP » AOR= " " XXX.XXX.XXX.XXX » Src-port="51601" Protocol= de Src-ip= de " SIP » d'Event= expositions de Service= : XXX.XXX.XXX.XXX ».

Afin de corriger cette question, vérifiez ces points :

- Le client de Jabber utilise-il un **profil de sécurité des périphériques sécurisé** dans CUCM quand l'intention n'est pas d'utiliser un profil de sécurité des périphériques non-sécurisé ?
- Si les clients de Jabber utilisent un profil de sécurité des périphériques sécurisé, est-ce que nom du profil de Sécurité dans le format FQDN et ce nom FQDN est-il est configuré sur le certificat du l'Expressway-c comme SAN ?
- Si les clients de Jabber utilisent un profil de sécurité des périphériques sécurisé, naviguez vers le **System > Enterprise Parameters > les paramètres de Sécurité > la security mode** et le contrôle de **batterie** que la security mode de batterie est placée à 1 afin de vérifier que la batterie CUCM a été sécurisée. Si la valeur est **0**, l'administrateur doit passer par la procédure documentée pour sécuriser la batterie.

Le téléphone IP ne peut pas s'enregistrer, raisonner "Idle countdown expired"

Quand vous passez en revue Expressway-e se connecte pendant le délai que le client de Jabber introduit un message de REGISTRE, vous pourrait rencontrer l**dle countdown expired** une erreur comme indiqué dans le snippet de code ici.

```
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-ip="92.90.21.82" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

Cet extrait indique que le Pare-feu a le port 5061 ouvert ; cependant, il n'y a aucun trafic d'application-couche qui est passé plus de dans une durée suffisante ainsi la connexion TCP clôture.

Si vous rencontrez cette situation, il y a un degré élevé de probabilité que le Pare-feu devant Expressway-e a l'inspection de SIP/la fonctionnalité de la passerelle couche application (ALG) activées. Remediate cette question, vous devez diable cette fonctionnalité. Si vous êtes incertain de la façon faire ceci, vous devriez mettre en référence la documentation du produit de votre constructeur de Pare-feu.

Pour plus d'informations sur le SIP Inspection/ALG, vous pouvez mettre en référence l'annexe 4 de Cisco Expressway-e et

configuration Expressway-C-de base DeploymentGuide.

MRA échoue en raison du proxy de téléphone configuré en micrologiciel

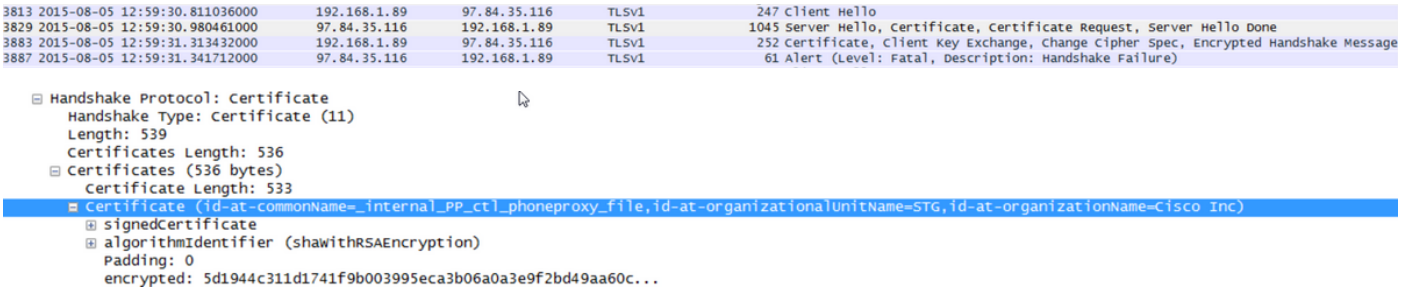
Un log diagnostique d'Expressway-e affiche une panne de négociation de TLS dans le port 5061, toutefois la prise de contact SSL a réussi au port 8443.

```
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp"
Level="DEBUG": Src-ip="173.38.117.81" 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-ip="173.38.117.81" 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-ip="173.38.117.81" 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-
ip="173.38.117.81" 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 de Jabber :

```
-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of
identity: 'expe.korteco.com' 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=expe.korteco.com: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 paquet du Jabber affiche une négociation SSL avec l'IP d'Expressway E ; cependant le certificat envoyé ne provient pas ce serveur :



Le FW a le proxy de téléphone configuré.

Solution :

Confirmez que les passages FW téléphonent le proxy. Afin de vérifier cela, sélectionnez **show run policy-map** la commande et elle t'affichera quelque chose semblable à :

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

Désactivez le proxy de téléphone pour que les services de téléphonie se connectent avec succès.

J'appelle des questions

Aucun medias quand vous appelez par MRA

Ce sont certains des disparus et des configurations incorrectes qui peuvent poser ce problème dans des déploiements simples et doubles NIC :

- NAT statique n'est pas configuré dans Expressway-e sous le système > les interfaces réseau > l'IP. NAT à la couche réseau doit toujours être fait dans le Pare-feu, mais cette configuration traduira l'IP à la couche application.
- Les ports TCP/UDP ne sont pas ouverts dans le Pare-feu. Pour une liste de ports référez-vous au guide de configuration d'utilisation de port IP de Cisco Expressway

Le NIC simple avec des déploiements NAT statiques ne sont pas recommandés. Voici quelques considérations pour empêcher des questions de medias :

- Dans la zone de traversée UC, Expressway-C doit indiquer l'adresse IP publique configurée dans Expressway-e.
- Les medias doivent « épingle à cheveux » ou se refléter dans le pare-feu externe. Un exemple de configuration utilisant un Pare-feu de Cisco ASA peut être trouvé dedans configurent la réflexion NAT sur L'ASA pour les périphériques de TelePresence d'Expressway de VCS.

Plus d'informations sur ceci peuvent être trouvées dans l'annexe 4 de Cisco Expressway-e et du guide de déploiement de configuration de base d'Expressway-C.

Aucun rappel quand appel au-dessus de MRA au PSTN

Cette question est due à une limite sur des autoroutes avant la version X8.5. L'ID de bogue Cisco CSCua72781 décrit comment Expressway-C n'expédie pas des medias tôt dans la progression de 183 sessions ou 180 sonnant à travers la zone de traversée. Si vous exécutez les versions X8.1.x ou X8.2.x, vous pouvez améliorer à la version X8.5 ou alternativement exécuter le contournement répertorié ici.

Il est possible d'utiliser un contournement sur le Logiciel Cisco Unified Border Element (CUBE) si vous faites un profil de SIP qui transforme les 183 en 180 et l'applique sur l'homologue de numérotation en entrée. Exemple :

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

Après ils désactiveraient 180 medias tôt sur le profil de SIP du **CUCM > CUBE** ou le CUBE lui-même dans le mode de configuration de sip-ua.

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

Questions CUCM et IM&P

Erreur ASCII qui empêche CUCM d'être ajouté

Quand vous ajoutez CUCM à Expressway-C, vous rencontrez une erreur ASCII qui empêche CUCM d'être ajouté.

Quand Expressway-C ajoute CUCM à sa base de données, elle fonctionne par une gamme de requêtes AXL qui associent pour obtenir et répertorier des fonctions. Les exemples de ces derniers incluent le **getCallManager**, le **listCallManager**, le **listProcessNode**, le **listProcessNodeService**, et le **getCCMVersion**. Après que le processus de **getCallManager** soit exécuté, il est réussi par un positionnement d'**ExecuteSQLQuery** pour récupérer toute la Gestionnaire-confiance d'appel CUCM ou Tomcat-confiances.

Une fois que CUCM reçoit la requête et exécute là-dessus, CUCM puis fait rapport tous ses Certificats. Si un des Certificats contient un caractère non ASCII, Expressway génère une erreur dans l'interface web semblable àascii codec can't decode byte 0xc3 in position 42487: ordinal not in range(128).

Cette question est dépistée avec l'ID de bogue Cisco CSCuo54489 et est résolue dans la version X8.2.

Pannes sortantes de TLS sur 5061 d'Expressway-C à CUCM dans les déploiements sécurisés

Cette question se produit quand vous utilisez les Certificats auto-signés sur CUCM et Tomcat.pem/CallManager.pem avez le même sujet. La question est abordée avec l'ID de bogue Cisco CSCun30200. Le contournement pour corriger la question est de supprimer le tomcat.pem et le TLS de débronchement vérifient de la configuration CUCM sur Expressway-C.

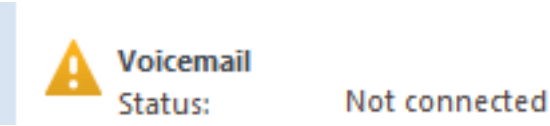
Serveur IM&P non ajouté et erreurs produites

Quand vous ajoutez un serveur IM&P, Expressway-C signale « ce serveur ne ne peut pas pas un IM et Presence Server » ou « communiquer avec l'erreur "HTTPError:500"' de HTTP de requête .AXL, qui a comme conséquence le serveur IM&P n'étant pas ajouté.

En tant qu'élément de l'ajout d'un serveur IM&P, Expressway-C emploie 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 cette mémoire ; donc, vous rencontrez l'erreur fausse.

Questions diverses

L'état de messagerie vocale sur le client de Jabber affiche « non connecté »



Afin de faire l'état de messagerie vocale de client de Jabber avec succès se connecter, vous devez configurer l'adresse IP ou l'adresse Internet de Cisco Unity Connection dans le serveur HTTP Whitelist sur Expressway-C.

Afin de se terminer ceci d'Expressway-C, exécutez la procédure appropriée :

Procédure pour les versions X8.1 et X8.2

1. **La configuration de** clic **> des transmissions > configuration unifiées > configurent le serveur HTTP permettent la liste**.
2. Cliquez sur New **> entrez IP/Hostname > créent l'entrée**.
3. Déconnectez de-vous le client de Jabber, et puis connectez-vous de retour dedans.

Procédure pour la version X8.5

1. **Configuration de** clic **> transmissions unifiées > serveurs d'Unity Connection**.
2. Cliquez sur New **> écrivez IP/Hostname, des qualifications de compte utilisateur > ajoutent l'adresse**.
3. Déconnectez de-vous le client de Jabber, et puis connectez-vous de retour dedans.

Les photos de contact n'apparaissent pas sur des clients de Jabber par des autoroutes

Le mobile et la solution d'accès distant utiltizes seulement UDS pour la résolution de photo de contact. Ceci exige que vous avez un web server disponible pour enregistrer les photos. La configuration elle-même est double.

1. Le fichier jabber-config.xml doit être modifié pour diriger les clients vers le web server pour la résolution de photo de contact. La configuration ici devrait réaliser ceci.

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

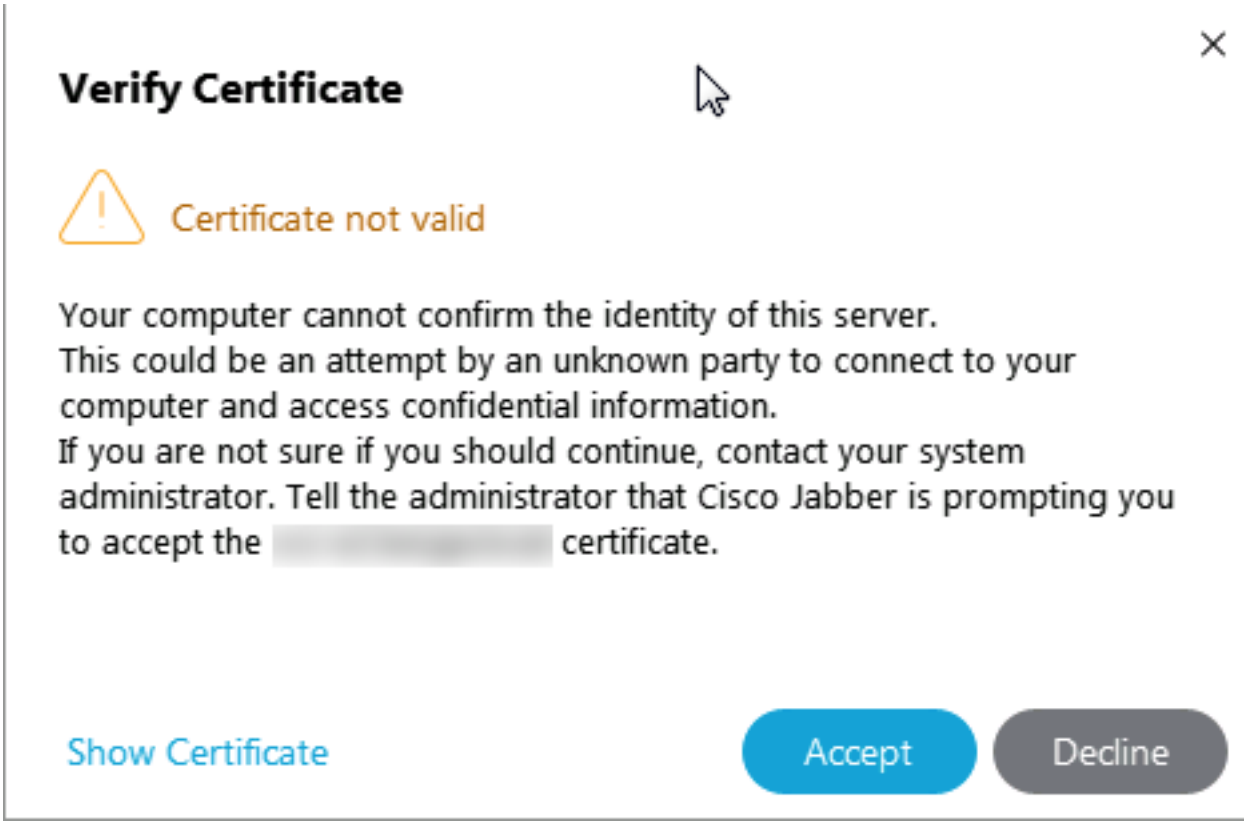
2. Expressway-C doit avoir le web server répertorié dans le serveur HTTP pour permettre la liste.

   La configuration de clic **> des transmissions > configuration unifiées > configurent le serveur HTTP permettent la**

liste.Cliquez sur New **> entrez IP/Hostname > créent l'entrée**.Déconnectez de-vous le client de Jabber, et puis connectez-vous de retour dedans.

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

Des clients de Jabber sont incités à recevoir le certificat d'Expressway-e pendant la procédure de connexion



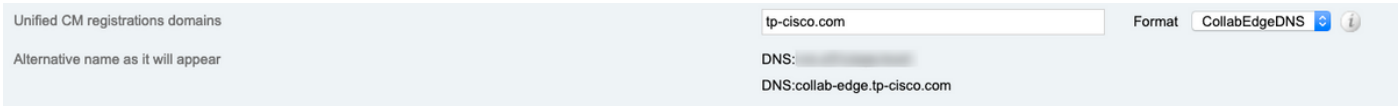
Ce message d'erreur peut être associé avec le certificat de périphérie d'Expressway non signé par un public CA qui est de confiance par le périphérique du client ou qui le domaine manque comme SAN dans le certificat de serveur.

Afin d'arrêter le client de Jabber de l'incitation pour recevoir le certificat d'Expressway, vous devez répondre aux deux critères répertoriés ci-dessous :

- Le périphérique/ordinateur qui exécute le client de Jabber doit avoir le signataire du certificat d'Expressway-e répertorié dans sa mémoire de confiance de certificat.

  Remarque: Ceci est facilement accompli si vous utilisez une autorité de certification publique parce que les périphériques mobiles contiennent une grande mémoire de confiance de certificat.

- Le domaine d'enregistrement d'Unified CM utilisé pour l'enregistrement de collab-périphérie doit être présent dans le SAN du certificat d'Expressway-e. L'outil CSR dans le serveur d'Expressway te donnera l'option d'ajouter le domaine d'enregistrement d'Unified CM comme SAN, il sera préchargé si le domaine est configuré pour MRA. Si le CA signant le certificat ne reçoit pas un domaine comme SAN, vous pouvez également utiliser l'option de « CollabEdgeDNS », qui préfixera la « collab-périphérie » au domaine :



Informations connexes

- **Guide de mobile et d'Accès à distance au-dessus des autoroutes**
- **Guide de déploiement de création et d'utilisation de certificat de Cisco Expressway**
- **Utilisation de port IP de serveur de communication vidéo Cisco TelePresence (VCS de Cisco) pour la traversée de**

Pare-feu

- **Déploiement et guide d'installation pour le Cisco Jabber**
- **Support et documentation techniques - Cisco Systems**