Périphérie de Collaboration la plupart des problèmes courants

Contenu

Introduction

La périphérie de Collaboration/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

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager (CUCM)
- Noyau d'autoroute de Cisco
- Périphérie d'autoroute de Cisco
- 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 du serveur de communication vidéo (VCS) ou plus tard
- Contrôle VCS et autoroute/noyau et périphérie d'autoroute
- Version 9.1(2)SU1 ou plus tard et IM CUCM et version 9.1(1) ou ultérieures P
- Version 9.7 ou ultérieures de Cisco Jabber

Questions de procédure de connexion

Jabber incapable à la connexion 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 l'autoroute-e répertoriée dans la réponse SRV.

L'enregistrement SRV de **_collab-edge** devrait indiquer le nom de domaine complet (FQDN) de l'autoroute-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.

2. Certificat inacceptable ou aucun disponible sur l'autoroute VCS

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

Si l'autoroute n'a pas un certificat signé valide qui contient le FQDN ou le domaine de l'autoroute, 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 l'autoroute, qui inclut automatiquement le FQDN de l'autoroute comme nom alternatif soumis (SAN).

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

Conditions requises de certificat de serveur d'autoroute-C :

- **Les pseudonymes de noeud de conversation** configurés sur les serveurs IM&P. Ceci est exigé si vous exécutez la fédération extensible de Protocol de Messagerie et de présence (XMPP).

L'autoroute-C devrait automatiquement inclure ces derniers dans le CSR à condition que un serveur IM&P ait été déjà découvert sur l'autoroute-C.

- Les noms dans le format FQDN de tous les **profils de degré de sécurité de téléphone** dans CUCM configuré pour le TLS et utilisé sur des périphériques configurés pour MRA. Ceci tient compte de la communication protégée entre le CUCM et l'autoroute-C pour les périphériques qui utilisent ces profils de degré de sécurité de téléphone.

Conditions requises de certificat de serveur d'autoroute-e :

1. Tous les domaines configurés pour des transmissions unifiées. Ceci inclut le domaine de l'autoroute-e et du C, le domaine d'adresse e-mail configuré pour le Jabber, et tous les domaines de présence.

2. **Les pseudonymes de noeud de conversation** configurés sur les serveurs IM&P. Ceci est exigé si vous exécutez la fédération XMPP.

Le guide de déploiement MRA décrit cette question plus en détail aux pages 17-18.

3. Aucun serveurs UDS trouvés dans la configuration de périphérie

Après que le client de Jabber établisse avec succès une connexion sécurisée avec l'autoroute-e, elle demande sa configuration de périphérie (**get_edge_config**). Cette configuration de périphérie contient les enregistrements SRV pour le **_cuplogin** et les **_cisco-uds**. Si ces enregistrements SRV 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 **_cisco-uds** et les enregistrements SRV de **_cuplogin** sont créés intérieurement et résoluble par l'autoroute-C.

Plus d'informations sur les enregistrements SRV de DN peuvent être trouvées à la page 10 du guide de déploiement MRA pour X8.5.

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 s'assurer que votre configuration suit la section de DN de la note de configuration : Mobile et Accès à distance par Expressway/VCS dans un déploiement de multi-domaine.

4. Les logs d'autoroute-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'autoroute-e (NIC) est inexactement configuré, ceci peut rendre le serveur extensible de la plate-forme de transmissions (XCP) mis à jour. Si l'autoroute-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 que l'autoroute-e écoute la session XCP sur l'interface réseau fausse, qui entraîne échouer de connexion pour/délai d'attente. L'autoroute-e écoute sur le port TCP 7400 la session XCP. Vous pouvez vérifier ceci si vous utilisez la commande de **netstat du** VCS comme racine.

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

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

C'est un exemple de ce que ressemble au xmppEdgeServer/adresse dans la réponse de **get_edge_config de l'**autoroute-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'autoroute-e. L'amélioration CSCuo83458 a été classée pour ceci.

6. Incapable de se connecter dans certains serveurs IM&P - les logs d'autoroute affichent une erreur

Affichage un de logs d'autoroute de ces erreurs :

```
"No realm found for host cups-example.domain.com, check connect auth configuration" Module="cm-
1.expressway-edge-example-com" Level="INFO " CodeLocation=
"SASLManager.cpp:198" Detail="Failed to query auth component for SASL mechanisms"
```

De l'autoroute-C, allez à la **configuration > des transmissions unifiées > des serveurs IM&P**. Sélectionnez la case à côté de chaque serveur IM&P et le clic **régénèrent des serveurs**.

> Remarque: Si ceci ne répare pas la question, le routeur XCP sur le serveur IM&P doit également être redémarré.

7. 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.

Contournement :

Àcourt terme, vous pouvez utiliser une de ces deux 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.

Questions d'enregistrement

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

Un log diagnostique d'autoroute-C affiche un message **non permis de la méthode SIP/2.0 405** 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 l'autoroute-C et le 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'autoroute-C pour CUCM à un port différent tel que 5065. Ceci est expliqué plus loin du guide de déploiement MRA à la page 39.

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'autoroute-C, le port 5060.

Autoroute-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'**autoroute-C, assurez-vous que l'autoroute-C écoute toujours sur 5060 le SIP.

Le téléphone IP ne peut pas s'enregistrer, Reason= " domaine inconnu »

Un log diagnostique de sip **" d'**expositions d'autoroute-C **inconnu du** " TCP » AOR= " " XXX.XXX.XXX.XXX » Src-port="51601" Protocol= de Src-ip= de " SIP » de Service= de **domaine rejeté " par enregistrement » » d'**Event= **Reason=** : 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'Autoroute-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 « compte à rebours chargé de veille a expiré »

Quand vous passez en revue l'autoroute-e se connecte pendant le délai que le client de Jabber introduit un message de REGISTRE, vous pourrait rencontrer un **compte à rebours chargé de veille a expiré** 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 l'autoroute-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 du guide de base de contrôle VCS et de déploiement d'autoroute (page 55).

Jabber et clients EX incapables au registre à l'autoroute-e une fois Provisioned avec un LSC

Afin de corriger ce problème, **téléchargez le certificat CAPF.pem à la** liste de confiance d'autorité de certification d'autoroute-e.

Questions de medias

Aucun medias quand vous appelez par MRA

Dans un déploiement simple NIC avec configuré NAT, ces paramètres manquent ou non configuré correctement :

- L'autoroute-C n'est pas indiquée l'adresse IP publique de l'autoroute-e, qui permet au Pare-feu à l'épingle à cheveux la signalisation.

- S'indiquant le FQDN de l'autoroute-e pour le TLS, vérifiez le FQDN doit le résoudre à l'adresse IP publique de l'autoroute-e.

- Ceux-ci ne sont pas configurés sur l'autoroute-e :

```
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"
```

Plus d'informations sur ceci peuvent être trouvées à la page 63 du guide de contrôle VCS et de déploiement d'autoroute.

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 l'autoroute-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 :

```
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"
```

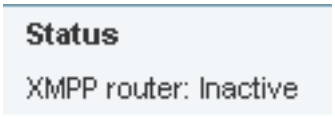
Après ils désactiveraient 180 medias tôt sur le profil de SIP du **CUCM > CUBE** ou le CUBE lui-même dans le mode de configuration de sip-ua.

```
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"
```

Questions Autoroute-centrales

L'autoroute-C pourrait afficher un « routeur XMPP : » Erreur inactive

Vous pourriez rencontrer cette erreur après que vous vous terminiez la configuration :



Cette erreur peut se produire pour plusieurs différentes raisons décrites ici :

- Le service d'Unified CM n'est pas activé sur Expressway-C/E.

  Afin de réparer cette question, terminez-vous ces étapes :

  Naviguez vers la **configuration > les zones > les zones > la zone de traversée**.Sélectionnez **oui** pour les services unifiés de Communcations sous la section de SIP.Cliquez sur **Save**.

- Le LAN2 est en activité mais non utilisable sur l'autoroute-e.

  Afin de réparer cette question, terminez-vous ces étapes :

  Naviguez vers le **système > l'IP de l'**autoroute-e.Sélectionnez **non** pour le double paramètre d'interfaces réseau d'utilisation.

- Un domaine de SIP n'a pas été défini sur l'autoroute-C.

  Afin de réparer cette question, terminez-vous ces étapes :

  Naviguez vers la **configuration > les domaines > nouveau**.Ajoutez votre domaine et tournez les **enregistrements de SIP et le ravitaillement sur l'Unified CM** et **IM et les services de présence sur l'Unified CM à en fonction**.Créez un domaine.

- L'autoroute-C **IM et les services de présence sur l'Unified CM** ne sont pas activés.

  Afin de réparer cette question, terminez-vous ces étapes :

  Naviguez vers la **configuration > le domaine > sélectionnent votre domaine**.Placez l'**IM et les services de présence sur l'Unified CM à en fonction.**Cliquez sur **Save**.

- La zone de traversée entre l'autoroute-C et l'autoroute-e n'est pas sécurisée.

  Afin de réparer cette question, terminez-vous ces étapes :

  Assurez-vous que la traversée est placée **pour forcer chiffré.**Assurez-vous que l'adresse de pair dans l'autoroute-C n'est placée à l'adresse Internet de l'autoroute-e et pas de l'adresse IP de sorte qu'elle apparie le certificat.

Questions CUCM et IM&P

Erreur ASCII qui empêche CUCM d'être ajouté

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

Quand l'autoroute-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, l'autoroute génère une erreur dans l'interface web semblable aux **codecs ASCII ne peut pas décoder l'octet 0xc3 en position 42487 : nombre ordinal pas en 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 de l'autoroute-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 l'autoroute-C.

Serveur IM&P non ajouté et erreurs produites

Quand vous ajoutez un serveur IM&P, l'autoroute-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, l'autoroute-C emploie une requête AXL pour rechercher les Certificats IM&P dans un répertoire explicite. Dû pour déserter CSCul05131, les Certificats ne sont pas dans cette mémoire ; donc, vous rencontrez l'erreur fausse.

Erreur du serveur XCP produite

Sur des affichages d'autoroute-C, sous l'**état > a unifié des transmissions**, d'une erreur du serveur XCP qui lit « accessible inactif mais la connexion n'est pas en hausse. Mot de passe de contrôle ».

La solution est de redémarrer les deux autoroutes.

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 l'autoroute-C.

Afin de se terminer ceci de l'autoroute-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 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.

```
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"
```

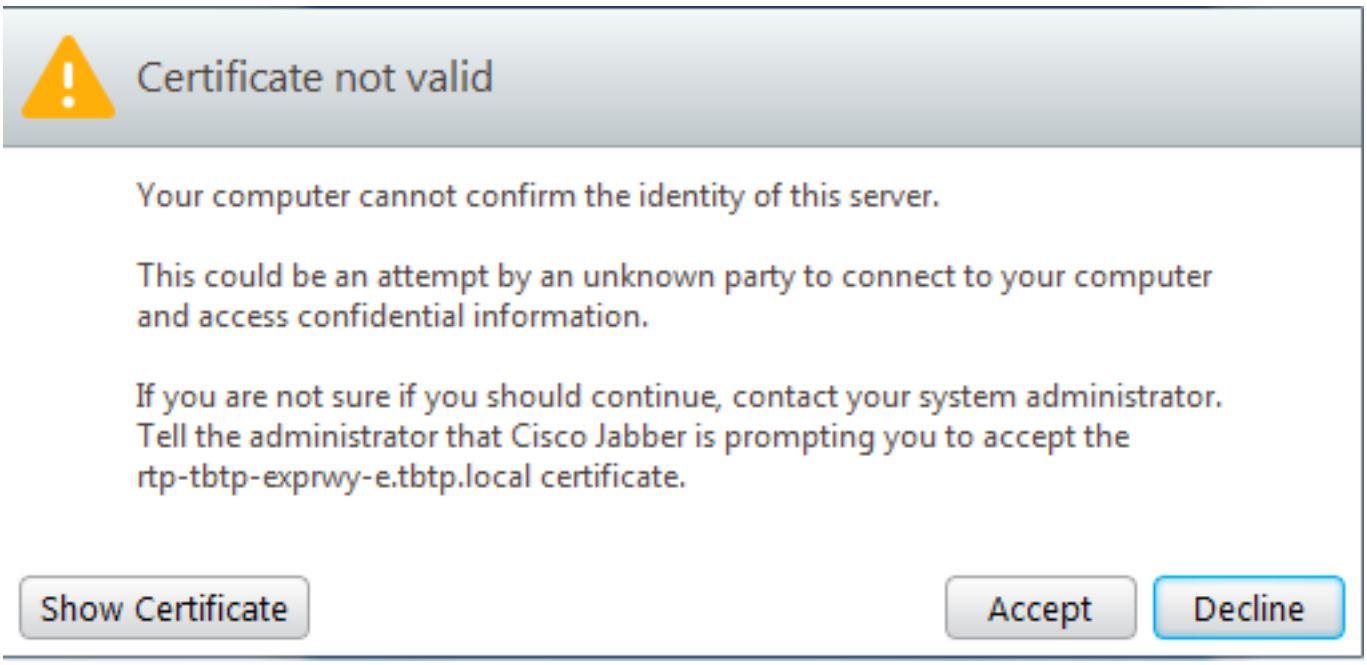
2. L'autoroute-C doit avoir le web server répertorié dans le serveur HTTP pour permettre la

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'autoroute-e pendant la procédure de connexion



Afin d'arrêter le client de Jabber de l'incitation pour recevoir le certificat d'autoroute, vous devez rencontrer le criteteria deux répertorié ci-dessous :

- Le périphérique/ordinateur qui exécute le client de Jabber doit avoir le signataire du certificat d'autoroute-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 externe utilisé pour l'enregistrement de collab-périphérie doit être présent dans le SAN du certificat d'autoroute-e.

  Remarque: Le client de Jabber recherche le SAN pour ce domaine quand il le reçoit. S'il n'est pas présent, il vous incite au recevoir.

Informations connexes

- Mobile unifié et Accès à distance de transmissions par l'intermédiaire de Cisco VCS

- Guide de déploiement de création et d'utilisation de certificat de la TelePresence Cisco VCS
- Utilisation de port IP de serveur de communication vidéo Cisco TelePresence (Cisco VCS) pour la traversée de Pare-feu
- Déploiement et guide d'installation pour le Cisco Jabber
- Support et documentation techniques - Cisco Systems