Résoudre les problèmes les plus courants pour les appels interentreprises au moyen d'Expressway

Contenu

Introduction

Ce document décrit les problèmes les plus courants lors d'un déploiement interentreprises (B2B). Comment résoudre les problèmes liés aux appels B2B sur les Expressways.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expressway-C (Exp-C)
- Expressway-E
- Cisco Unified Call Manager (CUCM)
- Téléprésence par Video Communication Server-C (VCS-C)

Components Used

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

logiciel suivantes :

- Expressway C et E X8.1.1 ou ultérieur
- Unified Communications Manager (CUCM) 10.0 ou ultérieur.

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 courants

1. Erreur « //SIP/SIPTcp/wait_SdlReadRsp: Ignoring large message. Only allow up to 5000 bytes. Resetting connection. » (Ignorer les messages volumineux. Permettre jusqu'à 5000 octets. Réinitialiser la connexion.)

Les appels provenant des points d'extrémité de téléprésence enregistrés de VCS et se dirigeant vers une ligne principale du protocole de SIP de CUCM échouent et reçoivent le message d'erreur suivant :« //SIP/SIPTcp/wait_SdlReadRsp: Ignoring large message. Only allow up to 5000 bytes. Resetting connection. » (Ignorer les messages volumineux. Permettre jusqu'à 5000 octets. Réinitialiser la connexion.)

La configuration de routage de l'appel est correcte dans l'Expressway-C/VCS-C et l'appel est envoyé vers CUCM. Le message d'invitation de SEP (SIP Invite) est envoyé vers CUCM. Toutefois, dans les journaux de SDL, il n'y a pas de messages de SIP. L'erreur suivante apparaît dans les journaux de SDL :

"|AppInfo |SIPTcp - Message important ignoré de xxx.xxx.xxx.xxx : [27469]. Only allow up to 5000 bytes. Resetting connection. » (Ignorer les messages volumineux. Permettre jusqu'à 5000 octets. Réinitialiser la connexion.)

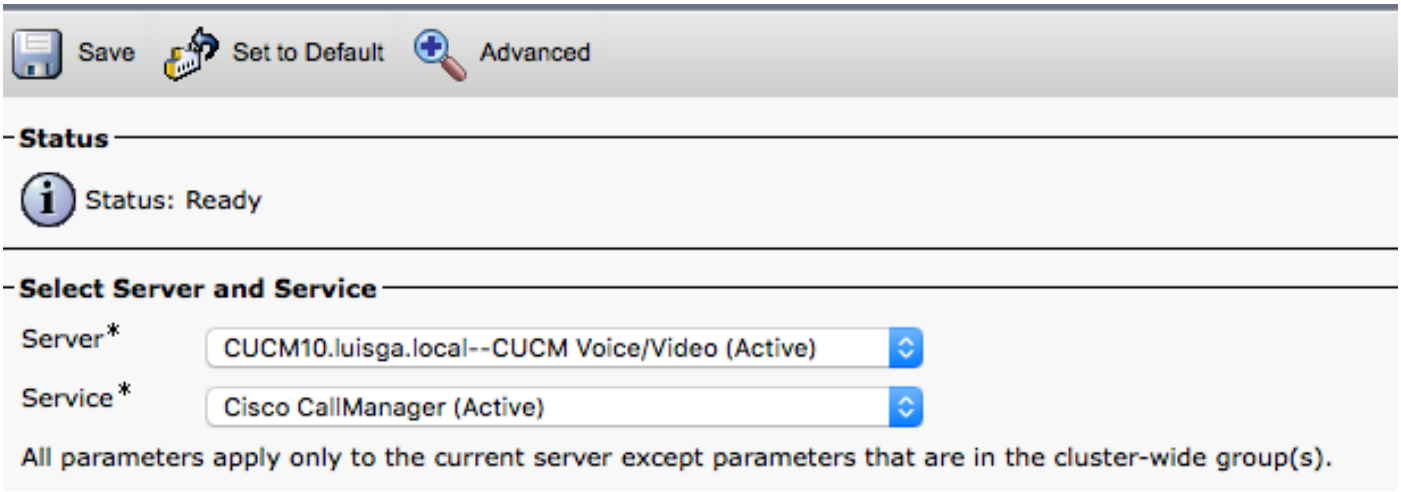
Dans CUCM 8.6 et les versions antérieures, la valeur par défaut pour la taille maximale d'un message entrant de SIP s'établissait à 5000. À partir de la version 9.X, de CUCM, cette valeur est passée à 11 000. Cependant, dans les mises à niveau des versions 8 ou antérieures vers la version 9 ou 10, la valeur par défaut de l'ancienne version du logiciel sera conservée (5 000).

Solution

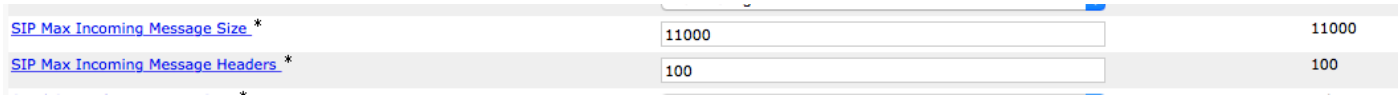
Ce problème est lié au bogue CSCts00642

Il faut augmenter le paramètre de service avancé de CUCM sur la taille maximale des messages entrants de SIP (**SIP Max Incoming Message Size), de la valeur par défaut (5 000) pour l'établir à une taille adéquate pour ces types d'appels.** 11 000 est une bonne valeur pour la majorité des scénarios de clientèle prévus.

Pour augmenter cette valeur, dans la **page d'administration de CUCM,** accédez aux Service Parameters (paramètres de service) et **sélectionnez votre serveur CUCM et le service CallManager** :



Sélectionnez l'option **avancée et faites une recherche pour repérer SIP Max Incoming Message Size (taille maximale des messages entrants de SIP)** :



2. Arrêt du flux multimédias si un autre serveur d'appels transfert l'appel.

Cela peut arriver dans des scénarios d'appels mobiles et distants (MRA) et d'appels interentreprises (B2B).

Le problème peut couper le son dans un sens ou encore, entraîner un bruit de bourdonnement (le même bruit que lorsque vous faites jouer une capture avec audio chiffrée) une fois que l'appel est transféré. Cette situation se produit lorsqu'une suite crypto est sélectionnée dans une configuration d'appel que ne prend pas en charge le point terminal vers lequel l'appel est transféré.

Vous pouvez comparer la négociation SIP avant et après le transfert de l'appel. Dans la première négociation dans les journaux VCS ou CUCM, vous pouvez voir des lignes crypto dans le message 200 OK de VCS :

```
m=audio 54582 RTP/SAVP 9 96 97 0 8 18 101
a=rtpmap:9 G722/8000
a=rtpmap:96 G7221/16000
a=fmtp:96 bitrate=32000
a=rtpmap:97 G7221/16000
a=fmtp:97 bitrate=24000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:ckXijkT3CcVY+xlOf3ozX/TjHPz05OzEdY49rAHA|2^48
a=sendrecv
a=rtcp:54583 IN IP4 10.1.201.7
m=video 54658 RTP/SAVP 96 97
b=TIAS:4000000
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e01e;max-fs=1621;packetization-mode=1;max-rcmd-nalu-
size=32000;level-asymmetry-allowed=1
```

```
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42e01e;max-fs=1621;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:S8BJvGB/2l6F7XP8izXxId443Xd9f27oUI/4gxSt|2^48
```

Les lignes crypto sont acceptées dans le premier appel, mais dans le deuxième appel, vous verrez que le message ACK supprime les lignes crypto :

```
m=audio 24826 RTP/AVP 0
c=IN IP4 10.1.231.30
a=ptime:20
a=rtpmap:0 PCMU/8000
m=video 0 RTP/AVP 126
c=IN IP4 10.1.98.80
b=TIAS:448000
a=label:11
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42E01F;packetization-mode=1;max-fs=3601;max-rcmd-nalu-
size=32000;level-asymmetry-allowed=1
a=content:main
```

VCS tente d'utiliser les lignes crypto négociées au début, même si le point de terminaison vers lequel l'appel est transféré ne prend pas en charge le chiffrement.

Solution

Ce problème est lié au bogue CSCuv11790

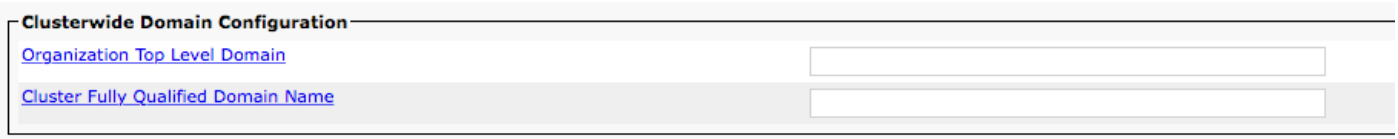
Une mise à niveau de VCS/Expressway vers la version x8.6.1 permettra de résoudre ce problème.

3. Le domaine de niveau supérieur n'est pas configuré dans CUCM.

Si le paramètre d'entreprise du domaine de niveau supérieur n'est pas défini, cela fera en sorte que CUCM acheminera des appels entrants vers son propre domaine et les schémas de routage de SIP seront utilisés. Cela pourrait créer une boucle parce que l'appel sera le plus susceptible d'être renvoyé à l'Exp-C. L'appel pourrait aussi s'interrompre et faire l'objet une erreur « 404 Not Found ».

Solution

Dans la **page d'administration de CUCM, accédez à System > Enterprise Parameters pour modifier ce paramètre.**



4. Le certificat de CUCM doit comprendre un attribut d'authentification de client.

Lorsqu'une connexion sécurisée est établie entre l'Exp-C et CUCM (avec TLS Verify), la prise de

contact mutuelle de SSL est amorcée par un serveur d'appel en particulier, selon l'orientation de l'appel. Par conséquent, les deux serveurs doivent avoir les attributs d'authentification du client et du serveur sur leur certificats. Cette erreur est visible dans les journaux VCS/Expressway si l'attribut n'est pas présent :

```
Line 190: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,060"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connecting"
Line 239: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,071"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Established"
Line 249: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,081"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Closed" Reason="no certificate returned"
```

Solution

Vous trouverez de plus amples renseignements sur la façon de configurer un modèle renfermant les attributs de client et de serveur Web dans le guide sur le certificat VCS

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-7/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-7.pdf

5. Problèmes d'interfonctionnement.

VCS/Expressway, version X8.6.x a eu certains problèmes dans le contexte de l'interfonctionnement.

Voici les bogues liés à la problématique :

Defect CSCuw85626 peut être détecté si vous vérifiez les journaux de diagnostic de VCS/Expressway à la recherche de ceci : videom lines being rejected:

Ce message d'erreur s'affiche lorsque les lignes de média dans la partie TCS de la circulation de H323 font l'objet de la négociation.

medialine index (index de lignes de média) : 1

rejected (refus) : true, direction (valeur réelle, orientation) : SDP_MEDIA_DIR_SENDRECV

type : video / SDP_MF_AU_VID

Defect CSCuw85715 est semblable, mais dans ce cas-ci, les journaux VCS/Expressway préciseront que la cause est la suivante : dataTypeNotSupported:

```
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="INFO": Action="Sent" Dst-ip="XXXXXXXXXXXXXXXX" Dst-port="49162"
Detail="Sending H.245 OpenLogicalChannelRejResponse "
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="DEBUG": Dst-ip="XXXXXXXXXXXXXXXX" Dst-port="49162"
Sending H.245 PDU:
value MultimediaSystemControlMessage ::= response : openLogicalChannelReject :
{
forwardLogicalChannelNumber 3,
```

```
cause dataTypeNotSupported : NULL
}
```

Solution

Mise à niveau vers X8.7 ou version ultérieure.

6. Le message ACK reçu de CUCM n'est pas envoyé à VCS-E/Expressway-E.

Cela se produit généralement lorsque la zone de traverse configurée n'est pas orientée vers la bonne adresse IP de VCS Expressway / Expressway-E.

Dans les déploiements faisant appel à un seul NIC (sur Expressway/Edge), la zone de traverse client sur Controle/Core doit correspondre à l'adresse IP publique du serveur de traverse.

Dans les déploiements faisant appel à deux NIC, la zone de traverse client doit s'orienter vers l'adresse IP interne (NIC interne est généralement LAN1, mais peut être LAN2) du serveur de traverse. N'oubliez pas que c'est l'adresse IP interne du LAN interne.

Solution

Veuillez vous reporter à l'Annexe 4 deCisco VCS Expressway and VCS Control - Configuration de base pour obrenir plus d'information et consulter un diagramme sur les différents déploiements de réseau.

7. CUCM abandonne la session TCP lors des appels entrants

Lorsque les appels sont transmis à VCS Control / Expressway Core, CUCM pourrait refuser ce processus et abandonner la session de TCP.

Cela peut arriver lorsque le port entre la zone voisin et le profil de sécurité de la ligne principale SIP ne correspondent pas ou sont configurés pour 5060/5061.

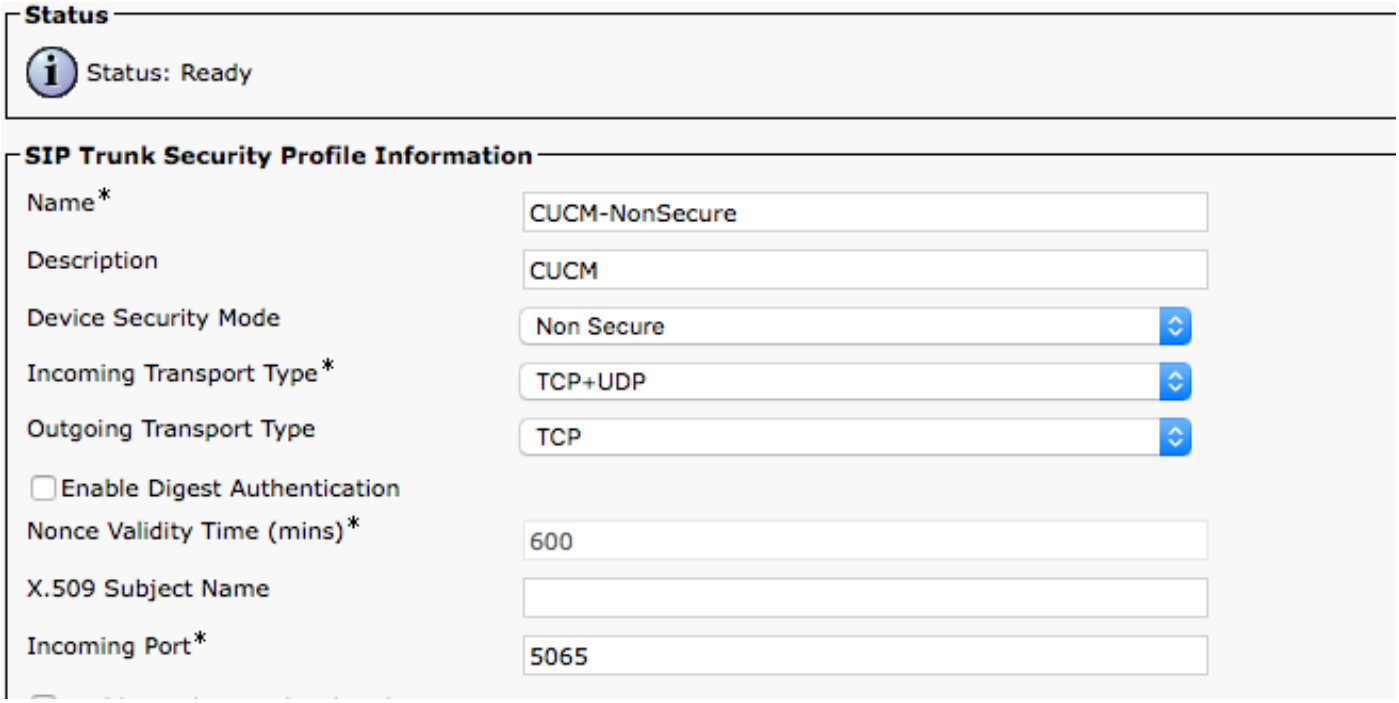
MRA utilise une communication en ligne, tandis que les appels B2B utilisent une communication par ligne principale. CUCM a certaines limites pour ce qui concerne les communications en ligne et par ligne principale, qui ne peuvent pas être transmises sur le même port. Puisque MRA fait surtout l'objet d'une configuration automatique, les déploiements B2B doivent utiliser un autre port.

Solution

Pour y parvenir, le port de destination configuré dans la zone voisine de CUCM (VCS-C/Expressway-C) doit être différent de 5060/5061. Normalement, le port 5065 est utilisé, mais d'autres ports peuvent aussi être utilisés. Le port configuré doit correspondre au port configuré dans le profil de sécurité de la ligne principale SIP affecté à la ligne principale SIP de ce serveur pour CUCM.

Dans le **page d'administration de CUCM,** naviguez jusqu'à **>** Device **>** Trunk.

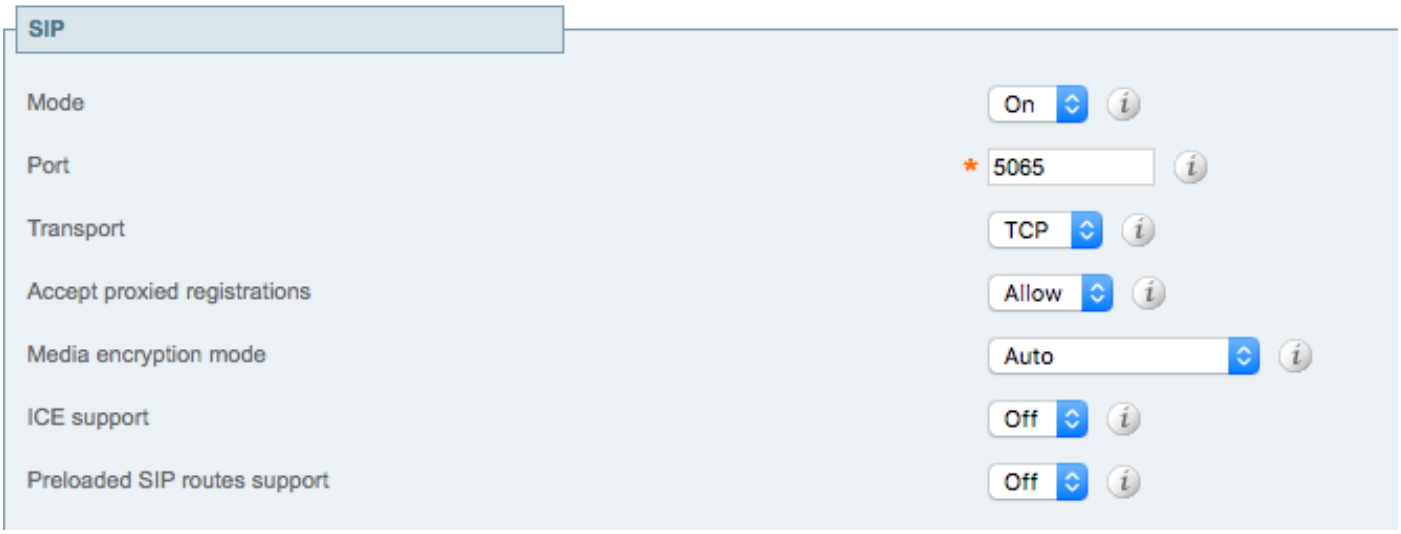
Profil de sécurité de la ligne principale SIP avec le port 5065.



Le port de destination de la ligne principale SIP peut être 5060/5061, comme l'illustre l'image.

Dans la zone voisine VCS/Expressway, le port SIP doit correspondre au port configuré dans le profil de sécurité de la ligne principale SIP, comme l'indique l'image.

À partir de la page d'administration d'Expressway, naviguez jusqu'à Configuration > Protocols > SIP



Si le VCS n'a pas cette limite ou ne s'applique pas pour ce scénario, cela signifie que la ligne réseau SIP pourrait être configurée pour 5060/5061.

8. VCS ne parvient pas à résoudre correctement FQDN ou ne parvient pas à interroger les enregistrements SRV.

Pour les appels B2B provenant de CUCM, un problème peut découler de la nature de la gestion et du routage des appels par CUCM.

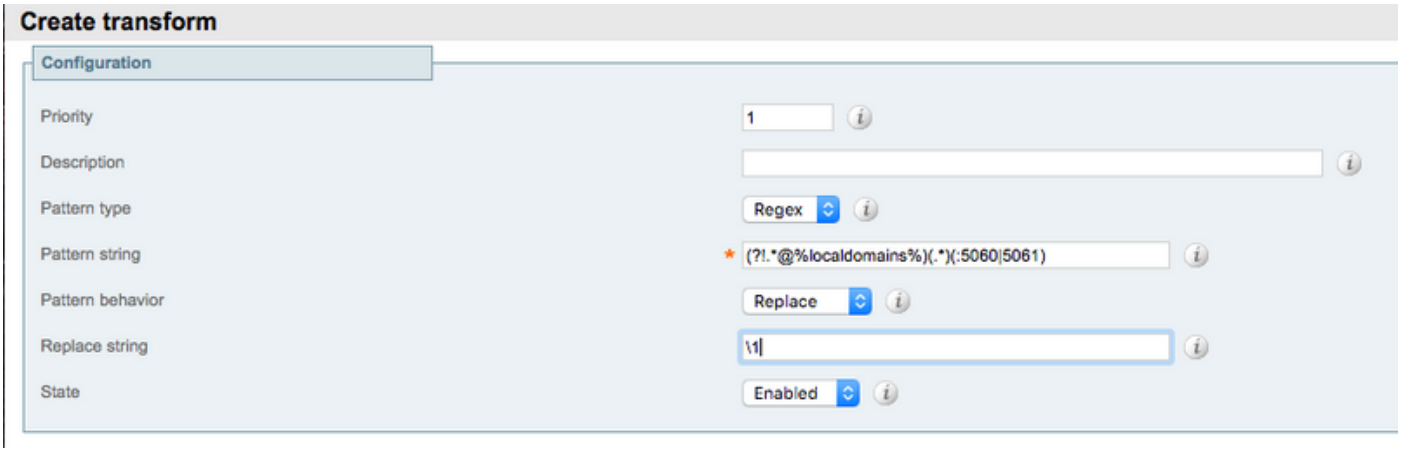
Lorsque CUCM transfère des appels vers les serveurs VCS, CUCM a tendance à ajouter :5060 ou :5061 (selon la configuration) à la fin de l'URI composé (test@lab.local » test@lab.local:5060) lorsqu'il atteint l'autoroute et atteint une règle de recherche vers la zone DNS, le VCS ne met pas en file d'attente d'enregistrement SRV, mais seulement en file d'attente pour les enregistrements A ou AAAA. Vous pouvez confirmer cette hypothèse dans les journaux de diagnostic de VCS/Expressway.

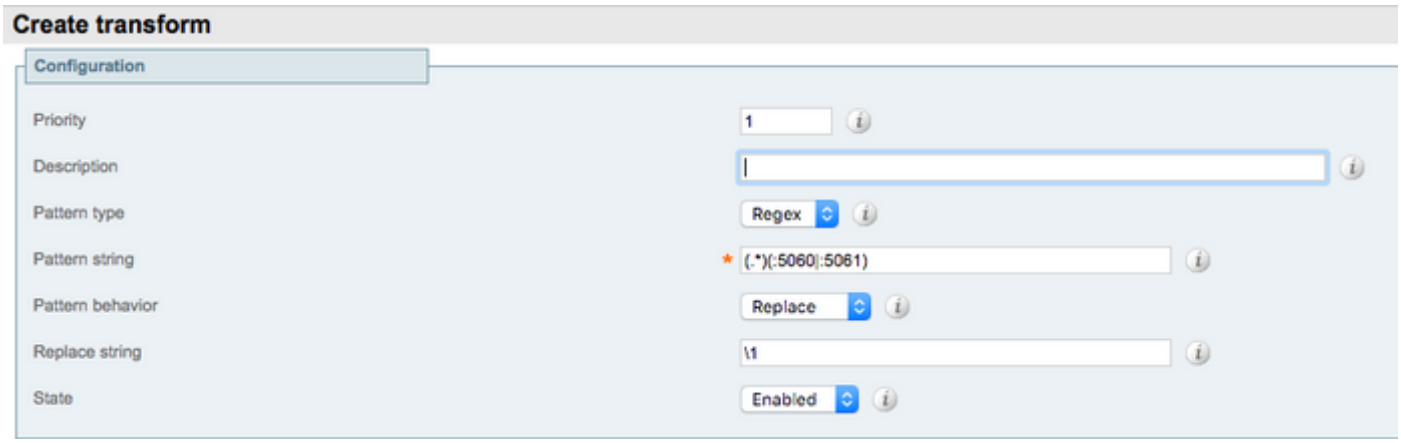
Solution

Afin de résoudre ce problème, il suffit de créer une transformation qui supprime le port à la fin (sur l'un ou l'autre des serveurs, ça n'a pas vraiment d'importance) avant qu'il atteigne la zone DNS.

Àpartir de **la page d'administration d'Expressway,** naviguez **à Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform**

Des exemples de transformations :





Si pour quelque raison que ce soit, il est impossible de créer une transformation, il est aussi possible de régler le problème au moyen des règles de recherche. Il est néanmoins recommandé de procéder avec les transformations.

Àpartir de la **page d'administration d'Expressway,** naviguez **jusqu'à Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Search Rules**

Informations connexes

- Cisco VCS Expressway et Contrôle VCS - Configuration de base