Risoluzione dei problemi più comuni delle chiamate da azienda a azienda tramite Expressway

Sommario

Introduzione

Questo documento descrive i problemi più comuni nella distribuzione Business to Business (B2B). Come risolvere i problemi relativi alle chiamate B2B tramite Expressways.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

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

- Expressway C e E X8.1.1 o versioni successive
- Unified Communications Manager (CUCM) versione 10.0 o successiva.

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

Problemi comuni

1. Errore "//SIP/SIPTcp/wait_SdlReadRsp: Il messaggio di grandi dimensioni verrà ignorato. Consentire solo fino a 5000 byte. Ripristino della connessione in corso."

Le chiamate dagli endpoint TelePresence registrati in VCS, in entrata su un trunk SIP (Session Initiation Protocol) a CUCM, hanno esito negativo con "//SIP/SIPTcp/wait_SdlReadRsp: Il messaggio di grandi dimensioni verrà ignorato. Consentire solo fino a 5000 byte. Ripristino della connessione in corso."

La configurazione di routing delle chiamate in Expressway-C/VCS-C è corretta e la chiamata viene inviata a CUCM. Il messaggio SIP Invite viene inviato a CUCM, ma nei log SDL non sono presenti messaggi SIP. Questo errore può essere visualizzato nei log SDL:

"|InfoApp |SIPTcp - Il messaggio di grandi dimensioni da xxx.xxx.xxx.xxx:[27469] verrà ignorato. Consentire solo fino a 5000 byte. Ripristino della connessione in corso."

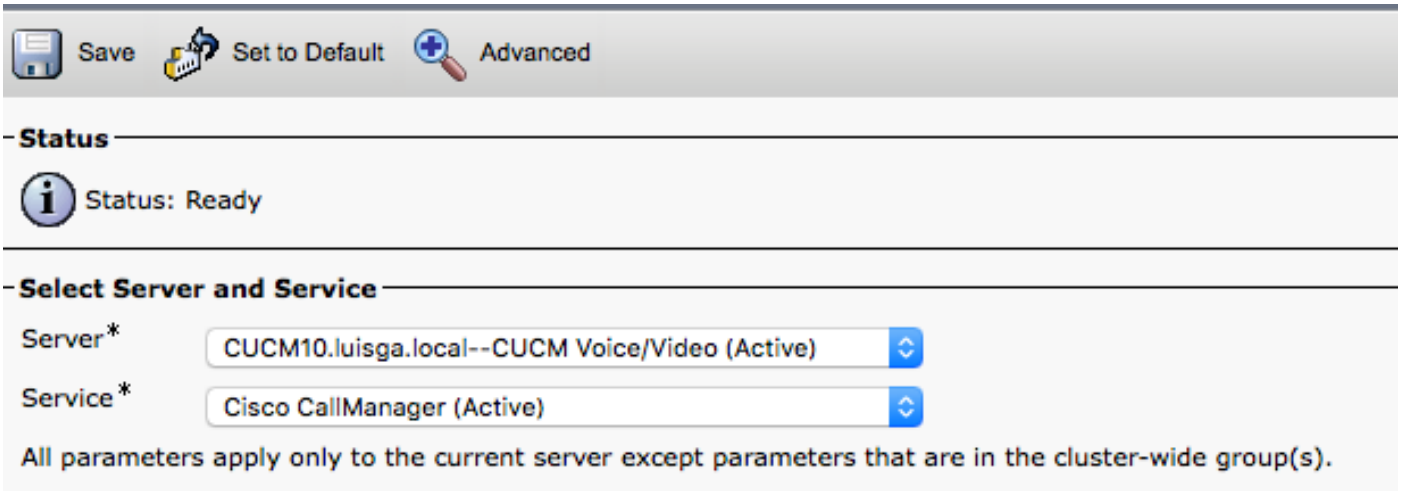
In CUCM 8.6 e versioni precedenti il valore predefinito per SIP Max Incoming Message Size era 5000, dopo che CUCM 9.X è stato modificato in 11000. Tuttavia, l'aggiornamento da 8 o versioni precedenti a 9 o 10 manterrà il valore predefinito nella versione precedente del software (5000).

Soluzione

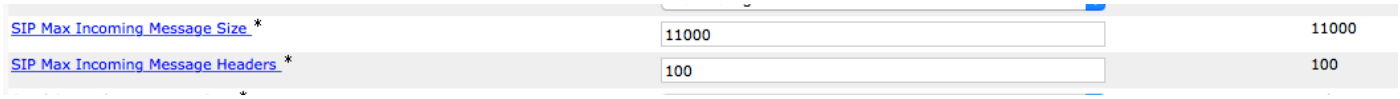
Questo problema è correlato al bug CSCts00642

Aumentare le **dimensioni massime dei messaggi in arrivo SIP del** parametro avanzato CUCM dal valore predefinito 5000 a una dimensione adeguata per questi tipi di chiamate. 11000 sembra essere un valore valido per la maggior parte degli scenari di clienti previsti.

Dalla **pagina Amministrazione CUCM,** passare **a Parametri servizio** e **selezionare** il **server CUCM e il servizio CallManager**:



Selezionare l'opzione **Advanced** (Avanzate) e cercare **SIP Max Incoming Message Size** (Dimensioni massime messaggi in arrivo SIP):



2. I flussi multimediali si arrestano se un altro server di chiamata trasferisce la chiamata.

Questa situazione può verificarsi nelle chiamate MRA (Mobile and Remote Access) e B2B.

Una volta trasferita la chiamata, non è possibile che si produca alcun suono in un modo o un ronzio (lo stesso rumore quando si tenta di riprodurre una cattura con audio crittografato). Ciò accade perché una suite di crittografia è selezionata nella configurazione della chiamata e non è supportata dall'endpoint a cui viene trasferita.

Èpossibile confrontare la negoziazione SIP prima e dopo il trasferimento della chiamata. Nella prima negoziazione nei log VCS o CUCM è possibile visualizzare le linee crittografiche nel messaggio 200 OK di 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
```

Le linee crittografiche vengono accettate nella prima chiamata, ma nella seconda si nota che il messaggio ACK rimuove le linee crittografiche:

```
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 tenta di utilizzare le linee crittografiche negoziate all'inizio, anche se l'endpoint a cui viene trasferita la chiamata non supporta la crittografia.

Soluzione

Questo problema è relativo al bug CSCuv1790

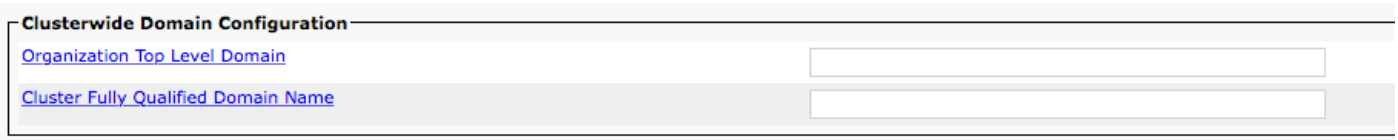
Per risolvere il problema, aggiornare VCS/Expressway a x8.6.1.

3. Dominio di livello superiore non configurato in CUCM.

Se il parametro Enterprise del dominio di primo livello non è impostato, CUCM instrada le chiamate in entrata verso il proprio dominio e vengono utilizzati i modelli di route SIP. Ciò potrebbe causare un loop perché la chiamata viene probabilmente rimandata a Exp-C oppure potrebbe non riuscire con un "errore 404 Non trovato".

Soluzione

Dalla **pagina Amministrazione CUCM, passare a Sistema > Parametri enterprise** per modificare questa impostazione



4. Al certificato CUCM deve essere applicato l'attributo di autenticazione client.

Quando viene impostata una connessione protetta tra Exp-C e CUCM (TLS Verify On), l'handshake SSL viene avviato da un server di chiamata specifico che dipende dalla direzione della chiamata. Ciò significa che i certificati di entrambi i server devono includere l'autenticazione client e server. Questo errore viene visualizzato nei log di VCS/Expressway se l'attributo non è

presente:

```
Line 190: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXX 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 XXXXXXXXXXXXXXX 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 XXXXXXXXXXXXXXX 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"
```

Soluzione

Per informazioni dettagliate su come configurare un modello con attributi sia del client Web che del server, vedere la guida ai certificati 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. Problemi di interworking.

VCS/Expressway versione X8.6.x presentava alcuni problemi con il processo di interworking.

Bug relativi al problema:

È possibile rilevare un difetto CSCuw85626 se si controllano i registri diagnostici da VCS/Expressway per individuare le righe video da rifiutare:

Questo messaggio di errore viene visualizzato quando le linee multimediali nella parte TCS del flusso H323 vengono negoziate.

indice medialine: 1

rifiutato: true, direzione: SDP_MEDIA_DIR_SENDRECV

tipo: video / SDP_MF_AU_VID

Il difetto CSCuw85715 è simile, ma in questo caso, nei log di VCS/Expressway verrà specificato che la causa è dataTypeNotSupported:

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

Soluzione

Eseguire l'aggiornamento a X8.7 o versioni successive.

6. Il messaggio ACK ricevuto da CUCM non viene inviato a VCS-E/Expressway-E.

Questa condizione si verifica in genere quando la zona laterale configurata non punta all'indirizzo IP corretto di VCS Expressway / Expressway-E.

Nelle installazioni con una singola NIC (Expressway/Edge), la zona client trasversale sul Control/Core deve puntare all'indirizzo IP pubblico del server trasversale.

Nelle installazioni con due schede di interfaccia di rete, il client laterale deve puntare all'indirizzo IP interno (la scheda di interfaccia di rete interna è generalmente LAN1, ma può essere LAN2) del server trasversale. Tenere presente che questo è l'indirizzo IP interno della LAN interna.

Soluzione

Fare riferimento all'Appendice 4 di Cisco VCS Expressway e VCS Control - Configurazione base per ulteriori informazioni e per un diagramma delle diverse implementazioni di rete.

7. CUCM interrompe la sessione TCP sulle chiamate in entrata

Quando le chiamate vengono inoltrate dal controllo VCS / Expressway Core, CUCM potrebbe rifiutare questa operazione eliminando la sessione TCP.

Questo problema può verificarsi quando la porta tra la zona adiacente e il profilo di sicurezza trunk sip non corrisponde o è configurata per essere 5060/5061.

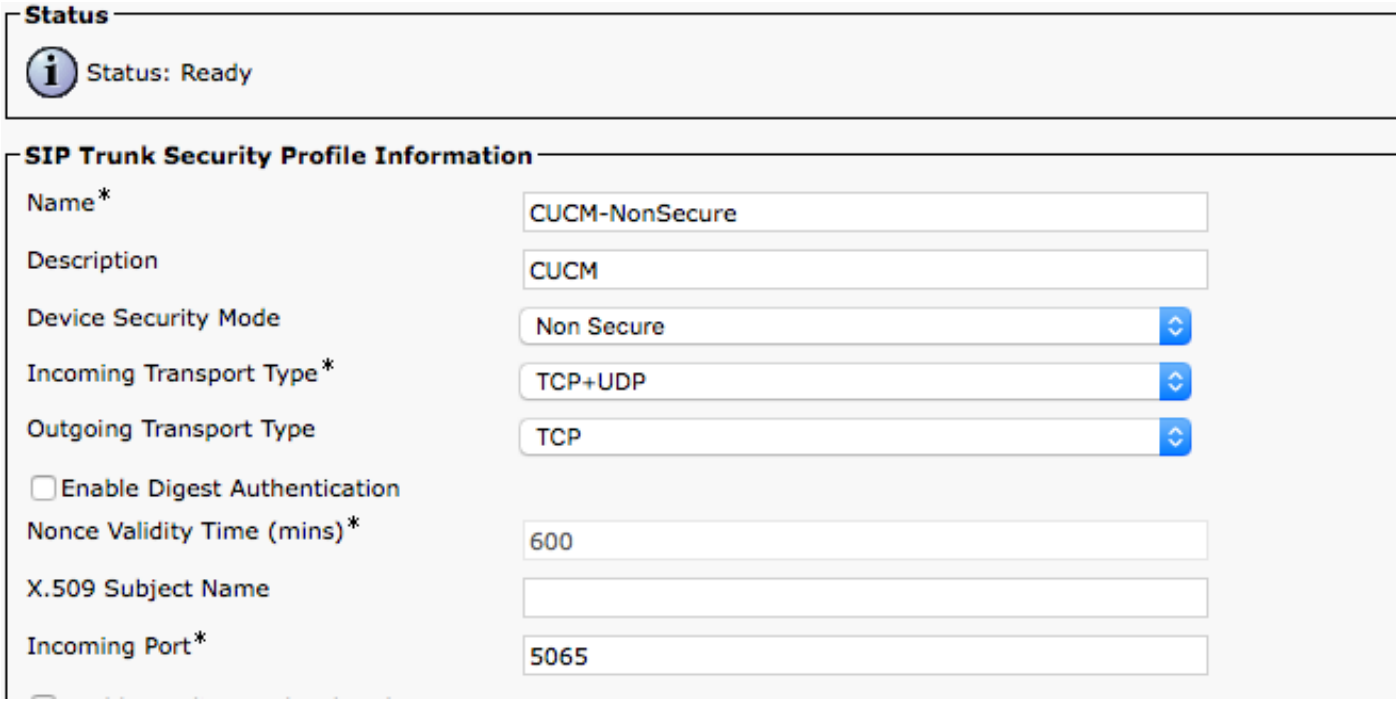
L'MRA utilizza una comunicazione in linea mentre le chiamate B2B utilizzano una comunicazione trunk, CUCM ha una limitazione che non consente alle comunicazioni in linea e trunk di passare attraverso la stessa porta. Poiché la maggior parte delle installazioni MRA è configurata automaticamente, le implementazioni B2B devono utilizzare una porta diversa.

Soluzione

A tale scopo, la porta di destinazione configurata nella zona adiacente su CUCM (su VCS-C/Expressway-C) deve essere diversa da 5060/5061. Normalmente viene utilizzato 5065, ma è possibile utilizzarne altri. La porta configurata deve corrispondere alla porta configurata nel profilo di sicurezza trunk sip assegnato al trunk sip su questo server su CUCM.

Dalla **pagina Amministrazione CUCM,** passare **a Dispositivo > Trunk.**

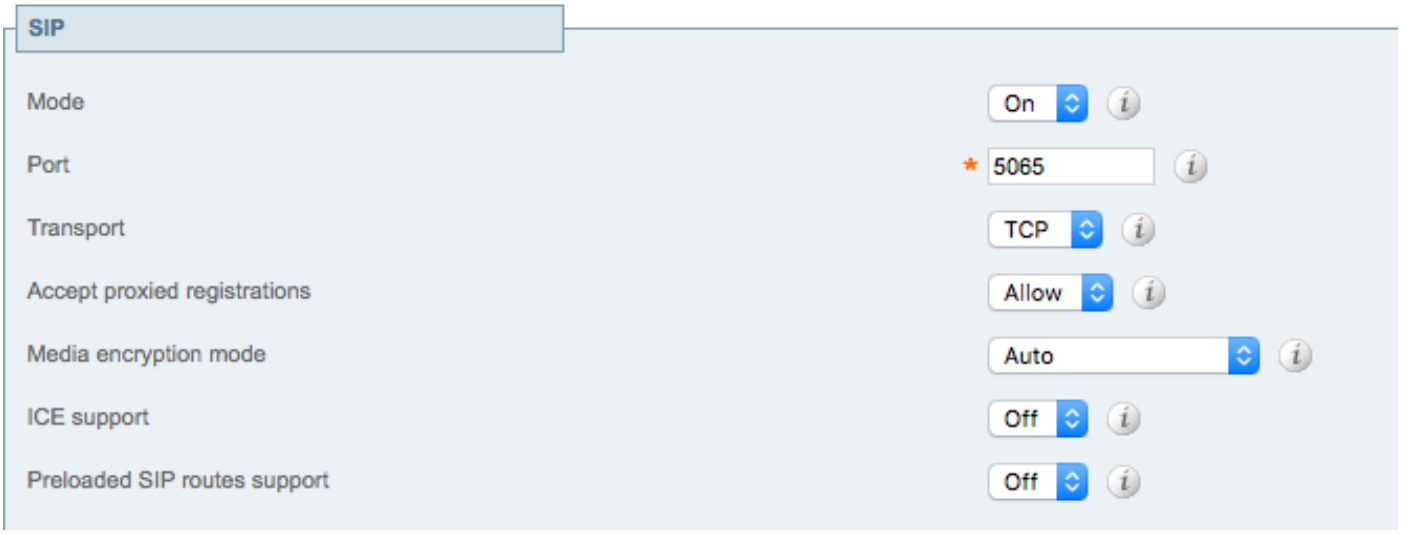
SIP Trunk Security Profile con porta 5065.



La porta di destinazione del trunk SIP può essere 5060/5061, come mostrato nell'immagine.

La porta SIP nella zona adiacente VCS/Expressway deve corrispondere alla porta configurata nel profilo di sicurezza trunk SIP, come mostrato nell'immagine.

Dalla **pagina Amministrazione di Expressway,** passare a **Configurazione > Protocolli > SIP**



Il software VCS non prevede questa limitazione o non è applicabile a questo scenario, pertanto è possibile configurare il trunk SIP con 5060/5061.

8. VCS non è in grado di risolvere correttamente i nomi di dominio completi (FQDN) o non riesce a eseguire query sui record SRV.

Per le chiamate B2B originate da CUCM, è possibile introdurre un problema a causa della natura del modo in cui CUCM gestisce e instrada le chiamate.

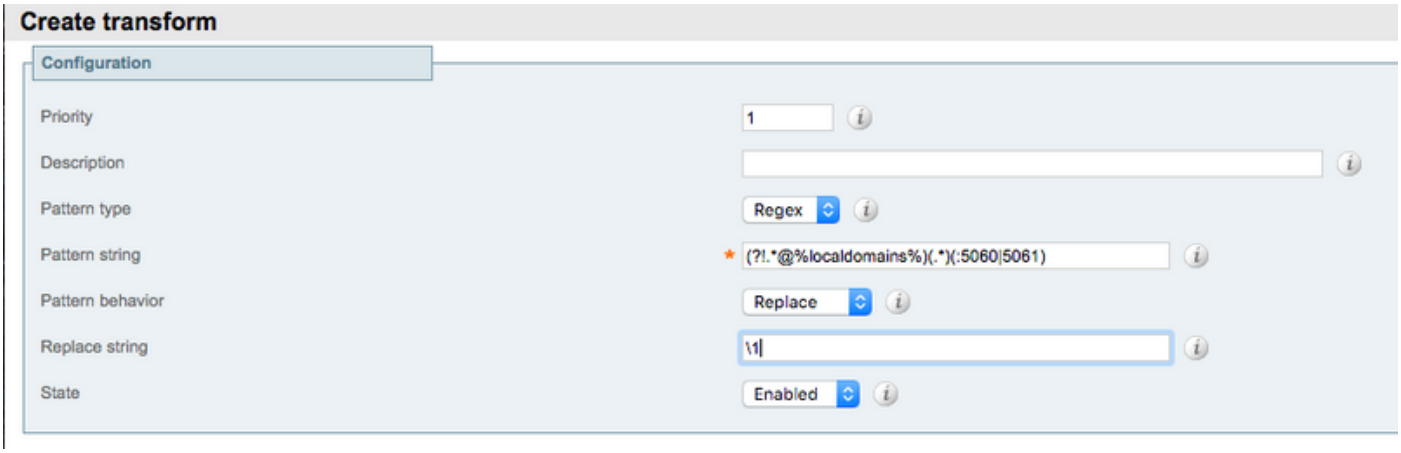
Quando CUCM inoltra le chiamate ai server VCS, CUCM tende ad aggiungere :5060 o :5061 (a seconda della configurazione) alla fine dell'URI composto (ad esempio test@lab.local >> test@lab.local:5060) quando raggiunge l'expressway e incontra una regola di ricerca verso la zona DNS, il VCS non interroga il record SRV, ma solo i record A o AAAA. È possibile verificare questa condizione nei log di diagnostica da VCS/Expressway.

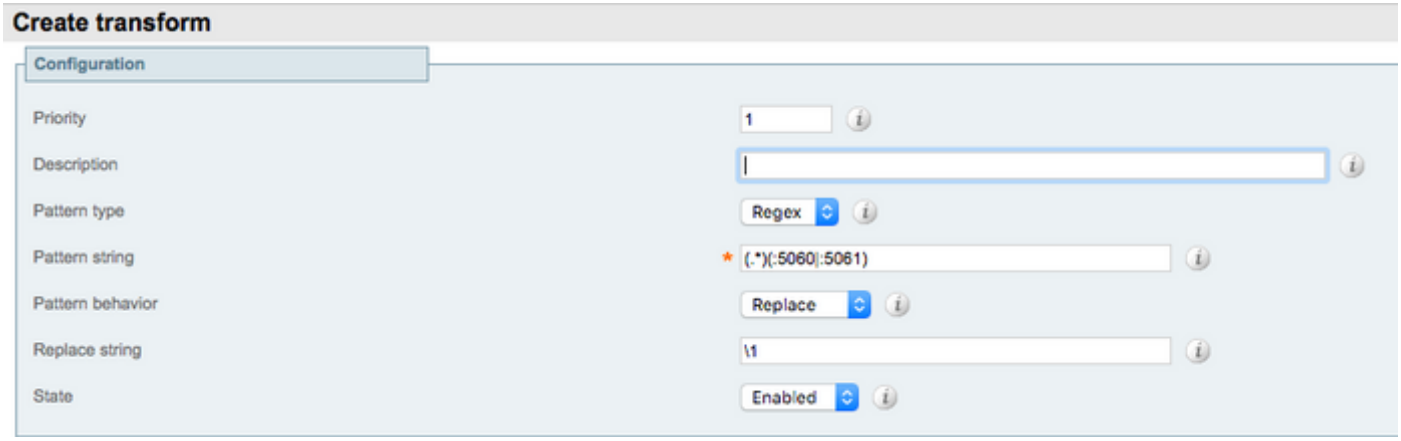
Soluzione

Per risolvere questo problema, è sufficiente creare una trasformazione che rimuova la porta all'estremità (su entrambi i server, non ha alcuna importanza) prima che raggiunga la zona DNS.

Dalla **pagina Amministrazione di Expressway,** passare **in Configurazione > Piano di composizione > Trasformazioni per configurazione > Piano di composizione > Trasforma**

Esempi di trasformazioni:





Se per qualche motivo non è possibile creare una trasformazione, questa può essere eseguita anche tramite le regole di ricerca, ma è consigliabile farlo tramite le trasformazioni.

Dalla **pagina Amministrazione di Expressway,** passare **a Configurazione > Dial Plan > Trasformazioni per configurazione > Dial Plan > Regole di ricerca**

Informazioni correlate

- Cisco VCS Expressway e VCS Control - Configurazione base