Fehlerbehebung für häufige Probleme bei Business-to-Business-Anrufen über Expressway

Inhalt

Einführung

In diesem Dokument werden die häufigsten Probleme bei der B2B-Bereitstellung (Business to Business) beschrieben. Beheben von B2B-Anrufen durch Expressways

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Expressway C und E X8.1.1 oder spätere Version

- Unified Communications Manager (CUCM) 10.0 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Häufige Probleme

1. Fehler "//SIP/SIPTcp/wait_SdlReadRsp: Große Nachricht ignorieren. Nur bis zu 5.000 Byte erlauben. Verbindung zurücksetzen."

Anrufe von an VCS registrierten TelePresence-Endpunkten, die über einen SIP-Trunk (Session Initiation Protocol) zum CUCM eingehen, schlagen mit "//SIP/SIPTcp/wait_SdlReadRsp fehl: Große Nachricht ignorieren. Nur bis zu 5.000 Byte erlauben. Verbindung zurücksetzen."

Die Konfiguration der Anrufweiterleitung im Expressway-C/VCS-C ist korrekt, und der Anruf wird an den CUCM gesendet. Die SIP-Einladungs-Nachricht wird an CUCM gesendet, in den SDL-Protokollen sind jedoch keine SIP-Nachrichten enthalten. Dieser Fehler wird in den SDL-Protokollen angezeigt:

"|AppInfo |SIPTcp - Große Nachricht von xxx.xxx.xxx.xxx wird ignoriert:[27469]. Nur bis zu 5.000 Byte erlauben. Verbindung zurücksetzen."

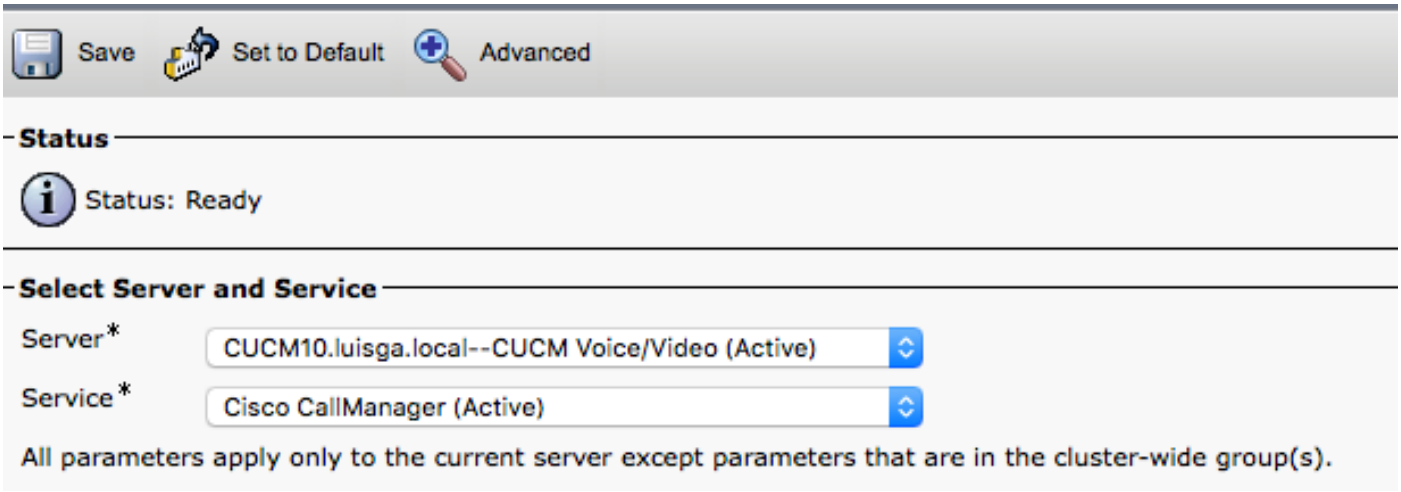
In CUCM 8.6 und niedriger als der Standardwert für die max. eingehende SIP-Nachrichtengröße betrug 5000, nachdem CUCM 9.X in 11000 geändert wurde. Bei einem Upgrade von 8 oder weniger auf Version 9 oder 10 wird der Standardwert in der vorherigen Version der Software (5000) beibehalten.

Lösung

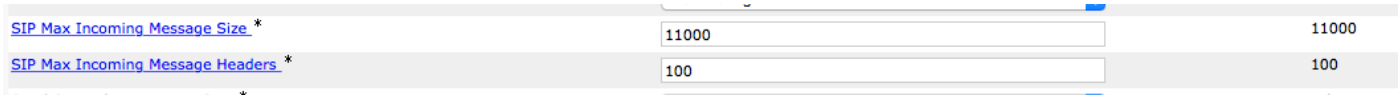
Dieses Problem betrifft den Fehler CSCts00642

Erhöhen Sie die **SIP**-Parameter **für** erweiterte Services **für** CUCM **für die maximale eingehende Nachrichtengröße** vom Standardwert 5000 auf eine für diese Anruftypen angemessene Größe. 11000 scheint für die Mehrzahl der erwarteten Kundenszenarien ein guter Wert zu sein.

Navigieren Sie auf der **Seite für die CUCM-Verwaltung** zu **den Serviceparametern,** und **wählen Sie** den **CUCM-Server und den CallManager-Dienst aus**:



Wählen Sie die **Option Erweitert aus**, und suchen Sie nach der **maximalen Größe eingehender SIP-Nachrichten**:



2. Medien-Streams werden angehalten, wenn ein anderer Anrufserver den Anruf weiterleitet.

Dies kann bei Anrufen für den mobilen und Remote-Zugriff (MRA) und B2B-Anrufe auftreten.

Es kann nach der Weiterleitung des Anrufs weder auf eine bestimmte Weise noch zu einem Fiebergeräusch (dasselbe Geräusch, wenn Sie versuchen, eine Aufzeichnung mit verschlüsseltem Audio abzuspielen) führen. Dies liegt daran, dass bei der Anrufeinrichtung eine Verschlüsselungs-Suite ausgewählt wird, die vom Endpunkt, an den sie übertragen wird, nicht unterstützt wird.

Sie können die SIP-Aushandlung vor und nach der Weiterleitung des Anrufs vergleichen. Bei der ersten Aushandlung in den VCS- oder CUCM-Protokollen werden die Kryptozeilen in der 200 OK-Nachricht aus dem VCS angezeigt:

```
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
```

Krypto-Leitungen werden im ersten Anruf akzeptiert, im zweiten Anruf sehen Sie jedoch, dass die ACK-Nachricht die Krypto-Leitungen entfernt:

```
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
```

Der VCS versucht, die zu Beginn ausgehandelten Kryptolinien zu verwenden, selbst wenn der Endpunkt, an den der Anruf weitergeleitet wird, keine Verschlüsselung unterstützt.

Lösung

Dieses Problem steht in Zusammenhang mit Bug CSCuv11790

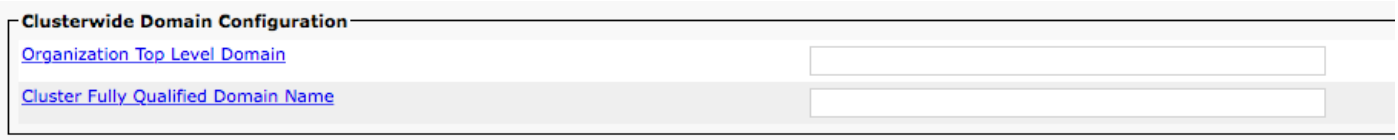
Aktualisieren Sie VCS/Expressway auf x8.6.1, um dieses Problem zu beheben.

3. Domäne oberster Ebene nicht in CUCM konfiguriert.

Wenn der Enterprise-Parameter der obersten Ebene nicht festgelegt ist, veranlasst er CUCM, eingehende Anrufe an die eigene Domäne weiterzuleiten, und es werden die SIP-Weiterleitungsmuster verwendet. Dies kann eine Schleife verursachen, da der Anruf höchstwahrscheinlich an Exp-C zurückgesendet wird, oder er kann auch mit dem Fehler "404 Not Found" fehlschlagen.

Lösung

Navigieren Sie auf der **CUCM-Verwaltungsseite zu System > Enterprise Parameters (System > Enterprise-Parameter**), um diese Einstellung zu ändern.



4. Das CUCM-Zertifikat muss über das Client-Authentifizierungsattribut verfügen.

Wenn eine sichere Verbindung zwischen dem Exp-C und dem CUCM (TLS Verify On) eingerichtet wird, wird der SSL-Handshake von einem bestimmten Anrufserver gestartet, der die Richtung des Anrufs bestimmt. Das bedeutet, dass beide Server über eine Client- und Serverauthentifizierung in

ihren Zertifikaten verfügen müssen. Dieser Fehler wird in den VCS/Expressway-Protokollen angezeigt, wenn das Attribut nicht vorhanden ist:

```
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"
```

Lösung

Einzelheiten zur Konfiguration einer Vorlage mit Webclient- und Serverattributen finden Sie im VCS-Zertifikatsleitfaden.

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. Probleme bei der Zusammenarbeit.

VCS/Expressway Version X8.6.x hatte einige Probleme mit dem Interworking-Prozess.

Probleme im Zusammenhang mit dem Problem:

Defekt CSCuw85626 kann erkannt werden, wenn die Diagnoseprotokolle von VCS/Expressway auf abgelehnte Video-M-Leitungen überprüft werden:

Diese Fehlermeldung wird angezeigt, wenn die Medienzeilen im TCS-Teil des H323-Datenflusses ausgehandelt werden.

Medialinindex: 1

abgelehnt: true, Richtung: SDP_MEDIA_DIR_SENDRECV

Typ: Video/SDP_MF_AU_VID

Defect CSCuw85715 ist ähnlich, aber in diesem Fall geben die VCS/Expressway-Protokolle an, dass die Ursache "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
}
```

Lösung

Aktualisieren Sie auf X8.7 oder höher.

6. Die vom CUCM empfangene ACK-Nachricht wird nicht an VCS-E/Expressway-E gesendet.

Dies ist in der Regel der Fall, wenn die konfigurierte Traversal-Zone nicht auf die richtige IP-Adresse des VCS Expressway/Expressway-E verweist.

Bei EinzelNIC-Bereitstellungen (auf dem Expressway/Edge) muss die durchlaufende Clientzone auf der Steuerungs-/Core-Ebene auf die öffentliche IP-Adresse des durchlaufenden Servers zeigen.

Bei dualen NIC-Bereitstellungen muss der Traversal-Client auf die interne IP-Adresse des Traversal-Servers zeigen (interne NIC ist normalerweise LAN1, kann aber LAN2 sein). Beachten Sie, dass dies die interne IP-Adresse des internen LANs ist.

Lösung

Weitere Informationen und ein Diagramm der verschiedenen Netzwerkbereitstellungen finden Sie in Anhang 4 Cisco VCS Expressway und VCS Control - Basic Configuration (Grundkonfiguration).

7. CUCM verwirft TCP-Sitzung bei eingehenden Anrufen.

Wenn Anrufe von VCS Control/Expressway Core weitergeleitet werden, kann der CUCM dies über die TCP-Sitzung ablehnen.

Dies kann vorkommen, wenn der Port zwischen der Nachbarzone und dem SIP-Trunk-Sicherheitsprofil nicht übereinstimmt oder als 5060/5061 konfiguriert wurde.

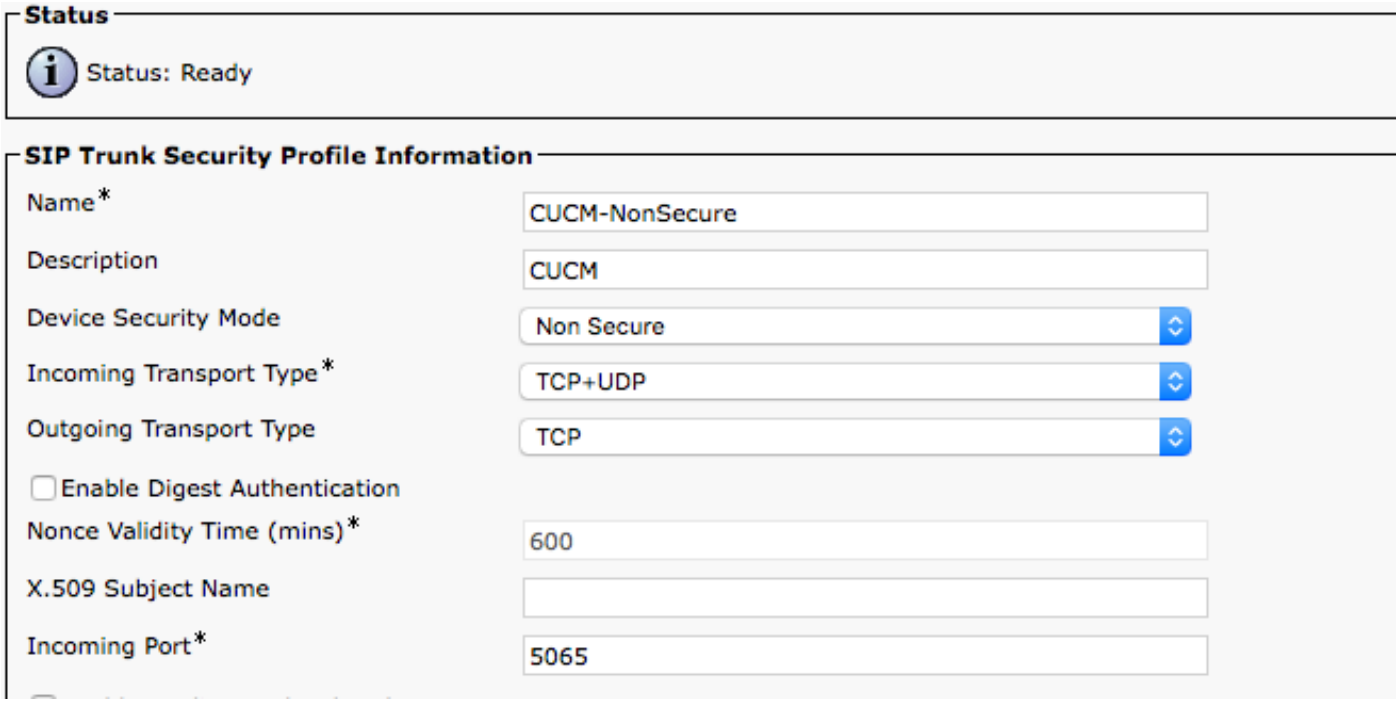
MRA verwendet eine Inline-Kommunikation, während B2B-Anrufe eine Trunk-Kommunikation verwenden. CUCM hat eine Einschränkung, die es nicht erlaubt, dass Inline- und Trunk-Kommunikation über denselben Port geleitet wird. Da MRA zumeist automatisch konfiguriert wird, müssen B2B-Bereitstellungen einen anderen Port verwenden.

Lösung

Dazu muss der für die Nachbarzone des CUCM konfigurierte Zielport (auf VCS-C/Expressway-C) anders sein als 5060/5061. Normalerweise wird 5065 verwendet. Andere können jedoch verwendet werden. Der konfigurierte Port muss mit dem Port übereinstimmen, der auf dem SIP-Trunk-Sicherheitsprofil konfiguriert ist, das dem SIP-Trunk zu diesem Server auf dem CUCM zugewiesen ist. M.

Navigieren Sie auf der **CUCM-Verwaltungsseite** zu **Gerät > Trunk.**

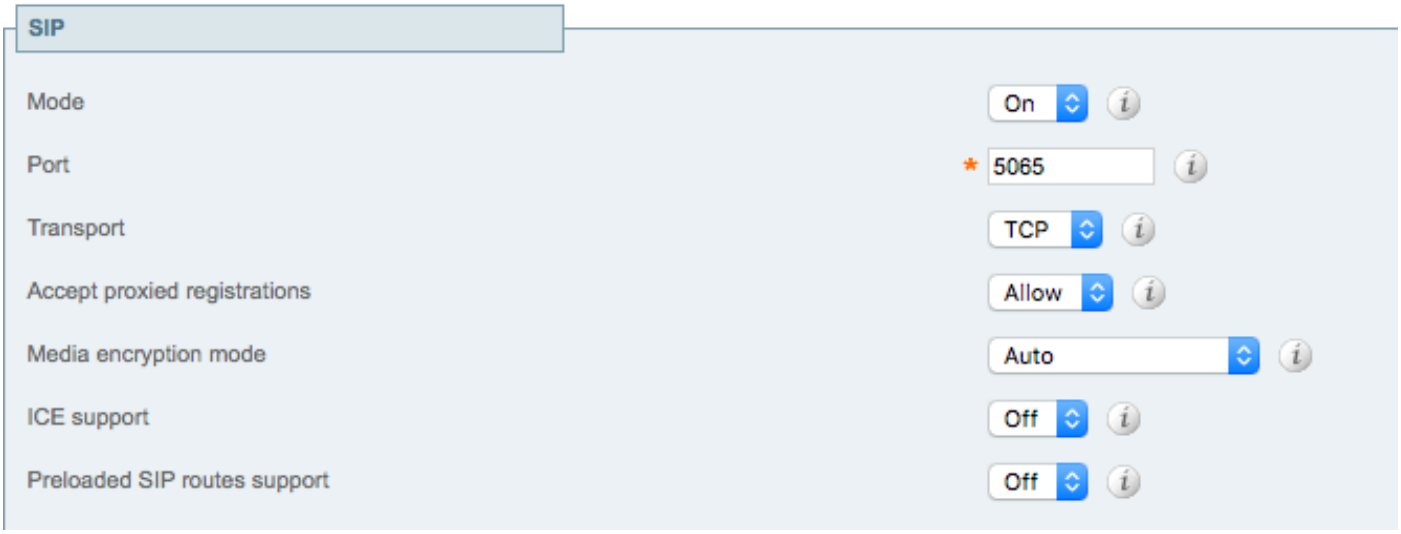
SIP-Trunk-Sicherheitsprofil mit Port 5065



Der SIP-Trunk-Ziel-Port kann 5060/5061 sein, wie im Bild gezeigt.

Der SIP-Port in der Nachbarzone VCS/Expressway muss mit dem im SIP-Trunk-Sicherheitsprofil konfigurierten Port übereinstimmen, wie im Bild gezeigt.

Navigieren Sie auf der **Expressway Administration-Seite** zu **Configuration>** Protocols > SIP.



Der VCS hat diese Einschränkung nicht oder gilt nicht für dieses Szenario. Das bedeutet, dass der SIP-Trunk selbst mit 5060/5061 konfiguriert werden kann.

8. VCS kann FQDNs nicht ordnungsgemäß auflösen oder Anfragen an SRV-Datensätze nicht durchführen.

Bei B2B-Anrufen, die vom CUCM ausgehen, kann aufgrund der Art und Weise, wie CUCM Anrufe verarbeitet und weiterleitet, ein Problem eingeführt werden.

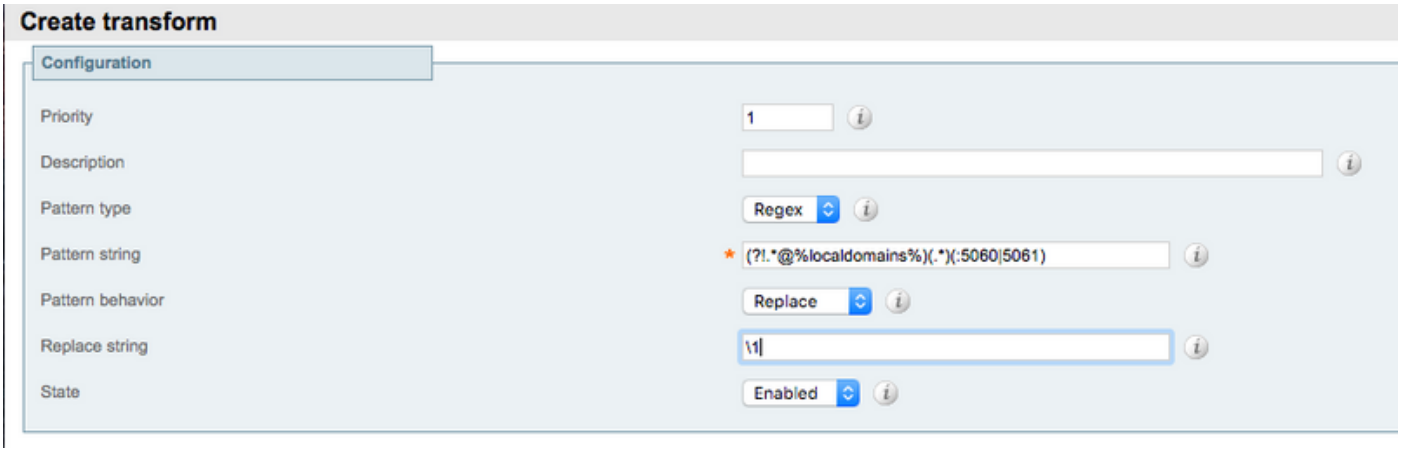
Wenn der CUCM die Weiterleitung an die VCS-Server anfordert, fügt der CUCM am Ende des gewählten URI tendenziell :5060 oder :5061 (abhängig von der Konfiguration) hinzu (z. B. test@lab.local >> test@lab.local:5060), wenn er den Autobahn erreicht und eine Suchregel in Richtung DNS-Zone abruft, fragt der VCS den SRV-Datensatz nicht ab, sondern fragt nur nach A oder AAAA ab Datensätze. Dies können Sie in den Diagnoseprotokollen von VCS/Expressway bestätigen.

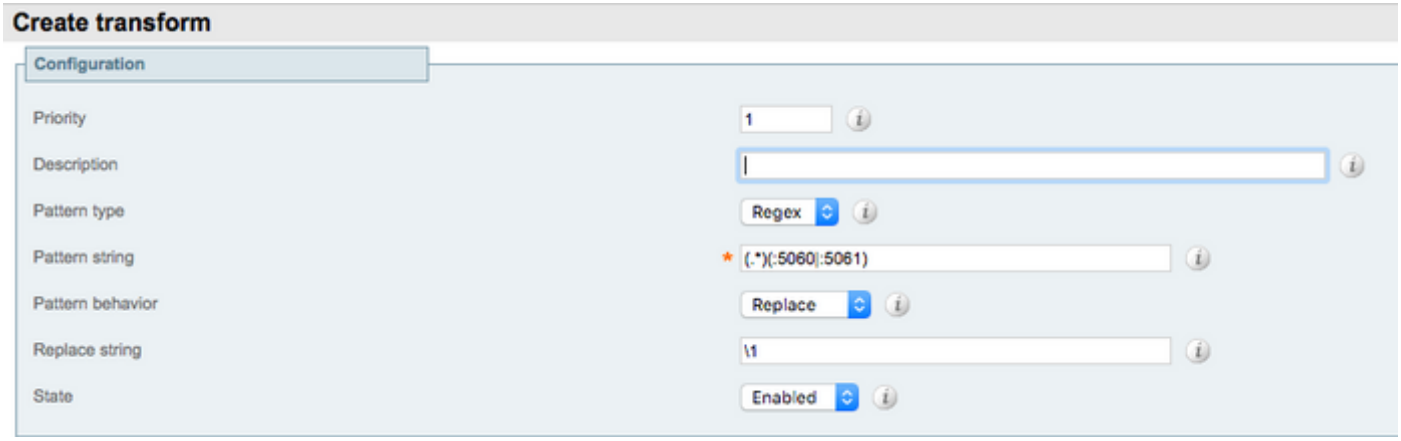
Lösung

Um dieses Problem zu beheben, erstellen Sie einfach eine Transformation, die den Port am Ende entfernt (auf jedem Server ist es egal), bevor er die DNS-Zone erreicht.

Navigieren Sie auf **der Expressway Administration-Seite zu Konfiguration > Wählplan > Umwandeln in Konfiguration > Wählplan > Umwandeln**

Transformiert Beispiele:





Wenn eine Transformation aus irgendeinem Grund nicht erstellt werden kann, kann sie auch mithilfe von Suchregeln durchgeführt werden. Es wird jedoch empfohlen, dies durch Transformationen zu tun.

Navigieren Sie auf der **Seite für die Schnellstraßen-Verwaltung** zu **Konfiguration > Wählplan > Umwandeln in Konfiguration > Wählplan > Suchregeln.**

Zugehörige Informationen

- Cisco VCS Expressway und VCS Control - Grundkonfiguration