在多域部署中通過Expressway/VCS配置移動和遠端訪問

目錄

簡介

本檔案介紹當使用多個網域時，如何設定行動遠端存取(MRA)的思科網真視訊通訊伺服器(VCS)。

當只有一個域時設定的MRA相對簡單，您可以按照部署指南中記錄的步驟操作。當部署涉及多個域時，會變得更加複雜。本文檔不是配置指南，但描述了涉及多個域時的重要方面。主要配置記錄在思科網真影片通訊伺服器(VCS)部署指南中。

必要條件

需求

本文件沒有特定需求。

採用元件

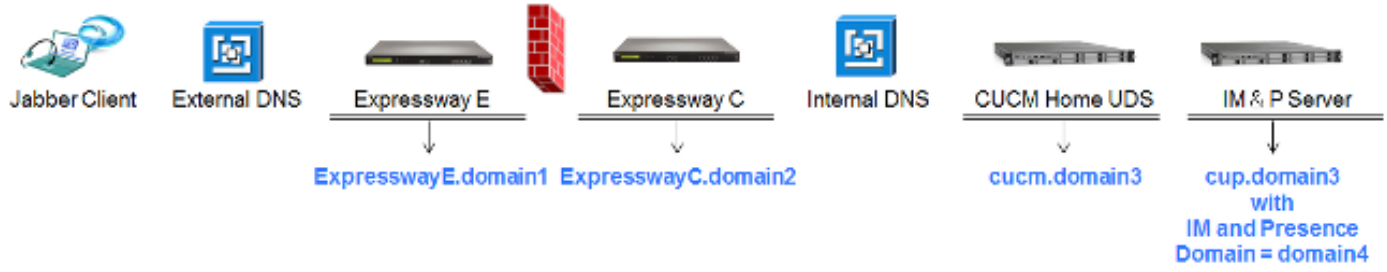
本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

使用本節中介紹的資訊配置VCS。

網路圖表

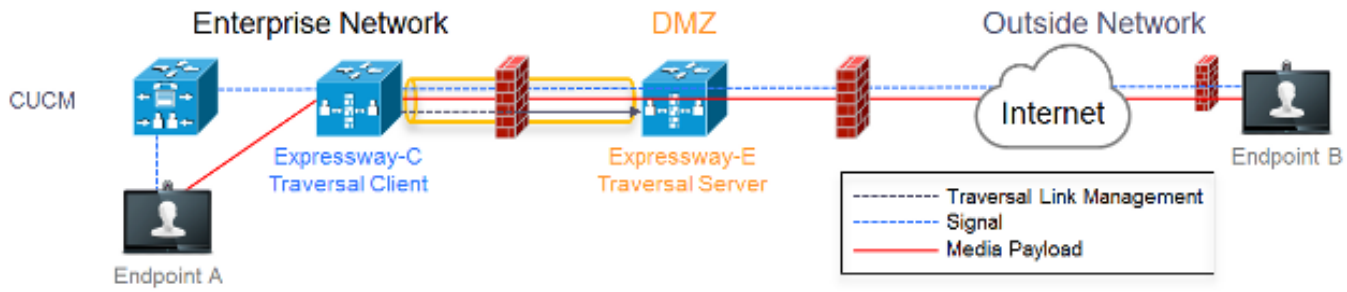


以下是不同網域的簡短概觀：

- **domain1** — 這是客戶端用於發現邊緣伺服器位置並從中發現使用者資料服務(UDS)的邊緣域。
- **domain2和domain3** -用於伺服器發現。
- **domain4** -這是可擴展通訊平台(XCP)和可擴展消息傳送和線上狀態協定(XMPP)流量使用的即時消息和線上狀態(IM&P)域。

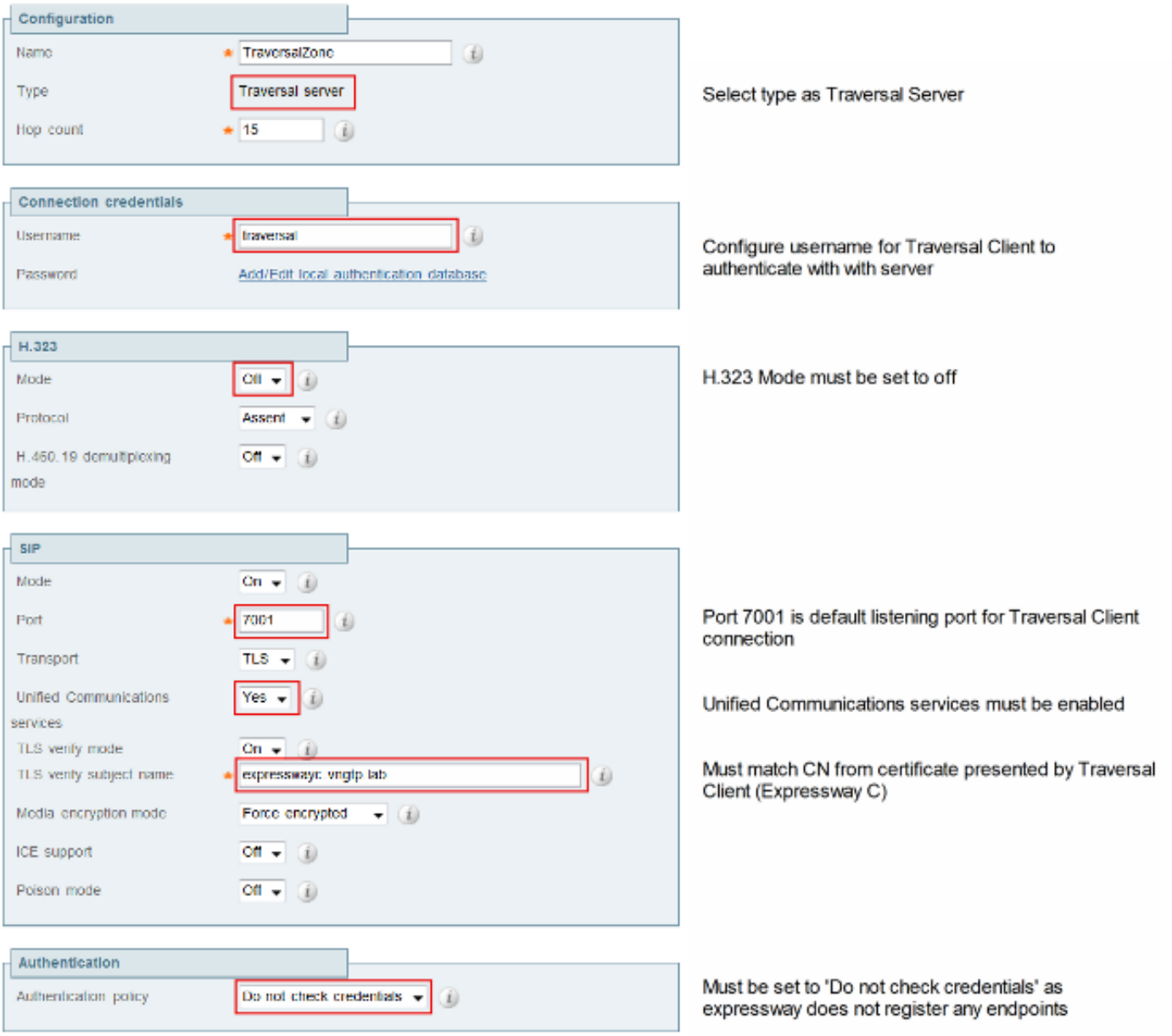
遍歷區域

遍歷區域由位於非軍事化區域(DMZ)中的遍歷伺服器(**expresswayE**)和位於網路內部的遍歷客戶端(**expresswayC**)組成：



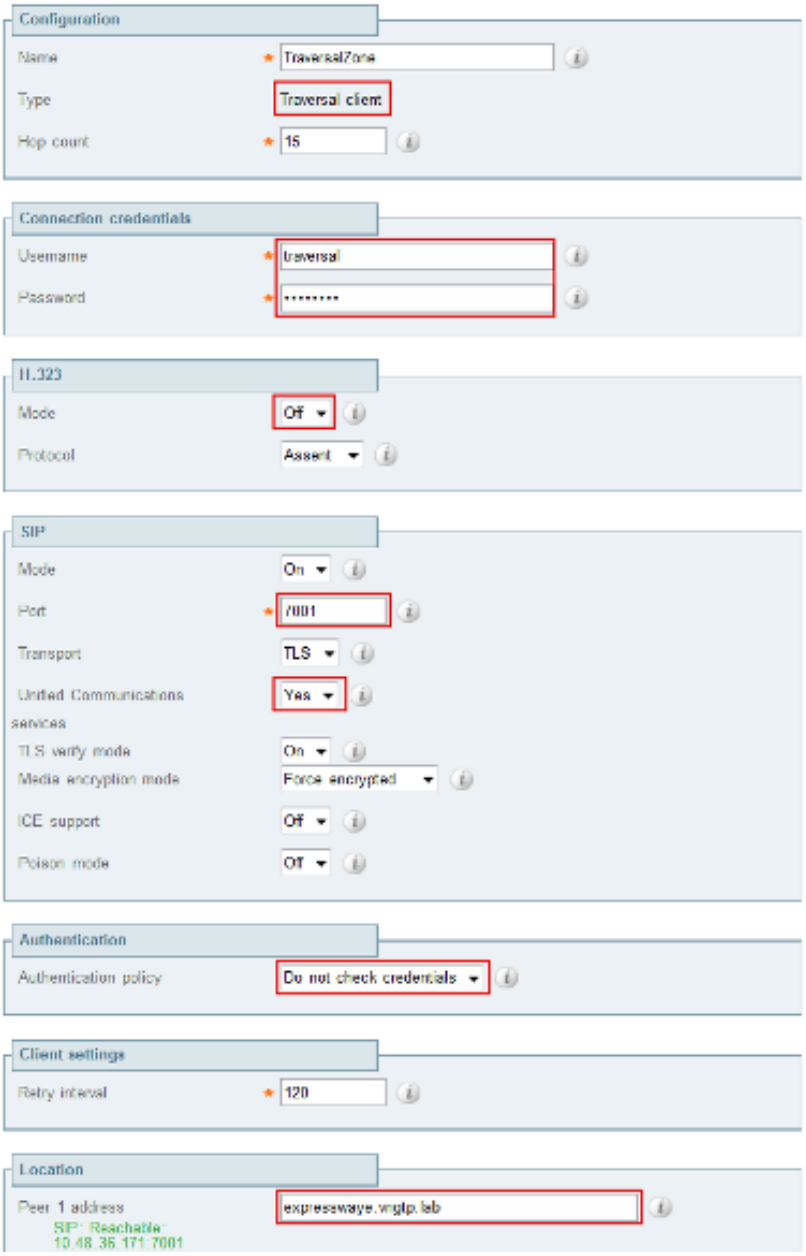
遍歷伺服器

遍歷伺服器位於Expressway E上的區域配置中：



穿越客戶端

穿越客戶端位於Expressway C上的區域配置中：



Select Traversal Client as Type

Configure same username and password as added on the Traversal Server (Expressway E)

H.323 mode must be set to off

Destination port Traversal Server is listening on

Unified Communications must be enabled

Must be set to 'Do not check credentials' as expressway does not register any endpoints

Must be FQDN
Must be DNS resolvable
Must match CN from certificate presented by Traversal Server (Expressway E)

語音服務網域

使用者一律使用**userid@domain4**登入，因為無論在內部還是外部使用者體驗方面應該沒有差異。這表示如果**domain1**與**domain4**不同，則必須在Jabber客戶端中配置語音服務域。這是因為登入名的域部分用於發現使用服務(SRV)記錄查詢的合作邊緣服務。

客戶端對_collab-edge._tls.<domain>執行域名**系統**(DNS)**SRV記錄查詢**。這意味著當登入使用者ID中的域與Expressway E中的域不同時，必須使用語音服務域配置。Jabber使用此配置來發現合作邊緣和UDS。

您可以使用多個選項來完成此任務：

1. 通過媒體服務介面(MSI)安裝Jabber時，請新增此引數作為引數：

```
msiexec /i CiscoJabberSetup.msi VOICE_SERVICES_DOMAIN=domain1 CLEAR=1
```

2. 導航到**%APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config**，然後在目錄中建立此**jabber-config-user.xml**檔案：

```
<?xml version="1.0" encoding="utf-8"?>
<config version ="1.0">
<Policies> <VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
</config>
```

附註：此方法只是實驗性的方法，不受Cisco正式支援。

3. 編輯**jabber-config.xml**文件。這要求客戶端首先在內部登入。Jabber組態檔產生器可用於以下專案：

```
<Policies>
<VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
```

4. 此外，移動Jabber客戶端可以預先配置語音服務域，因此無需先在內部登入。Service Discovery一章的《部署和安裝指南》中對此進行了說明。您必須建立使用者需要點選的配置URL：

```
ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1
```

附註：必須使用語音服務域，因為必須確保為外部域(**domain1)的合作邊緣SRV記錄執行查**找。

DNS記錄

本節介紹外部和內部DNS記錄的配置設定。

外部

類型	條目	解析為
SRV記錄	_collab-edge._tls.domain1	ExpresswayE.domain1
記錄	ExpresswayE.domain1	IP地址ExpresswayE

必須注意的是：

- SRV記錄返回完全限定的域名(FQDN)而不是IP地址。
- SRV記錄返回的FQDN必須與Expressway-E的實際FQDN匹配，或者SRV記錄目標為CNAME，且別名指向與Expressway-E位於同一域內的伺服器(掛起的思科錯誤ID CSCuo82526)。

這是必需的，因為Expressway-E在客戶端上設定了具有其自己的域(**domain1**)的cookie，並且如果該cookie與FQDN返回的域不匹配，則客戶端不會接受該設定。已開啟思科錯誤ID CSCuo83458，作為此案例的增強功能。

內部

類型	條目	解析為
SRV記錄	_cisco-uds._tcp.domain1	cucm.domain3
記錄	cucm.domain3	IP address CUCM

由於語音服務域設定為**domain1**，因此Jabber在合作邊緣配置發現(**get edge_config**)的轉換URL中嵌入**domain1**。 收到後，Expressway-C將對**domain1**執行SRV UDS記錄查詢，並返回**200 OK**消息

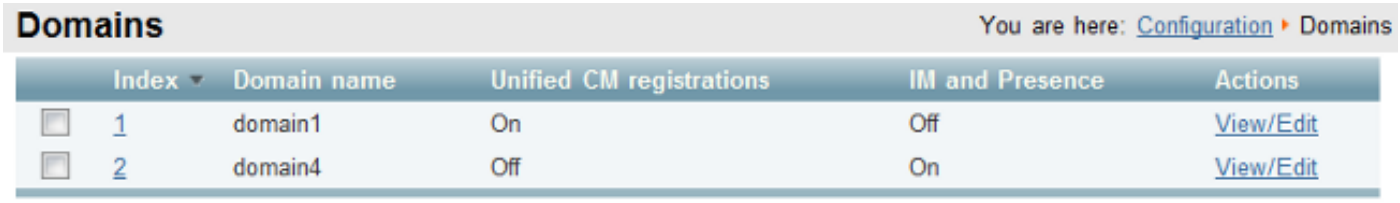
中的記錄。

類型	條目	解析為
SRV	_cisco-uds._tcp.domain4	cucm.domain3
記錄	cucm.domain3	IP address CUCM

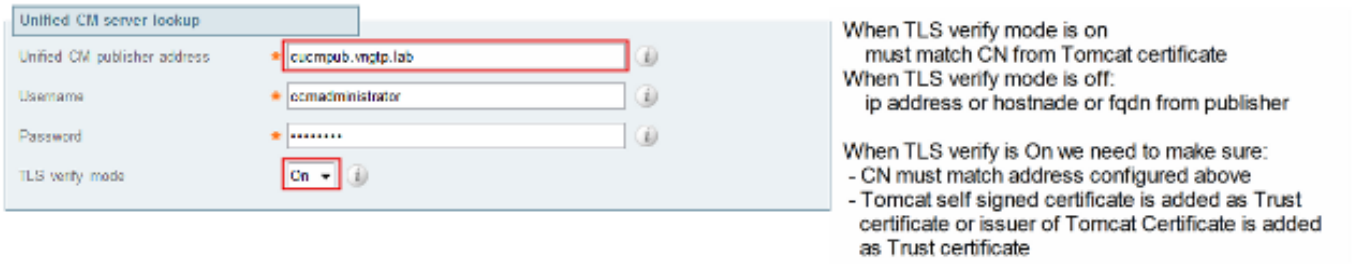
當客戶端在網上時，**domain4**需要SRV UDS記錄**發現**。

Expressway-C上的SIP域

您必須在Expressway-C上新增以下會話發起協定(SIP)域並啟用它們以進行MRA:



主機名/IP地址CUCM伺服器



配置Cisco Unified Communications Manager(CUCM)伺服器時，有兩種情況：

- 如果您的Expressway-C(**domain2**)配置了與CUCM伺服器(**domain3**)相同的域，則可以使用以下內容配置CUCM伺服器(**System > Servers**):

  IP地址主機名FQDN
- 如果為Expressway-C(**domain2**)配置的域與CUCM伺服器(**domain3**)不同，則必須使用以下內容配置CUCM伺服器：

  IP地址FQDN

這是必需的，因為當Expressway-C發現CUCM伺服器並返回主機名時，它會對**hostname.domain2**執行DNS查詢，如果**domain2**和**domain3**不同，則查詢不起作用。

憑證

除了常規證書要求外，還必須向證書的使用者替代名稱(SAN)新增一些內容：

- Expressway-C

  必須新增在IM&P伺服器上配置的聊天節點別名。只有打算同時使用傳輸層安全(TLS)和群聊的統一通訊XMPP聯合部署才需要此功能。如果已經發現IM&P伺服器，則會將此項自動新增到證書簽名請求(CSR)。

必須新增CUCM中所有為加密TLS配置並用於需要遠端訪問的裝置的電話安全配置檔案的名稱（FQDN格式）。
附註：僅當證書頒發機構(CA)在SAN中不允許主機名語法時，才需要FQDN格式。

- Expressway-E

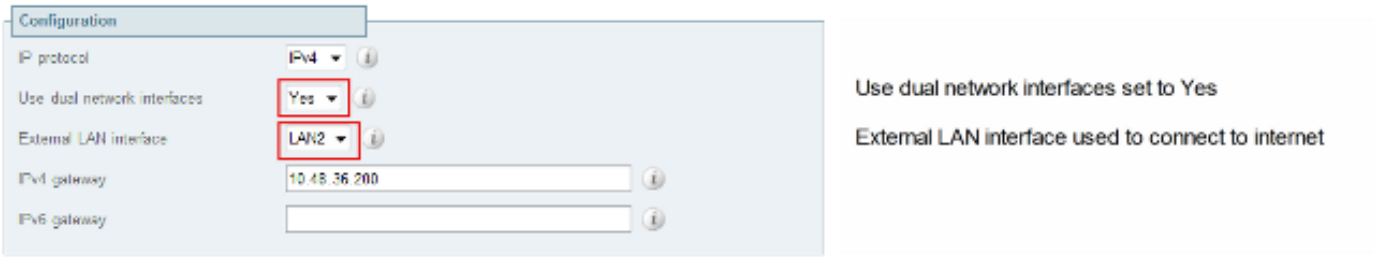
必須新增用於服務發現**的域**(**domain**1)。 XMPP聯合域。必須新增在IM&P伺服器上配置的聊天節點別名。只有打算同時使用TLS和群組聊天的Unified Communications XMPP聯合部署才需要此功能。可從Expressway-C上產生的CSR複製這些封包。

雙NIC

本節介紹使用雙網路介面卡(NIC)時的組態設定。

兩個介面

配置Expressway-E以使用雙網路介面時，確保兩個介面都配置並使用非常重要。



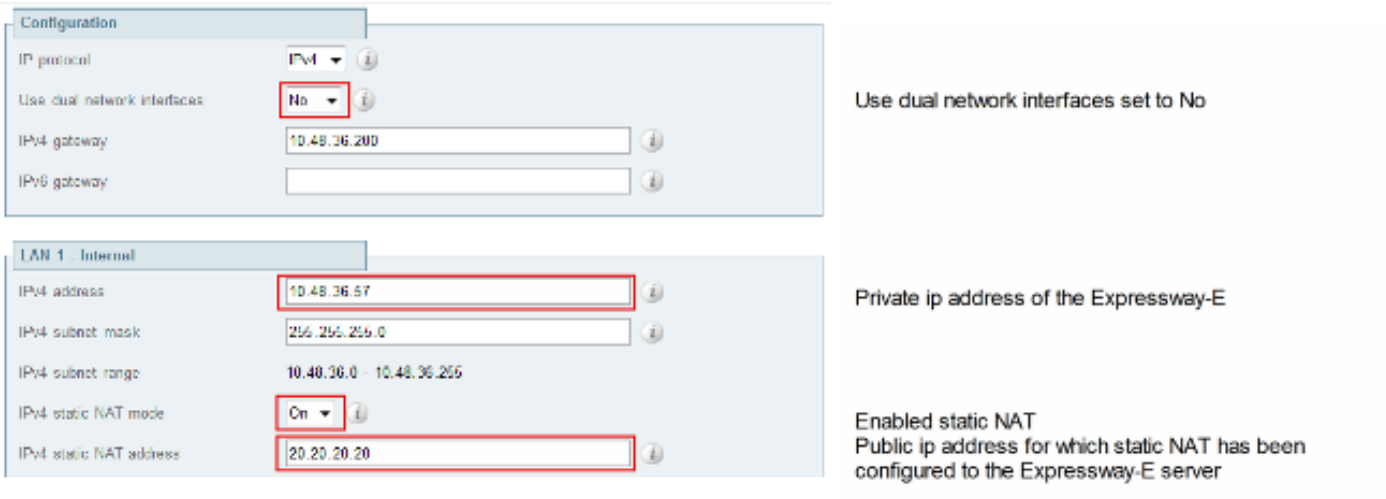
當**使用雙網路介面**配置了**Yes**值時，Expressway-E僅偵聽內部介面上與Expressway-C進行XMPP通訊。因此，必須確保已配置此介面並且工作正常。

一個介面 — 公共IP地址

如果僅使用一個介面，並且使用公共IP地址配置Expressway-E，則無需考慮任何特殊因素。

一個介面 — 專用IP地址

如果僅使用一個介面，並且使用私有IP地址配置Expressway-E，則必須配置靜態網路地址轉換(NAT)地址：



在這種情況下，必須確保：

- 防火牆允許Expressway-C將流量傳送到公共IP地址。這稱為*NAT反射*。
- Expressway-C上的遍歷客戶端區域配置了與Expressway-E上的靜態NAT地址匹配的對等地址，在本例中為**20.20.20**。

  提示：有關高級網路部署的更多資訊，請參閱思科網真影片通訊伺服器基本配置（使用Expressway進行控制）部署指南的**附錄4**。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

本節將介紹一些特定案例，但是您還可以使用Collaboration Solutions Analyzer，它提供有關MRA登入嘗試的所有通訊的詳細資料以及基於診斷日誌的疑難排解資訊。

遍歷區域

當對等體位址設定為IP位址，或對等體位址與公用名稱(CN)不匹配時，會在記錄中看到以下內容：

```
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.80.161"
Src-port="25697" Dst-ip="10.48.36.171" Dst-port="7001" Detail="Peer's TLS
certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.36.171"
```

當密碼不正確時，您可以在Expressway-E日誌中看到以下內容：

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found in
directory for identity: traversal"

Module="developer.nomodule" Level="WARN" CodeLocation="ppcmains/sip/sipproxy/
```

```
SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::
checkDigestSAResponse" Thread="0x7f2485cb0700": calculated response does not
match supplied response, calculatedResponse=769c8f488f71eebdf28b61ab1dc9f5e9,
response=319a0bb365decf98c1bb7b3ce350f6ec

Event="Authentication Failed" Service="SIP" Src-ip="10.48.80.161"
Src-port="25723" Detail="Incorrect authentication credential for user"
Protocol="TLS" Method="OPTIONS" Level="1"
```

雙NIC

啟用雙NIC但第二個介面未使用或連線時，Expressway-C無法連線到Expressway-E進行埠7400上的XMPP通訊，而Expressway-C日誌會顯示此情況：

```
xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,843" ThreadID=
"139747212576512" Module="Jabber" Level="INFO " CodeLocation="mio.c:1109"
Detail="Connecting on fd 28 to host '10.48.36.171', port 7400"xwayc

XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID="139747212576512"
Module="Jabber" Level="ERROR" CodeLocation="mio.c:1121" Detail="Unable to
connect to host '10.48.36.171', port 7400:(111) Connection refused"

xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID=
"139747406935808" Module="Jabber" Level="ERROR" CodeLocation=
"base_connection.cpp:104" Detail="Failed to connect to component
jabberd-port-1.expresswayc-vngtp-lab"
```

DNS

當Collaboration Edge的SRV記錄查詢返回的FQDN與Expressway-E上配置的FQDN不匹配時，Jabber日誌會顯示以下錯誤：

```
WARNING [9134000] - [csf.edge][executeEdgeConfigRequest] XAuth Cookie expiration
time is invalid or not available. Attempting to Failover.

DEBUG [9134000] - [csf.edge][executeEdgeConfigRequest]Failed to retrieve
EdgeConfig with error:INTERNAL_ERROR
```

在Expressway-E的診斷日誌中，可以看到HTTPS消息中針對哪個域設定了cookie:

```
Set-Cookie: X-Auth=1e1111e1-dddb-49e9-ad0d-ab34526e2b00; Expires=Fri,
09 May 2014 20:21:31 GMT; Domain=.vngtp.lab; Path=/; Secure
```

SIP域

在Expressway-C上未新增所需的SIP域時，Expressway-E不接受此域的消息，並且在診斷日誌中您會看到傳送到客戶端的403 Forbidden消息：

```
ExpresswayE traffic_server[15550]:
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response"
Txn-id="2" Dst-ip="10.48.79.80" Dst-port="50314"
HTTPMSG:
|HTTP/1.1 403 Forbidden
Date: Wed, 21 May 2014 14:31:18 GMT
Connection: close
Server: CE_E
```

```
Content-Length: 0

ExpresswayE traffic_server[15550]: Event="Sending HTTP error response"
Status="403" Reason="Forbidden" Dst-ip="10.48.79.80" Dst-port="50314"
```