通過Expressway到Cisco Meeting Server對Microsoft Federation上的DNS和證書要求進行配置和故障排除

目錄

簡介

本文檔介紹Microsoft Lync/Skype for Business對通過Internet在不同域之間進行聯盟的DNS和證書要求。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Expressway
- CMS（思科會議伺服器）
- Microsoft Lync或Skype for Business伺服器
- CUCM（思科統一通訊管理器）

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Expressway X8.9或更高版本
- Cisco Meeting Server(CMS)2.1.2或更高版本

- Microsoft Lync 2010 server、Lync 2013 server或Skype for Business server — 內部部署或在雲中託管(Office365)

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

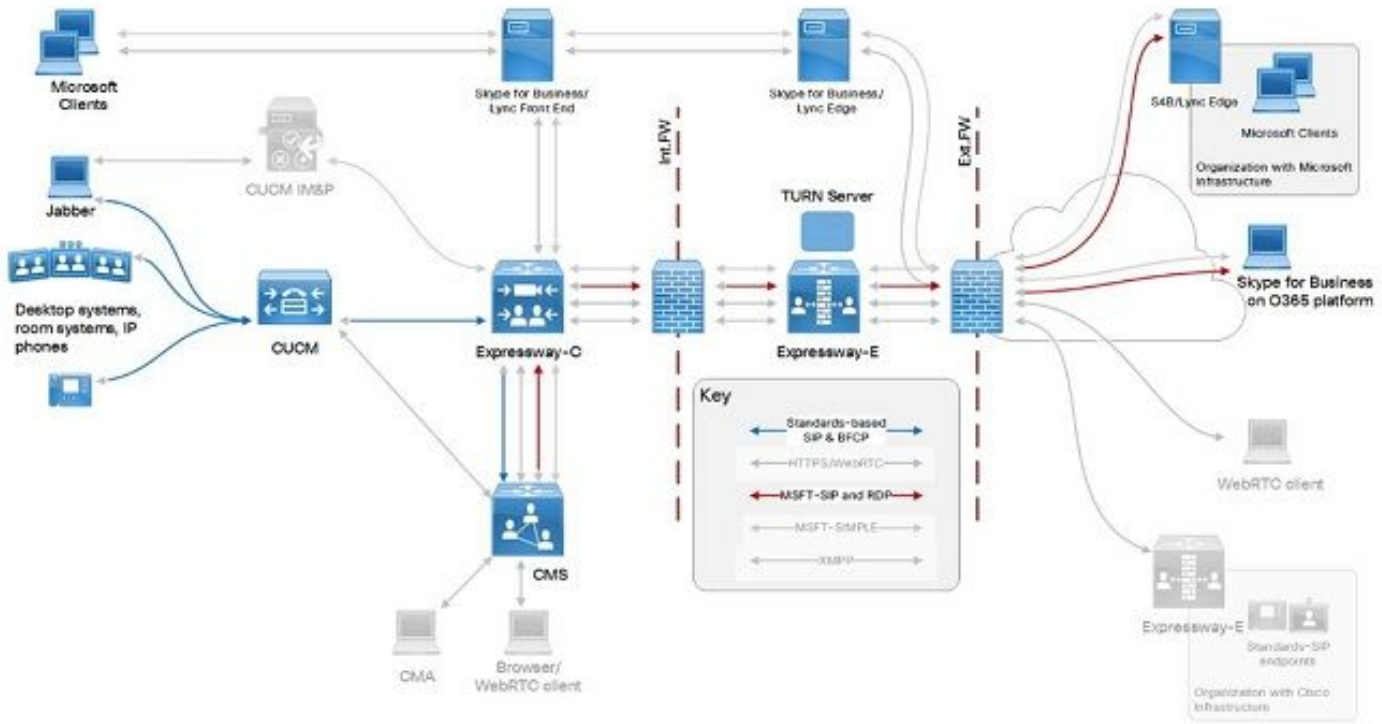
本文檔重點介紹使用Expressway和Cisco Meeting Server(CMS)與外部Microsoft客戶端與思科基礎設施整合的特定方面。 此整合的配置如**Cisco Expressway與Cisco會議伺服器的Cisco Expressway選項和/或Microsoft Infrastructure文檔(可從**Cisco Expressway系列配置指南清單中獲取您的版本)中所述。

當前文檔僅重點介紹用於外部聯盟的Microsoft Lync或Skype for Business終端上的DNS和證書要求。上述參考配置指南中介紹了其他配置。

設定

例如，呼叫流及其配置可以是CUCM註冊終端，該終端撥號到Skype客戶端（內部或外部或使用Office365在雲中註冊），反之亦然 — 使用CMS進行標準SIP和Microsoft協定之間的轉換。這可以通過使用Expressway伺服器的整合和呼叫路由實現，如下圖所示，該圖取自本文檔結尾處引用的**Cisco Expressway選項與Cisco Meeting Server和/或Microsoft基礎設施配置指南**。

網路圖表



附註：這只是一個示例性的呼叫流程場景。也可能出現其他呼叫情況。

DNS

Microsoft Lync/Skype for Business使用**_sipfederationtls._tcp.<domain>** SRV記錄來發現要將呼叫傳送到的外部聯合伺服器（以及狀態資訊）；或者，對於基於在傳入**SIP INVITE的From/P-Asserted-Identity標頭中指定的域的回叫**功能。在此案例中，兩個網域的DNS記錄必須在公用DNS上可用，以便彼此建立聯盟。

域的SRV記錄查詢返回的**FQDN**（完全限定域名）的域部分必須完全匹配（不允許其他域或子域）。 下表顯示名為**example.com**的域的DNS配置示例：

SRV記錄	_sipfederationtls._tcp.example.com	expe.example.com
記錄	expe.example.com	Expressway-E的IP地址

> **注意**：SRV解析為A記錄必須在配置的域上完全匹配。Microsoft Lync/Skype for Business不會信任子域(例如expe.sub.example.com)或其他域(expe.dummy.com)，這將導致呼叫失敗，即使子域可能具有適當的A記錄並解析為正確的IP。

憑證

Microsoft Lync/Skype for Business在Lync和Expressway端配置的域之間設定TLS連線。Microsoft Lync/Skype for Business對聯盟及其正在與之通訊的伺服器（本文檔中的Expressway-E）具有以下伺服器證書要求：

- 與A記錄匹配的伺服器提供的伺服器證書必須包含其主題備用名稱中包含的特定**FQDN**(如果不使用SAN，則為**公用名稱**)
- 伺服器提供的伺服器證書需要由Microsoft Lync/Skype for Business伺服器信任(由公共CA簽名，或由在Microsoft Lync/Skype for Business伺服器的**受信任CA清單中匯入其根/中間證書的專用CA簽名)。** 請注意，使用Office365時，需要公共CA簽名證書。

例如：

如上例所示，與**expe.example.com**匹配的Expressway-E伺服器的伺服器證書必須至少包含以下條目：

- (除非沒有**主題替代名稱**)**公用名**必須是**expe.example.com**
- (如果**主題備用名**稱可用)**主題備用**名必須包含**條目expe.example.com**
- 證書樹頂部的頒發者必須是公共CA(或者需要在Microsoft Lync/Skype伺服器的**受信任CA清單中新增**CA)

附註：

域(example.com)本身不需要作為主體替代名稱**包括在內**。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

本節包含從測試實驗室部署獲取的日誌資訊和跟蹤，其規格如下：

- Skype域是skype.lab
- UC域（Expressway-E、Expressway-C和CUCM）為steven.lab
- 使用者和空間的CMS域為acano.steven.lab（也可使用cms.steven.lab）

由於建議為思科會議伺服器使用單獨的域（不同於UCM/Expressway上的其他UC域），因此您的

Expressway-E伺服器上可能有不同的域，這可能導致與Microsoft Lync/Skype for Business伺服器端SIP聯合要求相關的整合問題。

症狀和日誌審查

Microsoft Lync/Skype伺服器端DNS證書的要求不匹配時，您會發現以下症狀：

- 當從您的UC基礎設施向Microsoft Lync/Skype發出呼叫時，您會看到在Expressway-E的DNS區域向Skype傳出的呼叫，但會立即引發(504)伺服器超時錯誤，在Expressway-E的**Status > Search History**頁面上會顯示此錯誤：

- 從Microsoft Lync/Skype向您的UC基礎設施發出呼叫時，您不會看到呼叫到達Expressway-E，如Expressway-E的**Status > Search History**頁面所示。

此小節說明如何使用詳細記錄來驗證此情境，並檢查究竟什麼配置錯誤。

致電Microsoft Lync/Skype

在此呼叫流程中，您在Expressway-E的診斷日誌記錄中會看到指向Skype的SIP INVITE(如果它可以將**_sipfederationtls._tcp** SRV記錄解析為FQDN和IP)，緊接著是**504 Server超時響應**，沒有任何詳細資訊，如以下日誌記錄片段所示：

```
2017-03-02T08:10:46.240+01:00 vcse tvcs: UTCTime="2017-03-02 07:10:46,240" Module="network.sip"
Level="DEBUG":  Action="Received" Local-ip="10.48.36.47" Local-port="25002" Src-ip="10.48.36.6"
Src-port="5061" Msg-Hash="13707918855517357847"
 SIPMSG:
 |SIP/2.0 504 Server time-out
 Via: SIP/2.0/TLS 10.48.36.47:5061;egress-
zone=DNSZone1;branch=z9hG4bK42ee6fd77d32cc8925196770b950b33554.731d73c3f4246d6a255e38a9f695bfc0;
proxy-call-id=6b2a018a-2da5-4013-a7e5-4e1455feadf7;rport;received=10.48.36.47;ms-received-
port=25002;ms-received-cid=100
 Via: SIP/2.0/TLS 10.48.36.46:5061;egress-
zone=TraversalZoneClient1;branch=z9hG4bK1f8bbe5926dc6abd06ea964d8fde1450156486;proxy-call-
id=e7e33845-c384-4c28-a42d-016863640fbb;received=10.48.36.46;rport=28119;ingress-
zone=TraversalZoneServer1
 Via: SIP/2.0/TLS
10.48.54.160:52768;branch=z9hG4bK6594a02846406f4a5459d5f58a8d26b3;received=10.48.54.160;ingress-
zone=NeighborZoneAcano1SIP
 Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960
 CSeq: 2066245576 INVITE
 From: "DX70 Steven" <sip:2000@acano.steven.lab>;tag=9fea3e7d70afd884
 To: <sip:stejanss@skype.lab>;tag=C65A7B0A8766A5F1D386474833D07882
 Server: RTC/6.0
 Content-Length: 0
```

無論是DNS記錄或Expressway-E的伺服器證書上的故障，都會顯示相同的響應（沒有任何詳細資訊）。

因此，要更詳細地檢視該報告，您必須檢視Lync/Skype邊緣伺服器日誌記錄，在該日誌中您可以看到警告和錯誤，具體取決於可能發生的故障：

- 可能的錯誤：SRV記錄的FQDN結果在域上不完全匹配，與傳入Skype的INVITE的**From/P-Asserted-Identity**標頭中的完全匹配。在此日誌代碼段中，SIP INVITE的From/P-Asserted-Identity標頭包含acano.steven.lab作為域，但**_sipfederationtls._tcp.acano.steven.lab**指向**vcse.steven.lab**，而不是**vcse.acano.steven.lab**:

TL_WARN(TF_DIAG) [sfvedge\sfvedge]0584.0A44::03/02/2017-07:10:46.230.0000773E (SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(830)) [156659184] $$begin_record Severity: warning Text: **The domain of the message resolved by DNS SRV but none of the FQDNs is in the same domain** Result-Code: 0xc3e93d6f SIPPROXY_E_EPROUTING_MSG_ALLOWED_DOMAIN_NO_SRV_MATCH SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0 SIP-Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960 SIP-CSeq: 2066245576 INVITE Peer: vcse.steven.lab:25002 Data: **domain**="**acano.steven.lab**";**fqdn1**="**vcse.steven.lab**:5061" $$end_record

- 可能的錯誤：Expressway-E伺服器的證書不包含由**_sipfederationtls._tcp SRV記錄生成**的FQDN。傳送相同的**SIP INVITE**，並且**_sipfederationtls._tcp.acano.steven.lab**指向**vcse.acano.steven.lab**，但Expressway-E伺服器的證書SAN清單中未包含該FQDN:

TL_ERROR(TF_DIAG) [sfvedge\sfvedge]0B60.0D6C::03/02/2017-06:30:40.025.00005602 (SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(833)) [3634190282] $$begin_record Severity: error Text: **Message cannot be routed because the peer's certificate does not contain a matching FQDN** Result-Code: 0xc3e93d67 SIPPROXY_E_ROUTING_MSG_CERT_MISMATCH SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0 SIP-Call-ID: e144704c-1dd0-4ea7-929f-77e7e071c24c SIP-CSeq: 1567605805 INVITE Peer: vcse.steven.lab:25001 Data: **expected-fqdn**="**vcse.acano.steven.lab**";**certName**="**vcse.steven.lab**";info="The peer certificate does not contain a matching FQDN" $$end_record

來自Microsoft Lync/Skype的呼叫

對於此呼叫流，您在Expressway-E的日誌記錄中看不到太多內容，因為Skype邊緣伺服器不會向外傳送INVITE，並且您需要依賴Skype日誌記錄。使用Lync/Skype（邊緣）伺服器日誌記錄或Lync/Skype客戶端日誌記錄本身來更深入地調查問題。

Windows PC上的Skype客戶端登入可從以下路徑獲得：

C:\Users\<username>\AppData\Local\Microsoft\Office\16.0\Lync\Tracing\Lync-UccApi-x.UccApiLog

當無法直接訪問Skype伺服器時，它對Office365 Skype使用者有用。*在此日誌記錄中，您可以看到客戶端發出的***SIP INVITE**消息以及相應的響應。

如果根據本文所述，您在Skype上遇到DNS或證書要求問題，則會從Skype伺服器收到**504 Server超時響應**（包括故障原因）：

- 可能的錯誤：在嘗試呼叫的域上，SRV記錄的FQDN結果不完全匹配。此日誌片段顯示嘗試使用域**cms.steven.lab**撥號到使用者或空間，並且**_sipfederationtls._tcp.cms.steven.lab**指向**vcse.sub.cms.steven.lab**:

SIP/2.0 **504 Server time-out** Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="8168D157", snum="38", rspauth="65d8d93b66e5b217115e3b1636bf433c9f5df54a", targetname="SfBFE.skype.lab", realm="SIP Communications Service", version=4 From: "Steven Janssens"

INVITE Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00 ms-diagnostics: 1009;

reason="No match for domain in DNS SRV results";

domain="

cms.steven.lab";

fqdn1="

vcse.sub.cms.steven.lab:5061";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

- 可能的錯誤：Expressway-E伺服器證書不包含由_sipfederationtls._tcp SRV記錄生成的FQDN。此日誌代碼段顯示嘗試使用域cms.steven.lab撥號到使用者或空間，其中_sipfederationtls._tcp.cms.steven.lab正確解析為vcse.cms.steven.lab，但此FQDN未包含在Expressway-E伺服器證書上的主題備用名稱中(通用名稱為vcse.steven.lab):

SIP/2.0 **504 Server time-out** Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="1D8F66EF", snum="49", rspauth="67836c7ffc0f6132b2304006969a219d9252aabd", targetname="SfBFE.skype.lab", realm="SIP Communications Service", version=4 From: "Steven Janssens"

INVITE Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00 ms-diagnostics: 1010;

reason="Certificate trust with another server could not be established";ErrorType="The peer certificate does not contain a matching FQDN";

tls-target="

vcse.cms.steven.lab";

PeerServer="

vcse.steven.lab";HRESULT="0x80090322(SEC_E_WRONG_PRINCIPAL)";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

相關資訊

- Cisco Expressway系列配置指南