通过 Expressway 连接思科 Meeting Server 实现 Microsoft 联合的 DNS 和证书要求的配置与故障排除

目录

简介

本文档介绍实现互联网上不同域的联合对 Microsoft Lync/Skype for Business 的 DNS 和证书的要求。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科 Expressway
- CMS（思科 Meeting Server）
- Microsoft Lync 或 Skype for Business 服务器
- CUCM（思科统一通信管理器）

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

- Microsoft Lync 2010 服务器、Lync 2013 服务器或 Skype for Business 服务器 - 本地或托管于云中 (Office365)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

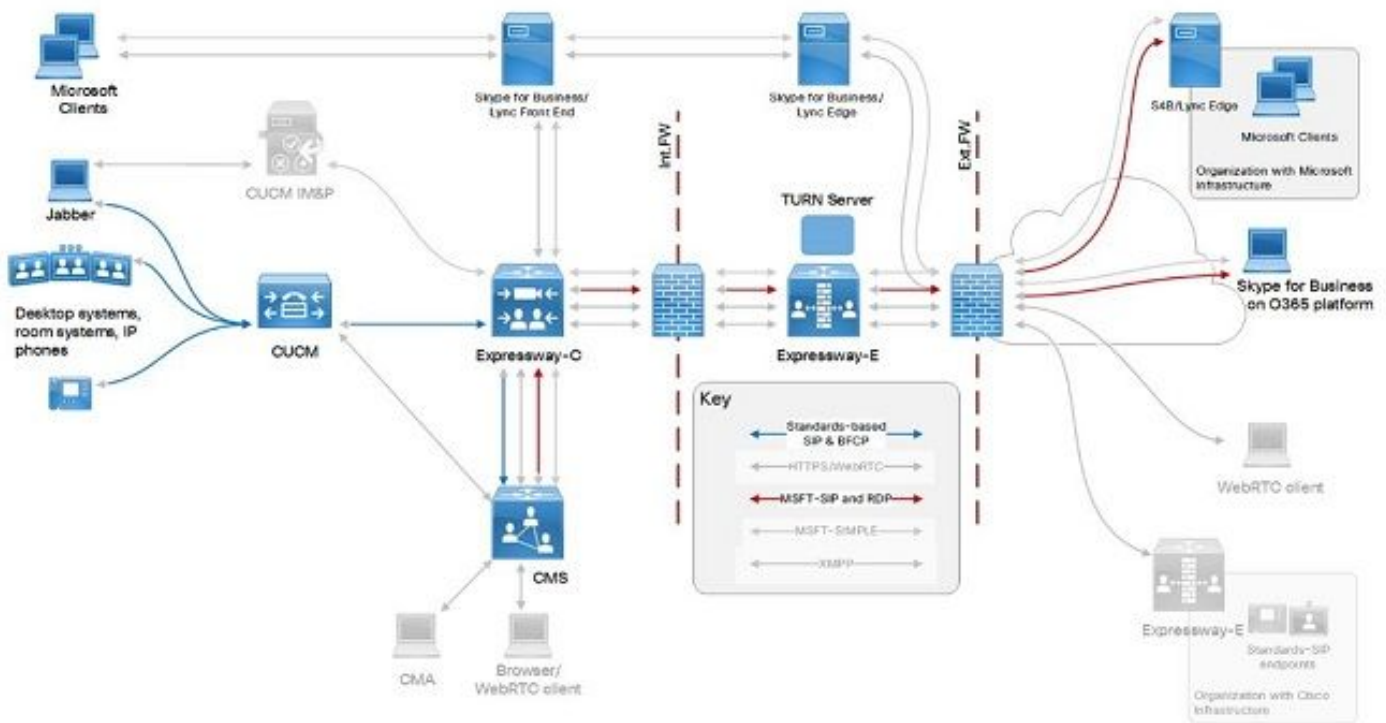
本文档重点介绍外部 Microsoft 客户端与使用 Expressway 和思科 Meeting Server (CMS) 的思科基础设施之间特定方面的集成。 此集成的配置详见于**思科 Expressway 的思科 Meeting Server 和/或 Microsoft 基础设施选项文档，可供您查看的版本位于**思科 Expressway 系列配置指南列表中。

目前的文档仅重点介绍实现外部联合对 Microsoft Lync 或 Skype for Business 终端的 DNS 和证书要求。其他配置信息涵盖在上面引用的配置指南中。

配置

呼叫流程及其配置的示例可以是 CUCM 注册终端向 Skype 客户端（本地或远程，或者使用 Office365 在云中注册）拨号，反之亦然，即使用 CMS 在标准 SIP 和 Microsoft 协议之间转换。这可通过集成和利用 Expressway 服务器实现呼叫路由实现（如下图所示），该图取自本文档末尾引用的**思科 Expressway 的思科 Meeting Server 和/或 Microsoft 基础设施选项配置指南**。

网络图



注意：这只是一个理论性的呼叫流程场景，也存在其他呼叫场景。

DNS

Microsoft Lync/Skype for Business 使用 **_sipfederationtls._tcp.<domain> SRV 记录来发现可向其发出呼叫（以及在线状态信息）的外部联合服务器；**或者根据收到的 **SIP 邀请的 From/P-Asserted-Identity 信头**中指定的域实现回叫功能。在此场景中，DNS 记录必须在两个域的公共 DNS 上可用，这两个域才能相互联合。

域的 SRV 记录轮询返回的 **FQDN（完全限定域名）的域名部分必须完全匹配（不允许使用其他域或子域）。** 下表显示了名称为 **example.com** 的域的 DNS 配置示例：

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

> **警告：**SRV 解析到的 A 记录必须是所配置的域上的完全匹配项。子域（例如 expe.sub.example.com）或不同域(expe.dummy.com)不受Microsoft Lync/Skype for Business信任，这将导致呼叫失败，即使它们可能具有适当的A记录并解析为正确的IP。

证书

Microsoft Lync/Skype for Business在Lync和Expressway端配置的域之间设置TLS连接。Microsoft Lync/Skype for Business对联盟及其通信的服务器（本文档中的Expressway-E）具有以下服务器证书要求：

- 符合 A 记录的服务器提供的服务器证书的**主题备用名称（如果使用 SAN，则为公用名）中必须包含该特殊的 FQDN**
- 服务器提供的服务器证书需要受 Microsoft Lync/Skype for Business 服务器信任（由公共 CA 签名，或者根/中间证书导入到 **Microsoft Lync/Skype for Business 服务器的受信任的 CA 列表中的私有 CA 签名）。** 请注意，使用 Office365 时，必须有使用公共 CA 签名证书。

例如：

符合 **expe.example.com 的 Expressway-E 的服务器证书（如上面的示例所示）必须至少有以下条目：**

- （仅当没有**主题备用名称**时）**公用名 必须是 expe.example.com**
- （如果有**主题备用名称）主题备用名称必须包含 entry expe.example.com**
- 证书树顶的颁发者必须是公共 CA（或者 CA 需要添加到 Microsoft Lync/Skype 服务器的**受信任的 CA 列表中）**

注意：

本身上的域(example.com)不需要作为主题备用名**包含在内**。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

该部分包含从具有以下规规格的测试实验室部署中获取的日志记录信息和跟踪信息：

- Skype 域是 skype.lab
- UC 域（Expressway-E、Expressway-C 和 CUCM）是 steven.lab
- 用户和空间的 CMS 域是 acano.steven.lab（也可以使用 cms.steven.lab）

因为建议为您的思科 Meeting Server 使用单独的域（不同于 UCM/Expressway 上的其他 UC 域

），很可能您的 Expressway-E 服务器上的域不同，这可能导致在 Microsoft Lync/Skype for Business 服务器端的 SIP 联合要求有关的集成问题。

症状和日志审核

如果 Microsoft Lync/Skype 服务器不符合 DNS 证书要求时，您会看到以下症状：

- 当从您的 UC 基础设施向 Microsoft Lync/Skype 发起呼叫时，您会看到呼叫通过 Expressway-E 的 DNS 区域传出到 Skype，但立即会抛出 (504) 服务器超时错误（详见于 Expressway-E 的**状态 > 搜索历史记录页面**）：

- 如果从 Microsoft Lync/Skype 向您的 UC 基础设施发起呼叫，则看不到呼叫到达 Expressway-E（如 Expressway-E 的**状态 > 搜索历史记录页面所示）。**

此子部分更详细地介绍如何使用日志记录验证此场景以及查看配置错误的具体设置。

呼叫 Microsoft Lync/Skype

在此呼叫流程中，您会在 Expressway-E 的诊断日志记录中看到 SIP 邀请前往 Skype（如果可以将 **_sipfederationtls._tcp SRV 记录解析为 FQDN 和 IP），随后立即出现 504 服务器超时响应，并且没有任何其他详细信息，如以下日志记录代码段所示：**

```
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
```

无论是 DNS 记录还是 Expressway-E 的服务器证书的故障问题，都会显示相同的响应（没有任何其他信息）。

要详细查看此响应，您必须查看 Lync/Skype Edge 服务器日志记录，在那里查看警告和错误（具体取决于可能发生的故障）：

- 可能的故障：域中 SRV 记录的 FQDN 结果与传入 Skype 的邀请的 **From/P-Asserted-Identity 信头不完全匹配。**在此日志代码段中，SIP INVITE的From/P-Asserted-Identity报头包含acano.steven.lab作为域，但**_sipfederationtls._tcp.acano.steven.lab**指向vcse.steven.lab，而非vcse.acano.

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

- 可能的故障：Expressway-E 服务器的证书不包含 **_sipfederationtls._tcp SRV 记录解析的 FQDN。**发送的是同一 **SIP 邀请，并且 _sipfederationtls._tcp.acano.steven.lab 指向 vcse.acano.steven.lab，但是 FQDN 未包含在 Expressway-E 服务器的证书 SAN 列表中：**

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

来自 Microsoft Lync/Skype 的呼叫

对于此呼叫流程，您通过 Expressway-E 的日志记录看不出很多信息，因为 Skype Edge 服务器未发送邀请，您需要依靠 Skype 日志记录。使用 Lync/Skype (Edge) 服务器日志记录或 Lync/Skype 客户端日志记录本身更深入地调查问题。

您可通过以下路径查找 Windows PC 上的 Skype 客户端日志记录：

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

如果在 Office365 Skype 用户无法直接访问 Skype 服务器时，这一点比较有用。在此日志记录中，您可以看到客户端发送了 **SIP 邀请消息以及该邀请相应的响应。**

如果您按照本文档中的操作方法遇到了 Skype 的 DNS 或证书要求方面的问题，会从 Skype 服务器收到 **504 服务器超时响应（包括失败原因）：**

- 可能的故障：尝试呼叫的域上的 SRV 记录的 FQDN 结果不完全匹配。此日志代码段显示尝试向域名为 **cms.steven.lab and the _sipfederationtls._tcp.cms.steven.lab 的用户或空间拨号指向 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
```

- 可能的故障：Expressway-E服务器证书不包含_sipfederationtls._tcp SRV记录产生的FQDN。此日志片段显示尝试使用域cms.steven.lab拨号到用户或空间 ,_sipfederationtls._tcp.cms.steven.lab正确解析为vcse.cms.stevenlab。包含在Expressway-E服务器证书上的“主题替代名称”(Subject Alternative Names)中（通用名称为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
```

相关信息

- 思科 Expressway 系列配置指南