Expressway 経由での Microsoft と Cisco Meeting Server のフェデレーションに関する DNS および証明書の要件の設定とトラブルシューティング

内容

概要

このドキュメントでは、インターネットでの異なるドメイン間のフェデレーションのための Microsoft Lync/Skype for Business の DNS および証明書の要件について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Expressway
- CMS（Cisco Meeting Server）
- Microsoft Lync または Skype for Business サーバ
- CUCM（Cisco Unified Communications Manager）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Expressway X8.9 以降
- Cisco Meeting Server（CMS）2.1.2 以降
- Microsoft Lync 2010 サーバ、Lync 2013 サーバまたは Skype for Business サーバ：オンプレミスまたはクラウド（Office365）でホスト

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

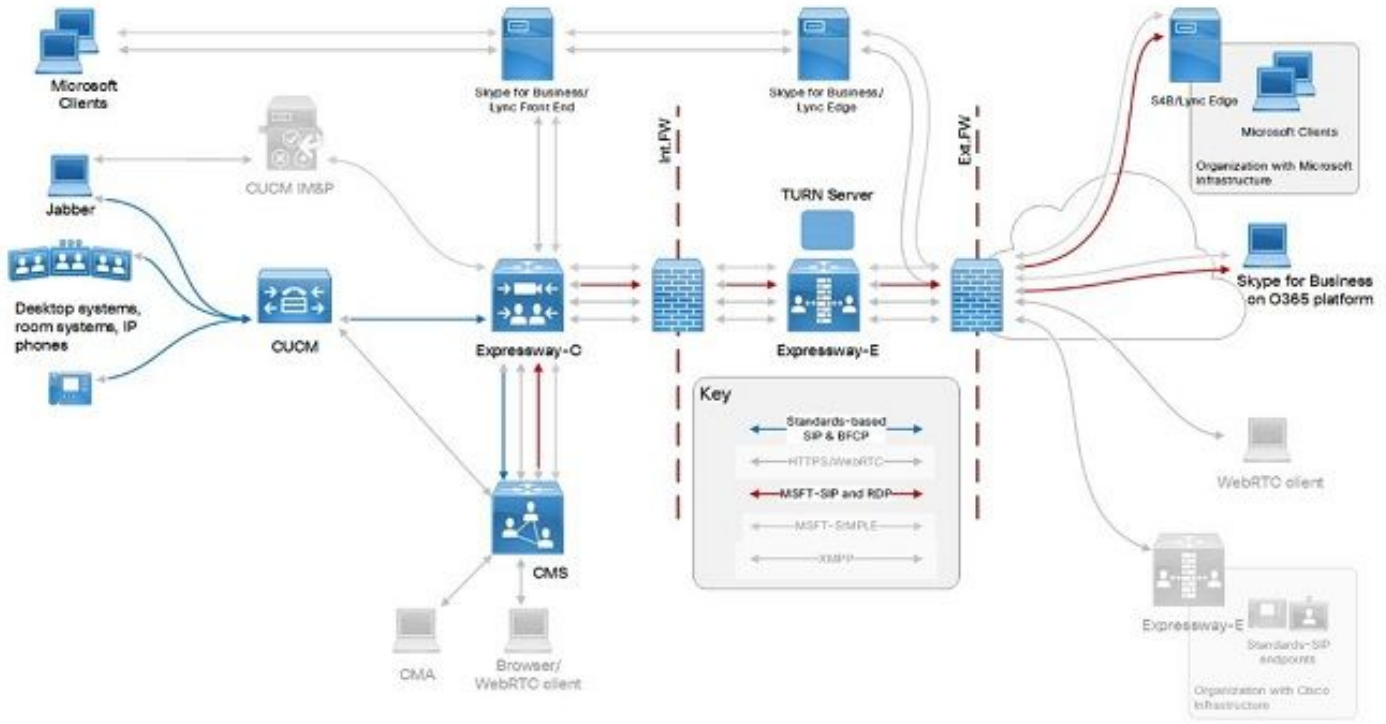
このドキュメントでは、Expressway および Cisco Meeting Server（CMS）を使用して外部 Microsoft クライアントとシスコ インフラストラクチャを統合する特定の側面について説明します。 この統合の設定については、Cisco Expressway Series 設定ガイド リストにある、ご使用のバージョン用の『**Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure』ドキュメントで説明しています。**

現在のドキュメントでは、外部フェデレーションのための Microsoft Lync または Skype for Businesse の DNS および証明書の要件のみを扱います。その他の設定については、上記の設定ガイドで説明しています。

設定

コール フローとその設定の例として、標準 SIP と Microsoft プロトコル間の会話に CMS を使用し、Skype クライアント（オンプレミス、オフプレミス、または Office365 を使用してクラウドに登録済み）にダイヤルする（または Skype クライアントからダイヤルされる）、CUCM に登録されている エンドポイントが考えられます。次の図に示すように、これは Expressway サーバを使用した統合およびコール ルーティングによって実現されます。これは、このドキュメントの最後に参照先として示す**『Cisco Expressway Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure』設定ガイド**からの引用です。

ネットワーク図



注：これは、模範的なコール フロー シナリオです。その他のコールのシナリオも可能です。

DNS

Microsoft Lync/Skype for Business は、**_sipfederationtls._tcp.<ドメイン> SRV レコードを、コール（およびプレゼンス情報）の送信先となる外部フェデレーション サーバを検出するために、**または、着信 **SIP INVITE の From/P-Asserted-Identity** ヘッダーで指定されているドメインに基づくコールバック機能用に使用します。このシナリオでは、両方のドメインが互いに連携するには、パブリック DNS で DNS レコードが使用可能である必要があります。

SRV レコードのドメイン検索で返される **FQDN（完全修飾ドメイン名）のドメイン部分は、正確に一致する必要があります（他のドメインまたはサブドメインは許可されません）。** 次の表に、**example.com** という名前のドメインの DNS 設定の例を示します。

SRV レコード	_sipfederationtls._tcp.example.com	expe.example.com
A レコード	expe.example.com	Expressway-E の IP アドレス

注意：SRV が解決する A レコードは、設定されているドメインと完全に一致する必要があります。サブドメイン(expe.sub.example.comなど)または異なるドメイン(expe.dummy.com)はMicrosoft Lync/Skype for Businessによって信頼されず、適切なAレコードを持っている可能性があり、IPを修正するために解決される場合でもコールが失敗します。

証明書

Microsoft Lync/Skype for Businessは、Lync側とExpressway側で構成されたドメイン間にTLS接続を設定します。Microsoft Lync/Skype for Businessには、フェデレーションと通信先のサーバ（このドキュメントのExpressway-E）に関する次サーバ証明書の要件があります。

- A レコードと一致するサーバによって提示されるサーバ証明書は、その**サブジェクト代替名（SAN を使用していない場合は共通名）に含まれている特定の FQDN** が存在する必要があります。
- サーバによって提示されるサーバ証明書は、Microsoft Lync/Skype for Business サーバによって信頼されている（パブリック CA またはプライベート CA（そのルート/中間証明書が **Microsoft Lync/Skype for Business サーバの信頼済み CA リストにインポートされている）のいずれかによって署名されている）必要があります。** Office365 を使用する場合はパブリック CA 署名付き証明書が必要です。

以下に、いくつかの例を示します。

上記の例に示した **expe.example.com と一致する Expressway-E サーバのサーバ証明書には、次の最小エントリが存在する必要があります。**

- （**サブジェクト代替名**がない場合のみ）**共通名は expe.example.com である必要があります。**
- （**サブジェクト代替名を使用できる場合）サブジェクト代替名に expe.example.com エントリが含まれている必要があります。**
- 証明書ツリーの最上位の発行元は、パブリック CA である必要があります（または CA を Microsoft Lync/Skype サーバの**信頼済み CA リストに追加する必要があります）。**

注：

ドメイン(example.com)自体をサブジェクト代替名として含める必要**はありません**。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

このセクションには、次の仕様のテスト ラボ展開環境から取得される口グ情報とトレースが含まれています。

- Skype ドメインは skype.lab
- UC ドメイン（Expressway-E、Expressway-C および CUCM）は steven.lab
- ユーザとスペース用の CMS ドメインは acano.steven.lab（cms.steven.lab も使用可能）

Cisco Meeting Server 用に別個の（UCM/Expressway 上の他の UC ドメインとは異なる）ドメインを使用することが推奨されているため、Expressway-E サーバ上に異なるドメインが存在する可能性があります。その場合、Microsoft Lync/Skype for Business サーバ側で SIP フェデレーションの要件に関連する統合の問題が発生する可能性があります。

症状とログのレビュー

DNS 証明書の要件が Microsoft Lync/Skype サーバ側で一致しない場合は、次のような症状が発生します。

- コールが UC インフラストラクチャから Microsoft Lync/Skype へと行われた場合は、コールは Expressway-E の DNS ゾーンから Skype に発信されますが、直後に（504）サーバ タイムアウト エラーがスローされます（Expressway-E の [ステータス（Status）] > [検索履歴（Search History）] ページで表示できます）。

- コールが Microsoft Lync/Skype から UC インフラストラクチャへと行われた場合は、Expressway-E の [ステータス（Status）] > [検索履歴（Search History）] ページに表示されるように、コールは Expressway-E に到達しません。

このサブセクションでは、ログを使用してこのシナリオをより詳しく確認し、設定の誤りを厳密に確認する方法について説明します。

Microsoft Lync/Skype へのコール

このコール フローでは、次のログ スニペットに示すように、Expressway-E の診断ログに、SIP INVITE が Skype へと発信され（**_sipfederationtls._tcp SRV レコードを FQDN と IP に解決できる場合）、直後に 504 サーバ タイムアウト応答が発生したことが詳細情報なしで示されます。**

```
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
```

DNS レコード、または Expressway-E のサーバ証明書にエラーがあるかどうかにかかわらず、同じ応答が（詳細情報なしで）示されます。

したがって、これを詳細に確認するには、Lync/Skype Edge サーバ ログを調べる必要があります。このログでは、発生している可能性のある障害に応じて警告とエラーを確認できます。

- 想定される障害：SRV レコードの FQDN 結果が、Skype に発信された INVITE の**From/P-Asserted-Identity ヘッダー内のドメインと正確に一致していません。**このログのスニペットでは、SIP INVITEのFrom/P-Asserted-Identityヘッダーには、ドメインとしてacano.steven.labが含まれています。ただし、**_sipfederationtls._tcp.acano.steven.labは、vcse.acano.stevano.steven.steven.labではなくをを指定指定です。**

```
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
```

- 想定される障害：Expressway-E サーバの証明書に、**_sipfederationtls._tcp SRV レコードから**

の FQDN が含まれていません。同じ SIP INVITE が送信され、_sipfederationtls._tcp.acano.steven.lab がvcse.acano.steven.lab を指していますが、その FQDN が Expressway-E サーバの証明書 SAN リストに含まれていません。

```
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
```

Microsoft Lync/Skype からのコール

このコール フローの場合、Skype Edge サーバは INVITE を送信せず、Skype ログに依存する必要があるため、Expressway-E のログには詳細は表示されません。問題を詳しく調査するには、Lync/Skype (Edge) サーバ ログまたは Lync/Skype クライアント ログ自体のいずれかを使用します。

Windows PC 上の Skype クライアント ログは、次のパスで参照できます。

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

これは、Skype サーバに直接アクセスできない Office365 Skype ユーザにとって役立ちます。このログでは、クライアントによって発信された **SIP INVITE メッセージとその応答を確認できます。**

このドキュメントに示した Skype の DNS または証明書の要件に関する問題が発生した場合は、Skype サーバから **504 サーバ タイムアウト応答 (障害の理由を含む) を受信します。**

- 想定される障害：SRV レコードの FQDN 結果が、コール先のドメインと正確に一致しません。このログ スニペットには、**cms.steven.lab ドメインのユーザまたはスペースにダイヤルしようとし、_sipfederationtls._tcp.cms.steven.lab が vcse.sub.cms.steven.lab を指していることが示されます。**

```
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

- 想定される障害：Expressway-Eサーバー証明書に、_sipfederationtls._tcp SRVレコードから生成されたFQDNが含まれていません。このログスニペットは、_sipfederationtls._tcp.cms.steven.labをvcse.steven.labに正しく解決する、ドメインcms.steven.steven.lab.でのドメインユーザースペースにににダイヤルダイヤルををしますは、Expressway-Eサーバ証明書のサブジェクト代替名(Common Nameにvcse.steven.lab)には含まれていません。

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

関連情報

- Cisco Expressway シリーズ設定ガイド