CA 署名付き証明書のある Unified Communications Manager で SIP TLS トランクを設定します。

目次

概要

このドキュメントでは、認証機関（CA）署名付き証明書を使用して Communications Manager で Session Initiation Protocol（SIP）Transport Layer Security（TLS）トランクを構成するための順を追ったプロセスについて説明します。

このドキュメントに従った後、2 つのクラスタ間の SIP メッセージは、TLS を使用して暗号化されます。

前提条件

要件

以下について十分に理解しておくことをお勧めします。

- Cisco Unified Communications Manager（CUCM）
- SIP

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- CUCM バージョン 9.1(2)
- CUCM バージョン 10.5(2)
- CA としての Microsoft Windows Server 2003

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

証明書を使用する SSL ハンドシェイクについて、以下の図を参照してください。

設定

ステップ 1： Windows Server 2003 でのパブリック CA またはセットアップ CA

次のリンクを参照してください。 Windows 2003 Sever での CA のセットアップ

ステップ 2：ホスト名と設定の確認

証明書は名前で識別されます。 開始する前に、名前が正しいことを確認します。

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

ホスト名を変更するには、次のリンクを参照してください。 CUCM のホスト名の変更

ステップ 3：証明書署名要求（CSR）の生成とダウンロード

CUCM 9.1(2)

CSR を生成するには、[OS Admin] > [Security] > [Certificate Management] > [Generate CSR] に移動します。

[Certificate Name] フィールドで、ドロップダウンリストから [CallManager] オプションを選択します。

CSR をダウンロードするには、[OS Admin] > [Security] > [Certificate Management] > [Download CSR] に移動します。

[Certificate Name] フィールドで、ドロップダウンリストから [CallManager] オプションを選択します。

CUCM 10.5(2)

CSR を生成するには、[OS Admin] > [Security] > [Certificate Management] > [Generate CSR] に移動します。

1. [Certificate Purpose] フィールドで、**ドロップダウンリストから [CallManager]** を選択します。

2. [Key Length] フィールドで、ドロップダウンリストから [1024] を選択します。
3. [Hash Algorithm] フィールドで、ドロップダウンリストから、[SHA1] を選択します。

CSR をダウンロードするには、[OS Admin] > [Security] > [Certificate Management] > [Download CSR] に移動します。

[Certificate Purpose] フィールドで、ドロップダウンリストから [CallManager] オプションを選択します。

> **注:** CallManager CSR は、1024 ビットの Rivest-Shamir-Addleman（RSA）キーを使用して生成されます。

ステップ 4：Microsoft Windows 2003 認証機関による CSR の署名

これは Microsoft Windows 2003 CA によって CSR に署名するオプション情報です。

1. Certification Authority を開きます。

2. [CA] アイコンを右クリックし、[All Tasks] > [Submit new request] に移動します。

3. CSR を選択し、[Open] オプションをクリックします（CSR（CUCM 9.1(2) と CUCM 10.5(2)）に適用可能）

4. 開かれているすべての CSR が [Pending Requests] フォルダに表示されます。 各 CSR を右クリックし、証明書を発行するために [All Tasks] > [Issue] に移動します。 （CSR（CUCM 9.1(2) と CUCM 10.5(2)）に適用可能）

5. 証明書をダウンロードするには、[Issued Certificates] フォルダを選択します。

証明書を右クリックし、[Open] オプションをクリックします。

6. 証明書の詳細が表示されます。 証明書をダウンロードするには、[Details] タブを選択し、[Copy to File…] ボタンをクリックします。

7. [Certificate Export Wizard] ウィンドウで、[Base-64 encoded X.509(.CER)] オプション ボタンをクリックします。

8. ファイルの名前を正確に指定します。 この例は、**CUCM1052.cer** 形式を使用します。

CUCM 9.1(2) で、同じ手順に従います。

ステップ 5 : CA からのルート証明書の取得

[Certification Authority] ウィンドウを開きます。

ルート CA をダウンロードするには、次の手順を実行します。

1. [CA] アイコンを右クリックし、[Properties] オプションをクリックします。

2. [General] タブで、[View Certificate] をクリックします。

3. [Certificate] ウィンドウで、[Details] タブをクリックします。

4. [Copy to File...] をクリックします。

ステップ 6 : CallManager Trust としての CA ルート証明書のアップロード

CA ルート証明書をアップロードするには、[OS Admin] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain] にログインします。

注: 両方の CUCM（CUCM 9.1(2) と CUCM 10.5(2)）でこれらの手順を実行します。

ステップ 7 : CallManager 証明書としての CA 署名 CallManager CSR 証明書のアップロード

CA 署名 CallManager CSR をアップロードするには、[OS Admin] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain] にログインします。

注: 両方の CUCM（CUCM 9.1(2) と CUCM 10.5(2)）でこれらの手順を実行します。

ステップ 8 : SIP トランク セキュリティ プロファイルの作成

CUCM 9.1(2)

SIP トランク セキュリティ プロファイルを作成するには、[System] > [Security] > [SIP Trunk Security Profile] に移動します。

既存の Non Secure SIP Trunk Profile をコピーし、それに新しい名前を付けます。 この例では、Non Secure SIP Trunk Profile が Secure SIP Trunk Profile TLS で名前変更されています。

この図に示されているように、[X.509 Subject Name] では、CUCM 10.5(2)（CA 署名証明書）の共通名（CN）を使用します。

CUCM 10.5(2)

[System] > [Security] > [SIP Trunk Security Profile] に移動します。

既存の Non Secure SIP Trunk Profile をコピーし、それに新しい名前を付けます。 この例では、Non Secure SIP Trunk Profile が Secure SIP Trunk Profile TLS で名前変更されています。

強調表示されているように、[X.509 Subject Name] では、CUCM 9.1(2)（CA 署名証明書）の CN

を使用します。

どちらの SIP トランク セキュリティ プロファイルも、着信ポートとして 5061 を設定します。その場合、それぞれのクラスタが TCP ポート 5061 で新しいインバウンド SIP TLS 発信をリッスンします。

ステップ 9 : SIP トランクの作成

セキュリティ プロファイルを作成した後、SIP トランクを作成し、SIP トランクの次の設定パラメータの変更を行います。

CUCM 9.1(2)

1. SIP の [Trunk Configuration] ウィンドウで、設定パラメータ [SRTP Allowed] チェックボックスにチェックします。

これにより、このトランクを介した発信で使用される Real-time Transport Protocol（RTP）が保護されます。 このボックスは、SIP TLS を使用するときだけチェックする必要があります。Secure Real-time Transport Protocol（SRTP）のキーは、SIP メッセージの本文で交換されるからです。 SIP シグナリングは TLS で保護する必要があります。そうしないと、非セキュア SIP シグナリングを持つどのユーザも、対応する SRTP ストリームをトランクを介して復号できるようになってしまいます。

2. SIP の [Trunk Configuration] ウィンドウの [SIP Information] セクションで、[Destination Address]、[Destination Port]、および [SIP Trunk Security Profile] を追加します。

CUCM 10.5(2)

1. SIP の [Trunk Configuration] ウィンドウで、設定パラメータ [SRTP Allowed] チェックボックスにチェックします。

これにより、このトランクを介した発信で SRTP を使用できるようになります。 このボックスは、SIP TLS を使用するときだけチェックする必要があります。SRTP のキーは、SIP メッセージの本文で交換されるからです。 SIP シグナリングは TLS で保護する必要があります。そうしないと、非セキュア SIP シグナリングを持つどのユーザも、対応するセキュア RTP ストリームをトランクを介して復号できるようになってしまいます。

2. SIP の [Trunk Configuration] ウィンドウの [SIP Information] セクションで、[Destination IP Address]、[Destination Port]、および [Security Profile] を追加します。

ステップ 10 : ルート パターンの作成

最も簡単な方法は、各クラスタに、SIP トランクを直接指すルート パターンを作成することです。 ルート グループとルート リストも使用できます。

CUCM 9.1(2) は、CUCM 10.5(2) への TLS SIP トランクを経由して [Route Pattern] 9898 を指します。

CUCM 10.5(2) は、CUCM 9.1(2) への TLS SIP トランクを経由して [Route Pattern] 1018 を指します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

SIP TLS 発信は、次の手順でデバッグできます。

CUCM でのパケット キャプチャの収集

CUCM 9.1(2) と CUCM 10.5(2) の間の接続を確認するには、CUCM サーバでのパケット キャプチャを使用し、SIP TLS トラフィックを監視します。

SIP TLS トラフィックは TCP ポート 5061 で送信されます（sip-tls として表示される）。

次の例では、SSH CLI セッションが CUCM 9.1(2) に対して確立されています。

1. 画面での CLI パケット キャプチャ

この CLI は SIP TLS トラフィックの画面上の出力を印刷します。

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. ファイルへの CLI キャプチャ

この CLI はホストに基づいてパケット キャプチャを行い、packets というファイルを作成します。

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

SIP トランクを CUCM 9.1(2) で再起動し、内線 1018（CUCM 9.1(2)）からの発信を内線 9898（CUCM 10.5(2)）に対して行います。

ファイルを CLI からダウンロードするには、このコマンドを実行します。

```
admin:file get activelog platform/cli/packets.cap
```

キャプチャは、標準の .cap 形式で行われます。 この例では packets.cap ファイルを開くために Wireshark を使用していますが、任意のパケット キャプチャ表示ツールを使用できます。

1. CUCM 9.1(2)（クライアント）と CUCM 10.5(2)（サーバ）の間の TCP 通信を確立するための Transmission Control Protocol（TCP）の同期（SYN）。
2. CUCM 9.1(2) は、TLS セッションを開始するために Client Hello を送信します。
3. CUCM 10.5(2) は、証明書交換プロセスを開始するために Server Hello, Server Certificate, and Certificate Request を送信します。
4. 証明書の交換を完了するために、クライアント CUCM 9.1(2) が送信する証明書。
5. アプリケーション データは暗号化された SIP シグナリングであり、TLS セッションが確立

されていることを示します。
正しい証明書が交換されているかどうかさらにチェックされます。 Server Hello の後、サーバ CUCM 10.5(2) はその証明書をクライアント CUCM 9.1(2) に送信します。

CUCM サーバ 10.5(2) のシリアル番号および情報カテゴリに関する情報は CUCM 9.1(2) に提示されます。シリアル番号、件名、発行者、および利用可能日はすべて [OS Admin Certificate Management] ページの情報と比較されます。

サーバ CUCM 10.5(2) は、検証用の独自の証明書を提示した後に、クライアント CUCM 9.1(2) の証明書をチェックします。 検証は両方向で行われます。

パケット キャプチャの証明書と [OS Admin Web] ページの証明書の間に不一致がある場合、正しい証明書はアップロードされません。

正しい証明書を [OS Admin Cert] ページにアップロードする必要があります。

CUCM トレースの収集

CUCM トレースは、CUCM 9.1(2) サーバと CUCM 10.5(2) サーバの間で交換されるメッセージの特定、SSL セッションが適切に確立されているかどうかの判断にも役立ちます。

この例では、CUCM 9.1(2) からのトレースが収集されています。

コール フロー：

Ext 1018 > CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > Ext 9898

++ ディジット分析

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

++ SIP TLS は、この発信用にポート 5061 で使用されています。

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

++ Signal Distribution Layer (SDL) メッセージ SIPCertificateInd は、情報カテゴリ CN および接

続情報に関する詳細を提供します。

```
04530218.000 |19:59:21.323 |SdlSig   |SIPCertificateInd                    |wait
                  |SIPHandler(1,100,72,1)           |SIPTcp(1,100,64,1)
|1,100,17,11.3^*^*                       |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig   |SIPCertificateInd
|restart0                       |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1)           |1,100,17,11.3^*^*                       |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```