デフォルトの CUCM セキュリティ、ITL 操作、およびトラブルシューティング

目次

概要

このドキュメントでは、Cisco Unified Communications Manager (CUCM) バージョン 8.0 以降のデフォルトのセキュリティ (SBD) 機能について説明します。 このドキュメントは、公式のデフォルトのセキュリティに関するドキュメントの補足であり、管理者を支援し、トラブルシューティングを容易に実行できるようにするための動作情報とトラブルシューティングのヒントを収録しています。

背景説明

CUCM バージョン 8.0 以降で導入されている SBD 機能は、ID 信頼リスト (ITL) ファイルと信頼検証サービス (TVS) で構成されます。 すべての CUCM クラスタでは ITL ベースのセキュリティが自動的に使用されます。 バージョン 8.0 CUCM クラスタに対して特定の変更を行う前に管理

者が理解しておく必要がある、セキュリティと管理のしやすさ/使いやすさの間のトレードオフがあります。

SBD の中心となる概念を理解しておくことを推奨します。 Asymmetric Key Cryptography (Wikipedia) と Public Key Infrastructure Wikipedia (Wikipedia) 。

SBD の概要

ここでは、SBD の機能について概説します。 各機能の技術詳細については、「SBD の詳細とトラブルシューティング情報」セクションを参照してください。

SBD は、サポートされている IP 電話に対し 3 つの機能を提供します。

- 署名キーを使用する TFTP ダウンロード ファイル (コンフィギュレーション、ロケール、ringlist) のデフォルト認証
- 署名キーを使用する TFTP コンフィギュレーション ファイルのオプションの暗号化
- CUCM (TVS) のリモート証明書信頼ストアを使用する電話機により開始された HTTPS 接続の証明書検証

このドキュメントでは、各機能の概要を説明します。

TFTP ダウンロード認証

証明書信頼リスト (CTL) または ITL ファイルがある場合、IP 電話は CUCM TFTP サーバの署名済み TFTP コンフィギュレーション ファイルを要求します。 このファイルにより、電話機はコンフィギュレーション ファイルが信頼できるソースからのものであることを確認できます。 電話機に CTL/ITL ファイルがある場合は、信頼できる TFTP サーバによってコンフィギュレーション ファイルが署名されている必要があります。 このファイルはプレーン テキストでネットワーク上を送信されますが、特別な検証署名が設定されています。

電話機は、特殊署名が設定されたコンフィギュレーション ファイルを受信するために **SEP*<MAC Address>.cnf.xml.sgn*** を要求します。 このコンフィギュレーション ファイルは、[Operating System (OS) Administration Certificate Management] ページで CallManager.pem に対応する TFTP 秘密キーにより署名されます。

署名済みファイルには、ファイルを認証するための署名が上部にありますが、それ以外はプレーン テキスト XML です。 次の図では、コンフィギュレーション ファイルの署名者が **CN=CUCM8-Publisher.bbbburns.lab** であり、これは **CN=JASBURNS-AD** により署名されています。 つまり、このコンフィギュレーション ファイルを受け入れる前に、**CUCM8-Publisher.bbbburns.lab** の署名を ITL ファイルに突き合せて照合する必要があります。

以下の図は、署名済みファイルを作成するために、メッセージ ダイジェスト アルゴリズム (MD) 5 またはセキュア ハッシュ アルゴリズム (SHA) 1 ハッシュ機能とともに秘密キーがどのように使用されるかを示しています。

署名検証では、ハッシュを復号化するために、一致する公開キーを使用してこのプロセスが逆方向で行われます。 ハッシュが一致すると、次のように表示されます。

- このファイルは送信中に変更されません。
- このファイルは、署名にリストされている関係者からのものです。これは、公開キーで復号

化できるものはすべて秘密キーで暗号化されている必要があるためです。

TFTP コンフィギュレーション ファイルの暗号化

関連付けられている電話セキュリティ プロファイルでオプションの TFTP コンフィギュレーション暗号化が有効である場合、電話機は暗号化されたコンフィギュレーション ファイルを要求します。 このファイルは TFTP 秘密キーにより署名され、電話機と CUCM の間で交換される対称キーにより暗号化されています（詳細については『Cisco Unified Communications Manager セキュリティ ガイド、リリース 8.5(1)』を参照）。このため、傍聴者が必要なキーを所有していない限り、このファイルの内容をネットワーク スニファで読み取ることはできません。

電話機は署名済み暗号化ファイルを取得するために **SEP*<MAC Address>*.cnf.xml.enc.sgn** を要求します

暗号化されたコンフィギュレーション ファイルでも先頭に署名がありますが、その後にプレーンテキスト データは含まれておらず、暗号化データ（このテキスト エディタでは文字化けしたバイナリ文字）だけが含まれています。 次の図では、署名者が前述の例と同じであるため、電話機がこのファイルを受け取る前にこの署名者が ITL ファイルに含まれている必要があります。 電話機がファイルの内容を読み取ることができるようにするためには、復号化キーが正確である必要があります。

信頼検証サービス（リモート証明書と署名の検証）

IP 電話に搭載されているメモリは限られており、またネットワーク上では管理対象の電話機が多数ある可能性があります。 CUCM は TVS 経由でリモートの信頼されたストアとして機能します。そのため、完全な証明書信頼ストアを各 IP Phone に導入する必要がありません。 電話機は、CTL ファイルまたは ITL ファイルを使用して署名または証明書を検証できない場合、TVS サーバに対して検証を依頼します。 この中央信頼ストアは、信頼ストアが IP Phone に搭載されている場合よりも簡単に管理できます。

SBD の詳細とトラブルシューティング情報

ここでは SBD プロセスについて詳しく説明します。

CUCM に存在する ITL ファイルと証明書

まず、CUCM サーバ自体に存在する必要があるファイルが多数あります。 最も重要なものは、TFTP 証明書と TFTP 秘密キーです。 TFTP 証明書は、[OS Administration] > [Security] > [Certificate Management] > [CallManager.pem] にあります。

CUCM サーバは、TFTP サービス（および Cisco Call Manager（CCM）サービス）に対して CallManager.pem 証明書の秘密キーと公開キーを使用します。 次の図は、CallManager.pem 証明書が、JASBURNS-AD **によって署名された** CUCM8-publisher.bbbburns.laband に対して発行されることを示します。 **すべての** TFTP コンフィギュレーション ファイルは、次の秘密キーで署名されています。

すべての電話機は、TFTP 秘密キーで暗号化されているファイルの復号化と、TFTP 秘密キーで署名されているファイルの検証に、CallManager.pem 証明書の TFTP 公開キーを使用できます。

CallManager.pem 証明書の秘密キーの他に、CUCM サーバは 電話機に対して提示される ITL ファイルも保存します。 showitl **コマンドは**、CUCM サーバ OS CLI へのセキュア シェル（SSH）アクセスによってこの ITL ファイルのすべての内容を表示します。

ITL ファイルには、電話機が使用する重要なコンポーネントが複数含まれているため、このセクションでは、ITL ファイルのコンポーネントを 1 つずつ説明します。

最初の部分は、署名情報です。 ITL ファイルも署名済みファイルです。 次の出力は、以前の CallManager.pem 証明書に関連付けられた TFTP 秘密キーでファイルが署名されていることを示しています。

```
admin:show itl
Length of ITL file: 5438
The ITL File was last modified on Wed Jul 27 10:16:24 EDT 2011

       Parse ITL File
       ----------------

Version:        1.2
HeaderLength:   296 (BYTES)

BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
3       SIGNERID        2       110
4       SIGNERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
5       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
6       CANAME          15      CN=JASBURNS-AD
*Signature omitted for brevity*
```

以降の各セクションでは、特殊な Function パラメータ内部に各自の目的が含まれています。 1 番目の機能は、System Administrator Security Token です。 これは TFTP 公開キーの署名です。

```
        ITL Record #:1
                 ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
This etoken was used to sign the ITL file.
```

次の機能は CCM+TFTP です。 これもまた TFTP 公開キーであり、ダウンロードした TFTP コンフィギュレーション ファイルの認証と復号化に使用されます。

```
        ITL Record #:2
                 ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       CCM+TFTP
```

```
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
```

次の機能は TVS です。 電話機が接続する TVS サーバごとに公開キー エントリがあります。 これにより、電話機は TVS サーバとの間で Secure Sockets Layer（SSL）セッションを確立できます。

```
        ITL Record #:3
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
7       PUBLICKEY       270
8       SIGNATURE       256
11      CERTHASH        20      C7 E1 D9 7A CC B0 2B C2 A8 B2 90 FB
                                AA FE 66 5B EC 41 42 5D
12      HASH ALGORITHM  1       SHA-1
```

ITL ファイルに含まれる最後の機能は、Certificate Authority Proxy Function（CAPF）です。 この証明書により、電話機は CUCM サーバ上の CAPF サービスとのセキュアな接続を確立でき、これによりローカルで有効な証明書（LSC）をインストールまたは更新できます。 このプロセスについては、今後リリースされる別のドキュメントで説明する予定です。

```
        ITL Record #:4
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       455
2       DNSNAME         2
3       SUBJECTNAME     61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       CAPF
5       ISSUERNAME      61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       0A:DC:6E:77:42:91:4A:53
7       PUBLICKEY       140
8       SIGNATURE       128
11      CERTHASH        20      C7 3D EA 77 94 5E 06 14 D2 90 B1
                                A1 43 7B 69 84 1D 2D 85 2E
12      HASH ALGORITHM  1       SHA-1

The ITL file was verified successfully.
```

次のセクションでは、電話機の起動時に行われる処理について説明します。

電話機による ITL およびコンフィギュレーション ファイルのダウンロード

電話機が起動し、IP アドレスと TFTP サーバのアドレスを取得すると、電話機は最初に CTL および ITL ファイルを要求します。

次のパケット キャプチャは、ITL ファイルに対する電話機の要求を示します。 tftp.opcode == 1 でフィルタリングすると、この電話機からのすべての TFTP 読み取り要求が表示されます。

電話機は TFTP から CTL ファイルおよび ITL ファイルを正常に受信しているため、署名済みコンフィギュレーション ファイルを要求します。 この動作を示す電話機コンソール ログは、電話機の Web インターフェイスから取得できます。

最初に電話機は CTL ファイルを要求し、この要求が成功します。

```
837: NOT 09:13:17.561856 SECD: tlRequestFile: Request CTLSEP0011215A1AE3.tlv
846: NOT 09:13:17.670439 TFTP: [27]:Requesting CTLSEP0011215A1AE3.tlv from
14.48.44.80
847: NOT 09:13:17.685264 TFTP: [27]:Finished --> rcvd 4762 bytes
```

次に電話機は ITL ファイルも要求します。

```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14.48.44.80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

電話機による ITL およびコンフィギュレーション ファイルの検証

ITL ファイルは、ダウンロード後に検証が必要です。 この時点での電話機の状態としていくつかの状態が考えられるため、このドキュメントではこれらすべてについて説明します。

- Prepare Cluster for Rollback to Pre 8.0 パラメータが原因で、電話機に CTL ファイルまたは ITL ファイルがないか、または ITL がブランクである。 この状態では、電話機はダウンロードされる次の CTL ファイルまたは ITL ファイルを自動的に信頼し、この署名を使用します。
- 電話機にはすでに CTL はあるが、ITL がない。 この状態では、CTL ファイルの CCM+TFTP 機能によって ITL が検証可能である場合にだけ、電話機は ITL を信頼します。
- 電話機にはすでに CTL ファイルと ITL ファイルがある。 この状態では、電話機は最近ダウンロードしたファイルが CTL、 ITL、または TVS サーバのいずれかの署名に一致していることを検証します。

電話機が署名済みファイルと HTTPS 証明書を検証する方法を次のフローチャートに示します。

この場合、電話機は ITL ファイルと CTL ファイルの署名を検証できます。 電話機にはすでに CTL および ITL の両方があるため、これらを調べ、正しい署名を検出します。

```
877: NOT 09:13:17.925249 SECD: validate_file_envelope:
File sign verify SUCCESS; header length <296>
```

電話機に CTL および ITL ファイルがダウンロードされているため、この時点以降電話機は署名済みコンフィギュレーション ファイルだけを要求します。 これは、電話機の ロジックでは、CTL と ITL が存在するかどうかに基づいて TFTP サーバがセキュアであるかどうかが判別され、署名付きファイルが要求されることを示しています。

```
917: NOT 09:13:18.433411 tftpClient: tftp request rcv'd from /usr/tmp/tftp,
srcFile = SEP0011215A1AE3.cnf.xml, dstFile = /usr/ram/SEP0011215A1AE3.cnf.xml
max size = 550001
918: NOT 09:13:18.457949 tftpClient: auth server - tftpList[0] = ::ffff:
14.48.44.80
919: NOT 09:13:18.458937 tftpClient: look up server - 0
920: NOT 09:13:18.462479 SECD: lookupCTL: TFTP SRVR secure
921: NOT 09:13:18.466658 tftpClient: secVal = 0x9 922: NOT 09:13:18.467762
tftpClient: ::ffff:14.48.44.80 is a secure server
923: NOT 09:13:18.468614 tftpClient: retval = SRVR_SECURE
924: NOT 09:13:18.469485 tftpClient: Secure file requested
```

```
925: NOT 09:13:18.471217 tftpClient: authenticated file approved - add .sgn
-- SEP0011215A1AE3.cnf.xml.sgn
926: NOT 09:13:18.540562 TFTP: [10]:Requesting SEP0011215A1AE3.cnf.xml.sgn
from 14.48.44.80 with size limit of 550001
927: NOT 09:13:18.559326 TFTP: [10]:Finished --> rcvd 7652 bytes
```

署名済みコンフィギュレーション ファイルがダウンロードされると、電話機は ITL 内の CCM+TFTP 機能に対してこのファイルを認証する必要があります。

```
937: NOT 09:13:18.656906 SECD: verifyFile: verify SUCCESS
</usr/ram/SEP0011215A1AE3.cnf.xml>
```

不明な証明書を確認するための電話機による TVS への接続

TVS 機能を提供する ITL ファイルには、CUCM サーバの TCP ポート 2445 で稼働する TVS サービスの証明書が含まれています。 TVS は、CallManager サービスがアクティブになっているすべてのサーバで動作します。 CUCM TFTP サービスは、電話機が接続する必要がある TVS サーバのリストを電話機コンフィギュレーション ファイルに記述するため、設定済み CallManager グループを使用します。

一部のラボでは 1 つの CUCM サーバだけが使用されます。 マルチノード CUCM クラスタでは、1 台の電話機に対し最大 3 つの TVS エントリ（電話機の CUCM グループの CUCM ごとに 1 つ）を設定できます。

次の例は、IP Phone の [Directories] ボタンを押したときの動作を示します。 Directories URL は HTTPS に対応して設定されているため、Directories サーバの Tomcat Web 証明書が電話機に対して提示されます。 この Tomcat Web 証明書（OS Administration の tomcat.pem）は電話機にはロードされないため、電話機はこの証明書を認証するために TVS に接続する必要があります。

この相互作用の説明については、前の TVS 概要図を参照してください。 電話機コンソールのログを次に示します。

最初に Directory URL を見つけます。

```
1184: NOT 15:20:55.219275 JVM: Startup Module Loader|cip.dir.TandunDirectories:
? - Directory url https://14.48.44.80:8443/ccmcip/xmldirectory.jsp
```

これは、検証を必要とする SSL/Transport Layer Security（TLS）セキュア HTTP セッションです。

```
1205: NOT 15:20:59.404971 SECD: clpSetupSsl: Trying to connect to IPV4, IP:
14.48.44.80, Port : 8443
1206: NOT 15:20:59.406896 SECD: clpSetupSsl: TCP connect() waiting,
<14.48.44.80> c:8 s:9 port: 8443
1207: NOT 15:20:59.408136 SECD: clpSetupSsl: TCP connected,
<14.48.44.80> c:8 s:9
1208: NOT 15:20:59.409393 SECD: clpSetupSsl: start SSL/TLS handshake,
<14.48.44.80> c:8 s:9
1209: NOT 15:20:59.423386 SECD: srvr_cert_vfy: Server Certificate
Validation needs to be done
```

電話機は最初に、SSL/TLS サーバが提示する証明書が CTL に含まれているかどうかを確認します。 次に、電話機は ITL ファイルの Functions を調べ、一致するものがあるかどうかを確認します。 次のエラー メッセージには「HTTPS cert not in CTL」と出力されていますが、これは「証明書が CTL または ITL で見つからなかった」ことを意味します。

```
1213: NOT 15:20:59.429176 SECD: findByCertAndRoleInTL: Searching TL from CTL file
1214: NOT 15:20:59.430315 SECD: findByCertAndRoleInTL: Searching TL from ITL file
1215: ERR 15:20:59.431314 SECD: EROR:https_cert_vfy: HTTPS cert not in CTL,
```

```
<14.48.44.80>
```
CTL ファイルと ITL ファイルの直接の内容を調べ、証明書の有無を確認した後で、電話機は TVS キャッシュを調べます。 これは、電話機が最近 TVS サーバに対して同じ証明書を要求した場合に、ネットワーク トラフィックを削減する目的で行われます。 HTTPS 証明書が電話機のキャッシュにない場合、TVS サーバ自体へ TCP 接続できます。

```
1220: NOT 15:20:59.444517 SECD: processTvsClntReq: TVS Certificate
Authentication request
1221: NOT 15:20:59.445507 SECD: lookupAuthCertTvsCacheEntry: No matching
entry found at cache
1222: NOT 15:20:59.446518 SECD: processTvsClntReq: No server sock exists,
must be created
1223: NOT 15:20:59.451378 SECD: secReq_initClient: clnt sock fd 11 bound
to </tmp/secClnt_secd>
1224: NOT 15:20:59.457643 SECD: getTvsServerInfo: Phone in IPv4 only mode
1225: NOT 15:20:59.458706 SECD: getTvsServerInfo: Retreiving IPv4 address
1230: NOT 15:20:59.472628 SECD: connectToTvsServer: Successfully started
a TLS connection establishment to the TVS server: IP:14.48.44.80, port:2445
(default); Waiting for it to get connected.
```
TVS 自体への接続は SSL/TLS (セキュア HTTP : HTTPS) であるため、これは CTL または ITL と照合して認証する必要がある証明書であることに注意してください。 すべてが正しく処理されている場合、TVS サーバの証明書は ITL ファイルの TVS 機能で検出されるはずです。 前述の ITL ファイルの例の ITL Record #3 を参照してください。

```
1244: NOT 15:20:59.529938 SECD: srvr_cert_vfy: Server Certificate Validation
needs to be done
1245: NOT 15:20:59.533412 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from CTL file
1246: NOT 15:20:59.534936 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from ITL file
1247: NOT 15:20:59.537359 SECD: verifyCertWithHashFromTL: cert hash and
hash in TL MATCH
1248: NOT 15:20:59.538726 SECD: tvs_cert_vfy: TVS cert verified with hash
from TL, <14.48.44.80>
```
正常に完了しました。 これで電話機が TVS Server にセキュア接続されました。 次に、TVS サーバに対し、この Directories サーバ証明書を信頼できるかどうかを確認します。

次の例は、この質問に対する応答を示します。応答 0 は、正常完了 (エラーなし) を意味します。

```
1264: NOT 15:20:59.789738 SECD: sendTvsClientReqToSrvr: Authenticate
Certificate : request sent to TVS server - waiting for response
1273: NOT 15:20:59.825648 SECD: processTvsSrvrResponse: Authentication Response
received, status : 0
```
TVT から正常な応答が得られたため、その証明書の結果がキャッシュに保存されます。 つまり、これから 86,400 秒以内に [Directories] ボタンを押すときには、証明書を検証するために TVS サーバに接続する必要がありません。 ローカル キャッシュに直接アクセスできます。

```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```
最後に、Directories サーバに正常に接続したことを確認します。

```
1302: ERR 15:21:01.959700 JVM: Startup Module Loader|cip.http.ae:?
- listener.httpSucceed:  https://14.48.44.80:8443/ccmcip/
xmldirectoryinput.jsp?name=SEP0011215A1AE3
```
TVS が稼働している CUCM サーバで行われる処理の例を次に示します。 Cisco Unified Real-Time Monitoring Tool (RTMT) を使用して TVS ログを収集できます。

CUCM TVS のログは、電話機との SSL ハンドシェイクが行われ、電話機が TVS に対し Tomcat 証明書を照会し、TVS が TVS 証明書ストアで証明書が一致していることを示す応答を返したことを示しています。

```
15:21:01.954 |   debug 14.48.44.202: tvsSSLHandShake Session ciphers - AES256-SHA
15:21:01.954 |   debug TLS HS Done for ph_conn .
15:21:02.010 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_REQ
15:21:02.011 |   debug tvsGetIssuerNameFromX509 - issuerName : CN=CUCM8-
Publisher.bbbburns.lab;OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US and Length: 75

15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
15:21:02.011 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_RES
```

TVS 証明書ストアは、[OS Administration] > [Certificate Management] Web ページにあるすべての証明書のリストです。

電話機の ITL と CUCM ITL の一致の手動での検証

トラブルシューティングに関するよくある誤解の 1 つに、ファイル検証の問題を解決する目的での ITL ファイルの削除があります。 ITL ファイルの削除が必要な状況もありますが、これよりも適切な方法で解決できることがあります。

次のすべての条件に該当する場合にだけ、ITL ファイルを削除する必要があります。

- 電話機の ITL ファイルの署名が、CM TFTP サーバの ITL ファイルの署名と一致しない。
- ITL ファイルの TVS 署名が、TVS から提示される証明書と一致しない。
- 電話機が ITL ファイルまたはコンフィギュレーション ファイルをダウンロードしようとすると、「Verification Failed」が表示される。
- 古い TFTP 秘密キーのバックアップがない

最初の 2 つの条件を確認する方法を次に説明します。

最初に、CUCM 上の ITL ファイルのチェックサムと、電話機の ITL のチェックサムを比較できます。 Cisco Bug ID CSCto60209 のフィックスを適用したバージョンを実行していない限り、CUCM 自体から CUCM の ITL ファイルの MD5sum を確認する方法は、現時点ではありません。

暫定措置として、ご使用の GUI または CLI プログラムで次のように実行します。

```
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ tftp 14.48.44.80
tftp> get ITLSEP0011215A1AE3.tlv
Received 5438 bytes in 0.0 seconds
tftp> quit
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ md5sum
ITLSEP0011215A1AE3.tlv
b61910bb01d8d3a1c1b36526cc9f2ddc  ITLSEP0011215A1AE3.tlv
```

これは、CUCM の ITL ファイルの MD5sum が **b61910bb01d8d3a1c1b36526cc9f2ddc** であることを示しています。

これで、次のようにして電話機自体を調べ、電話機にロードされている ITL ファイルのハッシュを確認できます： [Settings] > [Security Configuration] > [Trust List]。

上記の図は、MD5sum が一致していることを示しています。 つまり、電話機の ITL ファイルと CUCM のファイルが一致しているため、削除する必要がありません。

一致する場合は、次の作業（ITL の TVS 証明書が TVS により提示される証明書と一致するかどうかの確認）に進む必要があります。 この作業は多少複雑です。

最初に、TVS サーバに TCP ポート 2445 で接続する電話機のパケット キャプチャを調べます。

Wireshark でこのストリームの任意のパケットを右クリックし、[Decode As] をクリックし、[SSL] を選択します。 次のようなサーバ証明書を見つけます。

前述の ITL ファイルに含まれている TVS 証明書を確認します。 シリアル番号 2E3E1A7BDAA64D84 の項目があるはずです。

```
admin:show itl
       ITL Record #:3
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
```

ITL ファイル内の TVS.pem が、ネットワークで提示される TVS 証明書に一致しているため、成功です。 ITL を削除する必要はありません。TVS は正しい証明書を提示します。

それでもファイル認証が失敗する場合は、前述のフローチャートの残りの部分を確認してください。

制約事項と相互作用

証明書の再生成/クラスタの再構築/証明書の有効期限

ここで最も重要な証明書は、CallManager.pem 証明書です。 この証明書の秘密キーは、ITL ファイルを含むすべての TFTP コンフィギュレーション ファイルの署名に使用されます。

CallManager.pem ファイルが再生成されると、新しい CCM+TFTP 証明書が新しい秘密キーで生成されます。 さらに ITL ファイルはこの新しい CCM+TFTP キーで署名されるようになります。

CallManager.pem を再生成し、TVS および TFTP サービスを再起動すると、電話機の起動時に次のような動作が行われます。

1. 電話機は新しい CCM+TFTP によって署名された新しい ITL ファイルを TFTP サーバからダウンロードしようとします。 この時点では電話機には古い ITL ファイルだけが存在し、新しいキーは電話機の ITL ファイルには含まれていません。
2. 電話機は古い ITL では新しい CCM+TFTP 署名を検出できないため、TVS サービスへの接続を試みます。
   注: この部分は特に重要です。 古い ITL ファイルの TVS 証明書が引き続き一致している必要があります。 CallManager.pem および TVS.pem の両方が正確に同一の時刻で再生成された場合、電話機から手動で ITL を削除しない限り、電話機は新しいファイルをダウンロード

できません。
3. 電話機が TVS に接続すると、TVS が稼働する CUCM サーバの OS Certificate Store に新しい CallManager.pem 証明書があります。
4. TVS サーバから成功が返され、電話機が新しい ITL ファイルをメモリにロードします。
5. 次に電話機は、新しい CallManager.pem キーで署名されたコンフィギュレーション ファイルをダウンロードしようとします。
6. 新しい ITL がロードされているため、新しい署名済みコンフィギュレーション ファイルはメモリ内の ITL により正常に検証されます。

キー ポイント：

- CallManager.pem 証明書と TVS.pem 証明書を同時に再生成しないでください。
- TVS.pem または CallManager.pem のいずれかを再生成した場合は、新しい ITL ファイルを取得するために TVS と TFTP を再起動し、電話機をリセットする必要があります。 CUCM の新しいバージョンでは、この電話機のリセットが自動的に実行され、証明書の再生成時にユーザに対して警告が表示されます。
- 複数の TVS サーバが存在する場合（CallManager Group に複数のサーバが存在する場合）、追加サーバによって新しい CallManager.pem 証明書を認証できます。

クラスタ間での電話機の移動

特定のクラスタから ITL が導入されているクラスタへ電話機を移動するときには、ITL と TFTP 秘密キーを考慮する必要があります。 電話機に対して提示される新しいコンフィギュレーション ファイルはすべて、電話機の現在の TVS サービスにある署名、または CTL、ITL にある署名に一致している必要があります。

次のドキュメントでは、新しいクラスタの ITL ファイルおよびコンフィギュレーション ファイルが電話機の現在の ITL ファイルによって信頼できることを確認する方法を説明します。
https://supportforums.cisco.com/docs/DOC-15799

バックアップと復元

CallManager.pem 証明書と秘密キーは、ディザスタ リカバリ システム（DRS）経由でバックアップされます。 TFTP サーバが再構築される場合、秘密キーを復元できるようにするため、このサーバはバックアップから復元する必要があります。 サーバに CallManager.pem 秘密キーがないと、現在の ITL が古いキー使用する電話機は、署名済みコンフィギュレーション ファイルを信頼しません。

クラスタが再構築されたが、バックアップから復元されない場合は、『クラスタ間での電話機の移動』ドキュメントの説明と同一です。 これは、電話機に関する限り、新しいキーを含むクラスタは異なるクラスタであるためです。

バックアップと復元に関して重大な問題が 1 つあります。 クラスタが Cisco Bug ID CSCtn50405 の影響を受ける場合は、DRS バックアップには CallManager.pem 証明書が含まれていません。 これが原因で、新しい CallManager.pem が生成されるまでは、このバックアップから復元されたすべてのサーバで壊れた ITL ファイルが生成されます。 バックアップと復元操作を行わなかった、正常に稼働する TFTP サーバが他にない場合、すべての ITL ファイルを電話機から削除する必要があります。

CallManager.pem ファイルを再生成する必要があるかどうかを確認するには、showitl **コマンドを**

入力し、続けて次のように入力します。

```
run sql select c.subjectname, c.serialnumber, c.ipv4address, t.name from
certificate as c, certificatetrustrolemap as r, typetrustrole as t where  c.pkid =
r.fkcertificate and t.enum = r.tktrustrole
```

ITL 出力で確認すべき主なエラーは次のとおりです。

```
This etoken was not used to sign the ITL file.
```

および

```
Verification of the ITL file failed.
Error parsing the ITL file!!
```

前述の Structured Query Language（SQL）クエリは、「Authentication and Authorization」の役割を持つ証明書を検索します。 Authentication and Authorization の役割を持つ、前述のデータベース クエリの CallManager.pem 証明書は、「OS Administration Certificate Management」Web ページにも含まれている必要があります。 前述の問題が検出された場合、クエリの CallManager.pem 証明書と OS Web ページの CallManager.pem 証明書が一致していません。

ホスト名またはドメイン名の変更

CUCM サーバのホスト名またはドメイン名を変更すると、そのサーバのすべての証明書が一括で再生成されます。 証明書の再生成のセクションでは、TVS.pem と CallManager.pem の両方の再生成は「適切ではない」と説明しました。

ホスト名の変更が失敗するシナリオと、問題なくホスト名を変更できるシナリオがいくつかあります。 ここでは、これらのシナリオすべてについて説明し、このドキュメントで TVS と ITL についてすでに説明した内容との関連を示します。

ITL のみが含まれている単一ノード クラスタ（突然壊れることがあるため、注意してください）

- Business Edition サーバまたはパブリッシャのみの導入環境では、ホスト名を変更すると、CallManager.pem と TVS.pem の両方が同時に再生成されます。
- 最初にここで説明した Rollback Enterprise パラメータを使用せずに単一ノード クラスタでホスト名が変更されると、電話機は新しい ITL ファイルまたはコンフィギュレーション ファイルを現在の ITL に照合して検証することができません。 また、TVS 証明書が信頼できなくなったため、TVS に接続できません。
- 電話機には「Trust List Verification Failed」に関するエラーが表示され、新しいコンフィギュレーション変更は反映されず、セキュア サービス URL は失敗します。
- ステップ 2 の注意事項に従わなかった場合の唯一の解決方法は、ITL をすべての電話機から手動で削除することです。

CTL と ITL の両方が含まれている単一ノード クラスタ（これは一時的に壊れることがありますが、容易に修正できます）

- サーバの名前変更後に、CTL クライアントを再実行します。 これにより、電話機がダウンロードする CTL ファイルに新しい CallManager.pem 証明書が記載されます。
- 新しい ITL ファイルを含む新しいコンフィギュレーション ファイルは、CTL ファイルの CCM+TFTP 機能に基づいて信頼できます。
- 更新された CTL ファイルは、変更されない USB eToken 秘密キーに基づいて信頼されるため、これは機能します。

ITL だけが含まれているマルチノード クラスタ（一般にこれは機能しますが、慎重に行わないと

永久に壊れた状態になることがあります）

- マルチノード クラスタには複数の TVS サーバが含まれているため、どのサーバでも証明書を問題なく再生成できます。 電話機に対してこの新しい署名が提示されると、電話機は新しいサーバ証明書を検証するため TVS サーバに別の署名を要求します。
- これが失敗する原因として、主に次の 2 つの問題があります。
  すべてのサーバの名前変更と再起動を同時に実行すると、サーバと電話機が復旧した場合に、既知の証明書ではどの TVS サーバにも到達できません。電話機の CallManager Group に含まれているサーバが 1 つだけである場合は、TVS サーバを追加しても無効です。 これを解決するには、「単一ノード クラスタ」のシナリオを参照するか、または電話機の CallManager Group に別のサーバを追加してください。

CTL と ITL の両方を含むマルチノード クラスタ（永久に壊れた状態になることはありません）

- 名前変更後に、TVS サービスは新しい証明書を認証します。
- 何らかの理由ですべての TVS サーバが使用できない場合でも、新しい CallManager.pem CCM+TFTP 証明書で電話機を更新するために CTL クライアントを引き続き使用できます。

中央集中型 TFTP

ITL が含まれている電話機は、起動時に次のファイルを要求します： **CTLSEP*<MAC Address>.tlv***、**ITLSEP*<MAC Address>.tlv***、および **SEP*<MAC Address>.cnf.xml.sgn*。**

電話機は、これらのファイルを検出できないと **ITLFile.tlv** および **CTLFile.tlv** を要求します。中央集中型 TFTP サーバは、これらのファイルを要求するすべての電話機に対し、これらのファイルを提供します。

中央集中型 TFTP では、その他の多数のサブクラスタを指し示す 1 つの TFTP クラスタが存在します。 このような構造になるのは通常、複数の CUCM クラスタ上の電話機が同一の DHCP スコープを共有しているために、これらの電話機が DHCP オプション 150 TFTP サーバを必要とするためです。 すべての IP Phone は、他のクラスタに登録されている場合でも、中央集中型 TFTP クラスタを指し示します。 この中央集中型 TFTP サーバは、見つからないファイルに対する要求を受信するたびに、リモート TFTP サーバに照会します。

この動作のため、中央集中型 TFTP は ITL 同種環境でのみ機能します。 すべてのサーバで CUCM バージョン 8.x 以降が実行されているか、またはすべてのサーバでバージョン 8.x より前のバージョンが実行されている必要があります。

ITLFile.tlv が中央集中型 TFTP サーバから提示される場合、電話機はリモート TFTP サーバからのファイルを信頼しません。これは、署名が一致しないためです。 これは、異種環境で発生します。 同種環境では、電話機は正しいリモート クラスタから取得される ITLSEP**<MAC>.tlv** を要求します。

8.x 以前のバージョンのクラスタとバージョン 8.x クラスタが混在する異種環境では、バージョン 8.x クラスタで [Prepare Cluster for Rollback to Pre 8.0] が有効になっており（「Cisco Bug ID CSCto87262」を参照）、「Secured Phone URL パラメータ」が HTTPS ではなく HTTP を使用して設定されている必要があります。 これにより、電話機の ITIL 機能が無効になります。

FAQ

SBD をオフにできますか

SBD と ITL が現在動作している場合には、SBD だけをオフにできます。

SBD を電話機で一時的に無効にするには、[Prepare Cluster for Rollback to pre 8.0] エンタープライズ パラメータを使用するか、または HTTPS ではなく HTTP を使用して「Secured Phone URL パラメータ」を設定します。 Rollback パラメータを設定すると、機能エントリが空白な署名済み ITL ファイルが作成されます。 ITL ファイルは「空」ですが署名済みであるため、このパラメータを有効にするにはその前に、クラスタのセキュリティが完全に機能している状態である必要があります。

このパラメータを有効にし、空のエントリが含まれている新しい ITL ファイルをダウンロードして検証すると、電話機は、その署名者に関係なくすべてのコンフィギュレーション ファイルを受け入れます。

クラスタをこの状態のままにしておくことは推奨されません。これは、前述の 3 つの機能（認証済みコンフィギュレーション ファイル、暗号化コンフィギュレーション ファイル、HTTPS URL）がすべて使用できないためです。

CallManager.pem が失われた場合、すべての電話機から ITL ファイルを簡単に削除できますか

現在シスコでは、電話機からすべての ITL をリモートで削除する方法は提供していません。 このため、このドキュメントで説明する手順と介入方法を覚えておくことが重要です。

現在、Cisco Bug ID CSCto47052 に対する未解決の拡張でこの機能が必要とされますが、まだ実装されていません。

暫定期間において、Cisco Bug ID CSCts01319 により新しい機能が追加されています。この機能を使用すると、Cisco Technical Assistance Center（TAC）は、以前の信頼されていた ITL がまだサーバ上で使用可能であれば、この ITL を復元できる可能性があります。 これは、この問題が修正されているバージョンにクラスタがあり、サーバ上の特別な場所に保存されているバックアップに以前の ITL が存在している特定の状況でのみ機能します。 この問題を参照し、ご使用のバージョンにフィックスが適用されているかどうかを確認してください。 この問題で説明されている回復手順を実行するには、Cisco TAC にご連絡ください。

前述の手順が使用できない場合は、電話機のボタンを手動で押して ITL ファイルを削除する必要があります。 これが、セキュリティと管理容易性の間のトレードオフです。 ITL ファイルが真にセキュアであるためには、このファイルはリモート操作で簡単に削除できるものであってはなりません。

Simple Object Access Protocol（SOAP）XML オブジェクトを使用したスクリプトによるボタン プッシュでも、ITL はリモート操作で削除できません。 これは、この時点で TVS アクセス（および着信する SOAP XML ボタン プッシュ オブジェクトを検証するためのセキュア認証 URL アクセス）は機能しないためです。 認証 URL がセキュアに設定されていない場合、ITL を削除するためのキーを押す操作をスクリプト化できる可能性がありますが、シスコはこのようなスクリプトを提供していません。

認証 URL を使用せずにキーを押すリモート操作をスクリプト化するその他の手法がサードパーティから入手可能な場合もありますが、シスコではこのような手法を提供していません。

ITL を削除する方法として最もよく使用されるのは、すべての電話機ユーザに対し、キー シーケンスを指示する電子メール ブロードキャストです。 設定へのアクセスが [Restricted] または [Disabled] に設定されている場合、ユーザは電話機の [Settings] メニューにアクセスできないため、電話機を工場出荷時設定にリセットする必要があります。