# CAPFオンラインCAのトラブルシューティング

## 内容

概要 前提条件 要件 使用するコンポーネント フィーチャコンポーネントの概要 登録局(RA) Enrollment over Secure Transport(EST) libEST Engine-X(NGINX) <u>証明書登録サービス(CES)</u> Certificate Authority Proxy Function (CAPF) <u>メッセージフロー図</u> メッセージフローの説明 /.well-known/est/simpleenroll /certsrv /certsrv/certrgxt.asp /certsrv/certfnsh.asp /certsrv/certnew.cer トラブルシューティングに関連するトレース/ログ CAPFログ CiscoRAログ NGINX error.log CA Webサーバのログ ログファイルの場所 CAPFログ: Cisco RA: Nginxエラーログ: MS IISログ: ログ分析例 正常に起動するサービス NGINXログに表示されるCES起動 NGINXエラー.logに表示されるCES起動 IISログに表示されるCESの起動 CAPFログに表示されるCAPFの起動 電話LSCのインストール操作 CAPFログ IIS ログ 一般的な問題 IIS ID証明書の発行者チェーンにCA証明書がありません 自己署名証明書を提示するWebサーバ

 URLホスト名と共通名が一致しません

 DNS解決の問題

 証明書の有効期間の問題

 証明書テンプレートの設定ミス

 CES認証タイムアウト

 CES登録タイムアウト

 既知の注意事項

 関連情報

## 概要

このドキュメントでは、Certificate Authority Proxy Function(CAPF)自動登録および更新機能のト ラブルシューティングについて説明します。この機能は、CAPF Online CAとも呼ばれます。

## 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。

- •証明書
- Cisco Unified Communications Manager(CUCM)セキュリティ

### 使用するコンポーネント

このドキュメントの情報は、CUCM 12.5でCAPFオンラインCA機能が導入されたため、CUCMバ ージョン12.5に基づいています。

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 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

## フィーチャコンポーネントの概要

### 登録局(RA)

RAは、デジタル証明書のユーザ要求を検証し、証明書を発行するように認証局(CA)に指示するネットワーク内の機関です。RAは公開キーインフラストラクチャ(PKI)の一部です。

### Enrollment over Secure Transport(EST)

ESTは、Transport Layer Security(TLS)およびHyperText Transfer Protocol(HTTP)を介して Certificate Management over CMS(CMC)メッセージを使用するクライアントの証明書登録用に、 コメント要求(RFC)7030で定義されたプロトコルです。ESTは、ESTクライアントが登録要求を 送信し、ESTサーバがその結果を含む応答を送信するクライアント/サーバモデルを使用します。

## libEST

libESTは、シスコがESTを実装するためのライブラリです。libESTにより、X509証明書をエンド ユーザデバイスおよびネットワークインフラストラクチャデバイスにプロビジョニングできます 。このライブラリは、CiscoESTとCiscoRAによって実装されます。

## Engine-X(NGINX)

NGINXはApacheに似たWebサーバであり、逆プロキシです。NGINXは、CAPFとCES間の HTTP通信だけでなく、CESとCA Web Enrollment Service間の通信にも使用されます。libESTが サーバモードで動作する場合、libESTの代わりにWebサーバがTCP要求を処理する必要がありま す。

## 証明書登録サービス(CES)

CESは、CAPFサービスとCA間のRAとして機能するCUCM上のサービスです。CESは、 CiscoRAまたは単にRAとも呼ばれます。CESはRAとして動作するためにサーバモードで libESTを実装するため、CESはWebサーバとしてNGINXを使用します。

## Certificate Authority Proxy Function (CAPF)

CAPFは、証明書の登録要求を実行する際に電話が対話するCUCMサービスです。CAPFは電話の 代わりにCESと通信します。この機能モデルでは、CAPFはクライアントモードでlibESTを実装 して、CESを通じて電話機の証明書を登録します。

要約すると、各コンポーネントの実装方法は次のとおりです。

- 1. 電話機がCAPFに証明書要求を送信します
- 2. CAPFは、CESと通信するためにCiscoEST(クライアントモード)を実装します
- 3. CESは、ESTクライアントの要求を処理して応答するために、CiscoRA(サーバモード)を 実装します
- 4. CES/CiscoRAは、HTTPS経由でCAのWeb登録サービスと通信します



# メッセージフロー図



# メッセージフローの説明

## /.well-known/est/simpleenroll

ESTクライアントは、このURLを使用して、ESTサーバからの証明書登録を要求するAPIコールを 送信します。ESTサーバはAPIコールを受信すると、CAのWeb登録サービスとのHTTPS通信を含 む証明書登録プロセスを開始します。登録プロセスが成功し、ESTサーバが新しい証明書を受信 すると、CAPFは証明書のロードに進み、IP Phoneに返送します。

## /certsrv

/certsrv URL**は、ESTク**ライアントがCAとのセッションを認証および開始するために使用します。

次の図は、Webブラウザからの**/certsrv** URLの例です。これは、[Certificate Services]ランディン グページです。



Microsoft Active Directory Certificate Services -- LAB-DC-RTP

## Welcome

Use this Web site to request a certificate for your Web browser, depending upon the type of certificate you request, perform oth

You can also use this Web site to download a certificate authori

For more information about Active Directory Certificate Service:

## Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

## /certsrv/certrqxt.asp

/certsrv/certrqxt.asp URLは、新しい証明書の要求を開始するために使用されます。ESTクライア ントは/certsrv/certrqxt.aspを使用して、CSR、証明書テンプレート名、および必要な属性を送信 します。

次の図は、Webブラウザの/**certsrv/certrqxt.asp**の例です。



#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM Web server) in the Saved Request box.

| Saved Request:  |           |
|---|-----------|
| Base-64-encoded<br>certificate request<br>(CMC or<br>PKCS #10 or<br>PKCS #7): |           |
| Certificate Templ   | ate:      |
|   | CiscoRA 🗸 |
| Additional Attribu  | ites:     |
| Attributes:   |           |
|   | Submit >  |

### /certsrv/certfnsh.asp

/certsrv/certfnsh.asp URLは、証明書要求のデータを送信するために使用されます。これには、 CSR、証明書テンプレート名、および必要な属性が含まれます。送信を表示するには、ブラウザ の開発者ツールを使用してブラウザのコン**ソールを開**き、certrqxt.aspページからデータを送信し *て*ください。

次の図は、ブラウザのコンソールに表示されるデータの例です。

| POST https:/                                   | /lab-dc-iis.   | .michamen.c   | om/certsrv/ce  | rtfnsh.asp  |   |
|--|--|---|--|---|---|
| Headers  | Cookies  | Parans  | Response   | Timings   | Security  |
| P Filter rec                                   | quest paramet  | ers   |  |   |   |
| ⇒ Form data                                    |  |   |  |   |   |
| CertRe<br>CertAt<br>Friend<br>ThumbP<br>Tanget | quest:<br>EWNSV<br>CgCCA<br>09PHH<br>IDAQA<br>CSQSS<br>N/yIn<br>rvfzs<br>trib:<br>Certif<br>lyType: Save<br>rint:<br>StoreFlags: | BBGIN+CERTI<br>FAXDJAHBgW<br>QEAtk9AcGKA<br>IQIDdW/Ke3H<br>BOEAWPgY3KA<br>ID3OQEBCWUA<br>taI7eWQXSp<br>XrCgIYOHYRA<br>(cateTempla<br>d-Request+C<br>0 | IFICATE+REQUES<br>BAOTBUNDC2NW<br>CFSMEIZIBX9IyS<br>B3DT9YY86E0NR<br>D2IhvCNAQKOMTE<br>WAIBAQBDHrSQM<br>MPSQMpIsnxgO<br>AIBBY9K0030m<br>HE:CISCORA<br>D2<br>Certificate+(S | ST MIIC7<br>NQunCgYDVQQLE<br>te9p85WH9wevU<br>tsG8T15339555<br>EwLZAd BgWVH5<br>EVLZAd BgWVH5<br>EVLZAd BgWVH5<br>SFQk8r1wdCE1P<br>(jwf1xjLjTVDw<br>f8IQLFqFGUBCW<br>serAgent:Mozi<br>3/14/2019,+10 | TCCAduCAQAwaDELMAKGA1UEBhmCVVNxCZA3BgNvBAgTAKS<br>WNQUHXIDAeBgNvBAMTF2N1 Y20xHjVwdwIubwljaGFtDM<br>mn2N10K3PEqR8CTc2e+S3H0 D28rjqSyM+Th3gDj4b/SUn<br>X9CRvter4yr+/vmMaNIdaln oEP7GuV8dErnaxORjd3BhQ<br>WEFjAUBggr8gEF8QcDAQYIXHY88QUHAwIvDgYDvR0PAQH/<br>30jSPqeYg8hY4hVunmH+49m ZfFKGUXJtxy83SPa9VAdR4<br>fBOd/w8Yphn3S1bbHNQdul 6p46yFt0jujxlUr3Plf0mH<br>N1/M2M00DSgKNLI9+S2WC2 y1grvNvqN/vwdnb5E+T790<br>lla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:65.0)<br>:09:02+AM) |

/certsrv/certfnsh.aspからの送信応答には、CAによって発行された証明書の要求IDが含まれます。

#### 要求IDは、ページのソースコードが検査されるときにWebブラウザに表示されます。



#### Certificate Issued

The certificate you requested was issued to you.

ODER encoded or 
Base 64 encoded

 Download certificate

 Download certificate chain

#### **ヒント**:ページソースで「ReqID」を検索します

| $\underline{\Psi}_{\mathbf{k}}$ | I wiew-source:https://lab-dc-iis.michamen.com/certsrv/certfnsh.asp |
|---------------------------------|--|
| b-                              | - (max (max 🖉 🖉 🖉 👘 (max (n) 🖉 🛈 tar 🖄 🖉 🗛                         |
| 535                             | //   |
| 536                             | // LINK HANDLERS   |
| 537                             |  |
| 538                             | //   |
| 539                             | // Get the requested cert  |
| 540                             | function handleGetCert() {   |
| 541                             | <pre>location="certnew.cer?RegID=774"+getEncoding();</pre>         |
| 542                             | )  |
| 543                             |  |
| 544                             | // Get the requested certificate chain                             |
| 515                             | function handleGetChain() (  |
| 547                             | location="dertnew.p/b/Require=//a"+getEncoding();                  |
| 549                             |  |
| 549                             | //   |
| 550                             | // return the ecoding parameter based upon the radio button        |
| 551                             | function getEncoding() (   |
| 552                             | if (true==document.UIForm.rbEncoding[0].checked) {                 |
| 553                             | return "Enc=bin";  |
| 554                             | ) else (   |
| 555                             | return "Enc=b64";  |
| 556                             | )  |
| 557                             | 3  |

#### /certsrv/certnew.cer

この時点で、ESTクライアントは新しい証明書の要求IDを認識します。ESTクライアントは /certsrv/certnew.cerを使用して、要求IDとファイルのエンコードをパラメータとして渡し、拡張 子.cerを持つ証明書ファイルをダウンロードします。

これは、[証明書のダウンロード]リンクをクリックしたときにブラウザで実行される**処理と同**じで す。



#### Certificate Issued

The certificate you requested was issued to you.

DER encoded or OBase 64 encoded

| Download certificate<br>Download certificate chain | Opening certnew.cer  | × |
|--|--|---|
|  | You have chosen to open:                                       |   |
|  | certnew.cer  |   |
|  | which is: CER file (1.4 KB)                                    |   |
|  | from: https://lab-dc-iis.michamen.com                          |   |
|  |  |   |
|  | What should Firefox do with this file?                         |   |
|  | O Open with Browse   |   |
|  |  |   |
|  | Do this <u>a</u> utomatically for files like this from now on. |   |
|  | OK Cancel  |   |

要求URLとパラメータを表示するには、ブラウザのコンソールを使用します。

**注**:DERエンコーディングが選択されている場**合、ブラウザ**はエンコーディングパラメータのbinを指定します。ただし、Base64エンコーディングはb64と表示されます。



# トラブルシューティングに関連するトレース/ログ

これらのログは、ほとんどの問題の切り分けに役立ちます。

## CAPFログ

CAPFログには、電話機とのインタラクション、およびCiscoESTアクティビティの最小限のロギ ングが含まれます。 **注**:これらのログは、コマンドラインインターフェイス(CLI)またはReal Time Monitoring Tool(RTMT)で収集できます。 <u>CSCvo28048</u>が原因で、CAPFがRTMTのサービスのリストに 表示されない場合があります。

#### CiscoRAログ

CiscoRAログは、CESログと呼ばれることがよくあります。CiscoRAログにはCES初期起動アク ティビティが含まれ、CAによる認証時に発生する可能性のあるエラーが表示されます。CAによ る初期認証が成功した場合、電話登録の後続のアクティビティはここではログインしません。し たがって、CiscoRAログは、問題のトラブルシューティングに役立つ最初のポイントとなります。

注:これらのログは、このドキュメントの作成時点でCLIからのみ収集できます。

#### NGINX error.log

NGINX error.logは、起動時のすべてのアクティビティとNGINXとCA側の間のHTTPインタラクションをログに記録するため、この機能に最も有用なログです。これには、CAから返されたエラーコードと、要求の処理後にCiscoRAによって生成されたエラーコードが含まれます。

注:このドキュメントの作成時に、CLIからでもこのログを収集する方法はありません。こ れらのログは、リモートサポートアカウント(ルート)を使用してのみダウンロードできま す。

### CA Webサーバのログ

CA Webサーバのログは、要求URL、応答コード、応答期間、応答サイズを含むHTTPアクティビ ティを表示するため、重要です。これらのログを使用して、CiscoRAとCA間のインタラクション を関連付けることができます。

注:このドキュメントのコンテキストでのCA Webサーバのログは、MS IISのログです。将 来、他のWeb CAがサポートされる場合、CA Webサーバのログとして機能する別のログフ ァイルが存在する可能性があります

## ログファイルの場所

#### CAPFログ:

- ・ルートから:/var/log/active/cm/trace/capf/sdi/capf<*number*>.txt
- ・CLI から: file get activelog cm/trace/capf/sdi/capf\*

**注**:CAPFトレースレベルを[Detailed]に設定し、テストを実行する前にCAPFサービスを再 起動します。

Cisco RA:

- ・ルートから:/var/log/active/cm/trace/capf/sdi/nginx<number>.txt
- ・CLI から: file get activelog cm/trace/capf/sdi/nginx\*

## Nginxエラーログ:

- ・ルートから:/usr/local/thirdparty/nginx/install/logs/error.log
- CLIからは使用できません。

## MS IISログ:

- MMCを開く
- ・インターネット情報サービス(IIS)スナップインの選択
- サーバ名をクリックします
- •[既定のWebサイト]をクリックします
- [Logging]をダブルクリックして、ロギングオプションを表示します
- •「アクション」メニューで「ログファイルの表示」を選択



| Logging  | B                     |
|--|-----------------------|
|  | By Apply              |
| Use this feature to configure how IIS logs requests on the Web server. | B <sub>K</sub> Cancel |
| One log file per:  | Disable               |
| Site v   | View Log Files        |
|  | 😢 Help                |
| Log File   |                       |
| Format:  |                       |
| W3C V Select Fields  |                       |
| Directory:   |                       |
| %SystemDrive%\inetpub\logs\LogFiles Browse                             |                       |
| Encoding:  |                       |
| UTF-8 ~  |                       |
|  |                       |
| Log Event Destination  |                       |
| Select the destination where IIS will write log events.                |                       |
| O Log file only  |                       |
| O ETW event only   |                       |
| Both log file and ETW event  |                       |

## ログ分析例

## 正常に起動するサービス

#### NGINXログに表示されるCES起動

# このログからはほとんど情報が収集されていません。信頼ストアにロードされた完全な証明書チェーンは、ここに表示されます。1つはWebコンテナ用で、もう1つはEST用です。

```
nginx: [warn] CA Chain requested but this value has not yet been set
nginx: [warn] CA Cert response requested but this value has not yet been set
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco/CN=ACT2 SUDI CA)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco
Manufacturing CA)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Manufacturing CA
SHA2)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco Root CA
2048)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Root CA M2)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/DC=com/DC=michamen/CN=lab-
ca.michamen.com)
***EST [INFO][est_log_version:216]--> libest 2.2.0 (API level 4)
***EST [INFO][est_log_version:220]--> Compiled against CiscoSSL 1.0.2n.6.2.194-fips
***EST [INFO][est_log_version:221]--> Linking to CiscoSSL 1.0.2n.6.2.194-fips
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco/CN=ACT2 SUDI
CA)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store
(/C=US/O=cisco/OU=tac/CN=CAPF-eb606ac0/ST=nc/L=rtp)
```

\*\*\*EST [INFO][ossl\_init\_cert\_store\_from\_raw:182]--> Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-eb606ac0/ST=nc/L=rtp) \*\*\*EST [INFO][ossl\_init\_cert\_store\_from\_raw:182]--> Adding cert to store (/O=Cisco Systems/CN=Cisco Manufacturing CA) \*\*\*EST [INFO][ossl\_init\_cert\_store\_from\_raw:182]--> Adding cert to store (/O=Cisco/CN=Cisco Manufacturing CA SHA2) \*\*\*EST [INFO][ossl\_init\_cert\_store\_from\_raw:182]--> Adding cert to store (/O=Cisco Systems/CN=Cisco Root CA 2048) \*\*\*EST [INFO][ossl\_init\_cert\_store\_from\_raw:182]--> Adding cert to store (/O=Cisco/CN=Cisco Root CA M2) \*\*\*EST [INFO][ossl\_init\_cert\_store\_from\_raw:182]--> Adding cert to store (/DC=com/DC=michamen/CN=lab-ca.michamen.com) nginx: [warn] pop\_enabled off in nginx.conf. Disabling EST Proof of Possession \*\*\*EST [INFO][set\_ssl\_option:1378]--> Using non-default ECDHE curve (nid=415) \*\*\*EST [INFO][set\_ssl\_option:1432]--> TLS SRP not enabled EnrollmentService.sh : nginx server PID value = 31070

## NGINXエラー.logに表示されるCESの起動

証明書テンプレートの設定とクレデンシャルを使用したログインは、次のスニペットで確認でき ます。

2019/03/05 12:31:21 [info] 31067#0: login\_to\_certsrv\_ca: Secure connection to MS CertServ completed successfully using the following URL https://lab-dc.michamen.com:443/certsrv

#### CA証明書チェーンの取得は、次のスニペットで確認できます。

2019/03/05 12:31:21 [info] 31067#0: retrieve\_cacerts: Secure connection to MS CertServ completed successfully using the following URL https://lab-dc.michamen.com:443/certsrv/certnew.p7b?ReqID=CACert&Renewal=0&Enc=bin [...] 2019/03/05 12:31:21 [info] 31067#0: ra\_certsrv\_ca\_plugin\_postconf: CA Cert chain retrieved from CA, will be passed to EST

#### 要求が成功すると、certnew.p7bファイルが取得されます。テンプレート認証情報を含む同じ URLを使用して、Webブラウザからcertnew.p7bファイルを取得できます。

### CESの起動 IISログに表示される

NGINX error.logに表示される同じCES起動イベントがIISログにも表示されます。ただし、IISロ グにはさらに2つのHTTP GET要求が含まれます。これは、最初の要求が401応答を介してWebサ ーバによって要求されるためです。認証されると、要求された要求は301応答を使用してリダイ レクトされます。

2019-03-05 17:31:15 14.48.31.152 GET /certsrv - 443 - 14.48.31.128 CiscoRA+1.0 - 401 1 2148074254 0 2019-03-05 17:31:15 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.128 CiscoRA+1.0 -301 0 0 16 2019-03-05 17:31:15 14.48.31.152 GET /certsrv/certnew.p7b ReqID=CACert&Renewal=0&Enc=bin 443 MICHAMEN\ciscora 14.48.31.128 CiscoRA+1.0 - 200 0 0 2

## CAPFログに表示されるCAPFの起動

#### CESの起動に関してCAPFログで発生する処理の大部分は、他のログで発生する処理と同じです 。ただし、オンラインCAの方法と設定を検出するCAPFサービスに注目してください。

12:31:03.354 CServiceParameters::Init() Certificate Generation Method=OnlineCA:4 12:31:03.358 | CServiceParameters::Init() TAM password already exists, no need to create. 12:31:03.358 |-->CServiceParameters::OnlineCAInit() 12:31:03.388 | CServiceParameters::OnlineCAInit() Online CA hostname is lab-dc.michamen.com 12:31:03.389 CServiceParameters::OnlineCAInit() Online CA Port : 443 12:31:03.390 | CServiceParameters::OnlineCAInit() Online CA Template is CiscoRA 12:31:03.546 | CServiceParameters::OnlineCAInit() nginx.conf Updated and Credential.txt file is created 12:31:03.546 CServiceParameters::OnlineCAInit() Reading CAPF Service Parameters done 12:31:03.546 |<--CServiceParameters::OnlineCAInit()</pre> 12:31:03.547 | CServiceParameters::Init() OnlineCA Initialized 12:32:09.172 CServiceParameters::Init() Cisco RA Service Start Initiated. Please check NGINX logs for further details

ログから次に重要な点は、CAPFサービスによってESTクライアントが初期化される場合です。

| ebug                             | CA Type is Online CA, setting up EST Connection   |
|----------------------------------|---|
| <debug< td=""><td></td></debug<> |   |
| >debug                           |   |
| debug                            | Inside setUpESTClient   |
|                                  |   |
| >debug                           |   |
| debug                            | cacert read success. cacert length : 1367   |
| <debug< td=""><td></td></debug<> |   |
| >debug                           |   |
| debug                            | EST context ectx initialized  |
| <debug< td=""><td></td></debug<> |   |
| >debug                           |   |
| debug                            | CA Credentials retrieved  |
| <debug< td=""><td></td></debug<> |   |
| >debug                           |   |
| debug                            | <pre>est_client_set_auth() Successful!!</pre>   |
| <debug< td=""><td></td></debug<> |   |
| >debug                           |   |
| debug                            | EST set server details success!!  |
|                                  | debug<br>  <debug<br>  debug<br/>  debug<br/>  debug<br/>  <debug<br>  <debug<br>  <debug<br>  <debug<br>  debug<br/>  <debug<br>  debug<br/>  <debug<br>  debug<br/>  <debug<br>  debug<br/>  <debug<br>  debug<br/>  <debug< td=""></debug<></debug<br></debug<br></debug<br></debug<br></debug<br></debug<br></debug<br></debug<br></debug<br> |

## 電話LSCのインストール操作

## CAPFログ

必要なすべてのログを収集し、CAPFログを確認して分析を開始することを推奨します。これに より、特定の電話機の時間基準を知ることができます。

シグナリングの最初の部分は、他のCAPF方式と同じですが、CAPFサービスで実行されている ESTクライアントが、ダイアログの最後に向けてCESを使用して登録を実行する点が異なります (CSRが電話機によって提供された後)。

14:05:04.628 |-->debug 14:05:04.628 | debug 2:SEP74A02FC0A675:**CA Mode is OnlineCA, Initiating Automatic Certificate Enrollment** 14:05:04.628 |<--debug 14:05:04.628 |-->debug
14:05:04.628 | debug 2:SEP74A02FC0A675:Calling enrollCertUsingEST()
csr\_file=/tmp/capf/csr/SEP74A02FC0A675.csr
14:05:04.628 | <--debug
14:05:04.628 | debug 2:SEP74A02FC0A675:Inside X509\_REQ \*read\_csr()
14:05:04.628 | <--debug
14:05:04.628 | debug 2:SEP74A02FC0A675:Completed action in X509\_REQ \*read\_csr()
14:05:04.628 | <--debug</pre>

#### CESが電話機の署名付き証明書を取得すると、その証明書が電話機に提供される前に、DER形式 に変換されます。

| 14:05:05.236 | >debug   |
|--------------|--|
| 14:05:05.236 | debug 2:SEP74A02FC0A675:Enrollment rv = 0 (EST_ERR_NONE) with pkcs7 length = |
| 1963         |  |
| 14:05:05.236 | <pre><debug< pre=""></debug<></pre>  |
| 14:05:05.236 | >debug   |
| 14:05:05.236 | debug 2:SEP74A02FC0A675:Signed Cert written to /tmp/capf/cert/ location      |
| 14:05:05.236 | <pre><debug< pre=""></debug<></pre>  |
| 14:05:05.236 | >debug   |
| 14:05:05.236 | <pre>debug 2:SEP74A02FC0A675:Inside write_binary_file()</pre>                |
| 14:05:05.236 | <pre><debug< pre=""></debug<></pre>  |
| 14:05:05.236 | >debug   |
| 14:05:05.236 | <pre>debug 2:SEP74A02FC0A675:Completed action in write_binary_file()</pre>   |
| 14:05:05.236 | <pre><debug< pre=""></debug<></pre>  |
| 14:05:05.236 | >debug   |
| 14:05:05.236 | debug 2:SEP74A02FC0A675:Converting PKCS7 file to PEM format and PEM to DER   |
| 14:05:05.236 | <pre><debug< pre=""></debug<></pre>  |
| 14:05:05.289 | >debug   |
| 14:05:05.289 | debug 2:SEP74A02FC0A675:Return value from enrollCertUsingEST() : 0           |
| 14:05:05.289 | <pre> <debug< pre=""></debug<></pre>   |
| 14:05:05.289 | >debug   |
| 14:05:05.289 | debug 2:SEP74A02FC0A675:Online Cert Signing successful                       |
| 14:05:05.289 | <pre><debug< pre=""></debug<></pre>  |
| 14:05:05.289 | >findAndPost   |
| 14:05:05.289 | findAndPost Device found in the cache map SEP74A02FC0A675                    |

CAPFサービスが再び引き継ぎ、上記のスニペットで書き込まれた場所(/tmp/capf/cert/)から CSRをロードします。 その後、CAPFサービスは署名付きLSCを電話機に提供します。同時に、 電話機のCSRが削除されます。

| 14:05:05.289  | <findandpost< th=""></findandpost<>  |
|---------------|--|
| 14:05:05.289  | >debug   |
| 14:05:05.289  | debug addded 6 to readset  |
| 14:05:05.289  | <debug< td=""></debug<>  |
| 14:05:05.289  | >debug   |
| 14:05:05.289  | debug Recd event   |
| 14:05:05.289  | <debug< td=""></debug<>  |
| 14:05:05.289  | >debug   |
| 14:05:05.289  | debug 2:SEP74A02FC0A675:CA CERT RES certificate ready .                      |
| 14:05:05.289  | <debug< td=""></debug<>  |
| 14:05:05.289  | >debug   |
| 14:05:05.289  | debug 2:SEP74A02FC0A675:CAPF CORE: Rcvd Event: CAPF_EV_CA_CERT_REP in State: |
| CAPF_STATE_AW | AIT_CA_CERT_RESP   |
| 14:05:05.289  | <debug< td=""></debug<>  |
| 14:05:05.289  | >debug   |
| 14:05:05.289  | debug 2:SEP74A02FC0A675:CAPF got device certificate                          |
|               |  |

14:05:05.289 <-- debug 14:05:05.289 |-->debug 14:05:05.289 debug loadFile('/tmp/capf/cert/SEP74A02FC0A675.der') 14:05:05.289 | <--debug 14:05:05.289 |-->debug 14:05:05.289 | debug loadFile() successfully loaded file: '/tmp/capf/cert/SEP74A02FC0A675.der' 14:05:05.289 | <--debug 14:05:05.289 |-->debug 14:05:05.289 debug 2:SEP74A02FC0A675:Read certificate for device 14:05:05.289 <--debug 14:05:05.289 |-->debug 14:05:05.289 debug LSC is verified. removing CSR at /tmp/capf/csr/SEP74A02FC0A675.csr 14:05:05.289 | <--debug 14:05:05.290 |-->debug 14:05:05.290 | debug 2:SEP74A02FC0A675:Sending STORE\_CERT\_REQ msg 14:05:05.419 | <--Select(SEP74A02FC0A675) 14:05:05.419 |-->SetOperationStatus(Success:CAPF\_OP\_SUCCESS):0 14:05:05.419 SetOperationStatus(Success:CAPF\_OP\_SUCCESS):0 Operation status Value is '0' 14:05:05.419 |-->CAPFDevice::MapCapf\_OpStatusToDBLTypeCertificateStatus(OPERATION\_UPGRADE, Suc 14:05:05.419 CAPFDevice::MapCapf\_OpStatusToDBLTypeCertificateStatus(OPERATION\_UPGRADE, Suc =>DbStatus=CERT\_STATUS\_UPGRADE\_SUCCESS 14:05:05.419 | <-- CAPFDevice:: MapCapf\_OpStatusToDBLTypeCertificateStatus(OPERATION\_UPGRADE, Suc 14:05:05.419 SetOperationStatus(Success:CAPF\_OP\_SUCCESS):0 Operation status is set to 1 SetOperationStatus(Success:CAPF\_OP\_SUCCESS):0 Operation status is set to 14:05:05.419 Success:CAPF\_OP\_SUCCESS 14:05:05.419 SetOperationStatus(Success:CAPF\_OP\_SUCCESS):0 sql query - (UPDATE Device SET tkCertificateOperation=1, tkcertificatestatus='3' WHERE my\_lower(name)=my\_lower('SEP74A02FC0A675')) 14:05:05.503 | <--SetOperationStatus(Success:CAPF\_OP\_SUCCESS):0 14:05:05.503 |-->debug 14:05:05.503 debug 2:SEP74A02FC0A675:In capf\_ui\_set\_ph\_public\_key() 14:05:05.503 |<--debug</pre> 14:05:05.503 |-->debug 14:05:05.503 | debug 2:SEP74A02FC0A675:pubKey: 0, [...] 14:05:05.503 | <--debug 14:05:05.503 |-->debug 14:05:05.503 debug 2:SEP74A02FC0A675:pubKey length: 270 14:05:05.503 |<--debug</pre> 14:05:05.503 |-->Select(SEP74A02FC0A675) Select(SEP74A02FC0A675) device exists 14:05:05.511 | 14:05:05.511 | Select(SEP74A02FC0A675) BEFORE DB query Authentication Mode=AUTH\_BY\_STR:1 14:05:05.511 | Select(SEP74A02FC0A675) KeySize=KEY\_SIZE\_2048:3 14:05:05.511 Select(SEP74A02FC0A675) ECKeySize=INVALID:0 14:05:05.511 Select(SEP74A02FC0A675) KeyOrder=KEYORDER\_RSA\_ONLY:1 14:05:05.511 Select(SEP74A02FC0A675) Operation=OPERATION\_NONE:1 14:05:05.511 Select(SEP74A02FC0A675) Operation Status =CERT\_STATUS\_UPGRADE\_SUCCESS:3 Select(SEP74A02FC0A675) Authentication Mode=AUTH\_BY\_NULL\_STR:2 14:05:05.511 14:05:05.511 Select(SEP74A02FC0A675) Operation Should Finish By=2019:01:20:12:00 [...] 14:05:05.971 |-->debug 14:05:05.971 debug MsgType : CAPF\_MSG\_END\_SESSION

## IIS ログ

次のスニペットは、電話機のLSCインストール手順に関するIISログのイベントを示しています (上記を参照)。 2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 - 14.48.31.125 CiscoRA+1.0 - 401 1 2148074254 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 -301 0 0 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certrqxt.asp - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 200 0 0 220 2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 - 14.48.31.125 CiscoRA+1.0 - 401 1 2148074254 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 301 0 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 301 0 0 2019-01-16 14:05:02 14.48.31.152 POST /certsrv/certfnsh.asp - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 301 0 0 2019-01-16 14:05:02 14.48.31.152 POST /certsrv/certfnsh.asp - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 301 0 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certfnsh.asp - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 301 0 0 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certfnsh.asp - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 301 0 0 0 2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certrqxt.asp 200 0 0 15 2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certnew.cer ReqID=10&ENC=b64 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 - 200 0 0 0

## 一般的な問題

#### CES側でエラーが発生すると、次のような出力がCAPFログに表示されます。問題の絞り込みを 続行するには、他のログを確認してください。

12:37:54.741 |-->debug 12:37:54.741 debug 2:SEP001F6C81118B:CA Mode is OnlineCA, Initiating Automatic Certificate Enrollment 12:37:54.741 <--debug 12:37:54.741 |-->debug 12:37:54.741 debug 2:SEP001F6C81118B:Calling enrollCertUsingEST() csr\_file=/tmp/capf/csr/SEP001F6C81118B.csr 12:37:54.741 <--debug 12:37:54.741 |-->debug 12:37:54.742 debug 2:SEP001F6C81118B:Inside X509\_REQ \*read\_csr() 12:37:54.742 |<--debug</pre> 12:37:54.742 |-->debug 12:37:54.742 debug 2:SEP001F6C81118B:Completed action in X509\_REQ \*read\_csr() 12:37:54.742 | <--debug 12:38:04.779 |-->debug 12:38:04.779 debug 2:SEP001F6C81118B:Enrollment rv = 35 (EST\_ERR\_SSL\_READ) with pkcs7 length = 0 12:38:04.779 |<--debug</pre> 12:38:04.779 |-->debug 12:38:04.779 | debug 2:SEP001F6C81118B:est\_client\_enroll\_csr() Failed! Could not obtain new certificate. Aborting. 12:38:04.779 | <--debug 12:38:04.779 |-->debug debug 2:SEP001F6C81118B:Return value from enrollCertUsingEST() : 35 12:38:04.779 12:38:04.779 |<--debug</pre> 12:38:04.779 |-->debug 12:38:04.779 debug 2:SEP001F6C81118B:Online Cert Signing Failed 12:38:04.779 |<--debug</pre> 12:38:04.779 |-->debug 12:38:04.779 debug addded 10 to readset 12:38:04.779 <--debug</pre>

## IIS ID証明書の発行者チェーンにCA証明書がありません

証明書チェーン内のルート証明書または中間証明書がCESによって信頼されていない場合、「 Unable to retrieve CA Cert chain from CA」エラーがnginxログに出力されます。 nginx: [warn] login\_to\_certsrv\_ca: Curl call for MS CA login failed with return code 60 (SSL certificate problem: unable to get local issuer certificate)

nginx: [warn] login\_to\_certsrv\_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve\_cacerts: Unable to execute login to certsrv with curl nginx: [warn] ra\_certsrv\_ca\_plugin\_postconf: Unable to retrieve CA Cert chain from CA

## 自己署名証明書を提示するWebサーバ

IISでの自己署名証明書の使用はサポートされておらず、CUCMでCAPF信頼としてアップロード された場合でも機能します。次のスニペットはnginxログからのもので、IISが自己署名証明書を 使用している場合に観察される内容が表示されます。

nginx: [warn] login\_to\_certsrv\_ca: Curl call for MS CA login failed with return code 60 (SSL
certificate problem: unable to get local issuer certificate)

nginx: [warn] login\_to\_certsrv\_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve\_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra\_certsrv\_ca\_plugin\_postconf: Unable to retrieve CA Cert chain from CA

#### URLホスト名と共通名が一致しません

IIS証明書の共通名(lab-dc)が、CAのWeb登録サービスのURL内のFQDNと一致しません。証明書 の検証が成功するには、URL内のFQDNが、CAによって使用される証明書の共通名と一致する必 要があります。

nginx: [warn] login\_to\_certsrv\_ca: Curl call for MS CA login failed with return code 51 (SSL: certificate subject name 'lab-dc' does not match target host name 'lab-dc.michamen.com')

nginx: [warn] login\_to\_certsrv\_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve\_cacerts: Unable to execute login to certsrv with curl

#### DNS解決の問題

#### CiscoRAは、サービスパラメータで設定されたオンラインCAのホスト名を解決できません。

nginx: [warn] CA Chain requested but this value has not yet been set nginx: [warn] CA Cert response requested but this value has not yet been set nginx: [warn] login\_to\_certsrv\_ca: Curl call for MS CA login failed with return code 6 (Could not resolve: lab-dcc.michamen.com (Domain name not found))

nginx: [warn] login\_to\_certsrv\_ca: URL used: https://lab-dcc.michamen.com:443/certsrv

nginx: [error] retrieve\_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra\_certsrv\_ca\_plugin\_postconf: Unable to retrieve CA Cert chain from CA

#### 証明書の有効期間の問題

ネットワークタイムプロトコル(NTP)が正常に動作しない場合は、証明書の有効期間が発生しま

#### す。このチェックは、起動時にCESによって実行され、NGINXログに記録されます。

nginx: [warn] login\_to\_certsrv\_ca: Curl call for MS CA login failed with return code 60 (SSL certificate problem: certificate is not yet valid)

nginx: [warn] login\_to\_certsrv\_ca: URL used: https://lab-dc-iis.michamen.com:443/certsrv

nginx: [error] retrieve\_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra\_certsrv\_ca\_plugin\_postconf: Unable to retrieve CA Cert chain from CA

## 証明書テンプレートの設定ミス

#### サービスパラメータ内の名前の入力が失敗します。CAPFログおよびNGINXログにはエラーは記 録されないため、NGINX error.logを確認する必要があります。

```
***EST [INFO][est_enroll_auth:356]--> TLS: no peer certificate
2019/02/27 16:53:28 [warn] 3187#0: *2 ossl_init_cert_store: Adding cert to store
(/DC=com/DC=michamen/CN=LAB-DC-RTP) while SSL EST handshaking, client: 14.48.31.128, server:
0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 ra_certsrv_auth_curl_data_cb: Rcvd data len: 163
while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 login_to_certsrv_ca: Secure connection to MS CertServ
completed successfully using the following URL
https://lab-dc-iis.michamen.com:443/certsrv
while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 ra_certsrv_auth_curl_data_cb: Rcvd data len: 11771
while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 navigate_to_certsrv_page: Secure connection to MS CertServ
completed successfully using the following URL
https://lab-dc-iis.michamen.com:443/certsrv/certrqxt.asp
while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
***EST [WARNING][est_enroll_auth:394]--> HTTP authentication failed. Auth type=1
***EST [WARNING][est_http_request:1435]--> Enrollment failed with rc=22 (EST_ERR_AUTH_FAIL)
***EST [INFO] [mg send http error: 389] --> [Error 401: Unauthorized
The server was unable to authorize the request.
]
***EST [ERROR][est_mg_handler:1234]--> EST error response code: 22 (EST_ERR_AUTH_FAIL)
***EST [WARNING][handle_request:1267]--> Incoming request failed rv=22 (EST_ERR_AUTH_FAIL)
***EST [INFO][log_access:1298]--> 14.48.31.128 [27/Feb/2019:16:53:28 -0500] "POST /.well-
known/est/simpleenroll HTTP/1.1" 401 0
***EST [INFO][log_header:1276]--> -
***EST [INFO][log_header:1278]--> "Cisco EST client 1.0"
***EST [WARNING][est_server_handle_request:1716]--> SSL_shutdown failed
```

## CES認証タイムアウト

次に示す抜粋は、最初のcertsrv認証プロセス中にデフォルトタイマーの10秒が経過した後のCES ESTクライアントのタイムアウトを示しています。

nginx: [warn] login\_to\_certsrv\_ca: Curl call for MS CA login failed with return code 28
(Operation timed out after 10000 milliseconds with 0 bytes received)

nginx: [warn] login\_to\_certsrv\_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve\_cacerts: Unable to execute login to certsrv with curl nginx: [warn] ra\_certsrv\_ca\_plugin\_postconf: Unable to retrieve CA Cert chain from CA

注: <u>CSCvo58656</u>と<u>CSCvf83629</u>は、どちらもCES認証タイムアウトに関係します。

## CES登録タイムアウト

CES ESTクライアントは、認証に成功した後にタイムアウトしますが、登録要求への応答を待っています。

nginx: [warn] retrieve\_cacerts: Curl request failed with return code 28 (Operation timed out after 10001 milliseconds with 0 bytes received)

```
nginx: [warn] retrieve_cacerts: URL used: https://lab-
dc.michamen.com:443/certsrv/certnew.p7b?ReqID=CACert&Renewal=0&Enc=bin
```

nginx: [warn] ra\_certsrv\_ca\_plugin\_postconf: Unable to retrieve CA Cert chain from CA

## 既知の注意事項

CSCvo28048 CAPF Service not listed in RTMT Collect Files menu J

<u>CSCvo58656</u> CAPFオンラインCAは、RAとCA間の最大接続タイムアウトを設定するオプション が必要

<u>CSCvf83629</u> ESTサーバの登録中にEST\_ERR\_HTTP\_WRITEが発生する

## 関連情報

・ <u>テクニカル サポートとドキュメント – Cisco Systems</u>