CAPFオンラインCAの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、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)

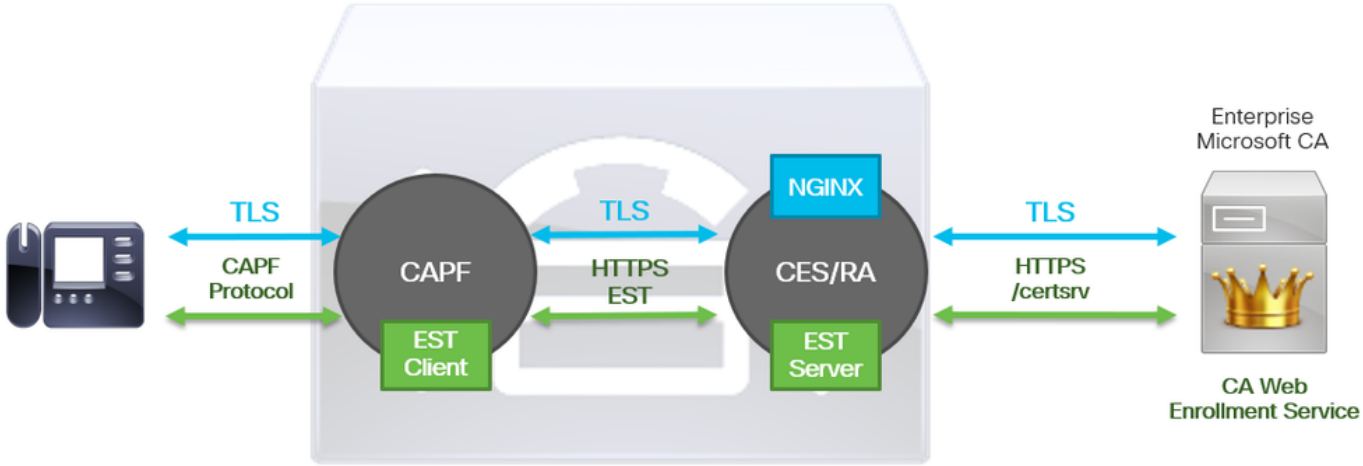
CESは、CAPFサービスとCA間のRAとして機能するCUCM上のサービスです。CESは、CiscoRAまたは単にRAとも呼ばれます。CESはRAとして動作するためにサーバモードでlibESTを実装するため、CESはWebサーバとしてNGINXを使用します。

Certificate Authority Proxy Function（CAPF）

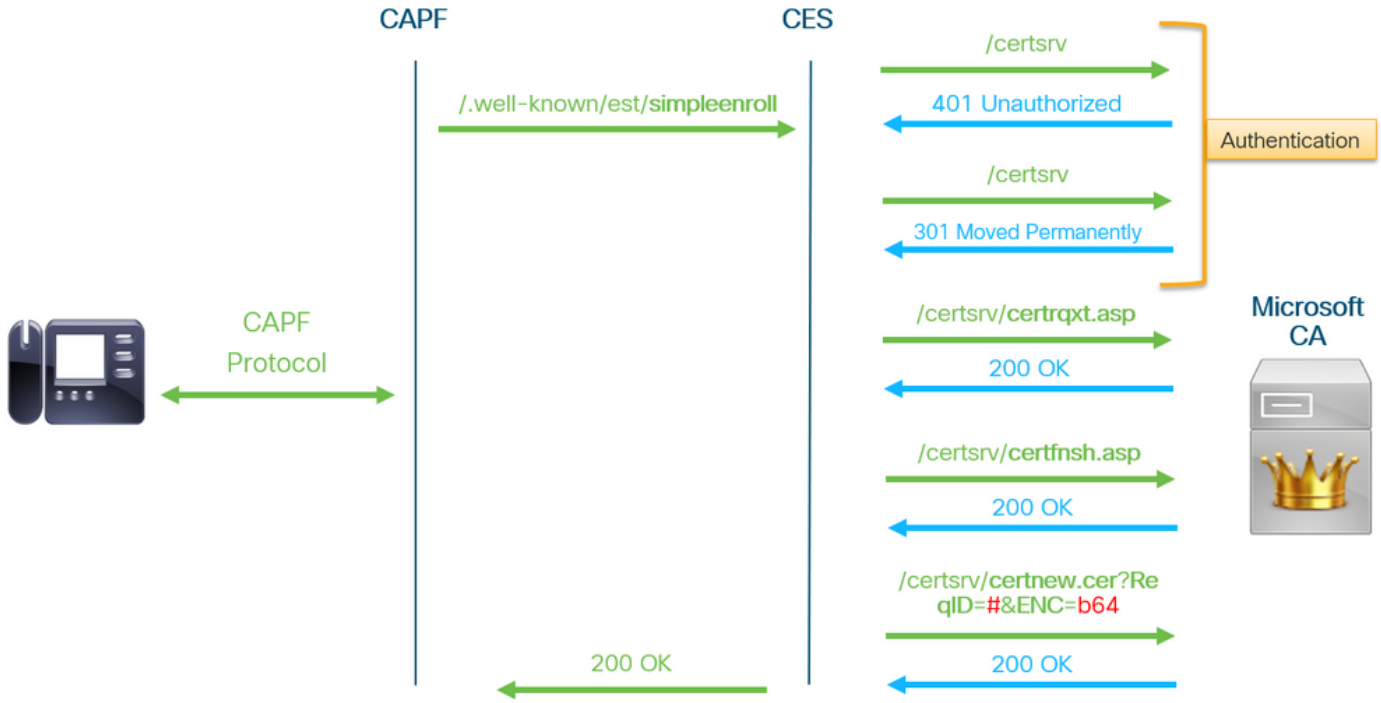
CAPFは、証明書の登録要求を実行する際に電話が対話するCUCMサービスです。CAPFは電話の代わりにCESと通信します。この機能モデルでは、CAPFはクライアントモードでlibESTを実装して、CESを通じて電話機の証明書を登録します。

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

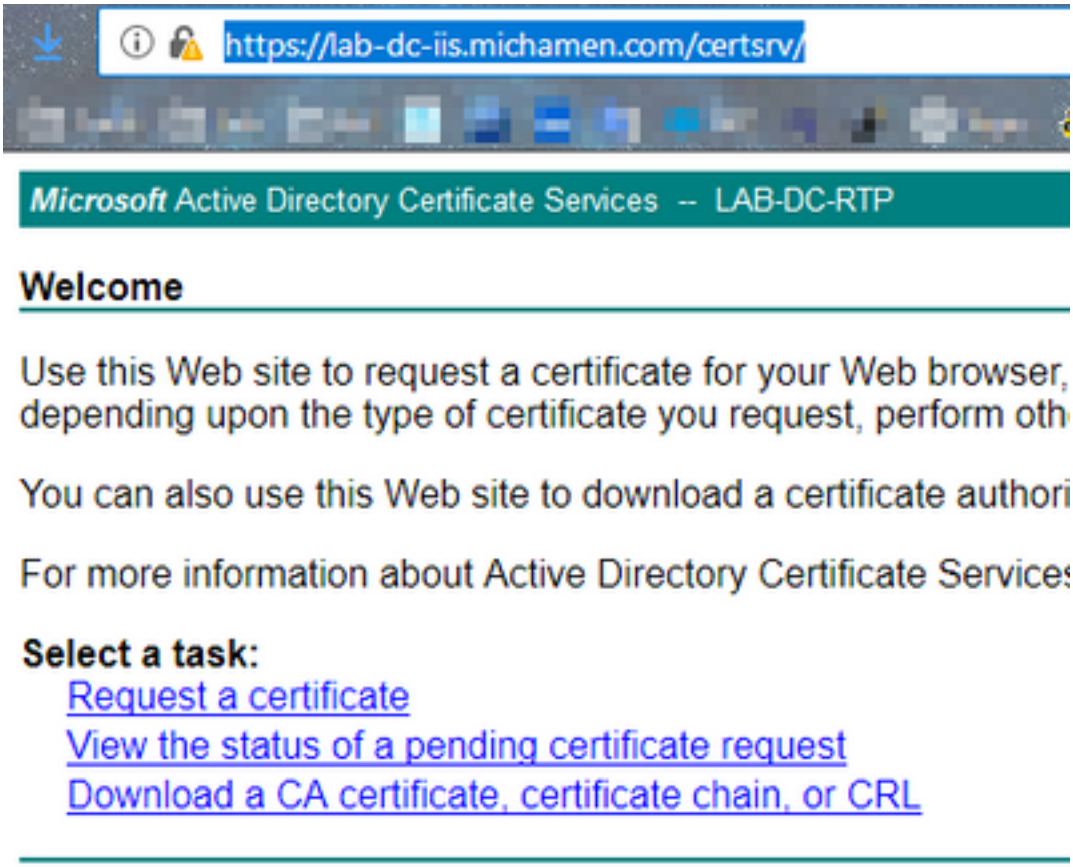
/.well-known/est/simpleenroll

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。

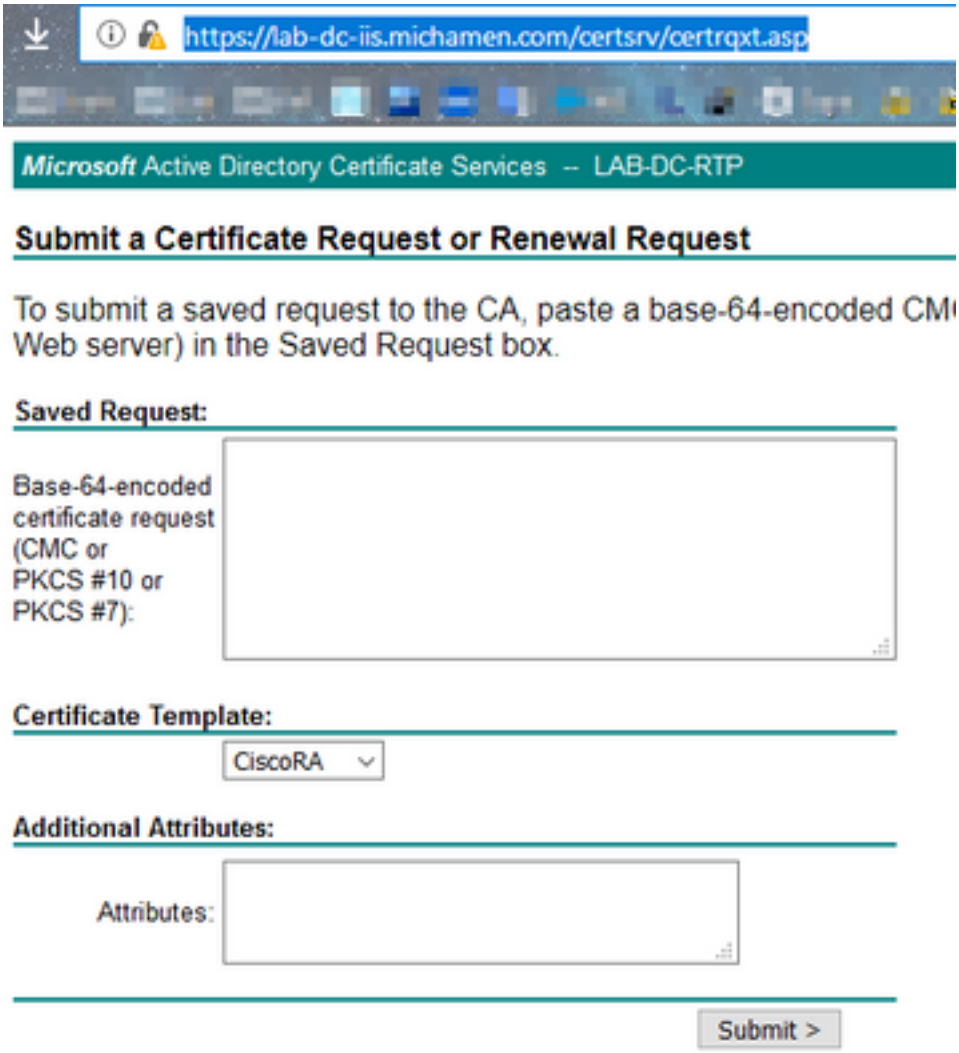
次の図は、Webブラウザからの**/certsrv** URLの例です。これは、[Certificate Services]ランディングページです。



/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。

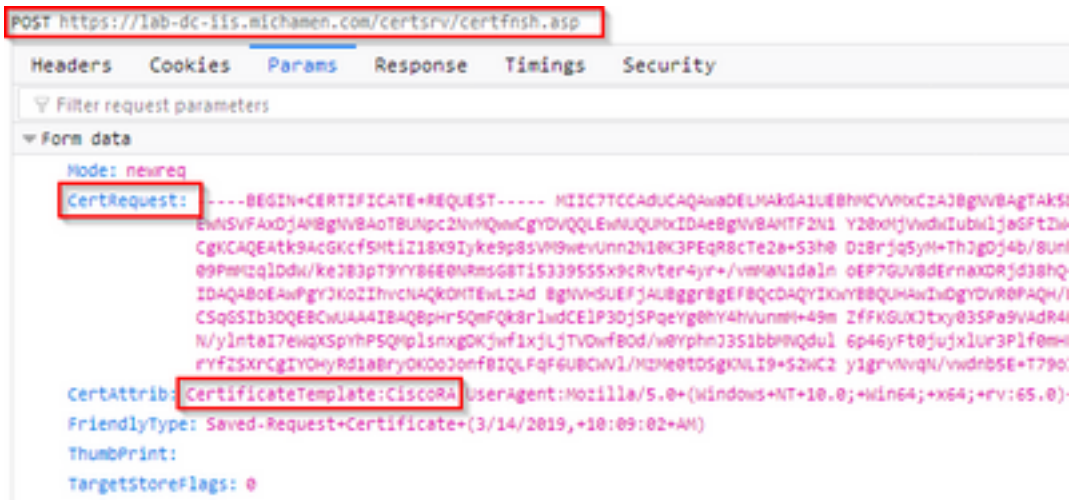
次の図は、Webブラウザの**/certsrv/certrqxt.asp**の例です。



/certsrv/certfnsh.asp

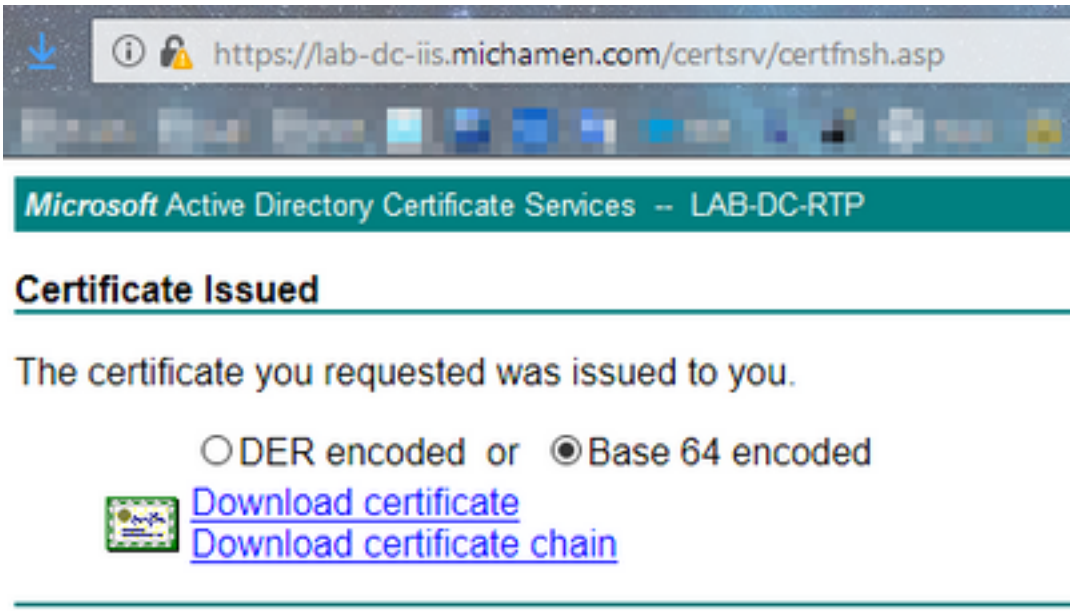
/certsrv/certfnsh.asp URLは、証明書要求のデータを送信するために使用されます。これには、CSR、証明書テンプレート名、および必要な属性が含まれます。送信を表示するには、ブラウザの開発者ツールを使用してブラウザのコン**ソールを開**き、certrqxt.aspページからデータを送信してください。

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。

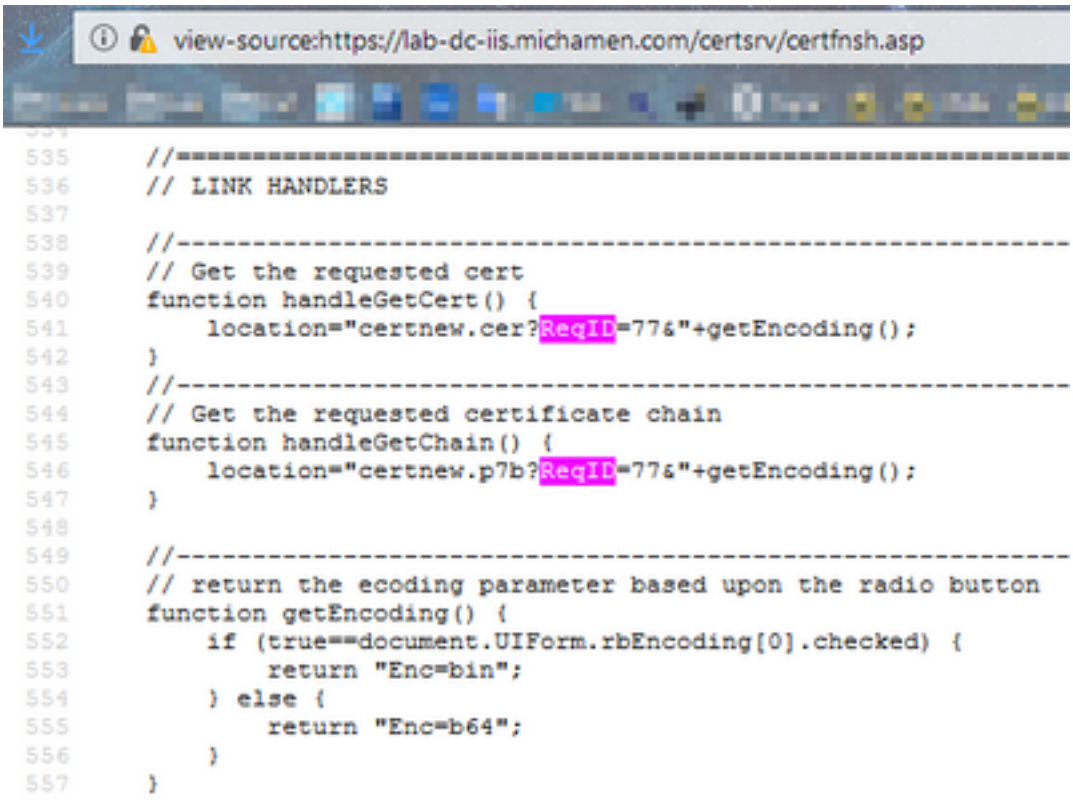


/certsrv/certfnsh.aspからの送信応答には、CAによって発行された証明書の要求IDが含まれます。

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。



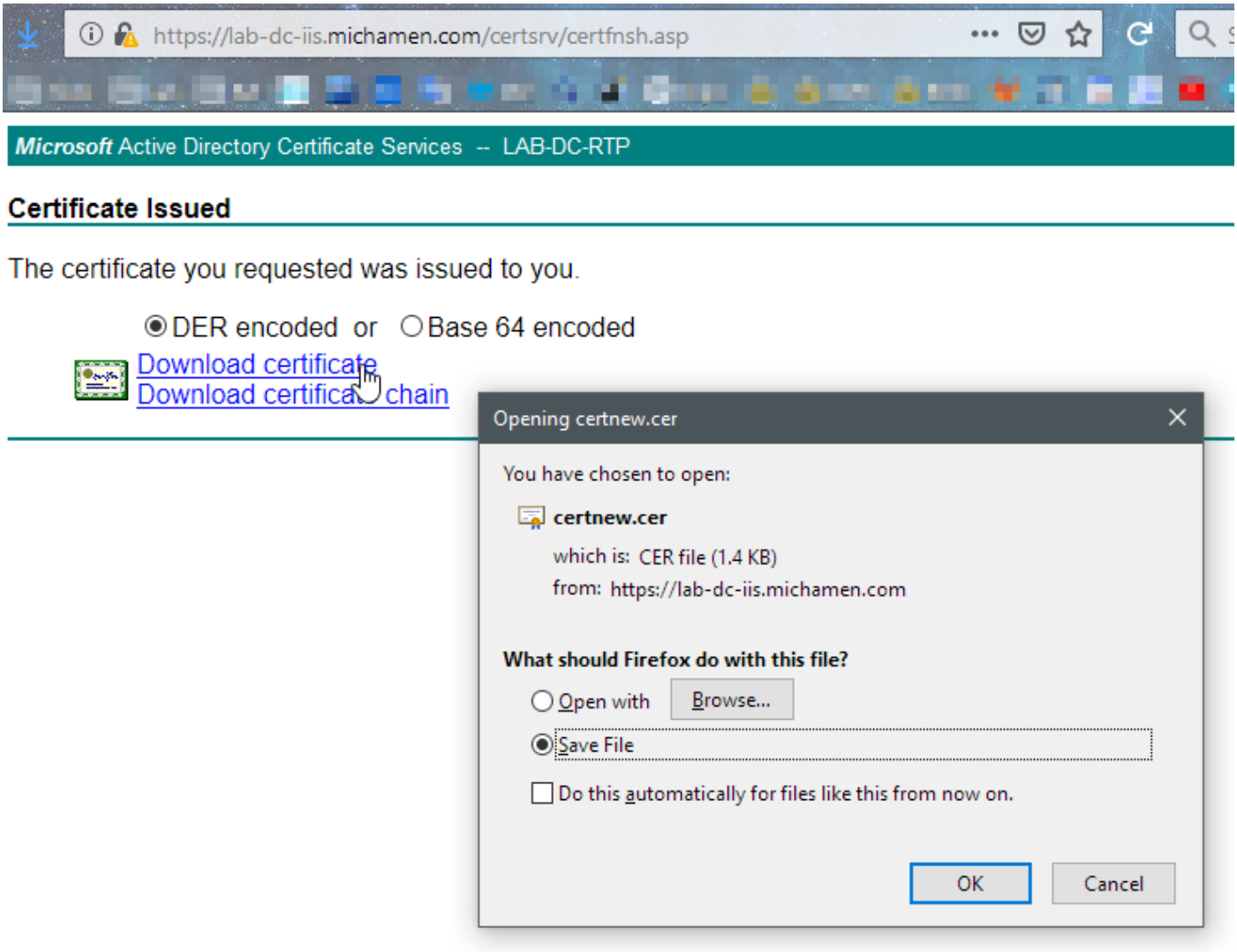
ヒント：ページソースで「ReqID」を検索します



/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。



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。 CSCvo28048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:

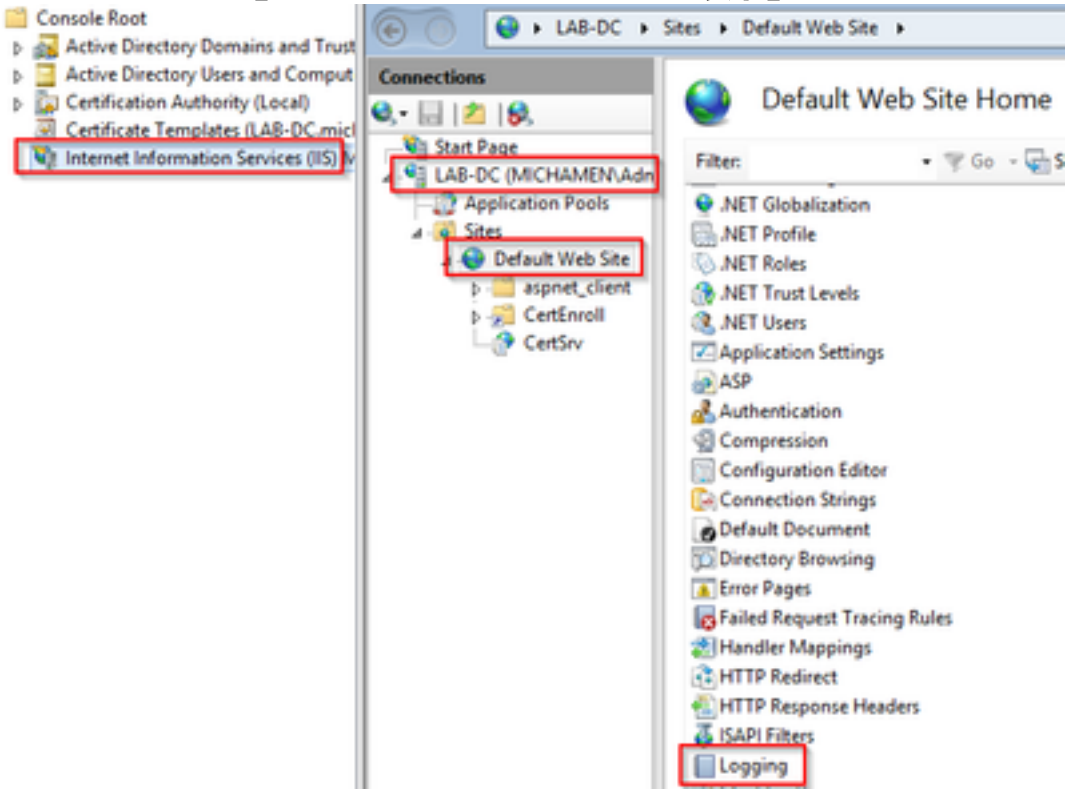
- ルートから：/var/log/active/cm/trace/capf/sdi/nginx<*number*>.txt
- CLI から：file get activelog cm/trace/capf/sdi/nginx*

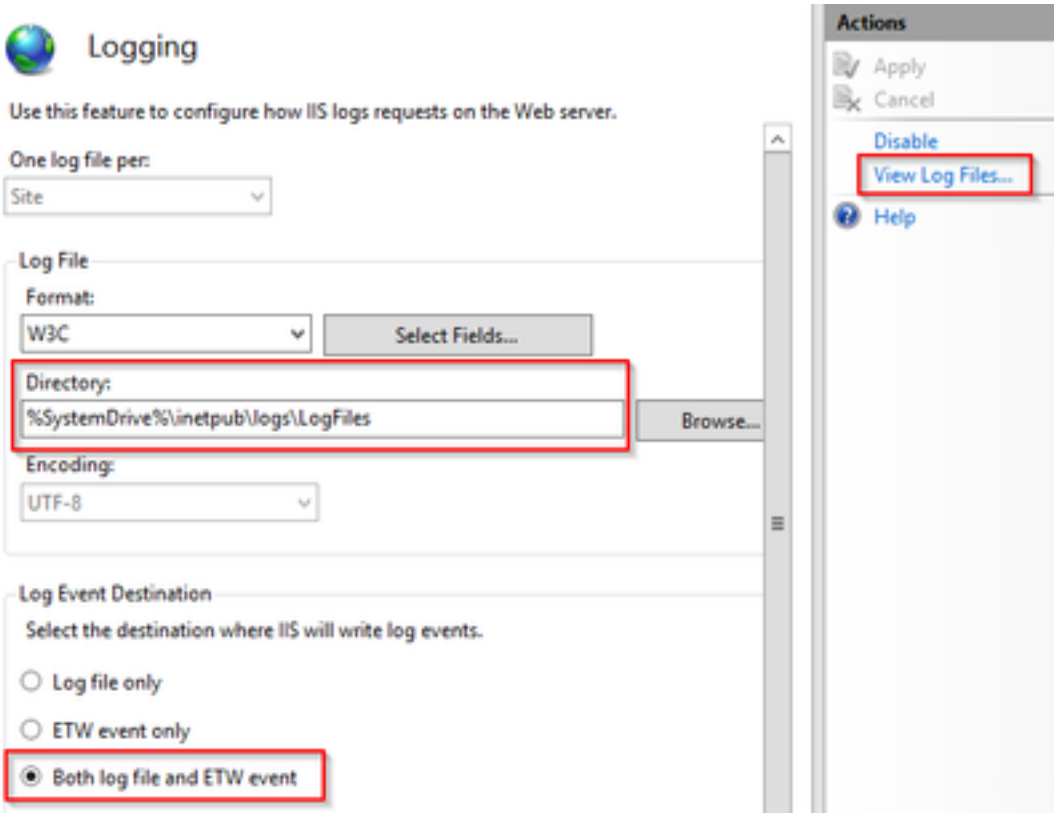
Nginxエラーログ：

- 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





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()
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。

```
12:32:09.231 |   debug CA Type is Online CA, setting up EST Connection
12:32:09.231 |<--debug
12:32:09.231 |-->debug
12:32:09.231 |   debug Inside setUpESTClient
[…]
12:32:09.231 |-->debug
12:32:09.231 |   debug cacert read success. cacert length : 1367
12:32:09.231 |<--debug
12:32:09.232 |-->debug
12:32:09.232 |   debug EST context ectx initialized
12:32:09.232 |<--debug
12:32:09.661 |-->debug
12:32:09.661 |   debug CA Credentials retrieved
12:32:09.661 |<--debug
12:32:09.661 |-->debug
12:32:09.661 |   debug est_client_set_auth() Successful!!
12:32:09.661 |<--debug
12:32:09.661 |-->debug
12:32:09.661 |   debug EST set server details success!!
```

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
14:05:04.628 |   debug 2:SEP74A02FC0A675:Inside  X509_REQ *read_csr()
14:05:04.628 |<--debug
14:05:04.628 |-->debug
14:05:04.628 |   debug 2:SEP74A02FC0A675:Completed action in X509_REQ *read_csr()
14:05:04.628 |<--debug
```

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 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Signed Cert written to /tmp/capf/cert/ location...
14:05:05.236 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Inside write_binary_file()
14:05:05.236 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Completed action in write_binary_file()
14:05:05.236 |<--debug
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 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:Return value from enrollCertUsingEST() : 0
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:Online Cert Signing successful
14:05:05.289 |<--debug
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
14:05:05.289 |-->debug
14:05:05.289 |   debug addded 6 to readset
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug Recd event
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:CA CERT RES certificate ready .
14:05:05.289 |<--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_AWAIT_CA_CERT_RESP
14:05:05.289 |<--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
14:05:05.419 |   SetOperationStatus(Success:CAPF_OP_SUCCESS):0 Operation status is set to
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
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
14:05:05.503 |-->Select(SEP74A02FC0A675)
14:05:05.511 |   Select(SEP74A02FC0A675) device exists
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
14:05:05.511 |   Select(SEP74A02FC0A675) Authentication Mode=AUTH_BY_NULL_STR:2
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 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 https://lab-dc.michamen.com:443/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
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
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
12:38:04.779 |   debug 2:SEP001F6C81118B:Return value from enrollCertUsingEST() : 35
12:38:04.779 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug 2:SEP001F6C81118B:Online Cert Signing Failed
12:38:04.779 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug addded 10 to readset
12:38:04.779 |<--debug
```

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口グに出力されます。

```
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：CSCvo58656とCSCvf83629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」

CSCvo58656 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

CSCvf83629 ESTサーバの登録中にEST_ERR_HTTP_WRITEが発生する

関連情報

- テクニカル サポートとドキュメント – Cisco Systems