CAPF オンライン CA のトラブルシューティング

目次

概要

この資料は（CAPF）自動登録および更新 機能のためにプロキシ 機能 認証局（CA）解決することを記述します。 この機能はまた CAPF オンライン CA と言われます。

前提条件

要件

次の項目に関する知識が推奨されます。

- 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 文書に記載されている 情報は CUCM バージョン 12.5 に CAPF オンライン CA 機能が CUCM 12.5 で導入されたので基づいています。

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。

機能コンポーネントの概要

Registration Authority （RA）

RA はデジタル認証のための User 要求を確認し、認証局（CA）を証明書を発行するように告げるネットワークの権限です。 RA は Public Key Infrastructure（PKI）の一部です。

セキュアな転送（EST）上の登録

EST は Transport Layer Security （TLS）およびハイパーテキスト転送プロトコル（HTTP）上の CMS （CMC）メッセージ上の証明書管理を使用するクライアントの証明書登録のための

Request For Comments（RFC）7030 で定義されるプロトコルです。 EST は EST クライアントが登録要求を送信 する EST サーバが結果を用いる応答を返すクライアント/サーバモデルを使用し。

libEST

libEST は Cisco の EST の実装のためのライブラリです。 libEST は X509 証明書がエンドユーザ デバイスおよびネットワークインフラストラクチャ デバイスで提供されるようにします。 このライブラリは CiscoEST および CiscoRA によって設定されます。

エンジンX（NGINX）

NGINX は Apache と同じような Webサーバおよび逆プロキシです。 NGINX は CAPF と CES 間の HTTP 通信、また CES と CA Web 登録サービス間の通信のために使用されます。 libEST が libEST に代わって TCP 要求を処理するためにサーバモードで動作するとき Webサーバが必要となります。

証明書登録サービス（CES）

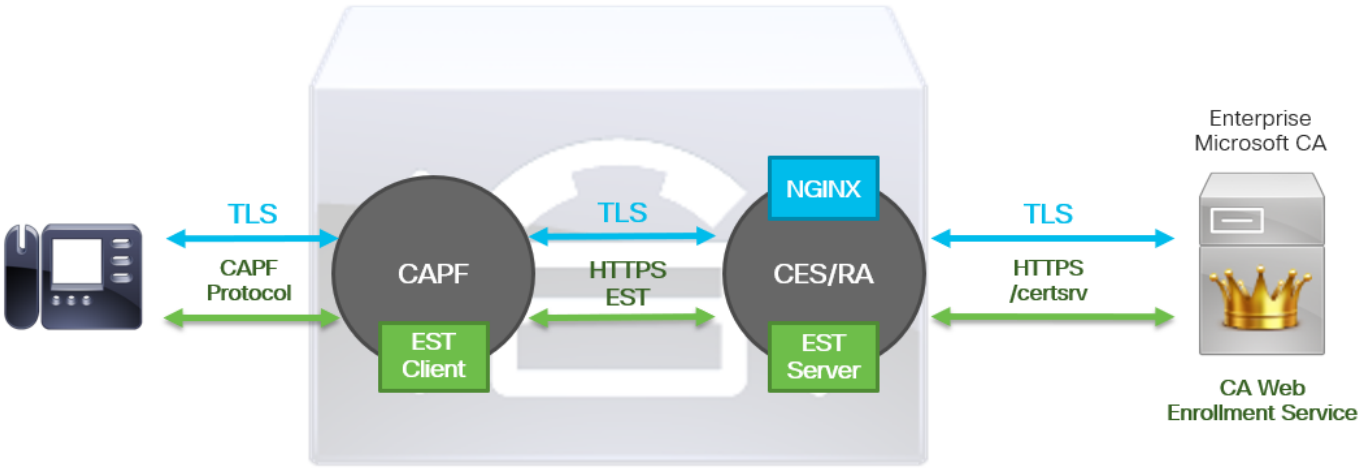
CES は CAPF サービスと CA. CES 間の RA がまた CiscoRA と言われる、または単に RA 機能するので CUCM のサービスです。 CES は CES が RA として機能するためにサーバモードの libEST を設定するのでそれが Webサーバであるので NGINX を使用します。

Certificate Authority Proxy Function（CAPF）

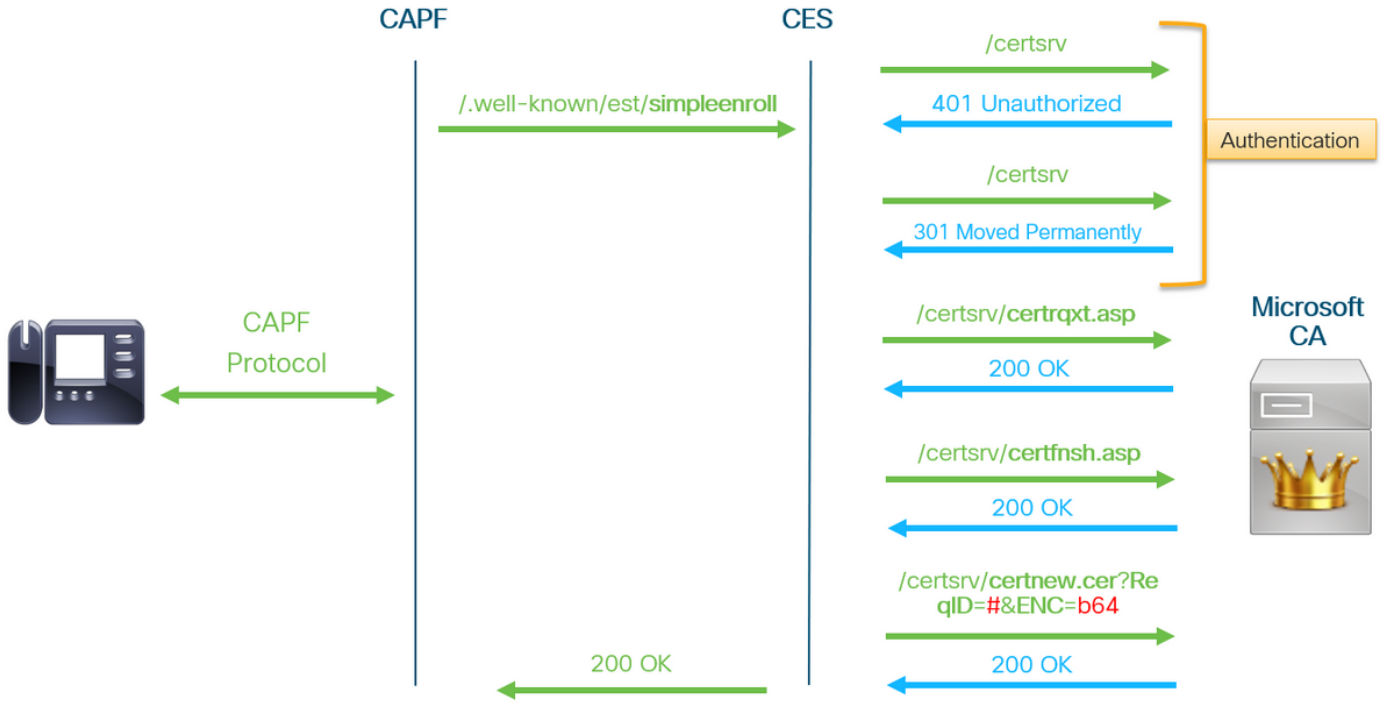
CAPF は電話が証明書登録を行うとき要求する相互に作用している CUCM サービスです。 CAPF は電話に代わって CES と相互に作用しています。 この機能 モデルで CAPF は CES によって電話の証明書を登録するためにクライアントモードの libEST を設定します。

要約すると、ここに各コンポーネントが設定されているどのようにかです:

1. 電話は CAPF に Certificate 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）を設定します
3. EST クライアント要求に処理し、応答する CES 実装 CiscoRA（サーバモード）
4. CES/CiscoRA は HTTPS によって CA の Web 登録サービスと通信します



メッセージフロー流れ図



メッセージフロー説明

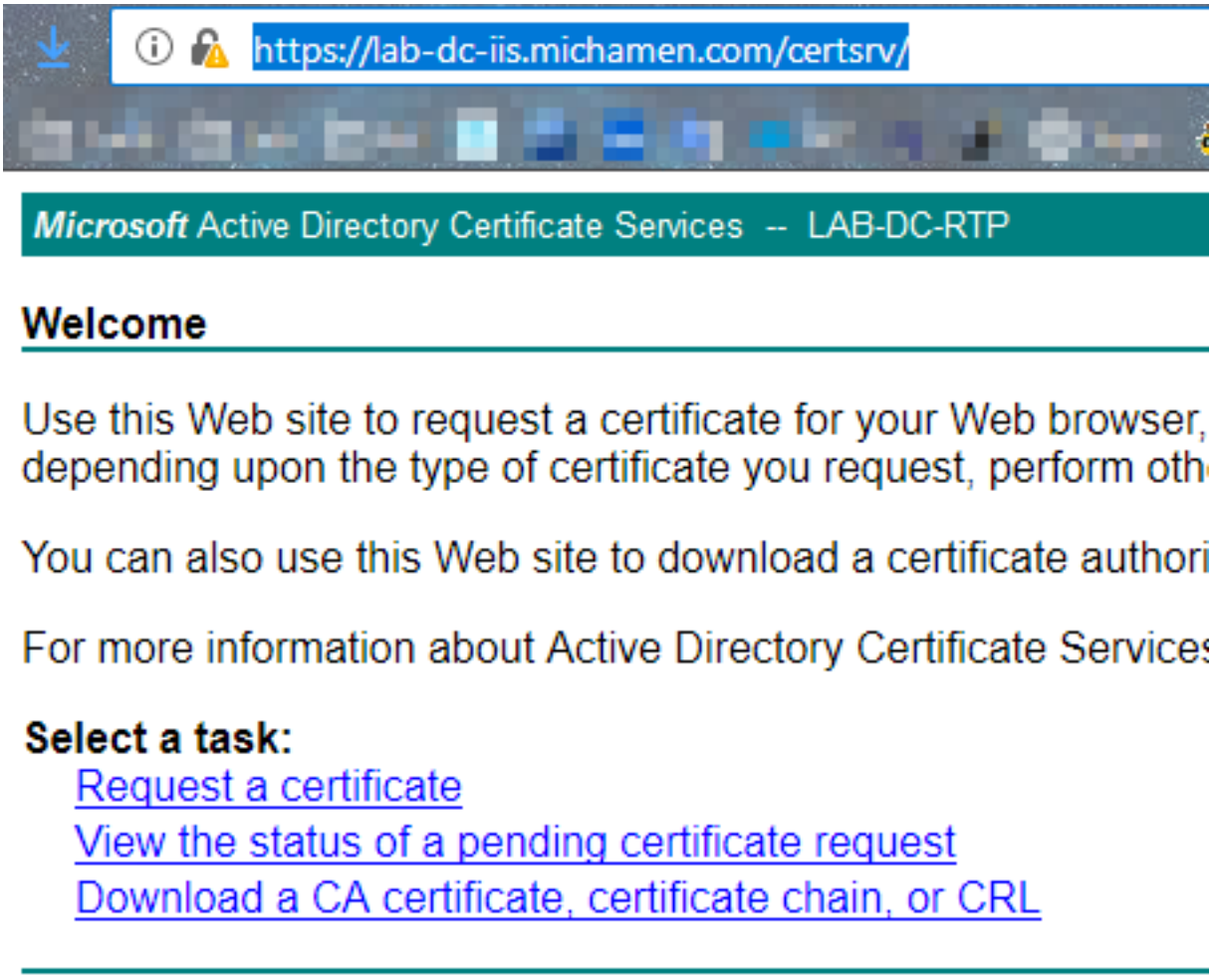
/.well-known/est/simpleenroll

EST クライアントは EST サーバからの証明書登録を要求する API コールを発信するのにこの URL を使用します。 EST サーバが API コールを受信すれば CA の Web 登録サービスの HTTPS コミュニケーションが含まれている証明書登録 プロセスを開始します。 登録プロセスが正常であり、EST サーバが新しい証明書を受け取れば場合、CAPF は証明書をロードし、IP Phone に戻って役立つことを続行します。

/certsrv

EST クライアントによって **/certsrv** URL が CA のセッションを認証し、開始するのに使用されています。

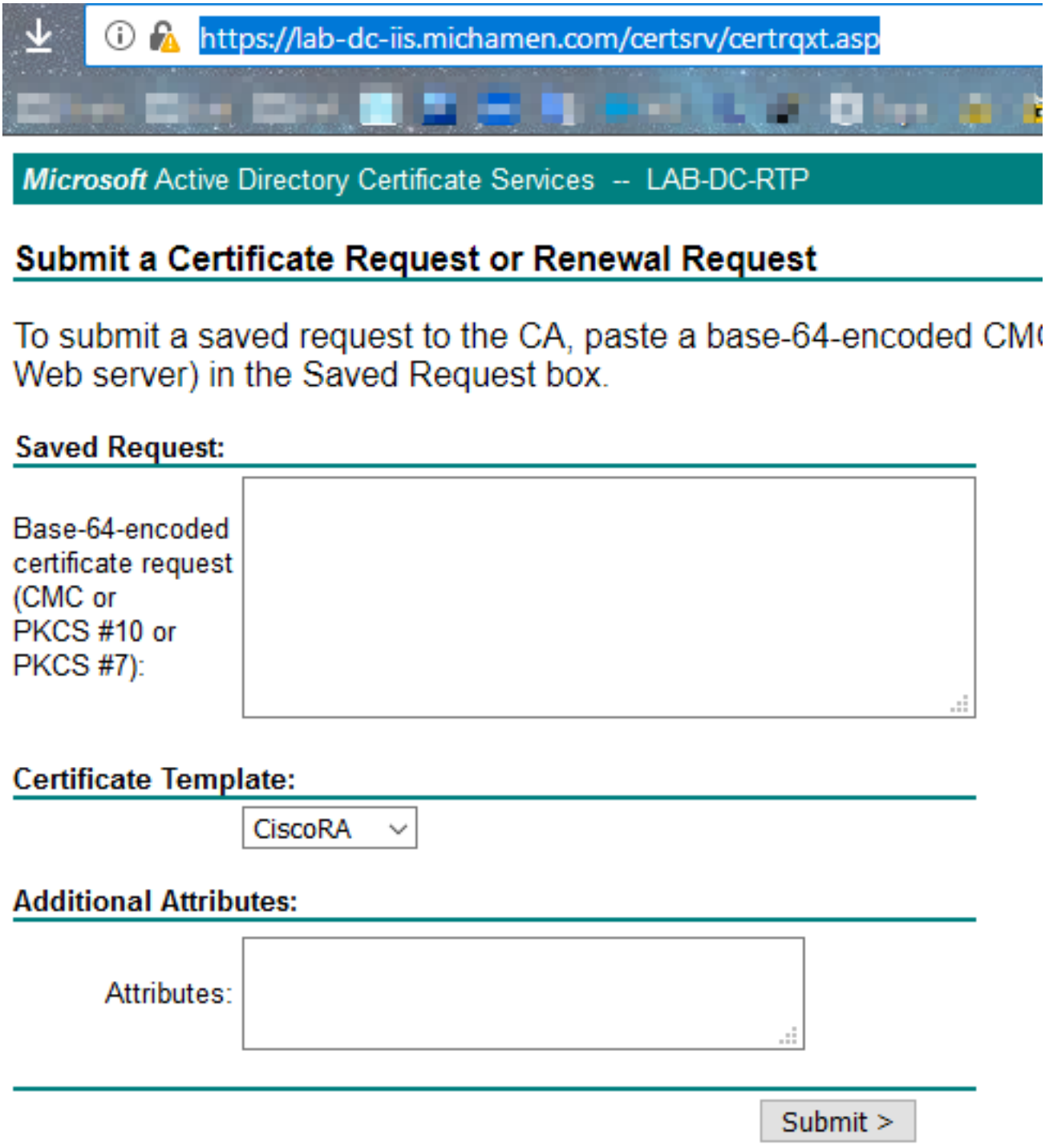
イメージは下記の Webブラウザから **/certsrv** URL の例です。 これはページを上陸させている認証 サービスです。



/certsrv/certrqxt.asp

/certsrv/certrqxt.asp URL が新しい証明書のための要求を始めるのに使用されています。 EST クライアントは CSR、証明書のテンプレート名前および望ましい属性を入れるのに **/certsrv/certrqxt.asp** を使用します。

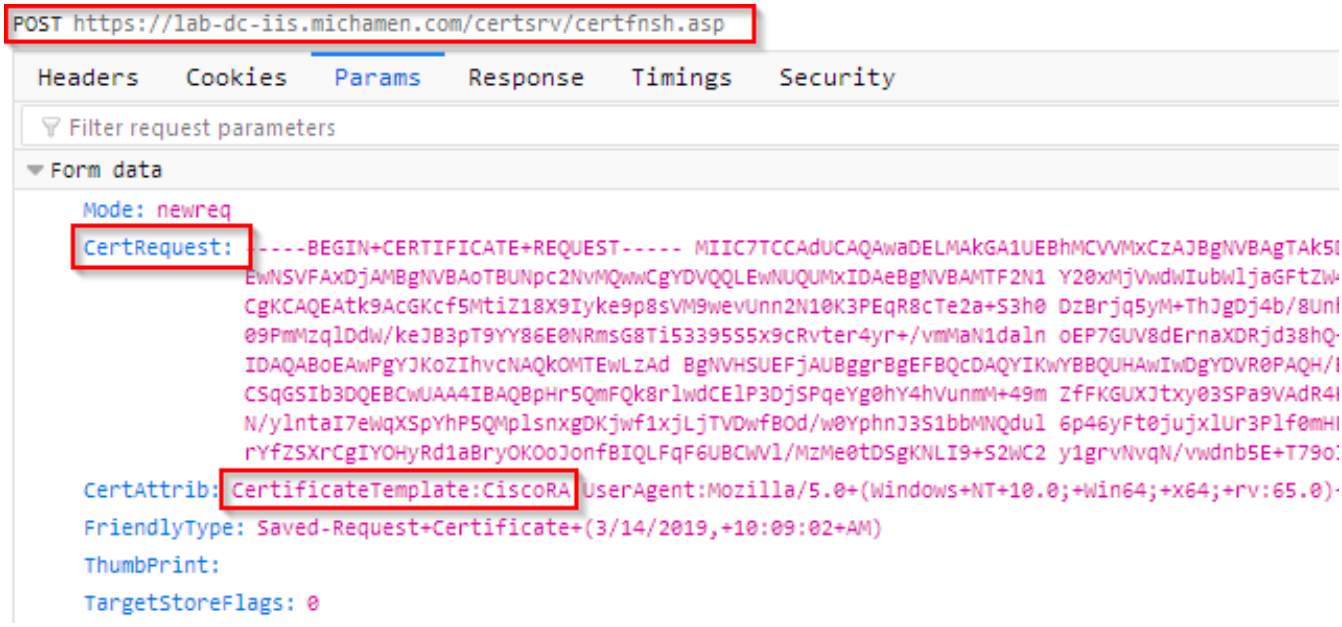
イメージは下記の Webブラウザから **/certsrv/certrqxt.asp** の例です。



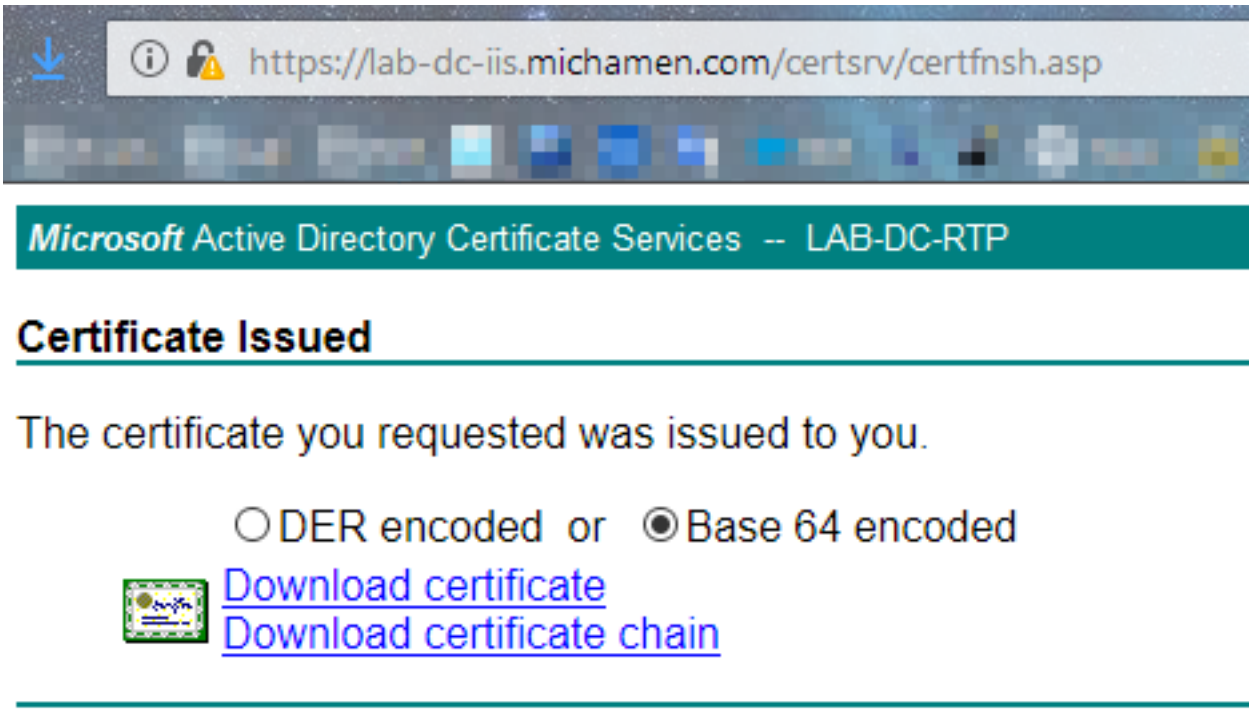
/certsrv/certfnsh.asp

/certsrv/certfnsh.asp URL が Certificate 要求のためにデータを入れるのに使用されています; CSR、証明書のテンプレート名前および望ましい属性が含まれているかどれが。 データが *certrqxt.asp* ページによって入る前に送信をブラウザのコンソールを開くのに表示するためにブラウザの**開発者ツールを**使用して下さい。

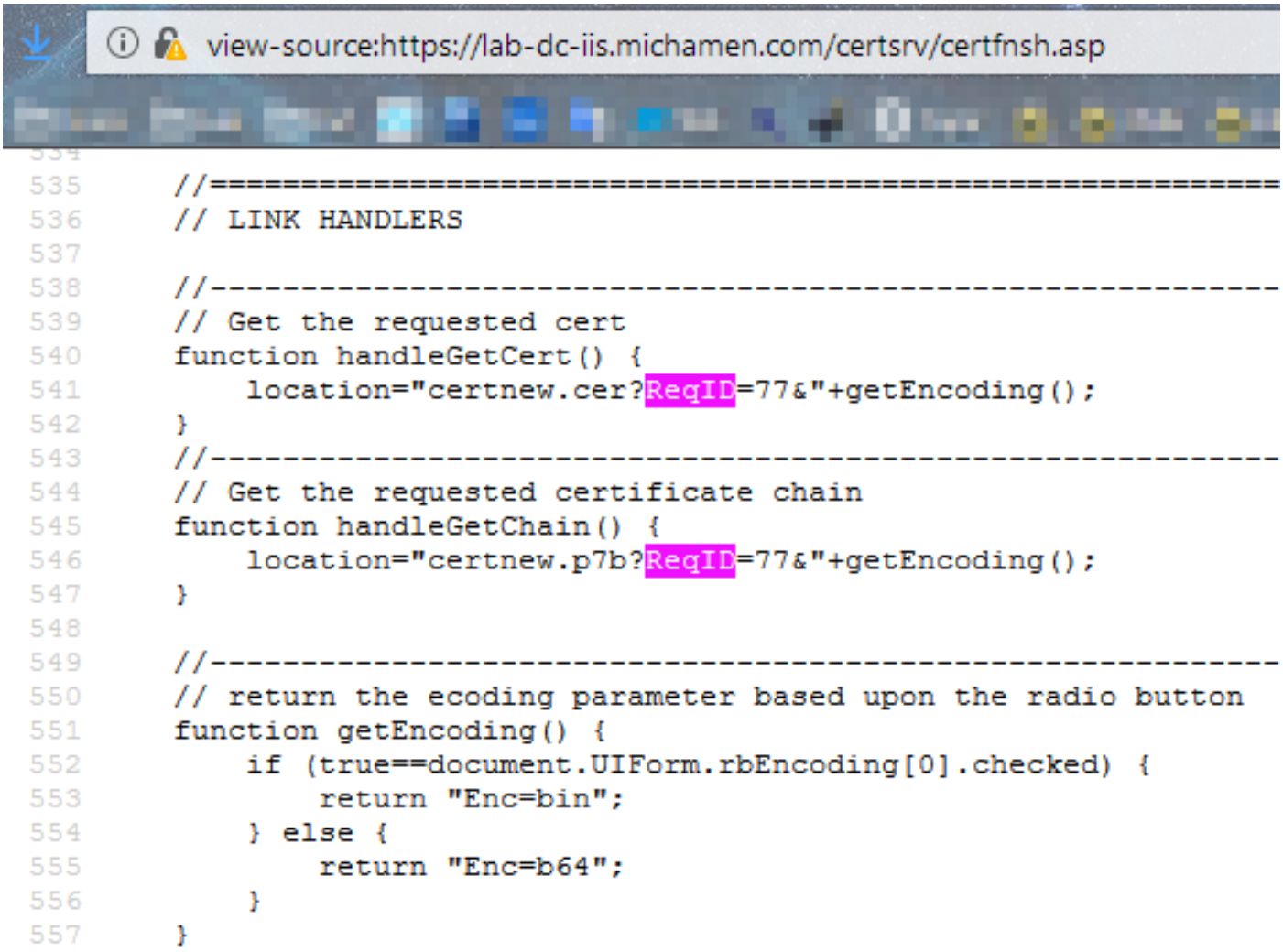
イメージは下記のブラウザのコンソールで表示する データの例です。



/certsrv/certfnsh.asp からの服従応答は CA によって発行される証明書の要求 ID が含まれています。 ページのソースコードが点検されるとき要求 ID は Webブラウザで見られます。



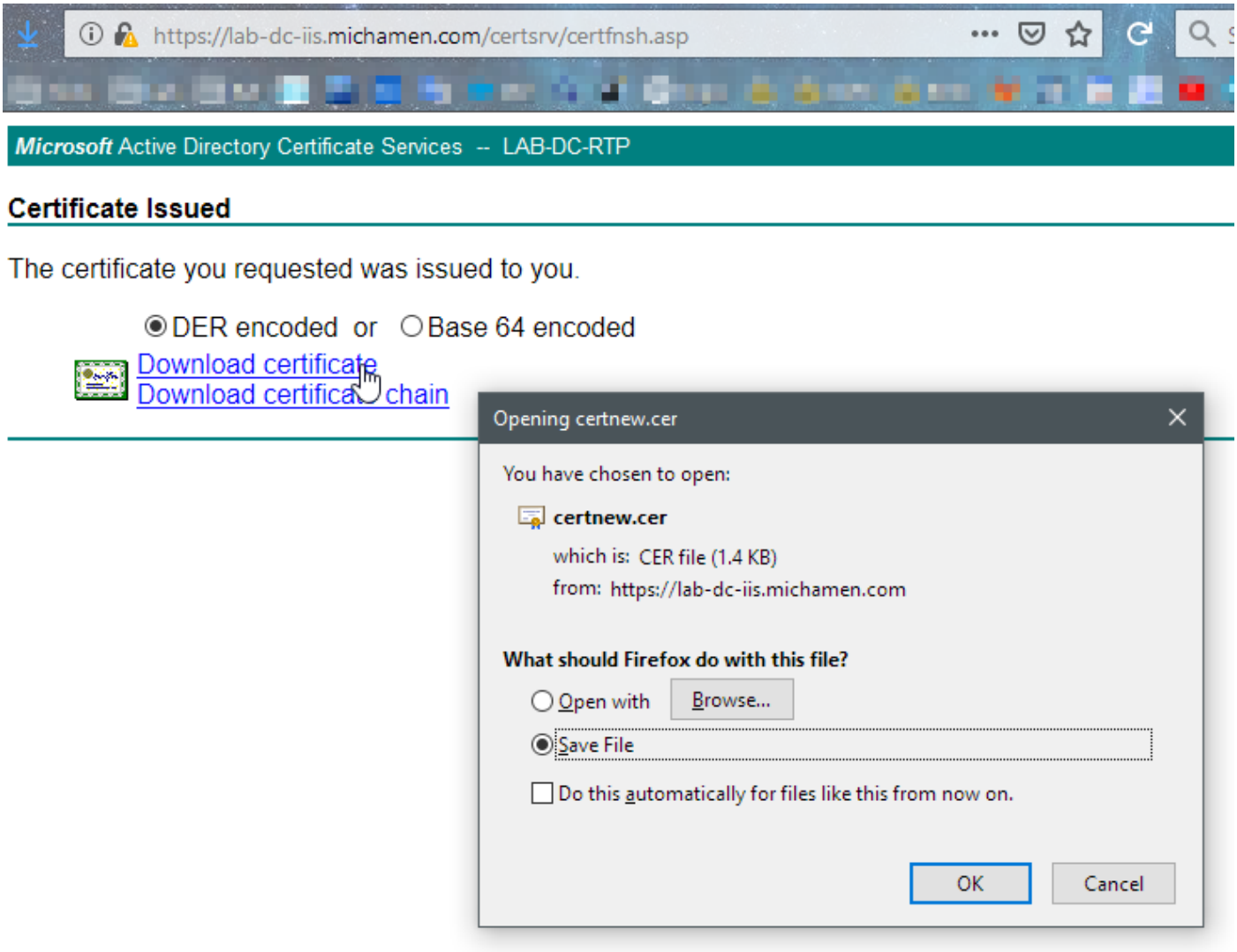
ヒント： 捜して下さい「ReqID」をページ 出典を



/certsrv/certnew.cer

この時点で EST クライアントは新しい証明書のための要求 ID に気づいています。 EST クライアントは .cer 拡張を用いる証明書ファイルをダウンロードするためにパラメータとして符号化する要求 ID およびファイルを渡すのに /certsrv/certnew.cer を使用します。

これは**ダウンロード証明書** リンクをクリックするとき起こることとブラウザで同等です。



要求 URL およびパラメータを表示するために、ブラウザのコンソールを使用して下さい。

> **注:** ブラウザは DER エンコードが選択される場合エンコード パラメータのための**ビンを**規定 します; ただし、Base64 エンコードは b64 として示します。

トラブルシューティングのための関連したトレース/ログ

これらの口グはほとんどの問題の分離と助けます。

CAPF ログ

CAPF ログは CiscoEST アクティビティの電話および最小ロギングの相互対話が含まれています。

> **注:** これらの口グは Command Line Interface （ CLI ）か実時間監視 ツール（ RTMT ）によって収集に利用できます。 CSCvo28048 CAPF が原因で RTMT でサービスのリストの中で示すかもしれなくないです。

CiscoRA ログ

CiscoRA ログは頻繁に CES が記録 すると同時に参照されます。 CiscoRA ログは CA の認証が行われる間、CES 初期スタートアップ アクティビティが含まれ、起こるかもしれないエラーを表示する。CA の最初の認証が正常である場合、電話登録のためのそれに続くアクティビティはここに口グオンされません。 従って問題を解決するのに、CiscoRA 口グはよい始点として動作します。

> **注:** これらの口グはこの文書作成現在で CLI によってしか集めることができません。

NGINX error.log

すべてのアクティビティをの間に開始する記録 する、また NGINX と CA 間のどの HTTP 相互対話でも味方するので NGINX error.log はこの機能のための最も有用な口グです; CA から戻るエラーコード、また要求をか処理した後 CiscoRA によって生成されるエラーコードが含まれているかどれが。

> **注:** この資料の作成の時に、CLI からこれらの口グを集める方法がありません。 これらの口グはリモート サポート アカウント（ルート）を使用してしかダウンロードすることができません。

CA Webサーバのログ

CA Webサーバの口グは要求 URL、応答コード、応答期間およびレスポンスサイズを含む HTTP アクティビティを表示するので重要です。 CiscoRA と CA 間の相互対話を関連させるのにこれらの口グを使用できます。

> **注:** CA Webサーバはこの資料のコンテキストをです MS IIS 口グ ログオンします。 他の Web CA が将来サポートされる場合、それらは CA Webサーバの口グとして動作する異なる口グファイルがあるかもしれません

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： ファイルは activelog cm/trace/capf/sdi/capf* を得ます

> **注:** CAPF トレース レベルをに「詳述し」、テストする前に再開します CAPF サービスを実

行された 設定 して下さい。

Cisco RA:

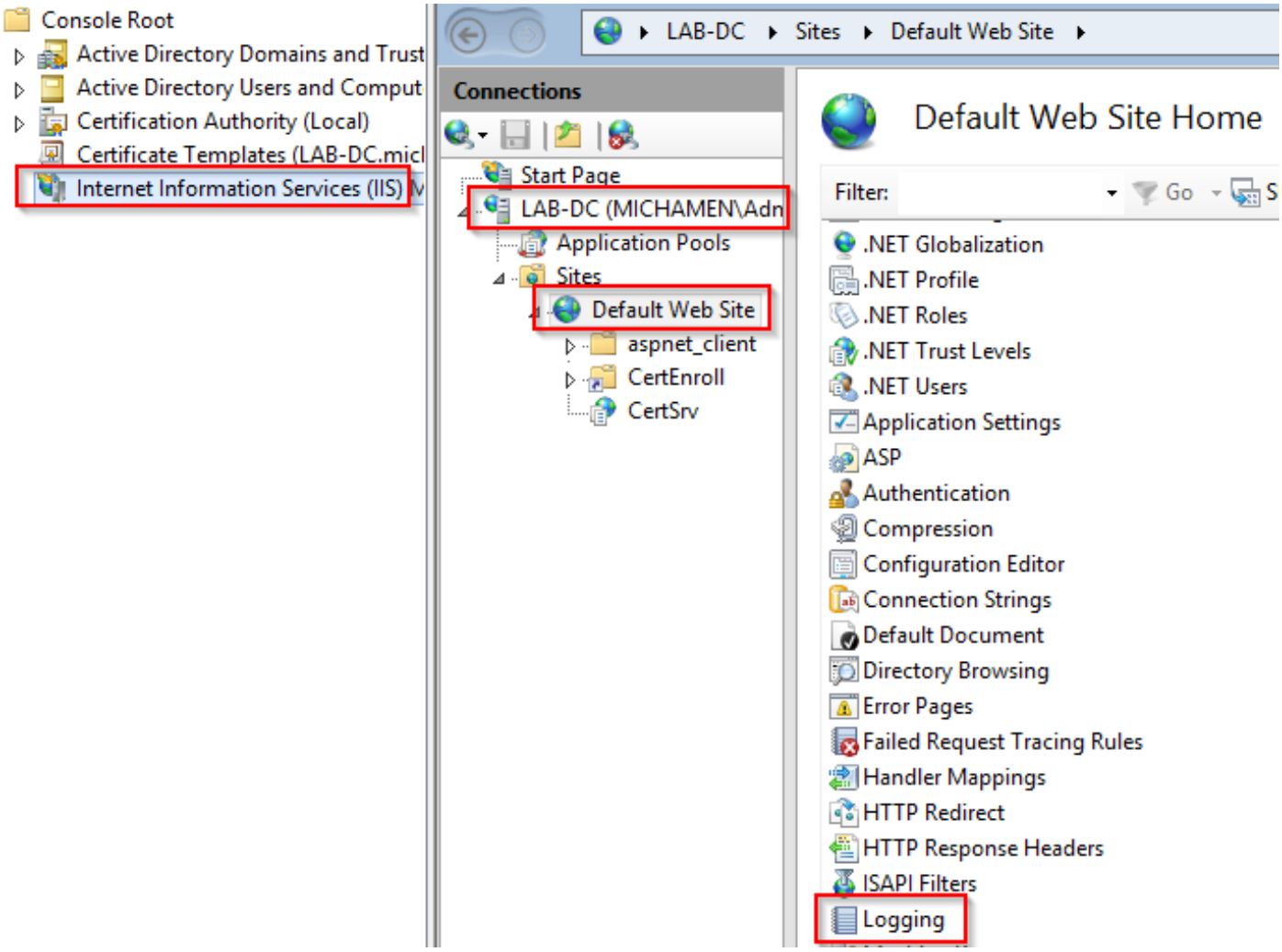
- ルートから: /var/log/active/cm/trace/capf/sdi/nginx <number >.txt
- CLI から ： ファイルは activelog cm/trace/capf/sdi/nginx* を得ます

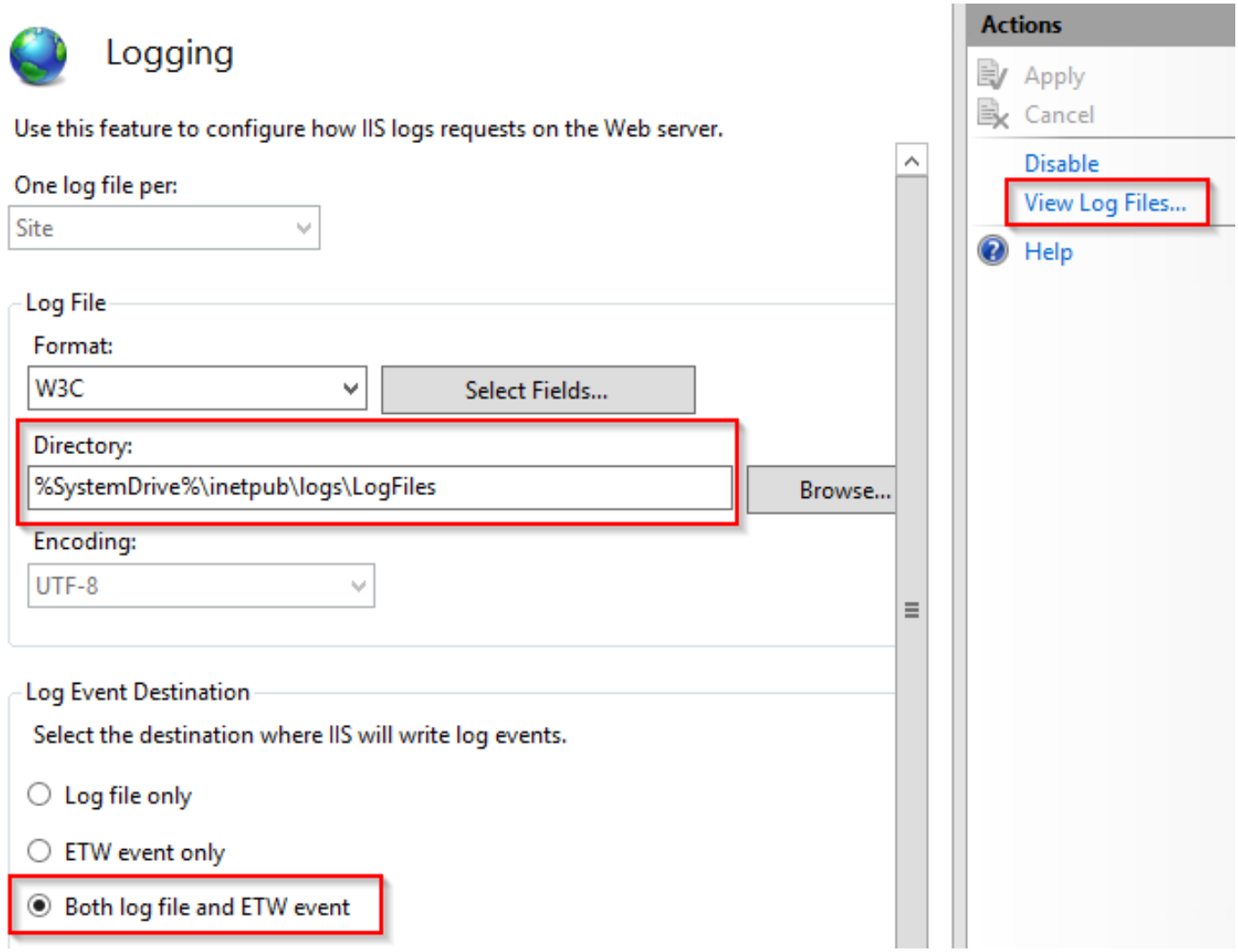
Nginx エラーログ:

- ルートから: /usr/local/thirdparty/nginx/install/logs/error.log
- CLI から使用不可能

MS IIS ログ:

- MMC を開いて下さい
- **Internet Information Services （ IIS ）**スナップインを選択して下さい
- サーバ名をクリックして下さい
- 『Default Web Site』 をクリック して下さい
- ロギング オプションを見るために**ロギングを**ダブル クリックして下さい
- **Actions メニューのログファイルを**『View』 を選択 して下さい





例ログ 分析

普通開始しているサービス

NGINX ログに見られるように開始する CES

少し informaiton はこのログから収集されます。 信頼ストアにロードされる完全な証明書 チェーンは Web 容器のため他が EST のためである間、1 ですここに見られ、：

```
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 error.log に見られるように開始する CES

証明書のテンプレート 設定および資格情報を使用してログインは断片でここに観察されます:

```
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 認証 チェーンの検索は断片でここに観察されます:

```
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
```

要求が正常なとき certnew.p7b ファイルは得られます。 テンプレート 資格情報との同じ URL が Webブラウザから certnew.p7b ファイルを得るのに使用することができます。

IIS ログに見られるように開始する CES

NGINX error.log で参照されるイベントの上で開始する同じ CES はまた IIS ログで観察されます; ただし、IIS ログは最初の要求が 401 応答による Webサーバによって挑戦されるので 2 つのより多くの HTTP GET 要求が含まれています; そして要求された一度認証された 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 ログに見られるように開始する CAPF

発生する何が開始する CES のための CAPF ログにほとんどは発生する何が他のログに同じを検知 します; しかしオンライン CA のための方式および設定を検出する CAPF サービスに注意します:

```
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
```

ログからの次の重要な観測は CAPF サービスがそれをである EST クライアント初期化するときあります。

```
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 インストール オペレーション

CAPF ログ

にすべての必要なログを集めることを推奨し、CAPF の確認との分析を開始するために記録 します。 これは私達が特定の電話のための時間の参照を知ることを可能にします。

シグナリングの最初の一部は他の CAPF メソッドと同様に（CSR が電話によって提供された後）CAPF サービスで動作している EST クライアントがダイアログの終わりの方の CES と登録を行う以外同じを検知 します。

```
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 が電話の署名入り認証を取得したら、証明書は DER 形式にそれが電話に提供される前に変換されます。

```
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 サービスは再度引き継ぎ、それが上記の断片にに書かれた位置から CSR を口ードします（/tmp/capf/cert/）。 CAPF サービスは電話にそれから署名された LSC を提供します。 同時に電話の CSR は削除されます。

```
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

断片は下記の上で説明されるように電話の LSC インストール手順のための IIS ログのイベントを表示する。

```
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 側にエラーがある時はいつでも、CAPF ログで下記の断片のような出力を見ることを期待します。 他の口グを問題の範囲を絞り続けるようにチェックすることを忘れないでいて下さい。

```
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
```

IIS ID証明の発行元 チェーンの抜けた CA 認証

証明書 チェーンにあるルート証明か中間物証明書が CES によって取得することが不可能なエラー「信頼されないとき CA からの CA CERT チェーンは」nginx 口グで印刷されます。

```
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
```

自己署名証明書を示す Webサーバ

IIS の自己署名証明書の使用は CUCM の CAPF 信頼としてアップ ロードされてサポートされなくてし、も作業に注意します。 断片は下記の nginx ログからあり、IIS が自己署名証明書を使用しているとき観察されるものが表示する。

```
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 ホスト名および Common Name のミスマッチ

IIS 証明書の Common Name （ラボ dc ）は CA の Web 登録サービスの URL の中の FQDN を一致する。 認証の検証に関しては URL の中の FQDN を成功することは CA によって使用される証明書の Common Name を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 解決問題

CiscoRA はオンライン CA によって設定される稼働中 パラメータのホスト名を解決することができません。

```
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
```

認証の妥当性日付においての問題

きちんとはたらかないネットワーク タイム プロトコル (NTP) が認証の妥当性日付においての発行するとき発生して下さい。 このチェックは CES によって開始します実行された、それは NGINX 口グで観察されます。

```
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
```

証明書のテンプレート ミスコンフィギュレーション

サービスパラメータ内の名前のタイプエラーにより失敗を引き起こします。 No エラーは CAPF NGINX ログ ログオンされます NGINX error.log をチェックすることを従って必要とします。

```
***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

下記に切り取られる最初の certsrv 認証プロセスの間に 10 秒のデフォルトタイマーの後で CES EST クライアントタイムを示します。

```
***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
```

注: CSCvo58656 および CSCvf83629 は両方 CES 認証 タイムアウトに関係します。

CES 登録タイムアウト

登録要求への応答を待っている間認証の成功の後の CES EST クライアントタイムしかし。

```
***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
```

既知の警告

RTMT にリストされていない CSCvo28048 CAPF サービスはファイル· メニューをもう集めます

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を必要とします

登録の間に EST_ERR_HTTP_WRITE を得る CSCvf83629 EST サーバ

関連情報

- テクニカル サポートとドキュメント – Cisco Systems