CAPF 온라인 CA 문제 해결

목차

소개

이 문서에서는 CAPF(Certificate Authority Proxy Function) 자동 등록 및 갱신 기능에 대한 트러블슈팅에 대해 설명합니다.이 기능을 CAPF Online CA라고도 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 인증서
- Cisco CUCM(Unified Communications Manager) 보안

사용되는 구성 요소

이 문서의 정보는 CUCM 12.5에 CAPF Online CA 기능이 도입되었으므로 CUCM 버전 12.5를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 구성 요소 개요

등록 기관(RA)

RA는 디지털 인증서에 대한 사용자 요청을 확인하고 CA(Certificate Authority)에 인증서를 발급하도록 지시하는 네트워크의 권한.RA는 PKI(Public Key Infrastructure)의 일부입니다.

EST(Secure Transport)를 통한 등록

EST는 TLS(Transport Layer Security) 및 HTTP(HyperText Transfer Protocol)를 통해 CMC(Certificate Management over CMS) 메시지를 사용하는 클라이언트의 인증서 등록을 위해 RFC(Request for comment) 7030에 정의된 프로토콜입니다.EST는 EST 클라이언트가 등록 요청을 전송하고 EST 서버가 결과와 함께 응답을 보내는 클라이언트/서버 모델을 사용합니다.

libEST

libEST는 Cisco가 구현하는 EST. libEST를 통해 X509 인증서를 최종 사용자 장치 및 네트워크 인프라 장치에 프로비저닝할 수 있는 라이브러리입니다.이 라이브러리는 CiscoEST 및 CiscoRA에 의해 구현됩니다.

엔진-X(NGINX)

NGINX는 Apache와 유사한 웹 서버이며 역방향 프록시입니다. NGINX는 CAPF와 CES 간의 HTTP 통신뿐 아니라 CES와 CA 웹 등록 서비스 간의 통신에도 사용됩니다.libEST가 서버 모드에서 작동하는 경우 libEST를 대신하여 TCP 요청을 처리하려면 웹 서버가 필요합니다.

CES(Certificate Enrollment Service)

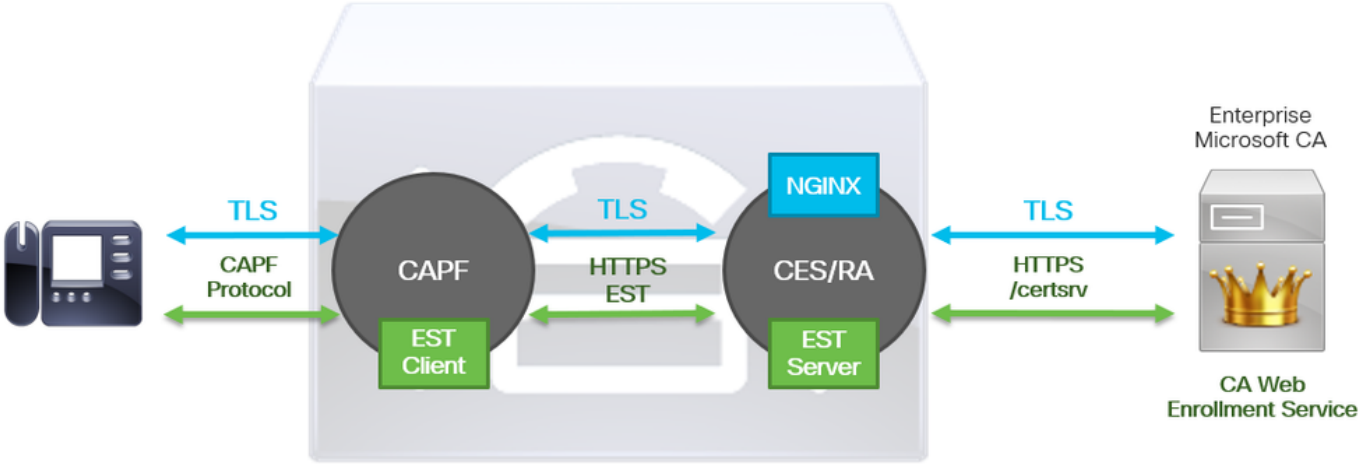
CES는 CAPF 서비스와 CA 간의 RA 역할을 하는 CUCM의 서비스입니다.CES는 CiscoRA 또는 RA라고도 합니다.CES는 RA의 역할을 하기 위해 서버 모드에서 libEST를 구현하므로 CES는 NGINX를 웹 서버로 사용합니다.

CAPF(Certificate Authority Proxy Function)

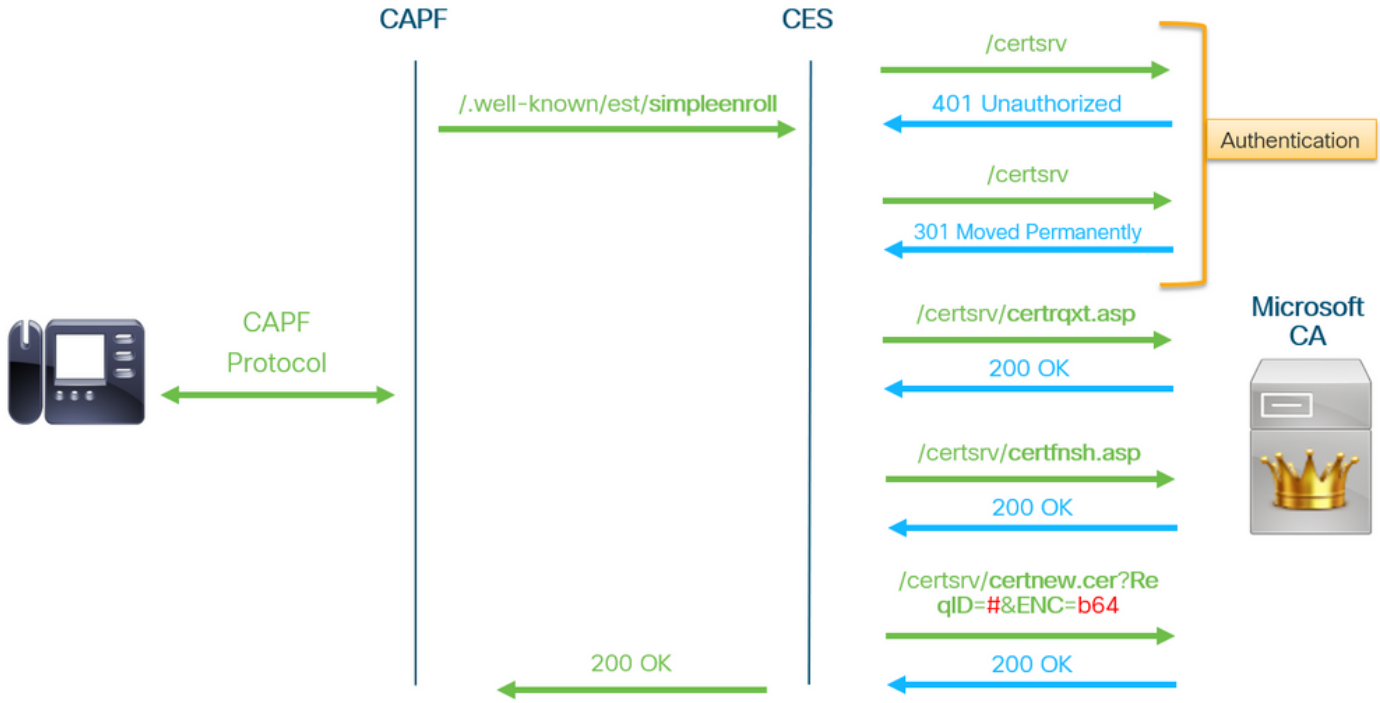
CAPF는 전화기가 인증서 등록 요청을 수행할 때 상호 작용하는 CUCM 서비스입니다.CAPF는 전화기 대신 CES와 상호 작용합니다.이 기능 모델에서 CAPF는 CES를 통해 전화기의 인증서를 등록하기 위해 클라이언트 모드에서 libEST를 구현합니다.

요약하면, 각 구성 요소가 구현되는 방법은 다음과 같습니다.

1. 전화기가 CAPF에 인증서 요청을 보냅니다.
2. CAPF는 CES와 통신하기 위해 CiscoEST(클라이언트 모드)를 구현합니다.
3. CES는 CiscoRA(서버 모드)를 구현하여 EST 클라이언트의 요청을 처리하고 응답합니다.
4. CES/CiscoRA는 HTTPS를 통해 CA의 웹 등록 서비스와 통신합니다.



메시지 흐름 다이어그램



메시지 흐름 설명

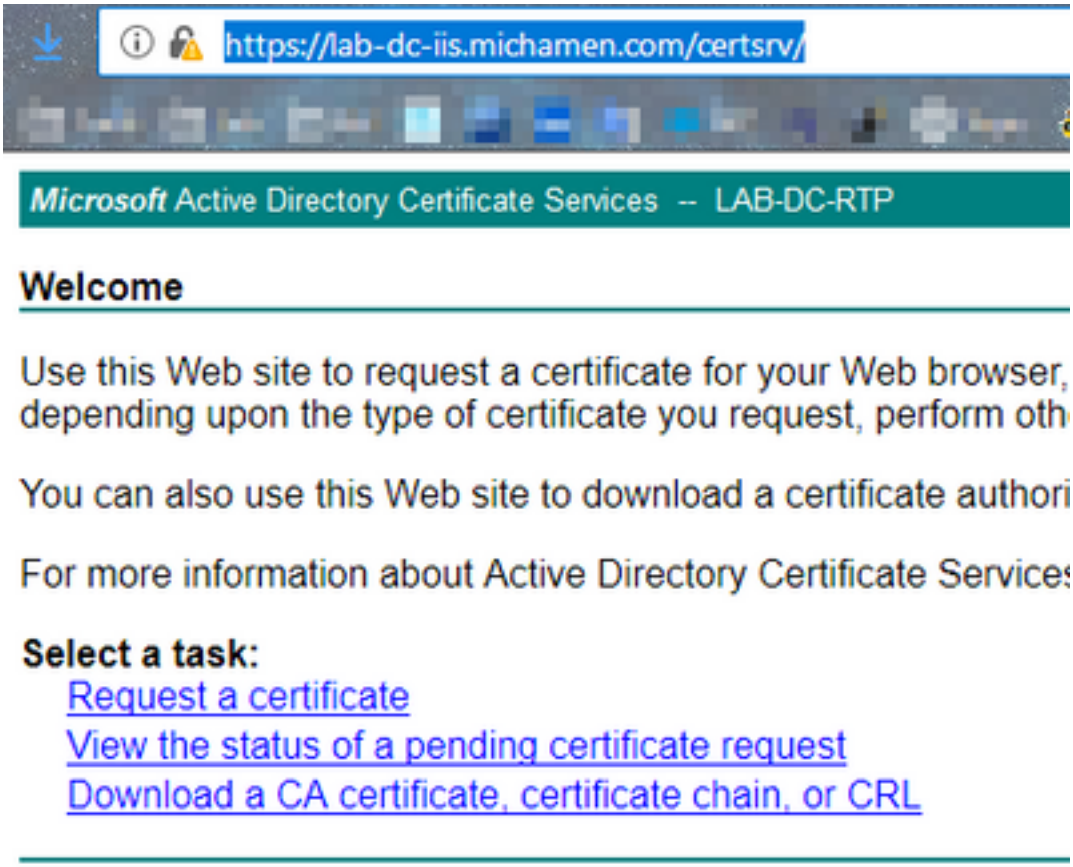
/.well-known/est/simpleenroll

EST 클라이언트는 이 URL을 사용하여 EST 서버의 인증서 등록을 요청하는 API 호출을 전송합니다.EST 서버가 API 호출을 받으면 CA의 웹 등록 서비스와의 HTTPS 통신을 포함하는 인증서 등록 프로세스가 시작됩니다.등록 프로세스가 성공하고 EST 서버가 새 인증서를 받으면 CAPF는 계속해서 인증서를 로드하고 IP 전화기에 다시 제공합니다.

/certsrv

/certsrv URL은 EST 클라이언트에서 CA를 인증하고 세션을 시작하는 데 사용됩니다.

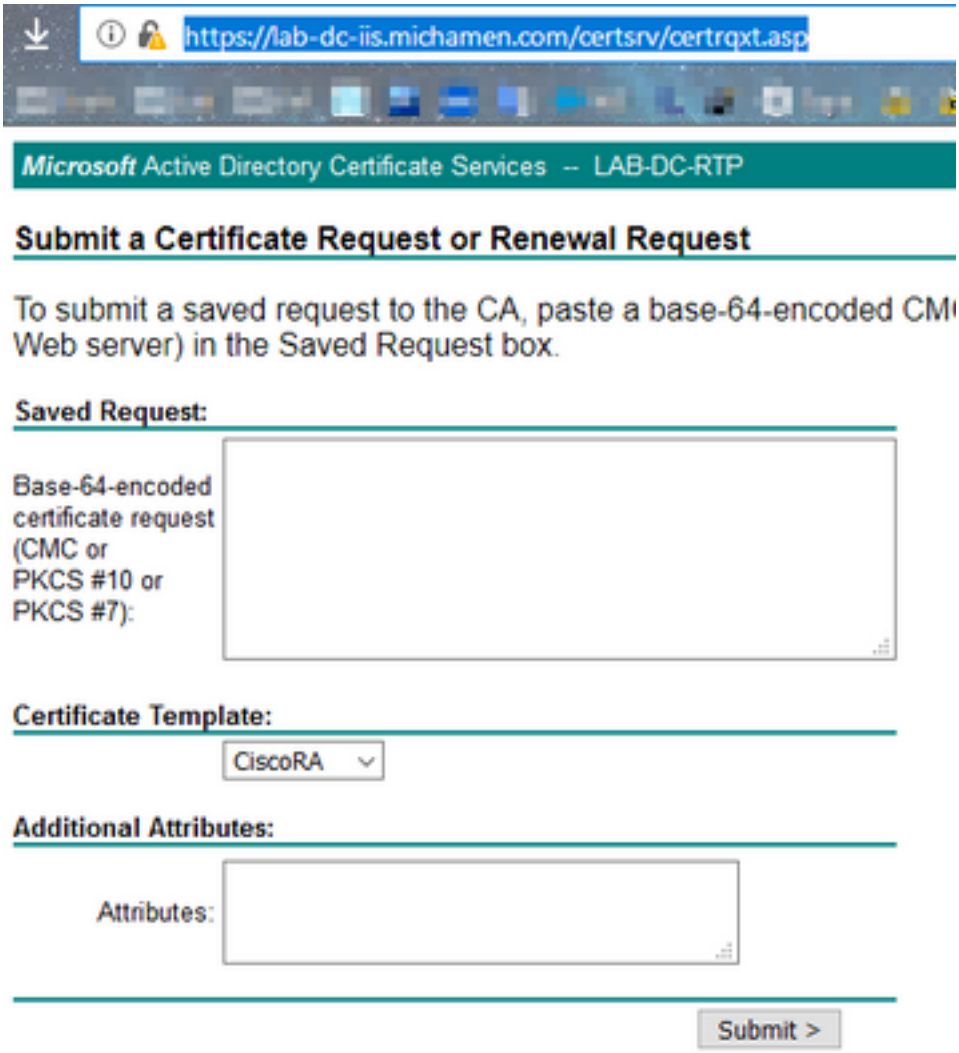
아래 이미지는 웹 브라우저의 **/certsrv** URL의 예입니다.인증서 서비스 랜딩 페이지입니다.



/certsrv/certrqxt.asp

/certsrv/certrqxt.asp URL은 새 인증서 요청을 시작하는 데 사용됩니다.EST 클라이언트는 **/certsrv/certrqxt.asp**을 사용하여 CSR, 인증서 템플릿 이름 및 원하는 특성을 제출합니다.

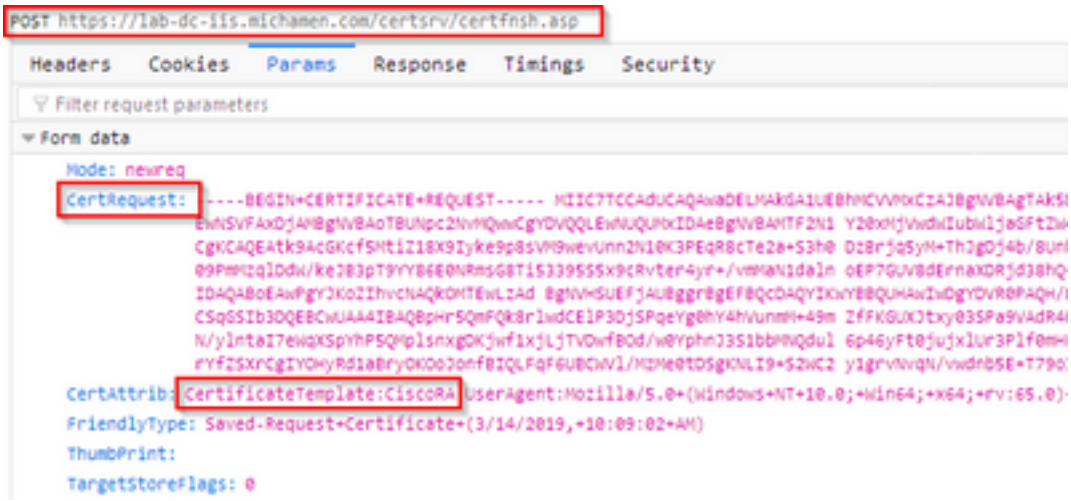
아래 이미지는 웹 브라우저의 **/certsrv/certrqxt.asp**의 예입니다.



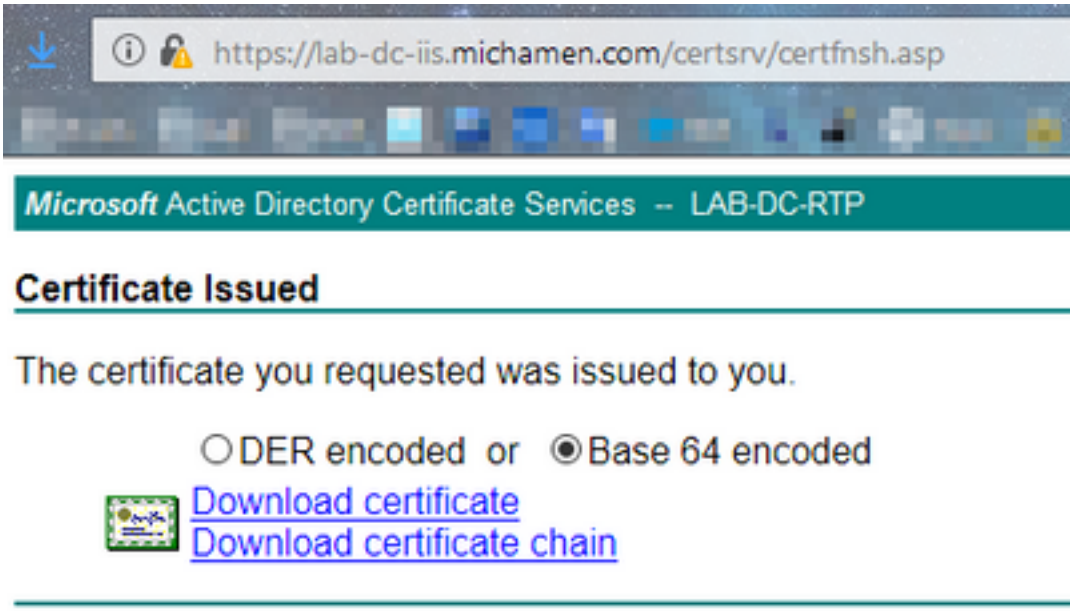
/certsrv/certfnsh.asp

/certsrv/certfnsh.asp URL은 인증서 요청에 대한 데이터를 제출하는 데 사용됩니다.CSR, 인증서 템플릿 이름 및 원하는 특성을 포함합니다.제출 서류를 보려면 브라우저의 **개발자 도구**를 사용하여 데이터가 certrqxt.*asp* 페이지를 통해 전송되기 전에 브라우저의 콘솔을 *엽니다*.

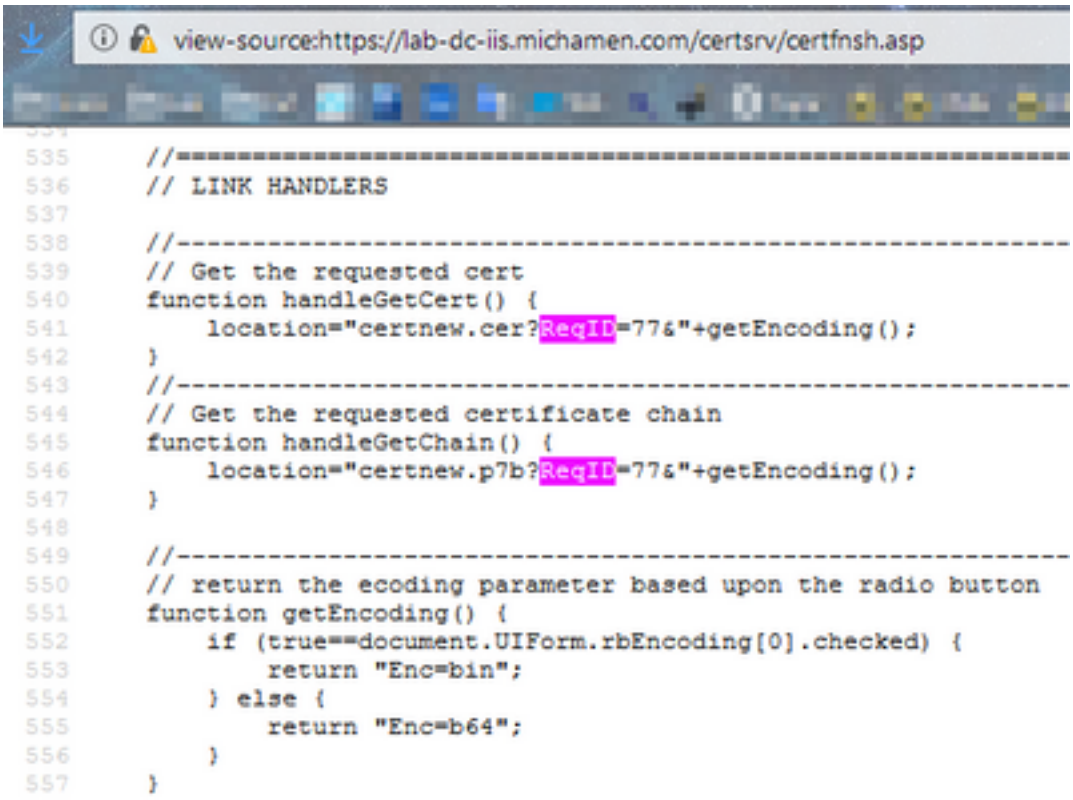
아래 이미지는 브라우저 콘솔에 표시되는 데이터의 예입니다.



/certsrv/certfnsh.asp의 제출 응답에는 CA에서 발급한 인증서의 요청 ID가 포함됩니다.페이지의 소스 코드를 검사할 때 웹 브라우저에서 요청 ID가 표시됩니다.



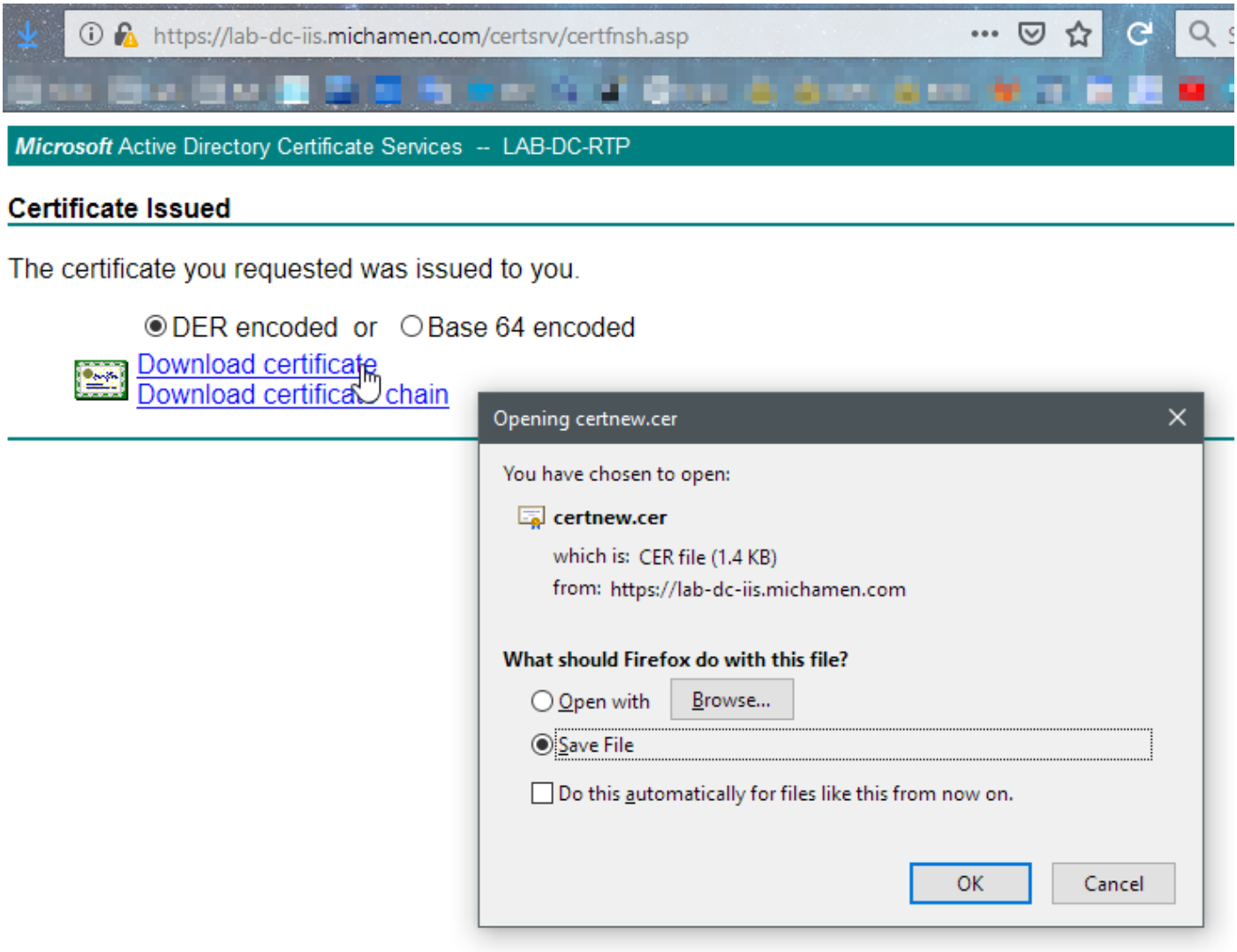
팁:페이지 원본에서 "ReqID"를 검색합니다.



/certsrv/certnew.cer

이 시점에서 EST 클라이언트는 새 인증서의 요청 ID를 인식합니다.EST 클라이언트는 /certsrv/certnew.cer을 사용하여 요청 ID 및 파일 인코딩을 매개변수로 전달하여 **.cer** 확장자로 인증서 파일을 다운로드합니다.

이는 **Download Certificate** 링크를 클릭할 때 브라우저에서 발생하는 것과 같습니다.



요청 URL 및 매개변수를 보려면 브라우저의 콘솔을 사용합니다.

> **참고:**DER 인코딩을 선택한 경우 브라우저는 인코딩 매개변수에 대한 **bin**을 지정합니다.그러나 Base64 인코딩은 b64로 표시됩니다.

문제 해결을 위한 관련 추적/로그

이러한 로그는 대부분의 문제를 격리하는 데 도움이 됩니다.

CAPF 로그

CAPF 로그에는 전화와의 상호 작용과 CiscoEST 활동의 최소 로깅이 포함됩니다.

참고:이러한 로그는 CLI(Command Line Interface) 또는 RTMT(Real Time Monitoring Tool)를 통해 수집할 수 있습니다. CSCvo28048 CAPF가 RTMT의 서비스 목록에 표시되지 않을 수 있습니다.

CiscoRA 로그

CiscoRA 로그는 종종 CES 로그라고 합니다.CiscoRA 로그에는 CES 초기 시작 활동이 포함되며 CA와의 인증이 발생하는 동안 발생할 수 있는 오류가 표시됩니다.CA와의 초기 인증이 성공하면 전화 등록에 대한 후속 활동이 여기에 로그인되지 않습니다.따라서 CiscoRA 로그는 문제 해결을 위한 좋은 초기 지점 역할을 합니다.

참고:이러한 로그는 이 문서 생성 시 CLI를 통해서만 수집할 수 있습니다.

NGINX error.log

NGINX error.log는 NGINX와 CA 측 간의 모든 HTTP 상호 작용과 시작 중 모든 활동을 로깅하므로 이 기능에 가장 유용한 로그입니다.여기에는 CA에서 반환된 오류 코드와 요청을 처리한 후 CiscoRA에서 생성된 오류 코드가 포함됩니다.

참고:이 문서를 만들 때는 CLI에서도 이러한 로그를 수집할 수 없습니다.이러한 로그는 원격 지원 계정(루트)을 통해서만 다운로드할 수 있습니다.

CA 웹 서버의 로그

CA 웹 서버의 로그는 요청 URL, 응답 코드, 응답 기간 및 응답 크기를 포함한 모든 HTTP 활동을 표시하므로 중요합니다.이러한 로그를 사용하여 CiscoRA와 CA 간의 상호 작용을 상호 연결할 수 있습니다.

참고:이 문서의 컨텍스트에 있는 CA 웹 서버 로그는 MS IIS 로그입니다.나중에 다른 웹 CA가 지원되는 경우 CA 웹 서버의 로그 역할을 하는 다른 로그 파일이 있을 수 있습니다

로그 파일 위치

CAPF 로그:

- 루트에서:/var/log/active/cm/trace/capf/sdi/capf<*number*>.txt
- CLI에서:activelog cm/trace/capf/sdi/capf* 가져오기

참고:CAPF 추적 수준을 "Detailed(세부)"로 설정하고 테스트를 수행하기 전에 CAPF 서비스를 다시 시작합니다.

Cisco RA:

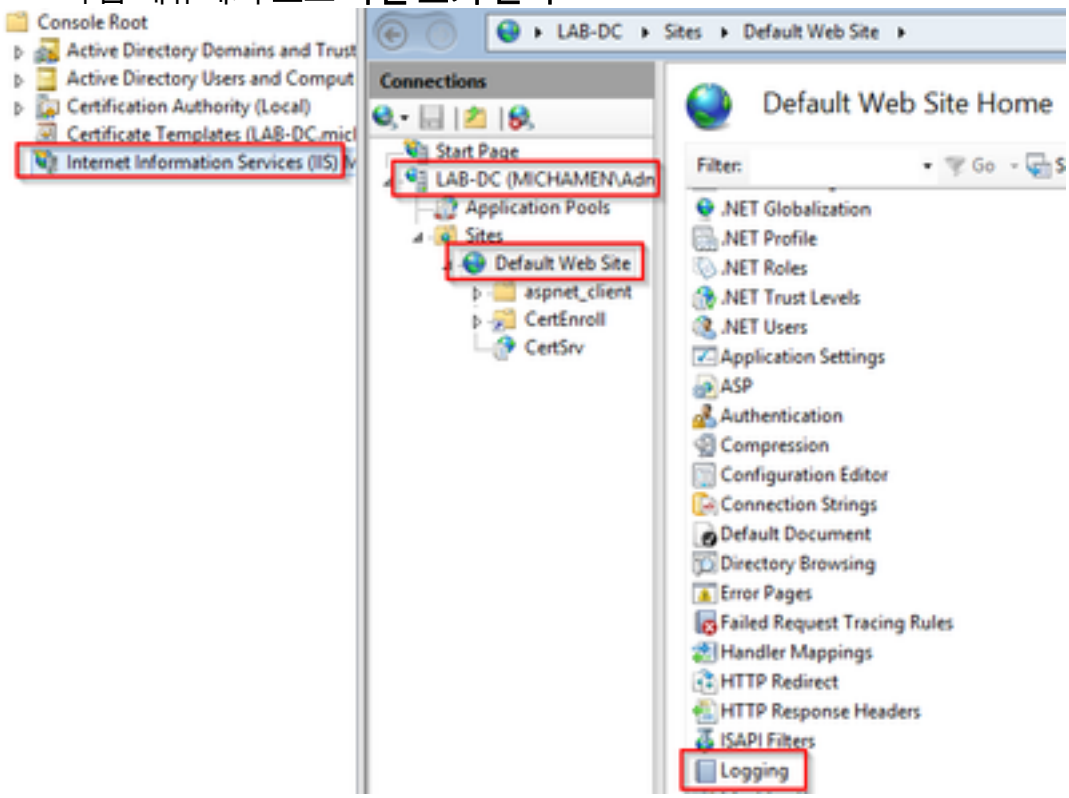
- 루트에서:/var/log/active/cm/trace/capf/sdi/nginx<*number*>.txt
- CLI에서:activelog cm/trace/capf/sdi/nginx* 가져오기

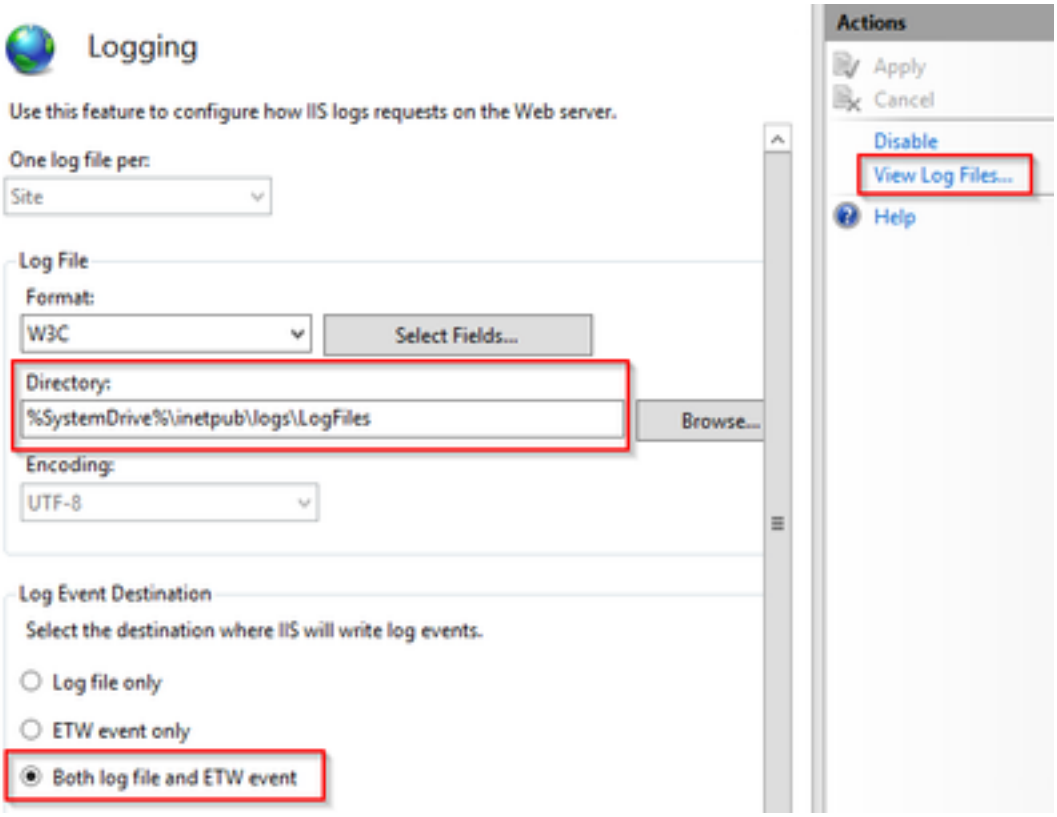
Nginx 오류 로그:

- 루트에서:/usr/local/thirdparty/nginx/install/logs/error.log
- CLI에서 사용할 수 없음

MS IIS 로그:

- MMC 열기
- **IIS(인터넷 정보 서비스)** 스냅인 선택
- 서버 이름을 클릭합니다.
- 기본 **웹 사이트 클릭**
- 로깅 옵션을 보려면 Logging(로깅)을 두 번 클릭합니다.
- 작업 메뉴에서 **로그 파일 보기 선택**





로그 분석 예

정상적으로 시작하는 서비스

NGINX 로그에 표시된 CES 시작

이 로그에서는 정보가 거의 수집되지 않습니다.신뢰 저장소에 로드된 전체 인증서 체인이 여기에 표시되고, 하나는 웹 컨테이너용이고 다른 하나는 EST용입니다.

```
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.log에 표시된 CES 시작

인증서 템플릿 컨피그레이션 및 자격 증명을 사용한 로그인은 다음 코드 조각에서 확인할 수 있습니다.

```
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 인증서 체인의 검색은 다음 코드 조각에서 확인할 수 있습니다.

```
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
```

요청이 성공하면 certnew.p7b 파일을 가져옵니다.템플릿 자격 증명이 있는 동일한 URL을 사용하여 웹 브라우저에서 certnew.p7b 파일을 가져올 수 있습니다.

CES 시작 IIS 로그에서 볼 수 있듯이

NGINX error.log에 표시된 것과 동일한 CES 시작 이벤트는 IIS 로그에서도 관찰됩니다.그러나 IIS 로그에는 웹 서버에서 401 응답을 통해 첫 번째 요청을 처리하기 때문에 2개의 HTTP GET 요청이 더 포함됩니다.그리고 인증 후 요청 수신은 301 응답을 사용하여 리디렉션됩니다.

```
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 로그에 표시된 CAPF 시작

CES 시작을 위한 CAPF 로그에서 발생하는 대부분의 내용은 다른 로그에서 발생하는 것과 같습니다.그러나 CAPF 서비스가 온라인 CA의 방법 및 컨피그레이션을 탐지하는 것을 확인할 수 있습니다.

```
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
```

로그에서 다음에 중요한 관찰은 CAPF 서비스가 EST 클라이언트를 초기화할 때입니다.

```
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!!
```

전화 LSC 설치 작업

CAPF 로그

필요한 로그를 모두 수집하고 CAPF 로그를 검토하여 분석을 시작하는 것이 좋습니다.이렇게 하면 특정 전화기의 시간 참조를 알 수 있습니다.

신호 내용의 초기 부분은 다른 CAPF 방법과 동일하게 보입니다. 단, CAPF 서비스에서 실행 중인 EST 클라이언트가 대화 상자의 끝 부분에 CES를 등록하여(전화기에서 CSR을 제공한 후) 수행합니다.

```
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
```

CES에서 전화기의 서명된 인증서를 검색하면 인증서가 전화기에 제공되기 전에 DER 형식으로 변환됩니다.

```
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 서비스는 다시 인계받아 위의 코드 조각(/tmp/capf/cert/)에 기록된 위치에서 CSR을 로드합니다. 그런 다음 CAPF 서비스는 서명된 LSC를 전화기에 제공합니다.동시에 전화기의 CSR이 삭제됩니다.

```
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 로그

아래 코드 조각은 위에서 설명한 대로 전화기의 LSC 설치 단계에 대한 IIS 로그의 이벤트를 표시합니다.

```
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
```

일반적인 문제

CES 측에 오류가 발생할 때마다 CAPF 로그에 아래의 코드 조각과 같은 출력이 표시됩니다.다른 로그를 확인하여 계속해서 문제를 해결하십시오.

```
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 인증서의 발급자 체인에 CA 인증서가 없습니다.

인증서 체인에 있는 루트 인증서 또는 중간 인증서가 CES에서 신뢰하지 않는 경우 "Unable to retrieve CA Cert chain from CA Ca Cert chain" 오류가 nginx 로그에 출력됩니다.

```
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
```

자체 서명 인증서를 제공하는 웹 서버

IIS에서 자체 서명 인증서의 사용은 지원되지 않으며 CUCM에서 CAPF-trust로 업로드된 경우에도 작동합니다.아래 코드 조각은 nginx 로그에서 가져온 것이며 IIS에서 자체 서명 인증서를 사용할 때 관찰된 내용을 표시합니다.

```
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 호스트 이름 및 일반 이름과 일치하지 않습니다.

IIS 인증서의 공용 이름(lab-dc)이 CA 웹 등록 서비스의 URL 내의 FQDN과 일치하지 않습니다.인증서 검증을 성공하려면 URL 내의 FQDN이 CA에서 사용하는 인증서의 일반 이름과 일치해야 합니다 .

```
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 확인 문제

CiscoRA가 서비스 매개변수에 구성된 온라인 CA의 호스트 이름을 확인할 수 없습니다.

```
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
```

인증서 유효 일자 발행

NTP(Network Time Protocol)가 인증서 유효 날짜에 대해 제대로 작동하지 않는 경우이 검사는 시작 시 CES에서 수행되며 NGINX 로그에서 관찰됩니다.

```
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
```

인증서 템플릿 구성 오류

서비스 매개 변수 내의 이름에 오류가 발생할 수 있습니다.CAPF 또는 NGINX 로그에 오류가 기록되지 않으므로 NGINX error.log를 확인해야 합니다.

```
***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 인증 시간 초과

아래에는 초기 certsrv 인증 프로세스 중에 기본 타이머인 10초 이후의 CES EST 클라이언트 시간 초과가 나와 있습니다.

```
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
```

참고:CSCvo58656 및 CSCvf83629 모두 CES 인증 시간 초과와 관련이 있습니다.

CES 등록 시간 초과

CES EST 클라이언트는 인증에 성공한 후 시간이 초과되지만 등록 요청에 대한 응답을 기다리는 동안 시간 초과됩니다.

```
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
```

알려진 주의 사항

CSCvo28048 CAPF 서비스가 RTMT Collect Files 메뉴에 더 이상 표시되지 않음

CSCvo58656 CAPF Online CA에는 RA와 CA 간의 최대 연결 시간 제한을 구성하는 옵션이 필요합니다.

등록 중 EST_ERR_HTTP_WRITE를 가져오는 CSCvf83629 EST 서버

관련 정보

- **기술 지원 및 문서 – Cisco Systems**