Probleemoplossing voor CAPF online CA

Inhoud

Inleiding

In dit document wordt de probleemoplossing beschreven voor de automatische inschrijving en hernieuwing van de functie certificaatproxy (CAPF). Deze optie wordt ook CAPF Online CA genoemd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Certificaten
- Cisco Unified Communications Manager (CUCM)-beveiliging

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM versie 12.5 aangezien de CAPF Online CA-functie is geïntroduceerd in CUCM 12.5.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Overzicht van functieonderdelen

Registratieautoriteit (RA)

RA is een instantie in een netwerk die gebruikersverzoeken om een digitaal certificaat verifieert en de certificeringsinstantie (CA) opgedragen het certificaat af te geven. RA's maken deel uit van een openbare sleutelinfrastructuur (PKI).

Inschrijven via Secure Transport (EST)

EST is een protocol dat in een verzoek om commentaar (RFC) 7030 is gedefinieerd voor certificaatinschrijving voor klanten die certificaatbeheer over CMS (CMC)-berichten via Transport Layer Security (TLS) en HyperText Transfer Protocol (HTTP) gebruiken. EST gebruikt een

client/server-model waarbij de EST-client inschrijvingsverzoeken verstuurt en de EST-server antwoorden met de resultaten verstuurt.

libEST

libEST is de bibliotheek voor Cisco's implementatie van EST. libEST maakt het mogelijk X509-certificaten aan te bieden op apparaten van eindgebruikers en netwerkinfrastructuren. Deze bibliotheek wordt geïmplementeerd door Cisco EST en CiscoRA.

Engine-X (NGINX)

NGINX is een webserver en omgekeerde proxy die vergelijkbaar is met Apache. NGINX wordt gebruikt voor HTTP-communicatie tussen CAPF en CES en voor communicatie tussen CES en de CA Web Enrollment Service. Wanneer libEST in servermodus werkt, moet een webserver TCP-verzoeken namens libEST's behandelen.

Certificaatinschrijving (CES)

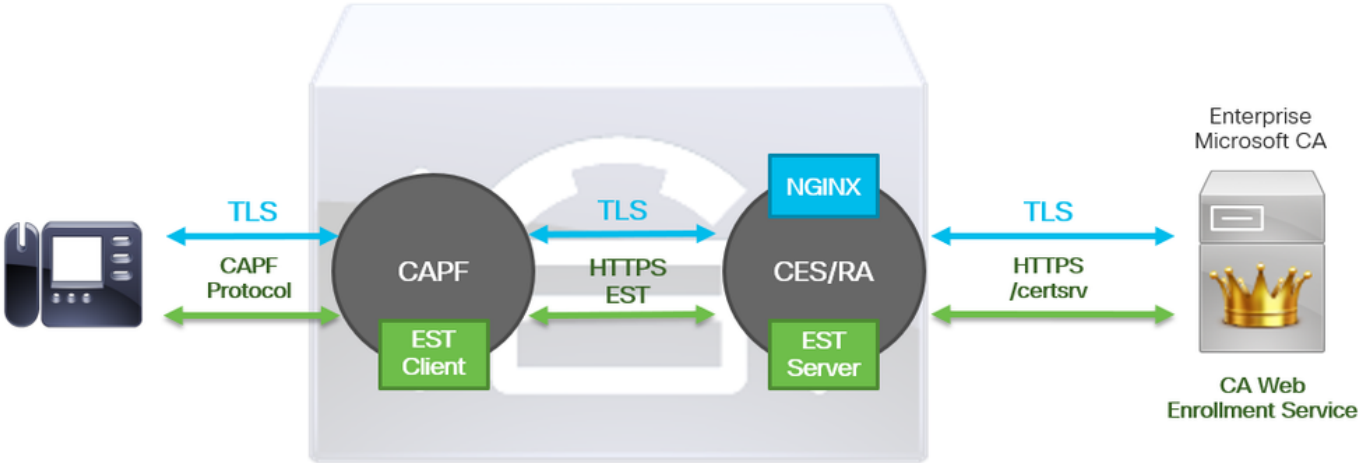
CES is de dienst op CUCM die als RA tussen de CAPF-dienst en de CA fungeert. CES wordt ook aangeduid als CiscoRA of gewoon RA. CES gebruikt NGINX als webserver omdat CES de libEST in servermodus implementeert om op te treden als RA.

Proxy-functie (CAPF) van certificeringsinstanties

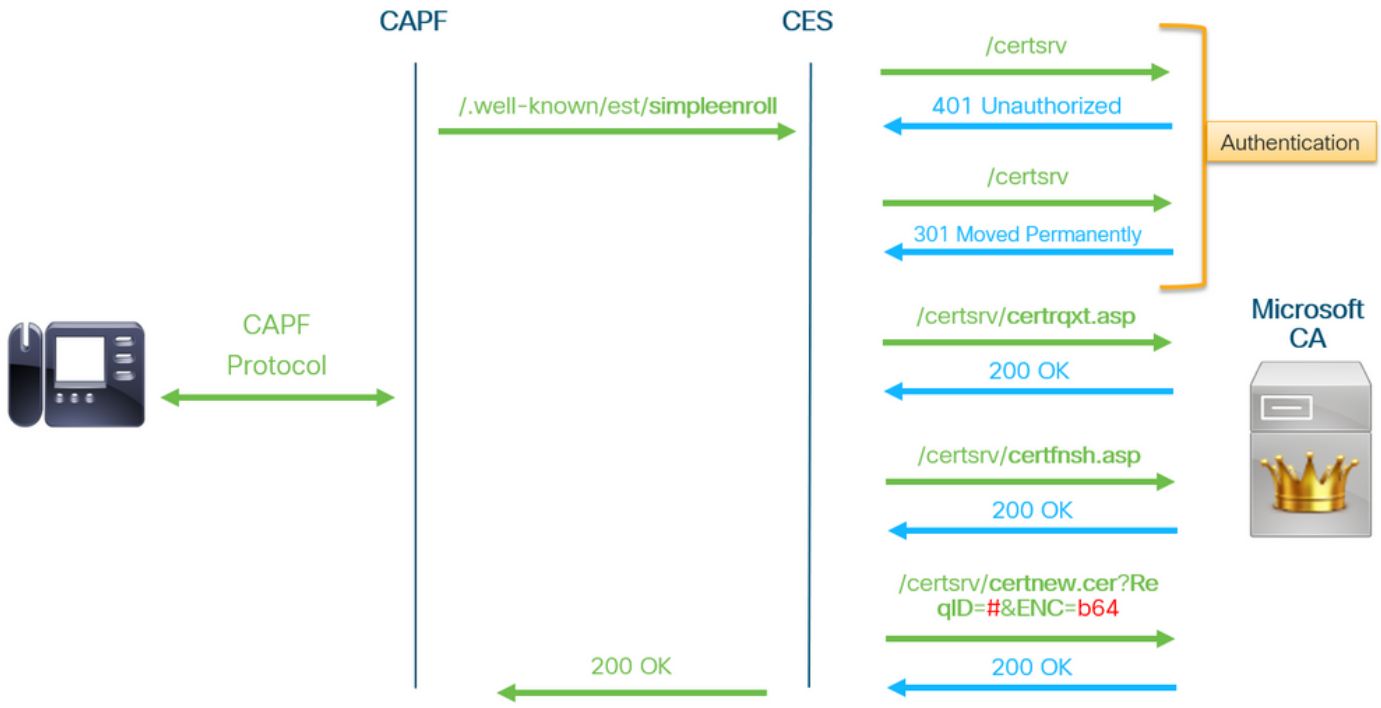
CAPF is een dienst van CUCM die de telefoons met elkaar in interactie treden wanneer het uitvoeren van de verzoeken van de inschrijving van certificaten. CAPF interageert met CES namens de telefoons. In deze optie implementeert model CAPF libEST in clientmodus om de certificaten van de telefoons in te schrijven via CES.

Samengevat, hier is hoe elk component wordt geïmplementeerd:

1. De telefoon stuurt een certificaataanvraag naar CAPF
2. CAPF implementeert Cisco EST (clientmodus) om met CES te communiceren
3. CES implementeert Cisco RA (servermodus) om de verzoeken van de EST-client te verwerken en te beantwoorden
4. CES/CiscoRA communiceren met HTTPS-service van de CA



Berichtstroomdiagram



BerichtFlow-verklaring

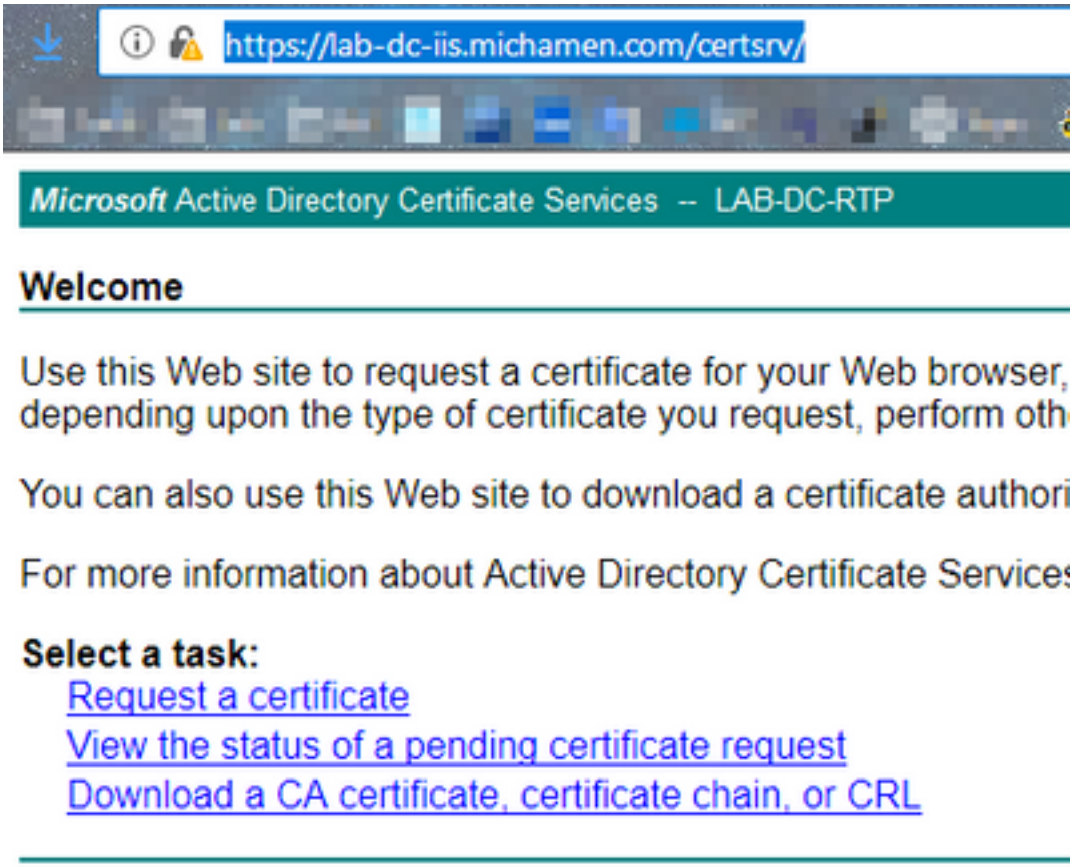
/.well-known/est/simpleenroll

De EST-client gebruikt deze URL om een API-oproep te verzenden met de certificaatinschrijving op de EST-server. Zodra de EST-server de API-oproep ontvangt, start hij het proces voor het inschrijven van certificaten, dat HTTPS-communicatie met de CA-webinschrijvingsservice omvat. Als het inlogproces succesvol is en de EST-server het nieuwe certificaat ontvangt, zal CAPF het certificaat laden en het terugsturen naar de IP-telefoon.

/certsrv

De URL **/certsrv** wordt gebruikt door de EST-client om een sessie met de CA te authentiseren en te starten.

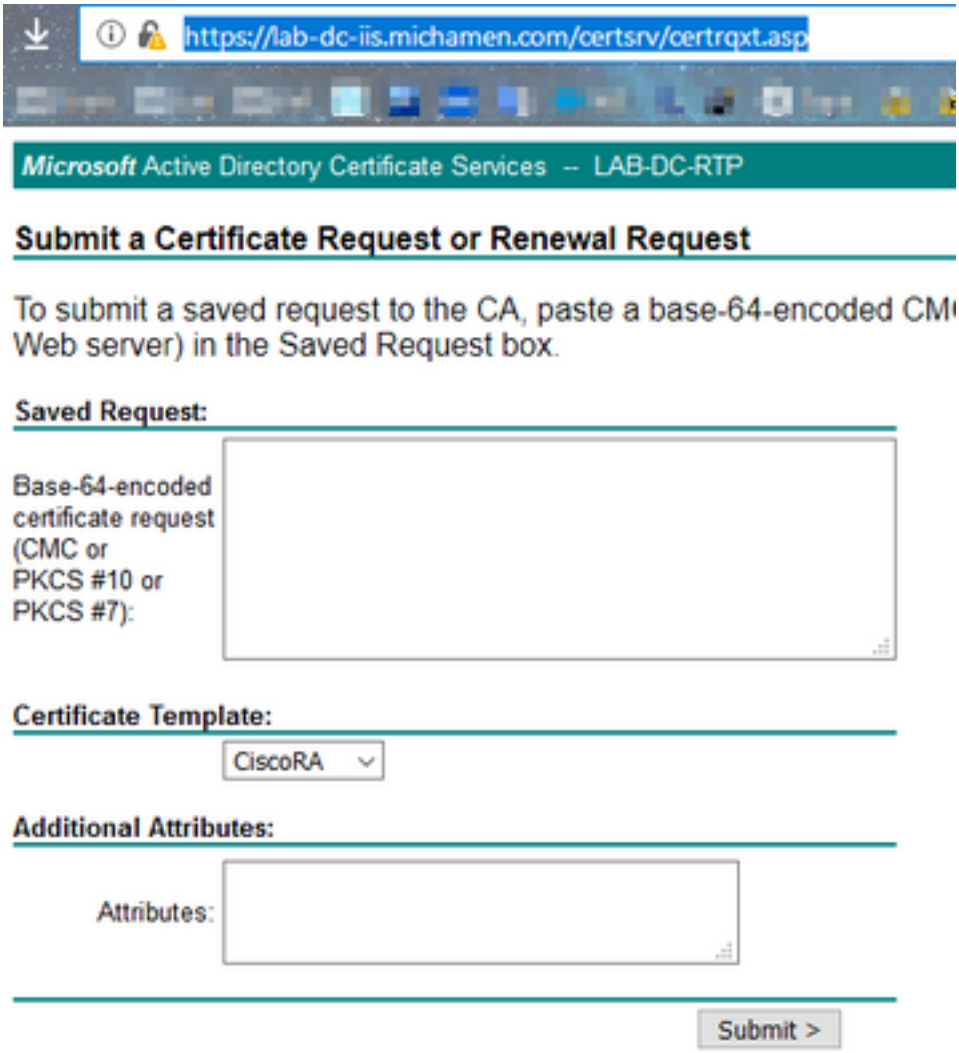
De afbeelding hieronder is een voorbeeld van **/certsrv** URL van een webbrowser. Dit is de startpagina van de certificaatservices.



/certsrv/certrqxt.asp

De **/certsrv/certrqxt.asp** URL wordt gebruikt om het verzoek om een nieuw certificaat te openen. De EST-client gebruikt **/certsrv/certrqxt.asp** om de CSR, de naam van de certificaatsjabloon en alle gewenste eigenschappen in te dienen.

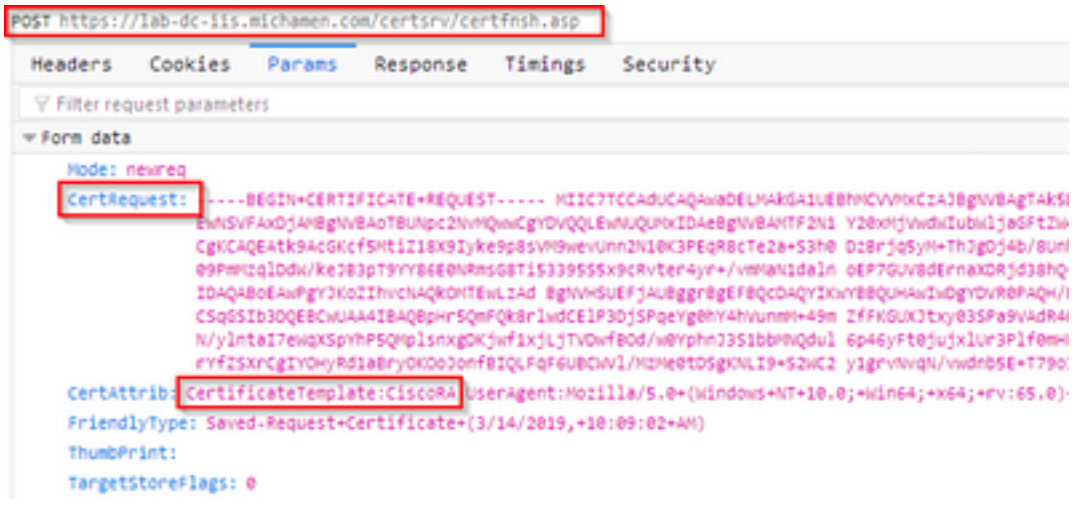
De afbeelding hieronder is een voorbeeld van **/certsrv/certrqxt.asp** van een webbrowser.



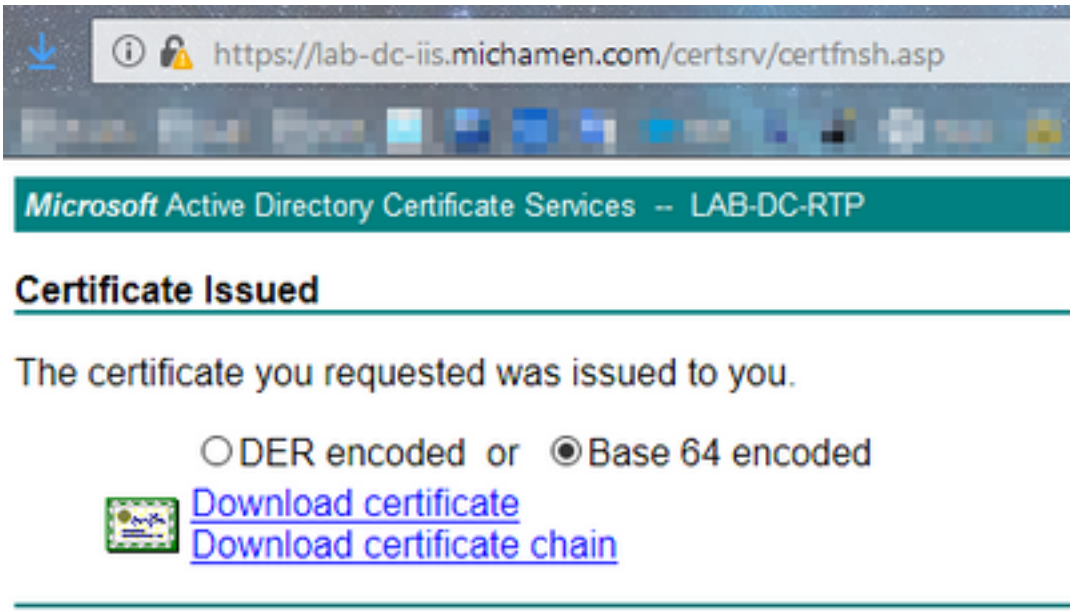
/certsrv/certfnsh.asp

De **/certsrv/certfnsh.asp** URL wordt gebruikt om gegevens voor de certificaataanvraag in te dienen; die de CSR, de naam van de certificaatsjabloon en alle gewenste eigenschappen omvat. Om de inzending te bekijken gebruikt de browser de **ontwikkelaar tools** van de browser om de console van de browser te openen voordat de gegevens via de *certrqxt.asp* pagina worden ingediend.

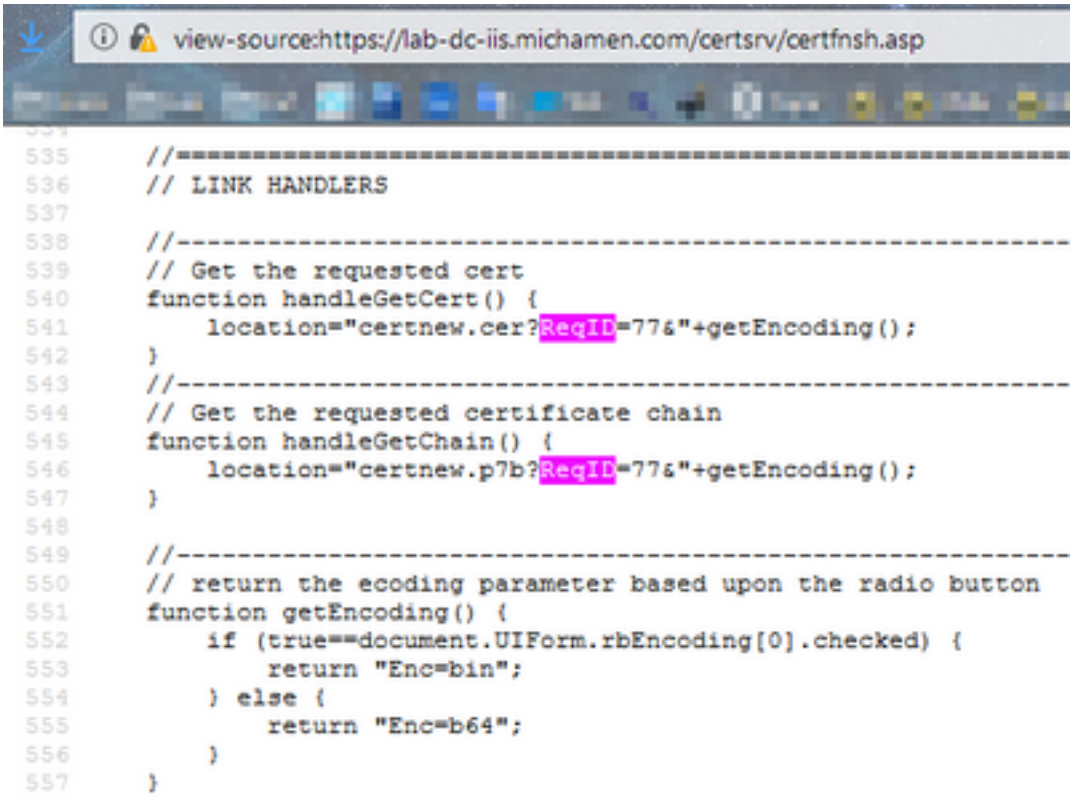
De afbeelding hieronder is een voorbeeld van de gegevens die in de console van de browser worden weergegeven.



De indieningsreactie van **/certsrv/certfnsh.asp** bevat de aanvraag-ID van het door de CA afgegeven certificaat. Het verzoek-ID wordt in een webbrowser gezien wanneer de broncode van de pagina wordt geïnspecteerd.



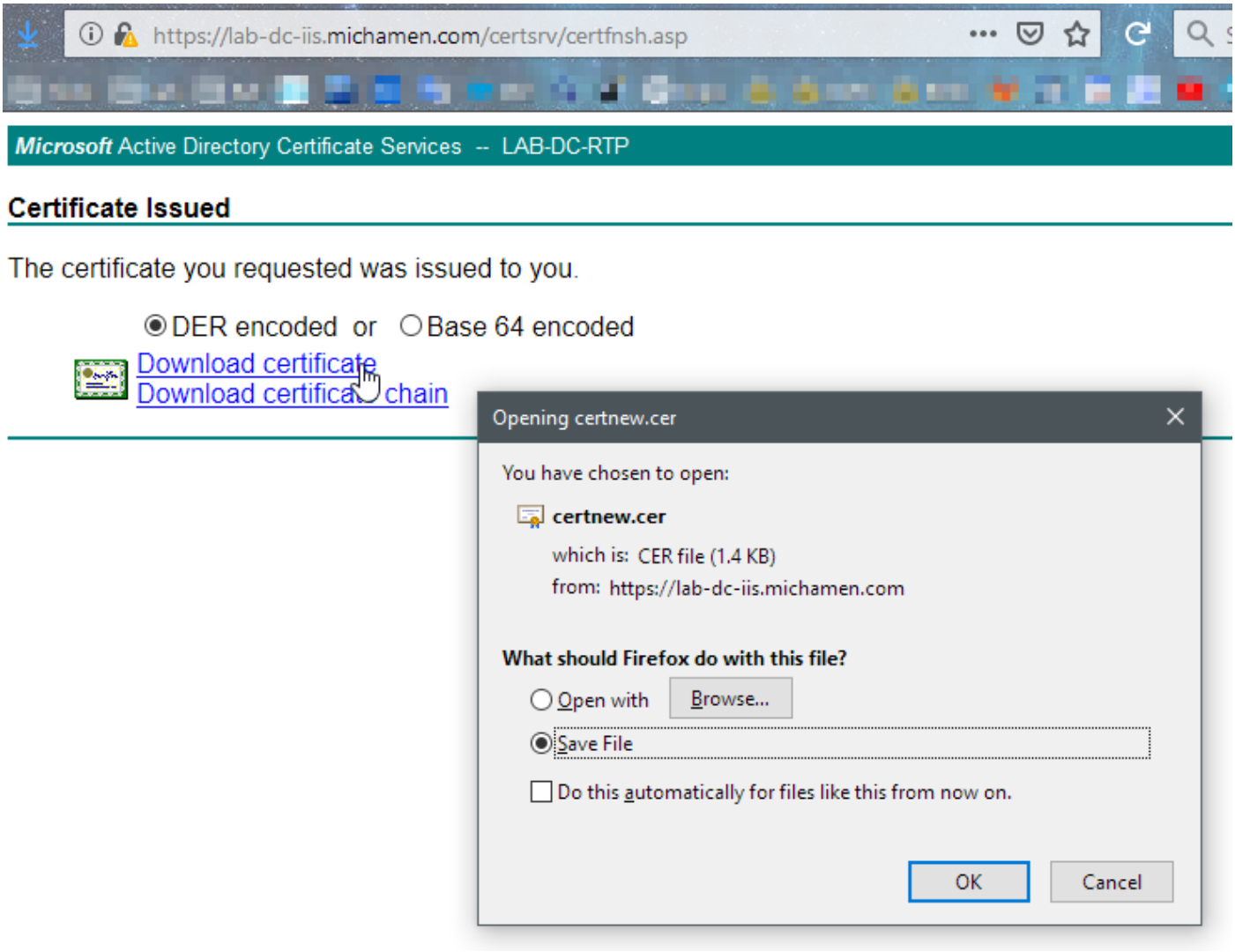
Tip: Zoek de pagina-bron voor "ReqID"



/certsrv/certnew.cer

Op dit moment is de EST-cliënt op de hoogte van de aanvraag-ID voor het nieuwe certificaat. De EST-client gebruikt **/certsrv/certnew.cer** om de aanvraag-ID en bestandscodering als parameters door te geven om het certificaatbestand met de **.cer-**extensie te downloaden.

Dit staat gelijk aan wat er in uw browser gebeurt wanneer u op de link **Downloadcertificaat** klikt.



Om het verzoek URL en de parameters te bekijken, gebruik de console van de browser.

> **Opmerking:** De browser specificeert **bin** voor de coderende parameter als DER-codering is geselecteerd; Base64-codering zal echter worden weergegeven als b64.

Relevante Traces/Logs voor probleemoplossing

Deze weblogs helpen bij het isoleren van de meeste problemen.

CAPF-bestanden

CAPF Logs bevatten interacties met telefoons en minimale houtkap van de activiteit van Cisco EST.

Opmerking: Deze logbestanden zijn beschikbaar voor verzameling via de Opdracht Line Interface (CLI) of het Real Time Monitoring Tool (RTMT). Ten gevolge van CSCvo28048 mag CAPF niet in de lijst van diensten in RTMT worden opgenomen.

CiscoRA-kaarten

CiscoRA-kaarten worden vaak aangeduid als CES-bestanden. CiscoRA-logbestanden bevatten de CES initiële opstartactiviteit en vertonen fouten die kunnen optreden bij verificatie met de CA. Als de eerste verificatie met de CA succesvol is, wordt de volgende activiteit voor telefooninschrijving hier niet ingelogd. Daarom dienen CiscoRA-logbestanden als een goed beginpunt voor problemen met probleemoplossing.

Opmerking: Deze logbestanden kunnen alleen via de CLI worden verzameld vanaf het moment dat deze documenten worden gemaakt.

NGINX fout.log

NGINX error.log is het meest handige logbestand voor deze functie omdat het alle activiteit tijdens het opstarten en elke HTTP-interactie tussen NGINX en de CA-zijde registreert; die foutcodes bevat die van de CA zijn teruggegeven, evenals die welke door Cisco RA zijn gegenereerd na verwerking van het verzoek.

Opmerking: Op het moment dat u dit document maakt, kun je deze logs niet bij CLI verzamelen. Deze logbestanden kunnen alleen worden gedownload via een externe ondersteuningsaccount (wortel).

VoS van CA Web Server

De logbestanden van CA Web Server zijn belangrijk aangezien ze elke HTTP-activiteit weergeven, inclusief aanvraag-URL's, responscodes, responsduur en responsgrootte. U kunt deze logs gebruiken om interacties tussen CiscoRA en de CA te correleren.

Opmerking: CA Web Server-logbestanden in de context van dit document zijn de MS IS-logbestanden. Als andere web CA's in de toekomst worden ondersteund, kunnen zij verschillende logbestanden hebben die dienen als de logbestanden van de CA Web Server

Logbestand-locaties

CAPF-logbestanden:

- Uit wortel: /var/log/active/cm/spoor/capf/sdi/capf<*number*>.txt
- Van CLI: activelog cm/spoor/capf/sdi/capf*

Opmerking: Stel het CAPF-spoorniveau in op "Gedetailleerd" en start de CAPF-service opnieuw voordat het testen wordt uitgevoerd.

Cisco RA:

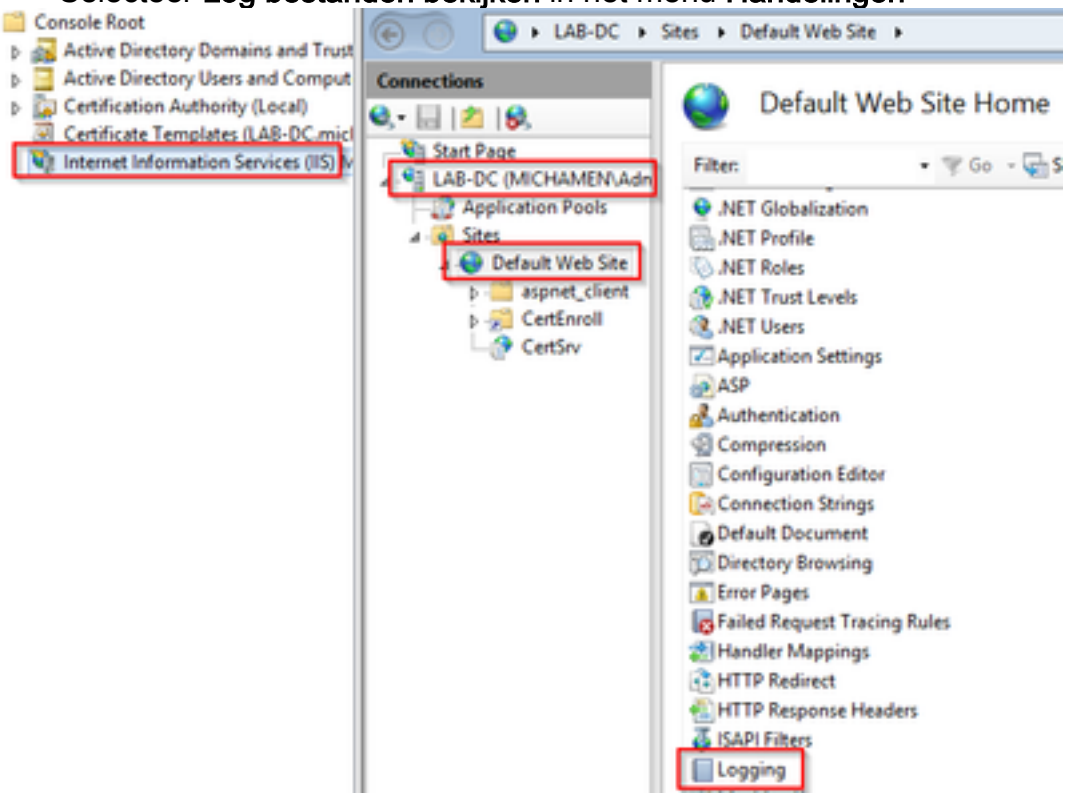
- Uit wortel: /var/log/active/cm/sporen/capf/sdi/nginx<*number*>.txt
- Van CLI: activelog cm/spoor/capf/sdi/nginx*

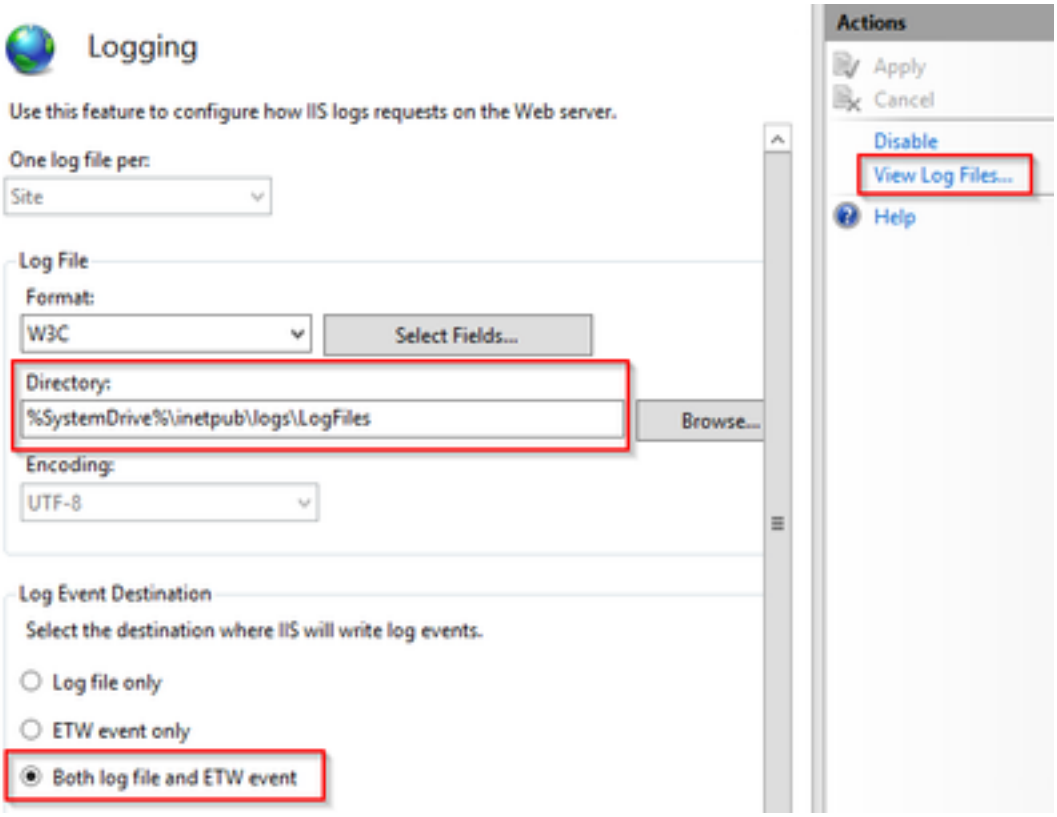
NGINX foutenlogboek:

- Uit wortel: /usr/local/thirdparty/nginx/install/logs/error.log
- Niet beschikbaar bij CLI

MS IS-logbestand:

- Open MMC
- Selecteer de optie **Internet Information Services (IS)**.
- Klik op de servernaam
- Klik op **Standaardwebsite**
- Dubbelklik op **vastlegging** om de logopties te zien
- Selecteer **Log bestanden bekijken** in het menu **Handelingen**





Voorbeeld

Normaal gesproken starten services

CES Opstarten zoals aangegeven in NGINX-log

Er is maar weinig informatie verzameld vanaf dit logbestand. De volledige certificatenketen die in zijn vertrouwenswinkel wordt geladen wordt hier bekeken en de ene is voor de webcontainer, de andere voor EST:

```
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
```

CES Start Up zoals gezien in NGINX error.log

De inlognaam met behulp van de configuratie van de certificaatsjabloon en de aanmeldingsgegevens worden in dit hoofdstuk waargenomen:

```
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
```

In het fragment hier wordt het ophalen van de CA-certificeringsketen waargenomen:

```
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
```

Wanneer het verzoek succesvol is, wordt het certnew.p7b bestand bereikt. Dezelfde URL met de sjabloon aanmeldingsgegevens kunnen worden gebruikt om het certnew.p7b-bestand van een webbrowser te krijgen.

CES starten zoals in de ISS-documenten wordt weergegeven

Dezelfde CES die in de NGINX error.log worden gezien, wordt ook in de IS-logboeken aangetroffen; de IS-bestanden bevatten echter nog 2 HTTP-verzoeken omdat het eerste verzoek door de webserver zal worden aangevochten door middel van een 401-respons; en zodra een geauthentiseerd verzoek is gewaarmerkt , zal het met een antwoord van 301 opnieuw worden gericht :

```
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 Opstarten zoals gezien in de CAPF-logboeken

Het grootste deel daarvan wat voorkomt in de CAPF-stammen voor CES-start ziet er hetzelfde uit als wat in de andere stammen voorkomt; maar u merkt dat de CAPF-service de methode en de configuratie van de online CA detecteert:

```
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
```

De volgende belangrijke observatie van de logbestanden is wanneer de CAPF-dienst zijn EST-client initialiseert.

```
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!!
```

Installatie van telefoon LSC

CAPF-bestanden

Aanbevolen wordt om alle benodigde stammen te verzamelen en de analyse te starten met een review van de CAPF-logbestanden. Dit stelt ons in staat de tijdreferentie voor een specifieke telefoon te kennen.

Het eerste gedeelte van de signalering ziet er hetzelfde uit als bij andere CAPF-methoden, behalve dat de EST-client die in de CAPF-dienst actief is, de inschrijving met CES zal uitvoeren

aan het eind van het dialoogvenster (nadat het CSR door de telefoon is verstrekt).

```
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
```

Zodra CES het ondertekende certificaat van de telefoon heeft opgehaald, wordt het certificaat in formaat DER geconverteerd voordat het aan de telefoon wordt verstrekt.

```
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
```

De CAPF-service neemt het opnieuw over en ladt de CSR op de locatie waar het in het fragment hierboven is geschreven (/tmp/capf/cert/). De dienst CAPF voorziet dan de ondertekende LSC aan de telefoon. Tegelijkertijd wordt de CSR van de telefoon verwijderd.

```
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
```

IOS-kaarten

Het fragment hieronder toont de gebeurtenissen in de IS-logboeken voor de installatiestappen van een telefoon van LSC zoals hierboven wordt uitgelegd.

```
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
```

Veelvoorkomende problemen

Als er een fout is in de CES-kant, wordt verwacht dat deze uitvoer zal zien zoals het fragment hieronder in de CAPF-bestanden. Controleer andere logs om het probleem verder af te zwakken.

```
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
```

Ontbrekend CA-certificaat in uitgevende keten van IIS-identiteitsbewijs

Wanneer een wortelcertificaat of een tussencertificaat, dat in de certificeringsketen is, niet door CES wordt vertrouwd, wordt de fout "Kan CA Cert chain from CA niet herstellen" in de nginx logbestanden afgedrukt.

```
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
```

Web server die een zelfondertekend certificaat presenteert

Het gebruik van een zichzelf ondertekend certificaat op het IS wordt niet ondersteund en zal nota nemen van werk zelfs wanneer het als CAPF-trust op het CUCM wordt geüpload. Het fragment hieronder is van de nginx-logboeken en het geeft weer wat er wordt waargenomen wanneer de IS een zelfondertekend certificaat gebruikt.

```
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
```

Onjuist maken met URL hostname en Common Name

De Gemeenschappelijke Naam van het certificaat van het IS (lab-dc) komt niet overeen met FQDN binnen de URL van de de dienst van het Web Enrollment van CA. Voor certificatie als opvolger moet de FQDN binnen de URL overeenkomen met de Gemeenschappelijke Naam op het certificaat dat door CA wordt gebruikt.

```
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-oplossing

Cisco RA is niet in staat om de hostname van de Online CA in serviceparameters op te lossen.

```
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
```

Afgifte met geldigheiddata van het certificaat

Wanneer Network Time Protocol (NTP) niet correct werkt, worden er kwesties met datums voor de geldigheid van certificaten opgeslagen. Deze controle wordt bij het opstarten uitgevoerd door CES en wordt in de NGINX-loggen waargenomen.

```
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
```

Misconfiguratie van certificaten

Een typografie in de naam binnen de serviceparameters veroorzaakt storingen. Er worden geen fouten geregistreerd in de logbestanden van CAPF of NGINX, zodat deze nodig zijn om de NGINX error.log te controleren.

```
***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
```

Time-out voor CES-verificatie

Hieronder staat de CES EST client-tijd na de standaardinstelling van 10 seconden tijdens het eerste certsrv-verificatieproces.

```
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
```

> **Opmerking:** CSCvo58656 en CSCvf83629 hebben beide betrekking op de CES authenticatie time-out.

Time-out voor CES-inschrijving

CES EST client time out na een succesvolle verificatie maar wacht op een antwoord op een inschrijvingsverzoek.

```
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
```

gekende Caveats

CSCvo28048 CAPF-services die niet in het menu RTMT Collect Files meer voorkomen

CSCvo58656 CAPF Online CA moet optie zijn om de max. verbindingstijd tussen RA en CA te configureren

CSCvf83629 EST-server krijgt EST_ERR_HTTP_SCHRIFT tijdens inschrijving

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems