CAPF線上CA故障排除

目錄

簡介

本檔案介紹憑證授權單位代理功能(CAPF)自動註冊和續訂功能的疑難排解。此功能也稱為CAPF Online CA。

必要條件

需求

思科建議您瞭解以下主題：

- 憑證
- 思科整合通訊管理員(CUCM)安全性

採用元件

本文檔中的資訊基於CUCM 12.5版，因為CUCM 12.5中引入了CAPF線上CA功能。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

功能元件概述

註冊機構(RA)

RA是網路中的一種頒發機構，它驗證使用者對數位證書的請求並通知證書頒發機構(CA)頒發證書。RA是公開金鑰基礎架構(PKI)的一部分。

通過安全傳輸註冊(EST)

EST是在客戶端的證書註冊請求註釋(RFC)7030中定義的協定，這些客戶端使用基於傳輸層安全(TLS)和超文本傳輸協定(HTTP)的證書管理(CMC)消息。EST使用客戶端/伺服器模型，其中EST客戶端傳送註冊請求，EST伺服器傳送包含結果的響應。

libEST

libEST是思科實施EST的庫。libEST允許在終端使用者裝置和網路基礎設施裝置上調配X509證書。

此庫由CiscoEST和CiscoRA實施。

引擎X(NGINX)

NGINX是類似於Apache的Web伺服器和反向代理。NGINX用於CAPF和CES之間的HTTP通訊以及CES和CA Web註冊服務之間的通訊。當libEST在伺服器模式下運行時，需要Web伺服器代表libEST處理TCP請求。

憑證註冊服務(CES)

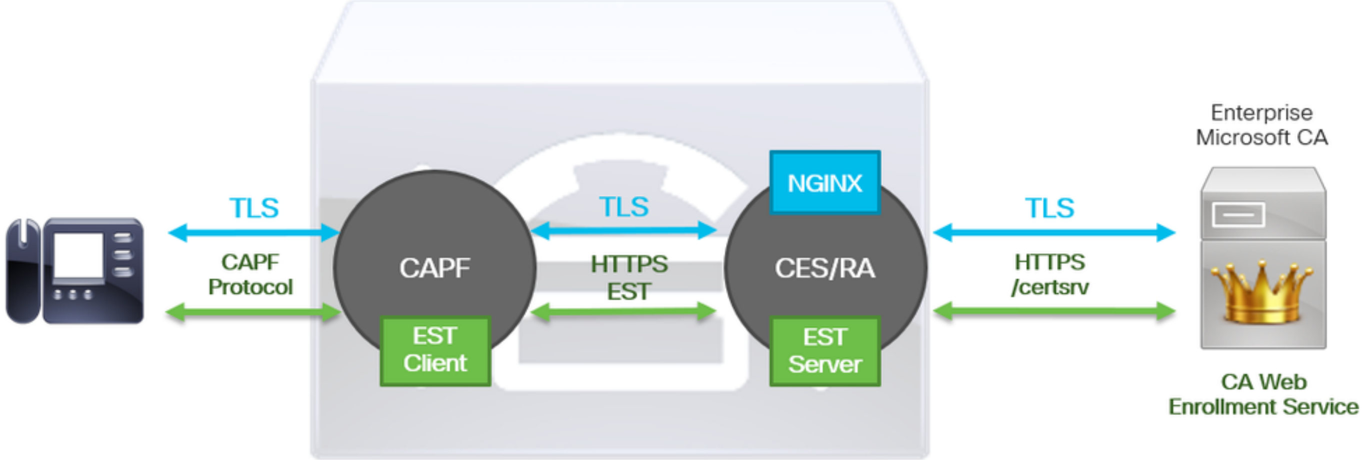
CES是CUCM上的服務，充當CAPF服務和CA之間的RA。CES也稱為CiscoRA，或簡稱為RA。CES使用NGINX作為Web伺服器，因為CES在伺服器模式下實現libEST以充當RA。

憑證授權單位代理功能(CAPF)

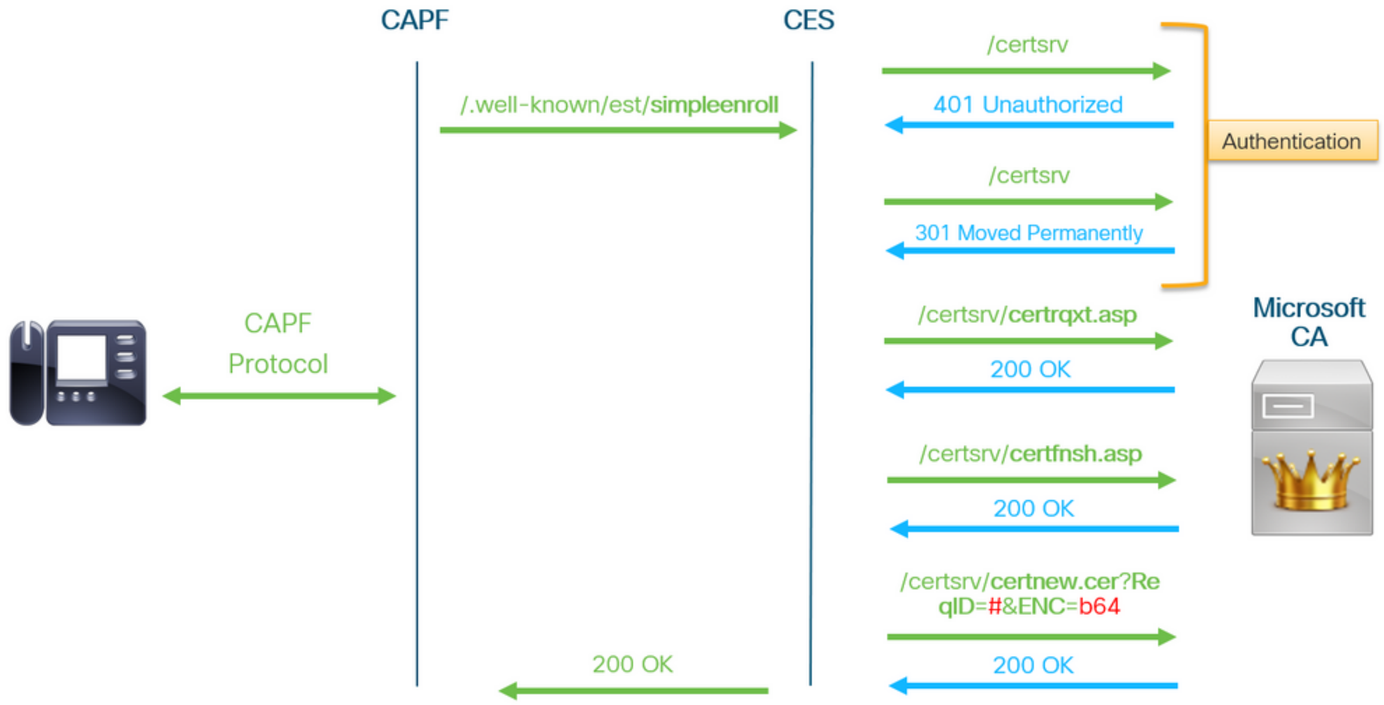
CAPF是電話在執行證書註冊請求時與之互動的CUCM服務。CAPF代表電話與CES互動。在此功能模型中，CAPF在客戶端模式下實現libEST，通過CES註冊電話證書。

總之，以下是每個元件的實施方式：

1. 電話向CAPF傳送證書請求
2. CAPF實施CiscoEST（客戶端模式）與CES通訊
3. CES實施CiscoRA（伺服器模式）以處理並響應EST客戶端的請求
4. CES/CiscoRA通過HTTPS與CA的Web註冊服務通訊



報文流圖



報文流說明

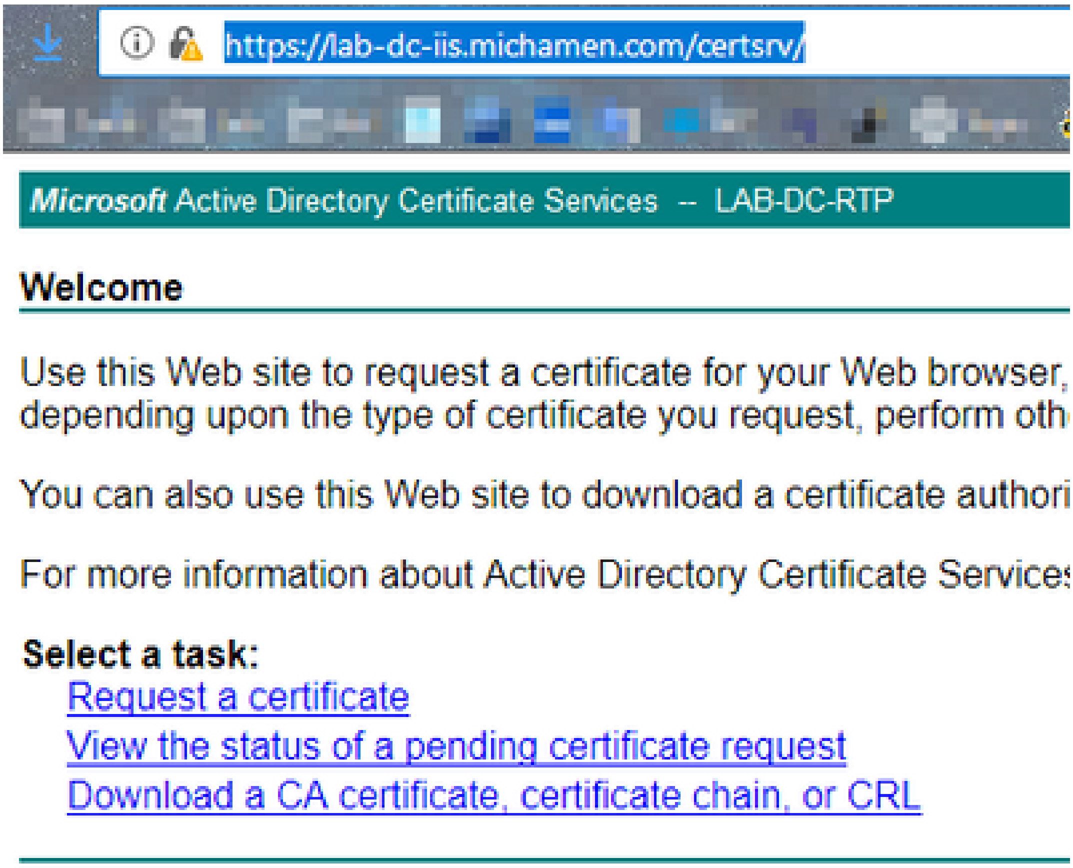
/.well-known/est/simpleenroll

EST客戶端使用此URL傳送請求從EST伺服器註冊證書的API呼叫。一旦EST伺服器收到API呼叫，它將啟動證書註冊過程，其中包括與CA的Web註冊服務進行HTTPS通訊。如果註冊過程成功，並且EST伺服器收到新證書，則CAPF將繼續載入該證書並將其發回IP電話。

/certsrv

EST客戶端使用**/certsrv** URL進行身份驗證，並啟動與CA的會話。

以下圖為來自Web瀏覽器**/certsrv** URL的範例。這是證書服務登入頁。



https://lab-dc-iis.michamen.com/certsrv/

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

Welcome

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

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

For more information about Active Directory Certificate Service

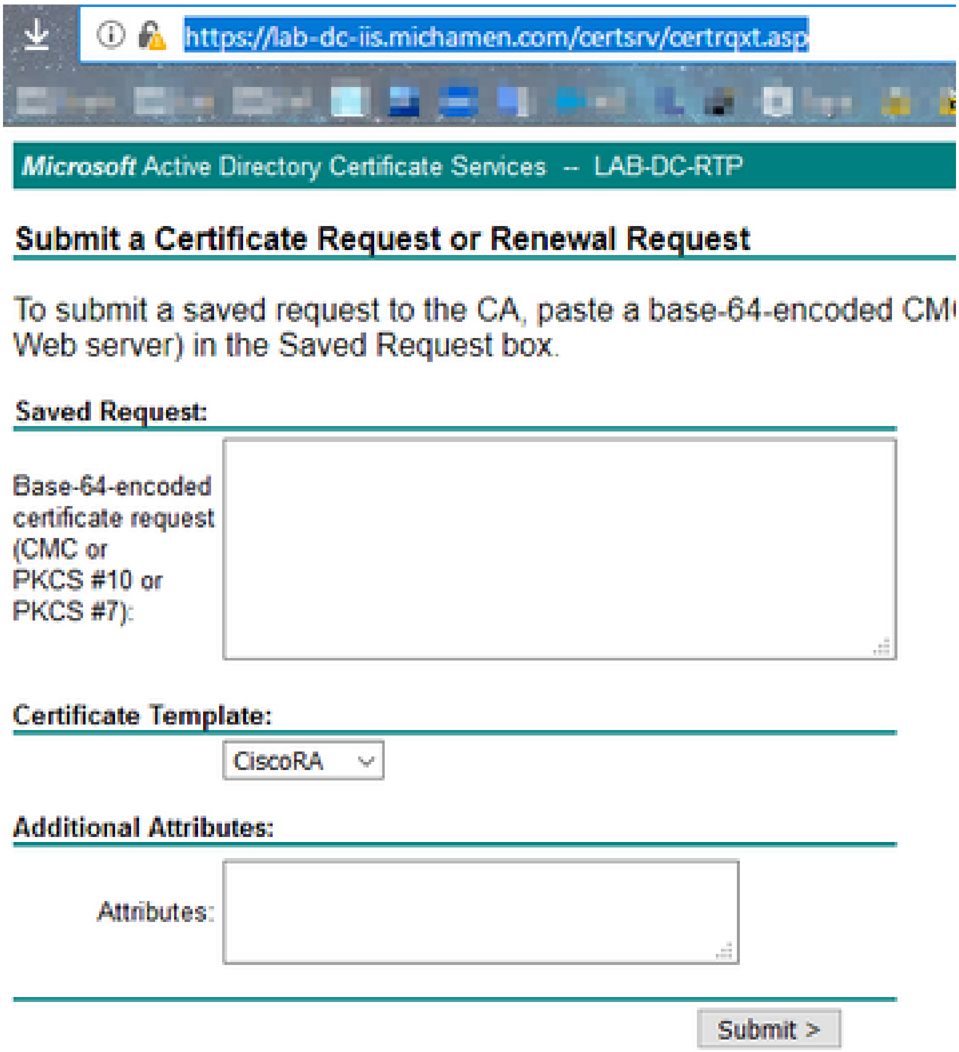
Select a task:

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

/certsrv/certrqxt.asp

/certsrv/certrqxt.asp URL用於啟動新證書的請求。EST客戶端使用**/certsrv/certrqxt.asp**提交CSR、證書模板名稱以及任何所需的屬性。

下圖為來自Web瀏覽器的**/certsrv/certrqxt.asp**範例。



https://lab-dc-iis.michamen.com/certsrv/certrqxt.asp

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

Submit a Certificate Request or Renewal Request

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

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

CiscoRA

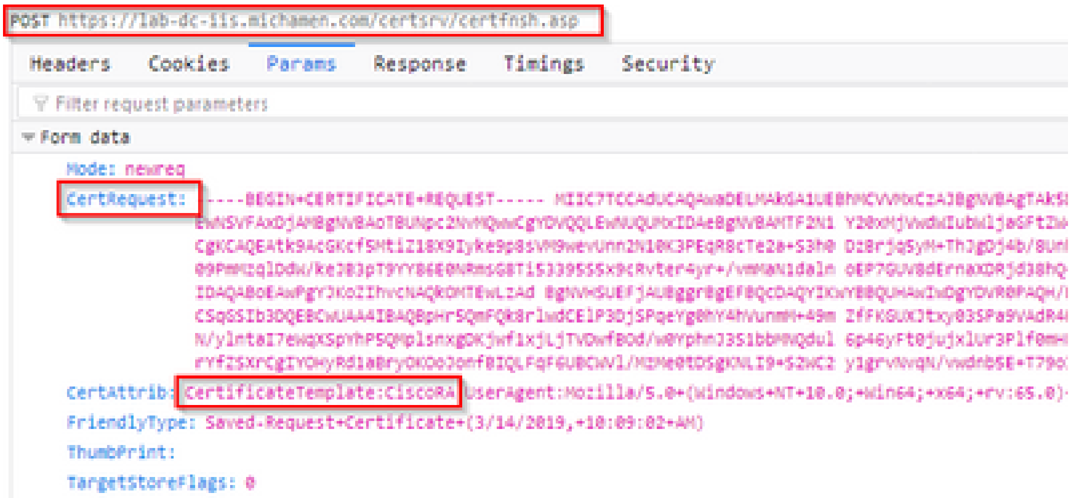
Additional Attributes:

Attributes:

/certsrv/certfnsh.asp

/certsrv/certfnsh.asp URL用於為證書請求提交資料；包括CSR、憑證模板名稱及任何所需的屬性。要檢視提交，請在通過*certrqxt.asp*頁提交資料之前，使用瀏覽器的**Developer Tools**開啟瀏覽器的控制檯。

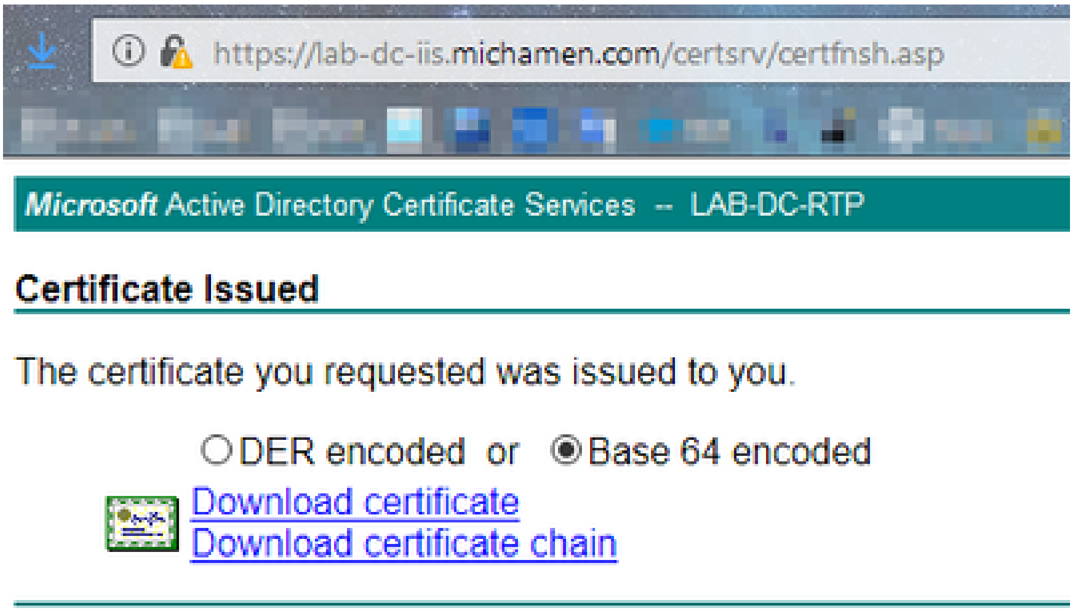
下圖為瀏覽器控制檯中顯示的資料示例。



POST https://lab-dc-iis.michamen.com/certsrv/certfnsh.asp

```
▾ Form data
    Mode: newreq
    CertRequest: -----BEGIN+CERTIFICATE+REQUEST----- MIIC7TCCAdUCAQAwaDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkS
                 EwNSVFAxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNUQUMxIDAeBgNVBAMTF2N1 Y20xMjVwdWIubWljaGFtZW
                 CgKCAQEAtk9AcGKcfSMtiZ18X9Iyke9p8sVM9wevUnn2N10K3PEqR8cTe2a+S3h0 DzBrjq5yM+Th3gDj4b/8Um
                 09PmMzqlDdw/ke283pT9YYB6E0NRmsG8Ti533955SX9CRvter4yr+/vmMaNidaln oEP7GUV8dErnaXDRjd38hQ
                 IDAQABoEAwPgYJKoZIhvcNAQkOMTEwLzAd BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDgYDVR0PAQH/
                 CSqGSIb3DQEBCwUAA4IBAQBpHr5QmFQk8rlwdCElP3DjSPqeYg0hY4hVunmM+49m ZfFKGUXJtxy03SPa9VAdR4
                 N/ylntaI7ewqXSpYhPSQMplsnxgDKjwf1xjLjTVOwfBOd/w0YphnJ351bbMNQdul 6p46yFt0jujxlUr3Plf0mH
                 rYfZSXrCgIYOHyRd1aBryOKOoJonf8IQLFqF6UBCWVl/MIMe0tDSgKNLI9+S2WC2 y1grVNvqN/vwdnb5E+T790
    CertAttrib: CertificateTemplate:CiscoRA UserAgent:Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:65.0)
    FriendlyType: Saved-Request+Certificate+(3/14/2019,+10:09:02+AM)
    ThumbPrint:
    TargetStoreFlags: 0
```

/certsrv/certfnsh.asp 的提交響應包括CA頒發的證書的請求ID。檢查頁面的原始碼時，會在Web瀏覽器中看到請求ID。



https://lab-dc-iis.michamen.com/certsrv/certfnsh.asp

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

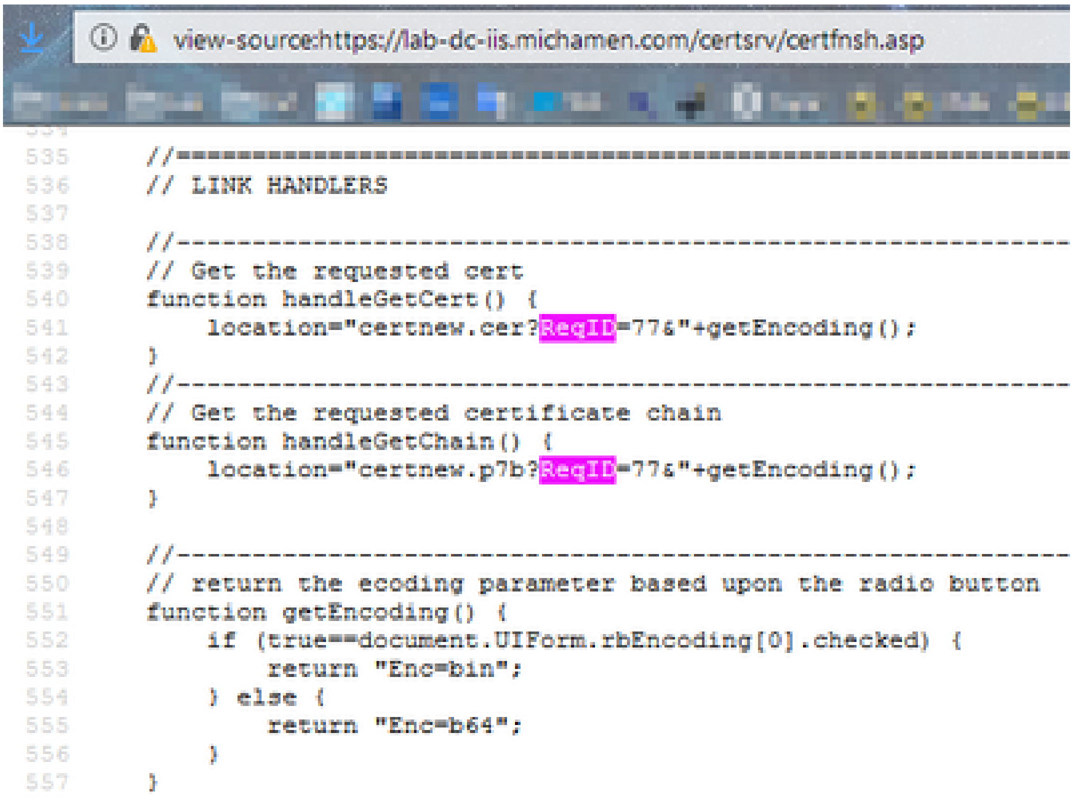
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

提示：在頁面源中搜尋「ReqID」



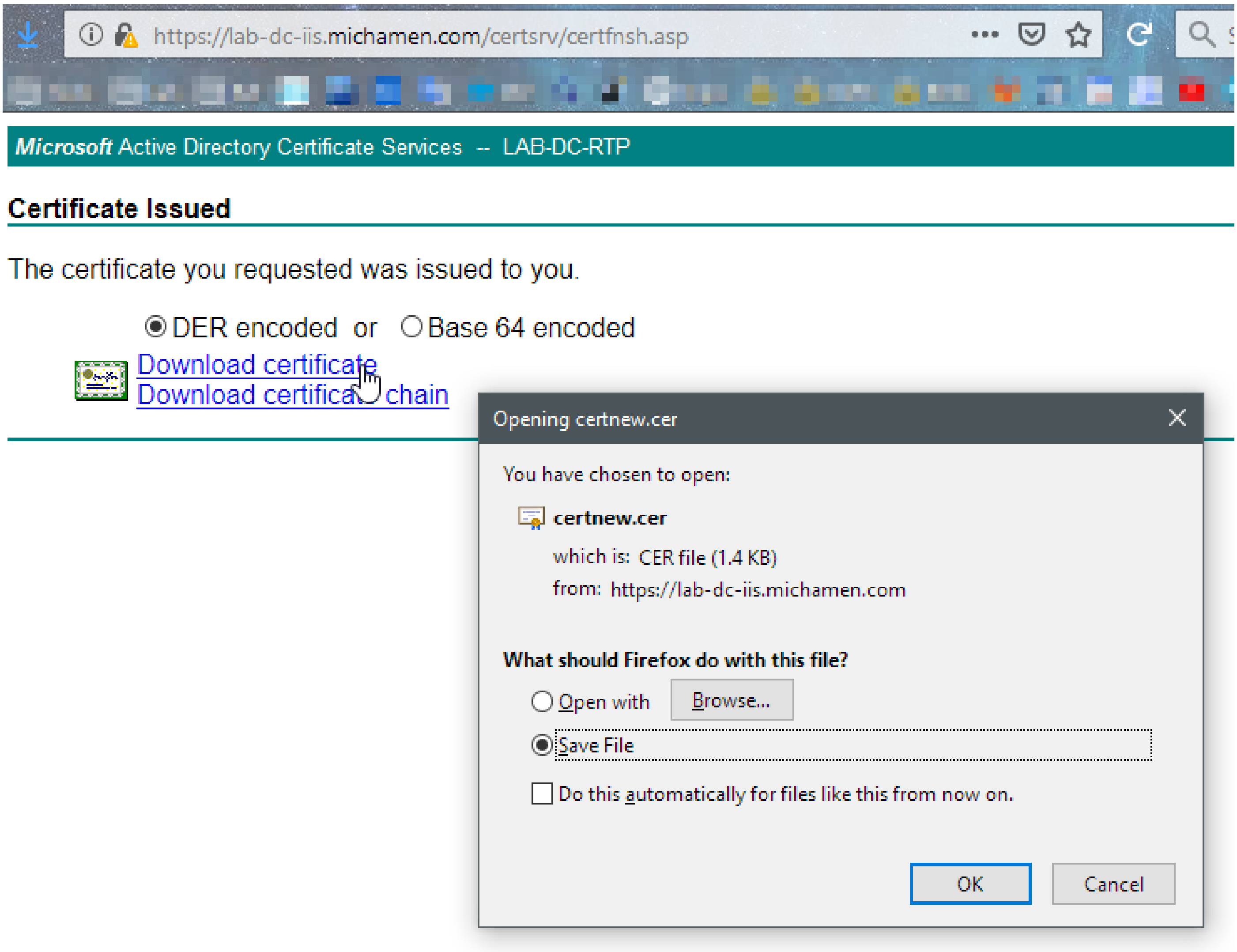
view-source:https://lab-dc-iis.michamen.com/certsrv/certfnsh.asp

```
//================================================================
// LINK HANDLERS

//----------------------------------------------------------------
// Get the requested cert
function handleGetCert() {
    location="certnew.cer?ReqID=77&"+getEncoding();
}
//----------------------------------------------------------------
// Get the requested certificate chain
function handleGetChain() {
    location="certnew.p7b?ReqID=77&"+getEncoding();
}

//----------------------------------------------------------------
// return the ecoding parameter based upon the radio button
function getEncoding() {
    if (true==document.UIForm.rbEncoding[0].checked) {
        return "Enc=bin";
    } else {
        return "Enc=b64";
    }
}
```

/certsrv/certnew.cer

此時，EST客戶端知道新證書的請求ID。EST客戶端使用**/certsrv/certnew.cer**傳遞請求ID和檔案編碼作為引數，下載副檔名為.cer的證**書**文件。

這等同於按一下**Download Certificate**連結時瀏覽器中發生的情況。



https://lab-dc-iis.michamen.com/certsrv/certfnsh.asp

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

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate

Download certificate chain

Opening certnew.cer

You have chosen to open:

certnew.cer

which is: CER file (1.4 KB)

from: https://lab-dc-iis.michamen.com

What should Firefox do with this file?

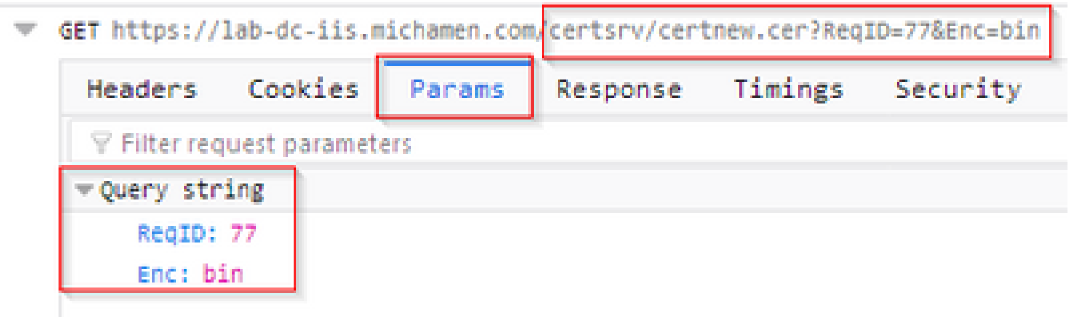
○ Open with [Browse...]

● Save File

□ Do this automatically for files like this from now on.

要檢視請求URL和引數，請使用瀏覽器的控制檯。

附註：如果選擇了DER編碼，瀏覽器將為編碼引數指定bin;但是，Base64編碼將顯示為b64。



```
GET https://lab-dc-iis.michamen.com/certsrv/certnew.cer?ReqID=77&Enc=bin
```

```
Query string
    ReqID: 77
    Enc: bin
```

用於故障排除的相關跟蹤/日誌

這些日誌有助於隔離大多數問題。

CAPF日誌

CAPF日誌包括與電話的互動和最小的CiscoEST活動記錄。

> **附註**：這些日誌可通過命令列介面(CLI)或即時監控工具(RTMT)收集。 由於CSCvo28048,CAPF可能無法在RTMT的服務清單中顯示。

CiscoRA日誌

CiscoRA日誌通常稱為CES日誌。CiscoRA日誌包含CES的初始啟動活動，並顯示進行與CA的身份驗證時可能出現的錯誤。如果成功進行與CA的初始身份驗證，則此處的電話註冊的後續活動不會記錄。因此，CiscoRA日誌是排查問題的良好起點。

> **附註**：自本文檔建立起，只能通過CLI收集這些日誌。

NGINX error.log

NGINX error.log是此功能最有用的日誌，因為它記錄了啟動期間的所有活動以及NGINX和CA端之間的任何HTTP互動；其中包括從CA返回的錯誤代碼，以及處理請求後由CiscoRA生成的錯誤代碼。

> **附註**：在建立此文檔時，甚至無法從CLI收集這些日誌。只能使用遠端支援帳戶(root)下載這些日誌。

CA Web伺服器的日誌

CA Web伺服器的日誌非常重要，因為它們顯示任何HTTP活動，包括請求URL、響應代碼、響應持續時間和響應大小。您可以使用這些日誌來關聯CiscoRA和CA之間的互動。

> **附註**：本文檔上下文中的CA Web Server日誌是MS IIS日誌。如果將來支援其他Web CA，則它們可能具有不同的日誌檔案作為CA Web伺服器的日誌

日誌檔案位置

CAPF日誌：

- 從根：/var/log/active/cm/trace/capf/sdi/capf<*number*>.txt
- 在 CLI 上：file get activelog cm/trace/capf/sdi/capf*

> **附註**：將CAPF跟蹤級別設定為「詳細」並在執行測試之前重新啟動CAPF服務。

Cisco RA:

- 從根：/var/log/active/cm/trace/capf/sdi/nginx<*number*>.txt
- 在 CLI 上：file get activelog cm/trace/capf/sdi/nginx*

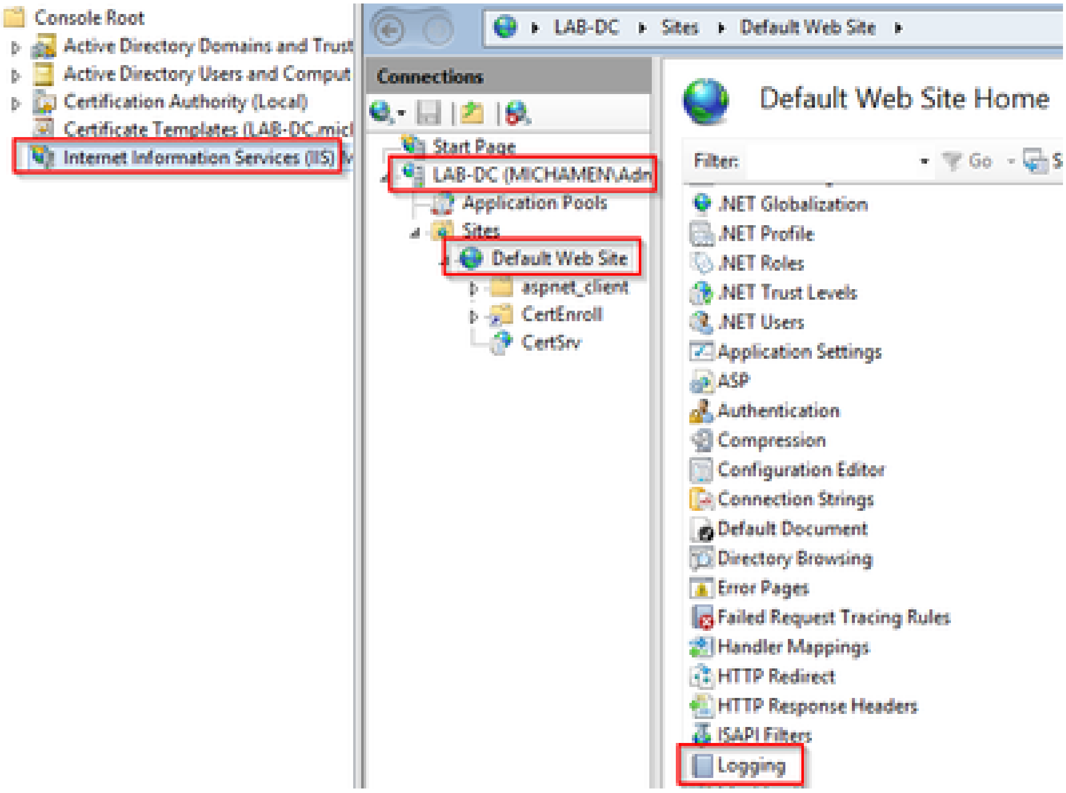
Nginx錯誤日誌：

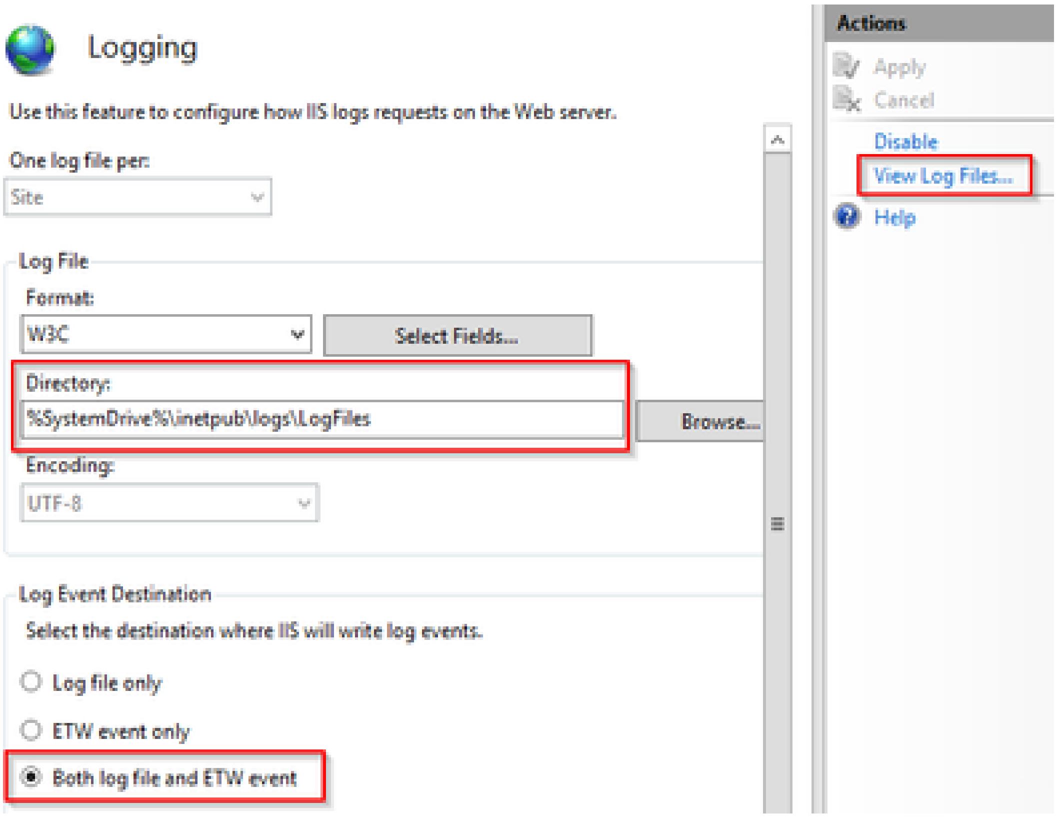
- 從根：/usr/local/thirdparty/nginx/install/logs/error.log

- 在CLI中不可用

MS IIS日誌：

- 開啟MMC
- 選擇**Internet Information Services(IIS)**管理單元
- 按一下伺服器名稱
- 按一下**Default Web Site**
- 按兩下**Logging**以檢視日誌記錄選項
- 在**操作**選單中選擇**檢視日誌檔案**





Use this feature to configure how IIS logs requests on the Web server.

One log file per:
Site

Log File
Format:
W3C
Directory:
%SystemDrive%\inetpub\logs\LogFiles
Encoding:
UTF-8

Log Event Destination
Select the destination where IIS will write log events.

○ Log file only
○ ETW event only
● Both log file and ETW event

日誌分析示例

服務正常啟動

CES啟動，如NGINX日誌中所示

從該日誌收集的資訊很少。此處可以看到載入到其信任儲存區的完整證書鏈，一個用於Web容器，另一個用於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啟動，如NGINX error.log中所示

使用憑證模板組態和憑證的登入在片段中觀察到：

```
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
```

在以下代碼片段中觀察到CA證書鏈的檢索：

```
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
```

請求成功時，會獲取certnew.p7b檔案。具有模板憑據的相同URL可用於從Web瀏覽器獲取certnew.p7b檔案。

CES啟動 如IIS日誌中所示

在NGINX錯誤.log中看到的相同CES啟動事件。在IIS日誌中也觀察到；但是，IIS日誌包括另外2個HTTP GET請求，因為第一個請求將由Web伺服器通過401響應來質詢；且通過驗證後，系統會使用301回應將要求重新導向：

```
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啟動(如CAPF日誌所示)

CES啟動時CAPF日誌中發生的大多數內容與其他日誌中的內容看起來相同；但是您會發現CAPF服

務正在檢測線上CA的方法和配置：

```
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
```

從日誌中得出的下一個重要發現是CAPF服務何時初始化其EST客戶端。

```
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安裝操作

CAPF日誌

建議收集所有必要的日誌，然後檢視CAPF日誌開始分析。這樣，我們就能夠知道特定電話的時間參考。

除了CAPF服務中運行的EST客戶端將在對話方塊快結束時（在電話提供CSR之後）使用CES執行註冊外，信令的初始部分看起來與其他CAPF方法相同。

```
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
```

一旦CES檢索到電話的簽名證書，證書將在提供給電話之前轉換為DER格式。

```
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服務將再次接管，並從其寫入上面的代碼段(/tmp/capf/cert/)中的位置載入CSR。 然後，CAPF服務將簽名的LSC提供給電話。同時刪除電話的CSR。

```
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日誌

下面的代碼片斷顯示了電話的LSC安裝步驟的IIS日誌中的事件，如上所述。

```
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
```

常見問題

當CES端出現錯誤時，它將會在CAPF日誌中看到與以下代碼片斷類似的輸出。請務必檢查其他日誌以繼續縮小問題範圍。

```
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標識證書的頒發者鏈中缺少CA證書

當CES不信任證書鏈中的根證書或中間證書時， nginx日誌中會顯示「無法從CA檢索CA證書鏈」錯誤。

```
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
```

呈現自簽名證書的Web伺服器

不支援在IIS上使用自簽名證書，即使在CUCM上以CAPF-trust形式上載，該證書仍會起作用。下面的代碼段來自nginx日誌，它顯示當IIS使用自簽名證書時觀察到的內容。

```
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
```

與URL主機名和公用名不匹配

IIS證書的公用名稱(lab-dc)與CA的Web註冊服務的URL中的FQDN不匹配。要使證書驗證成功URL中的FQDN，必須與CA使用的證書上的公用名匹配。

```
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解析問題

CiscoRA無法解析在服務引數中配置的線上CA的主機名。

```
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
```

頒發證書有效日期

網路時間協定(NTP)無法正常工作時，會出現證書有效日期問題。此檢查由CES在啟動時執行，並在NGINX日誌中觀察到。

```
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
```

證書模板配置錯誤

服務引數中的名稱中出現的拼寫錯誤將導致故障。CAPF和NGINX日誌中不會記錄任何錯誤，因此需要檢查NGINX error.log。

```
***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身份驗證超時

以下截圖顯示初始certsrv身份驗證過程中CES EST客戶端在預設計時器10秒後超時。

```
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
```

附註：CSCvo58656和CSCvf83629均與CES身份驗證超時有關。

CES註冊超時

CES EST客戶端在身份驗證成功後超時，但正在等待對註冊請求的響應。

```
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
```

已知警告

CSCvo28048 CAPF服務不再列在RTMT收集檔案選單中

CSCvo58656 CAPF線上CA需要選項配置RA和CA之間的最大連線超時

CSCvf83629 EST伺服器在註冊期間獲取EST_ERR_HTTP_WRITE

相關資訊

- **技術支援與文件 - Cisco Systems**