排除CAPF在线CA故障

目录

简介

本文档介绍证书颁发机构代理功能(CAPF)自动注册和续约功能的故障排除。此功能也称为CAPF Online CA。

先决条件

要求

Cisco 建议您了解以下主题：

- 证书
- 思科统一通信管理器(CUCM)安全

使用的组件

本文档中的信息基于CUCM 12.5版，因为CUCM 12.5中引入了CAPF Online CA功能。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

功能组件概述

注册机构(RA)

RA是网络中的一个机构，用于验证用户对数字证书的请求并通知证书颁发机构(CA)颁发证书。RA是公钥基础设施(PKI)的一部分。

通过安全传输(EST)注册

EST是请求注释(RFC)7030中定义的协议，用于为使用通过传输层安全(TLS)和超文本传输协议(HTTP)的CMS(CMC)证书管理消息的客户端注册证书。EST使用客户端/服务器模型，其中EST客户端发送注册请求，EST服务器发送包含结果的响应。

libEST

libEST是思科实施EST的库。libEST允许在最终用户设备和网络基础设施设备上调配X509证书。此

库由CiscoEST和CiscoRA实施。

引擎X(NGINX)

NGINX是类似于Apache的Web服务器和反向代理。NGINX用于CAPF和CES之间的HTTP通信以及CES和CA Web注册服务之间的通信。当libEST在服务器模式下运行时，需要Web服务器代表libEST处理TCP请求。

证书注册服务(CES)

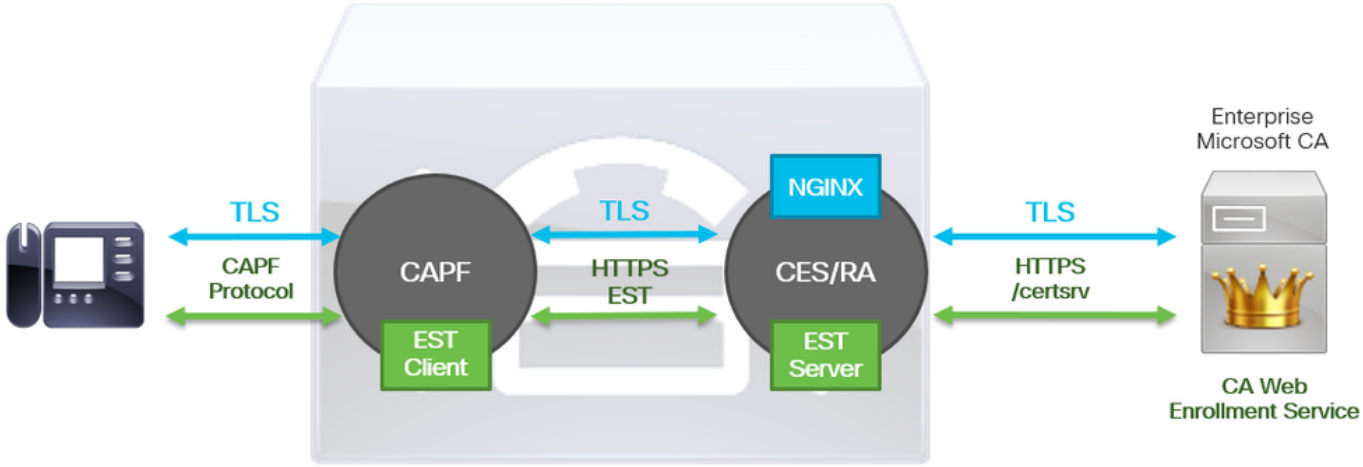
CES是CUCM上的服务，充当CAPF服务和CA之间的RA。CES也称为CiscoRA，或简称RA。CES使用NGINX作为其Web服务器，因为CES在服务器模式下实现libEST以充当RA。

证书颁发机构代理功能(CAPF)

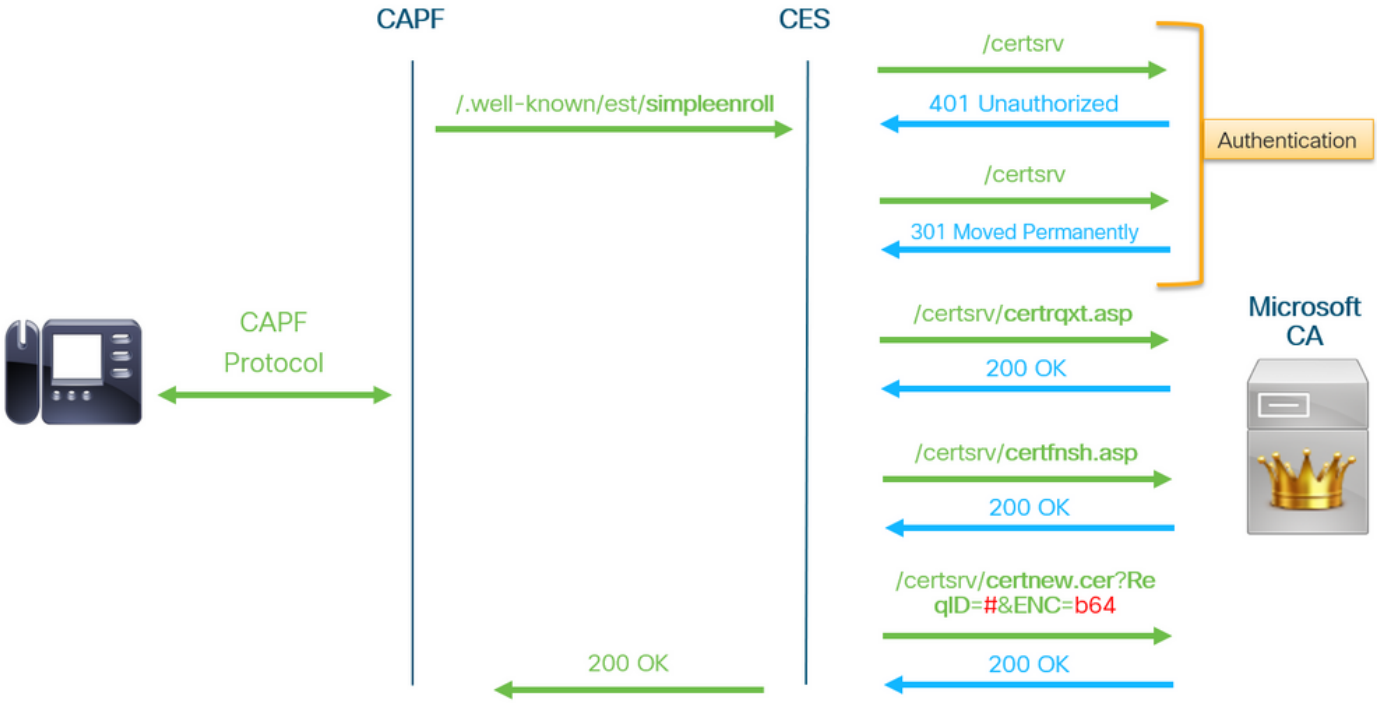
CAPF是CUCM服务，电话在执行证书注册请求时与其交互。CAPF代表电话与CES交互。在此功能模型中，CAPF在客户端模式下实施libEST，以通过CES注册电话的证书。

总之，以下是每个组件的实施方式：

1. 电话向CAPF发送证书请求
2. CAPF实施CiscoEST（客户端模式）以与CES通信
3. CES实施CiscoRA（服务器模式）以处理和响应EST客户端的请求
4. CES/CiscoRA通过HTTPS与CA的Web注册服务通信



消息流图



消息流说明

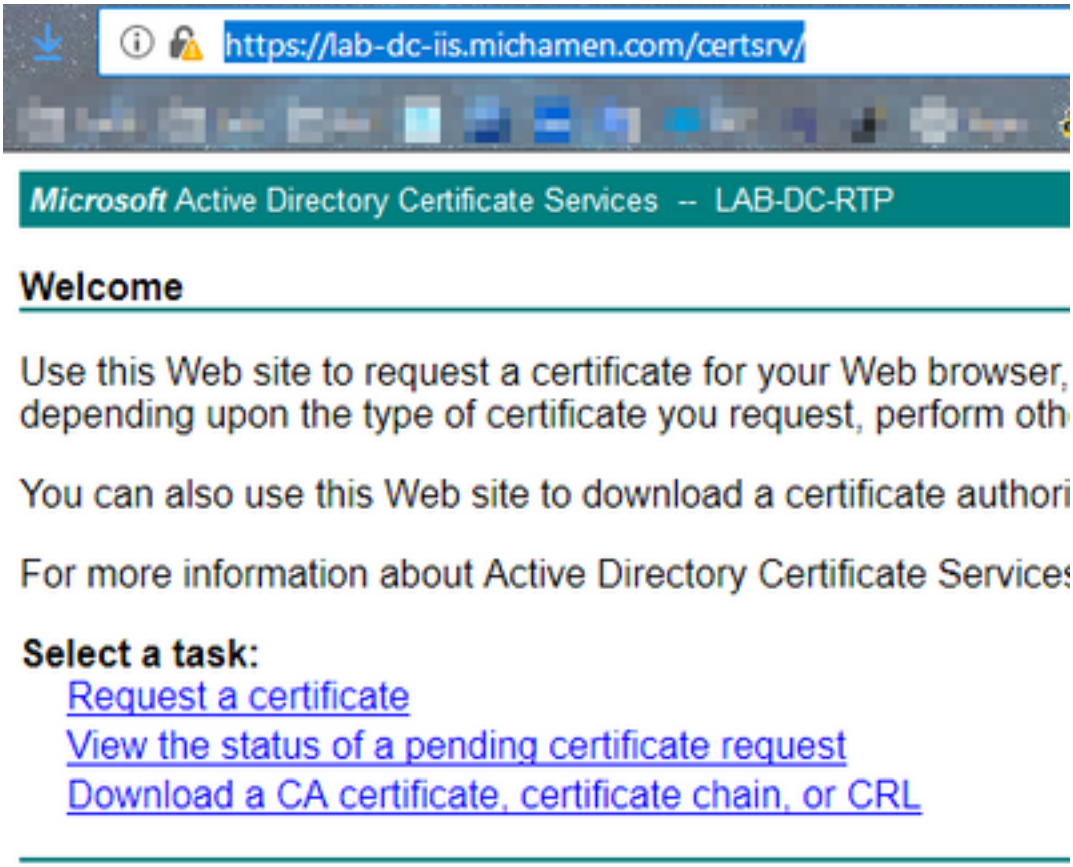
/.well-known/est/simpleenroll

EST客户端使用此URL发送API调用，该调用请求从EST服务器注册证书。EST服务器收到API调用后，将启动证书注册过程，其中包括与CA的Web注册服务的HTTPS通信。如果注册过程成功，并且EST服务器收到新证书，CAPF将继续加载证书并将其返回IP电话。

/certsrv

EST客户端使用/certsrv URL验证并启动与CA的会话。

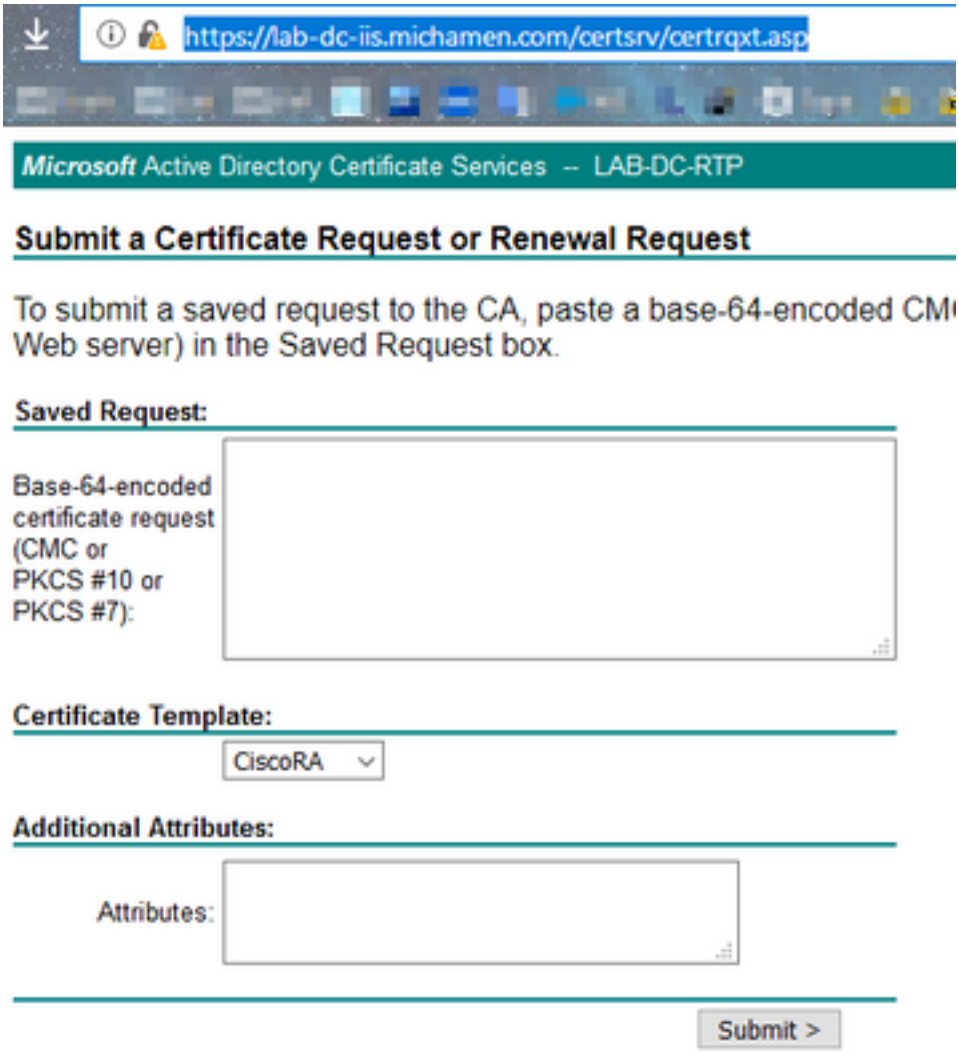
下图是Web浏览器/certsrv URL的示例。这是证书服务登录页。



/certsrv/certrqxt.asp

/certsrv/certrqxt.asp URL用于发起新证书的请求。EST客户端使**用/certsrv/certrqxt.asp**提交CSR、证书模板名称和任何所需属性。

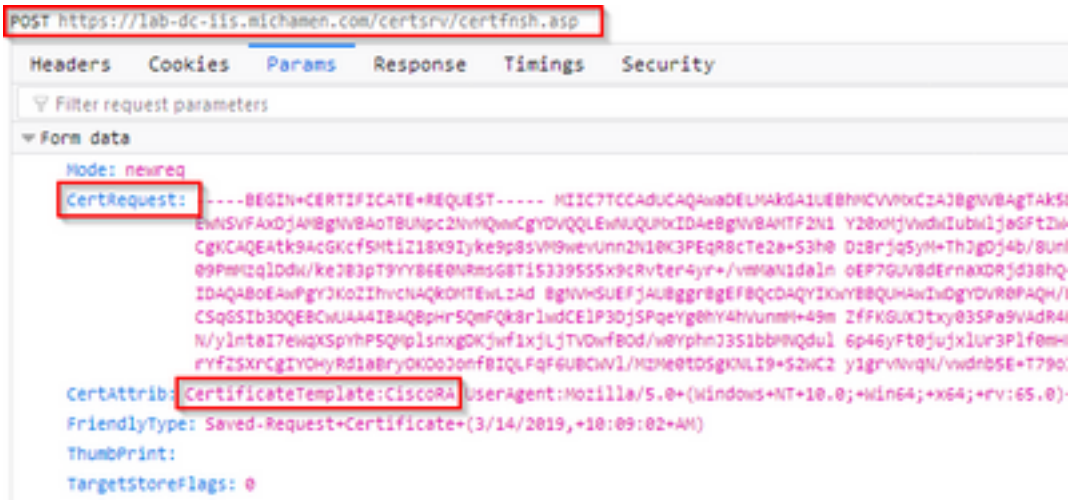
下图是Web浏览器**中**的/certsrv/certrqxt.asp示例。



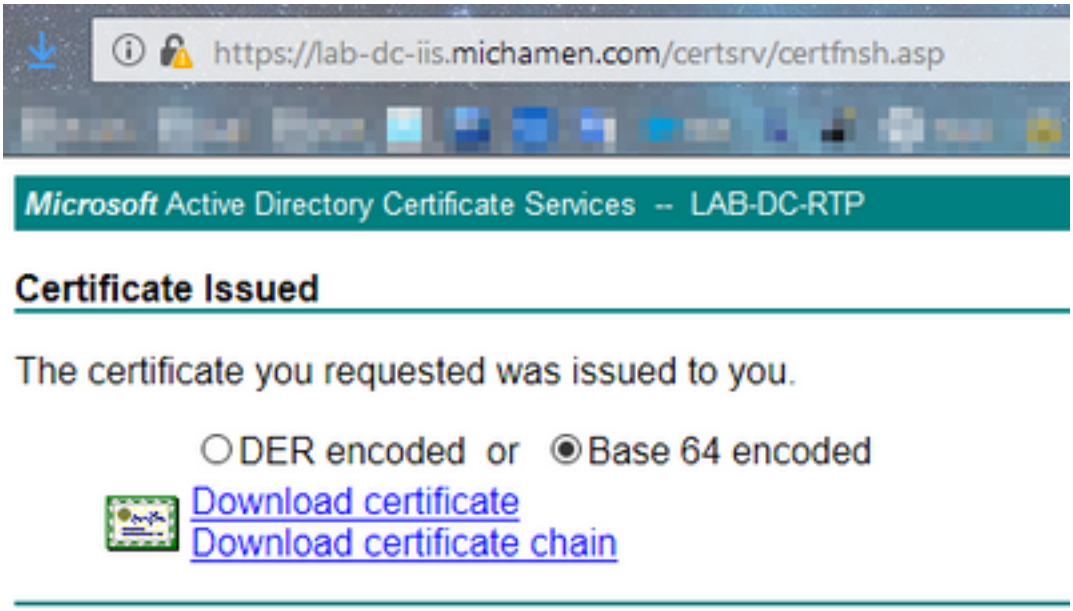
/certsrv/certfnsh.asp

/certsrv/certfnsh.asp URL用于提交证书请求的数据；包括CSR、证书模板名称和任何所需属性。要查看提交，请使用浏览器的“开**发人员工**具”在通过certrqxt.asp页提交数据之前打开浏*览器的*控制台。

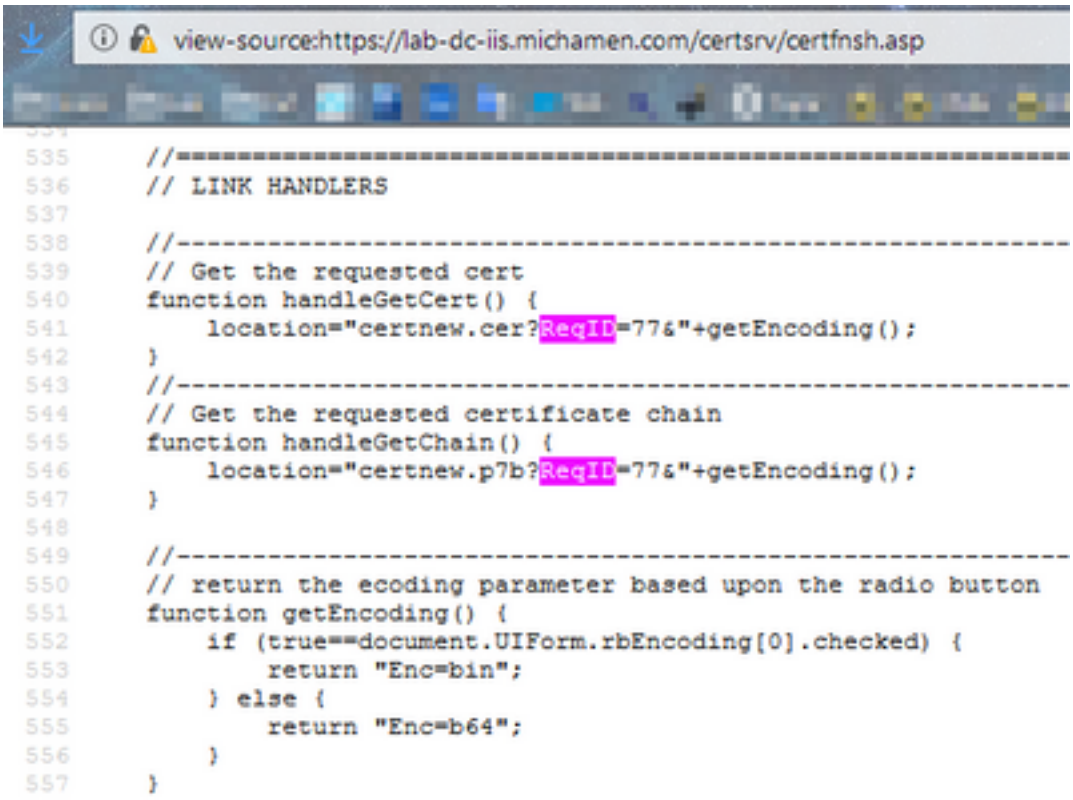
下图是浏览器控制台中显示的数据示例。



来自/certsrv/certfnsh.asp的**提交**响应包括CA颁发的证书的请求ID。检查页面的源代码时，在Web浏览器中可以看到请求ID。



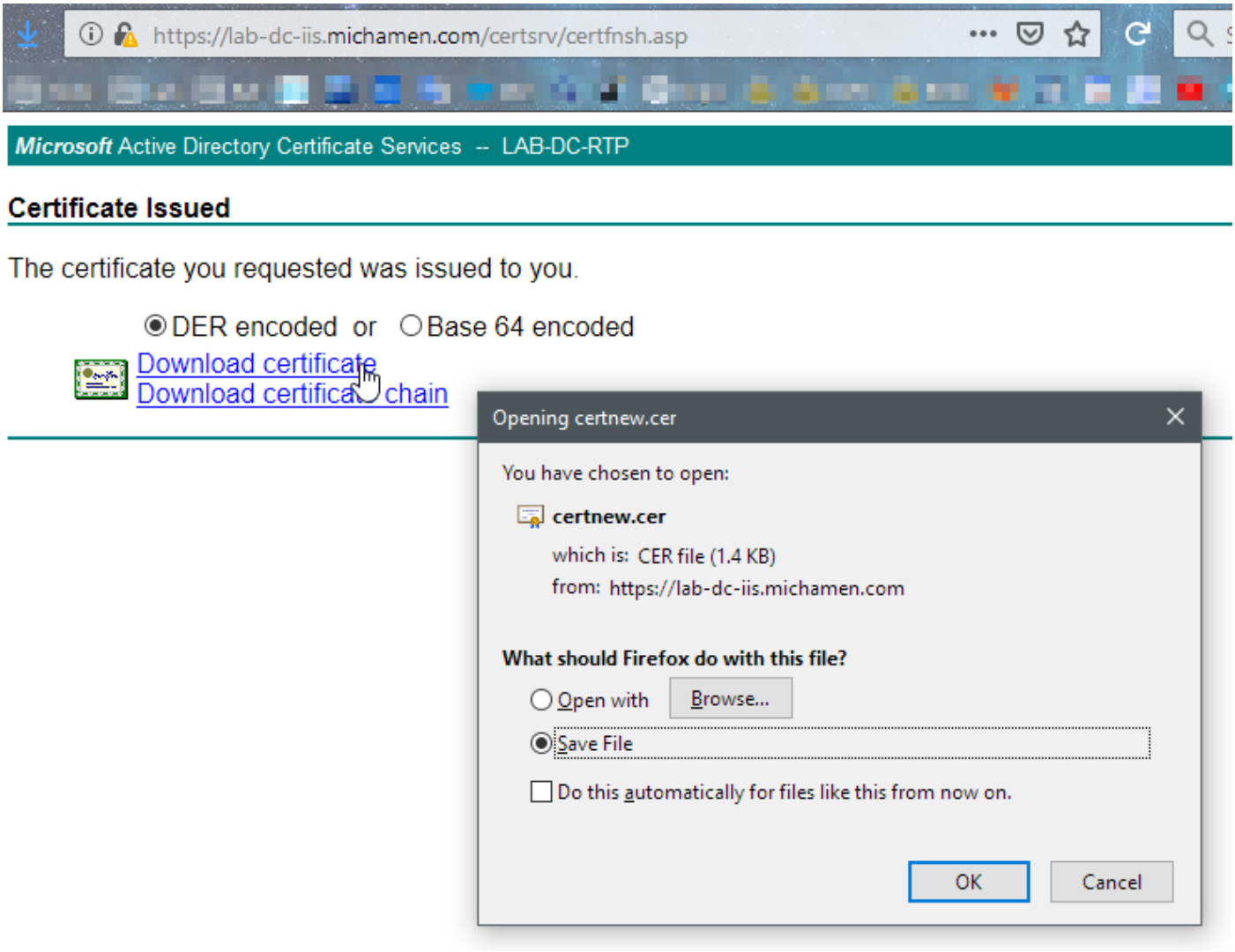
提示：搜索页面源以查找“ReqID”



/certsrv/certnew.cer

此时，EST客户端知道新证书的请求ID。EST客户端使用/certsrv/certnew.cer将请求ID和文件编码作为参数传递，以下载扩展名为.cer的证书文件。

这相当于您单击“下载证书”链接时在浏览器中发生的。



要查看请求URL和参数，请使用浏览器的控制台。

> **注意**：如果选择了DER**编码**，则浏览器会为编码参数指定bin;但是，Base64编码将显示为b64。

故障排除的相关跟踪/日志

这些日志有助于隔离大多数问题。

CAPF日志

CAPF日志包括与电话的交互和CiscoEST活动的最少日志记录。

注意：这些日志可通过命令行界面(CLI)或实时监控工具(RTMT)进行收集。 由于CSCvo28048,CAPF可能不会在RTMT中的服务列表中显示。

CiscoRA日志

CiscoRA日志通常被称为CES日志。CiscoRA日志包含CES初始启动活动，并显示在进行CA身份验证时可能出现的错误。如果CA的初始身份验证成功，则电话注册的后续活动不会记录在此处。因此，CiscoRA日志是排除故障的良好初始点。

注意：这些日志仅可在创建此文档时通过CLI收集。

NGINX error.log

NGINX error.log是此功能最有用的日志，因为它记录了启动期间的所有活动以及NGINX与CA端之间的任何HTTP交互；包括从CA返回的错误代码以及处理请求后由CiscoRA生成的错误代码。

注意：在创建本文档时，即使从CLI也无法收集这些日志。这些日志只能使用远程支持帐户（根）下载。

CA Web服务器日志

CA Web服务器的日志显示任何HTTP活动（包括请求URL、响应代码、响应持续时间和响应大小）非常重要。您可以使用这些日志关联CiscoRA和CA之间的交互。

注意：本文档中的CA Web Server日志是MS IIS日志。如果将来支持其他Web CA，则它们可能具有不同的日志文件作为CA Web服务器的日志

日志文件位置

CAPF日志：

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

注意：将CAPF跟踪级别设置为“Detailed”，并在执行测试之前重新启动CAPF服务。

思科RA:

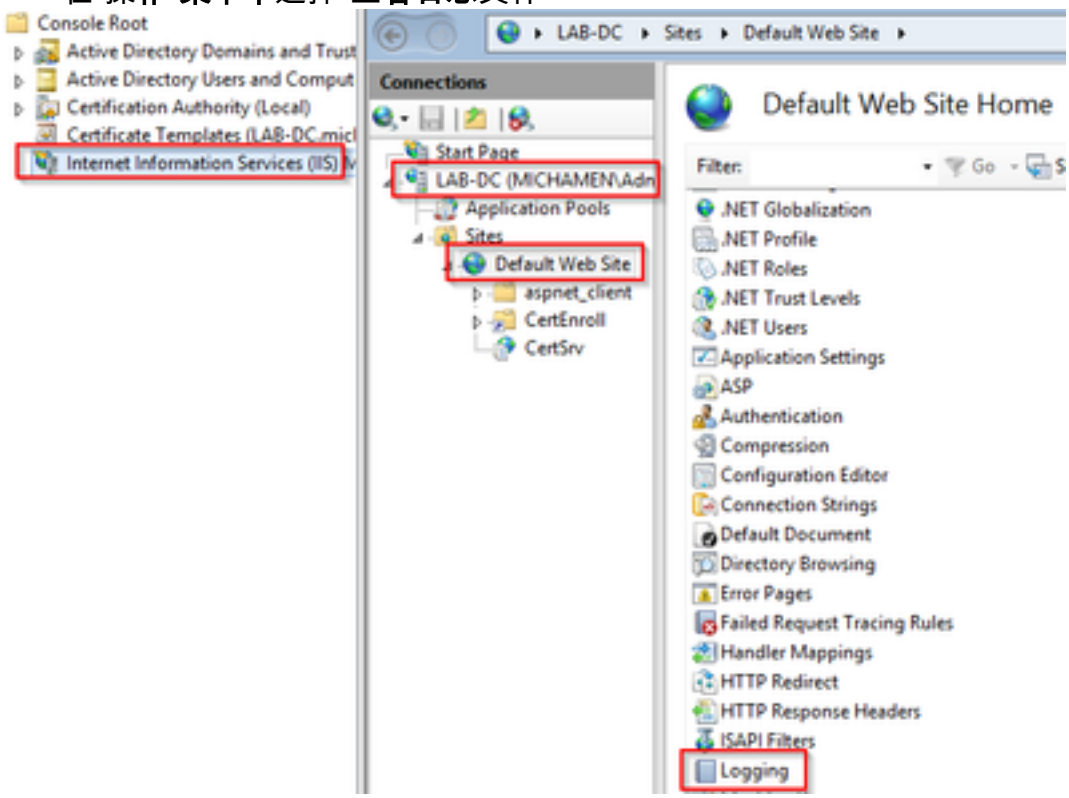
- 从根：/var/log/active/cm/trace/capf/sdi/nginx<*number*>.txt
- 从CLI:file get activelog cm/trace/capf/sdi/nginx*

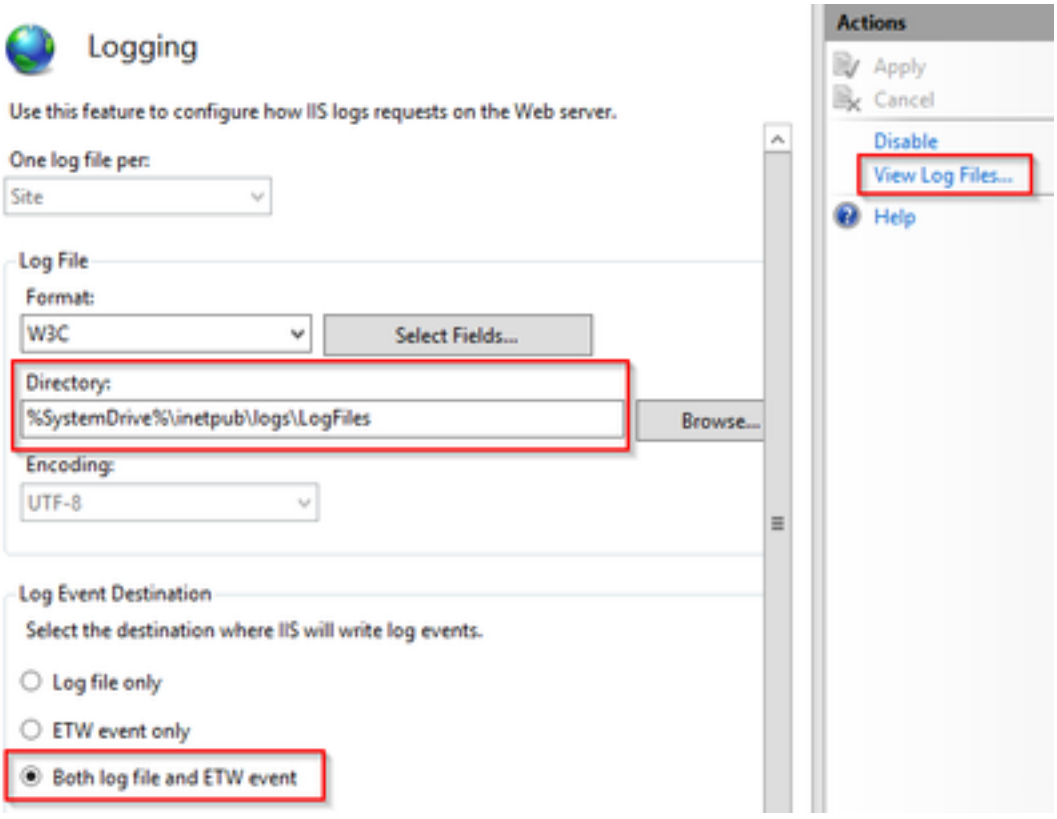
Nginx错误日志：

- 从根：/usr/local/thirdparty/nginx/install/logs/error.log
- 无法从CLI使用

MS IIS日志：

- 打开MMC
- 选择**Internet信息服务**(IIS)管理单元
- 单击服务器名称
- 单击“**默认网站**”
- 双击**Logging**以查看日志记录选项
- 在“**操作**”**菜单中**选择“**查看日志**文件”





日志分析示例

服务正常启动

CES启动，如NGINX日志所示

从此日志中收集的信息很少。此处可以看到加载到其信任库的完整证书链，其中一个用于Web容器，另一个用于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启动，如NGINX error.log所示

使用证书模板配置和凭证登录在以下代码片断中观察：

```
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证书链的检索在以下代码片断中观察：

```
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
```

请求成功时，将获取certnew.p7b文件。具有模板凭证的相同URL可用于从Web浏览器获取certnew.p7b文件。

CES启动 如IIS日志中所示

在IIS日志中也观察到NGINX error.log中显示的相同CES启动事件；但是，IIS日志中还包含2个HTTP GET请求，因为第一个请求将通过401响应受到Web服务器的质询；通过身份验证后，将使用301响应重定向请求：

```
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启动，如CAPF日志中所示

CES启动的CAPF日志中发生的大多数情况与其他日志中发生的情况相同；但您会注意到CAPF服务检测到在线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
```

日志中的下一个重要观察是CAPF服务何时初始化其EST客户端。

```
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!!
```

电话LSC安装操作

CAPF日志

建议收集所有必要的日志，并通过查看CAPF日志开始分析。这样，我们便可了解特定电话的时间参考。

信令的初始部分与其他CAPF方法的外观相同，但CAPF服务中运行的EST客户端将在对话结束时（在电话提供CSR后）执行CES注册。

```
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检索到电话的签名证书后，在将证书提供给电话之前，会将其转换为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服务再次接管并从其写入位置(/tmp/capf/cert/)上面的片段中加载CSR。 然后，CAPF服务将签名的LSC提供给电话。同时删除电话的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日志

以下代码段显示电话LSC安装步骤的IIS日志中的事件，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
```

常见问题

每当CES端出现错误时，CAPF日志中的输出应与下面的代码段类似。请务必检查其他日志以继续缩小问题范围。

```
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身份证书的颁发者链中缺少CA证书

当证书链中的根证书或中间证书不受CES信任时，nginx日志中会显示错误“Unable to retrieve CA Cert chain from CA”（无法从CA检索CA证书链）。

```
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
```

提供自签名证书的Web服务器

不支持在IIS上使用自签名证书，即使在CUCM上以CAPF-trust的形式上传，也会注意到其工作。以下代码段来自nginx日志，它显示IIS使用自签名证书时观察到的内容。

```
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
```

URL主机名和公用名不匹配

IIS证书的公用名(lab-dc)与CA的Web注册服务的URL中的FQDN不匹配。要使证书验证成功，URL内的FQDN必须与CA使用的证书的公用名称匹配。

```
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解析问题

CiscoRA无法解析在服务参数中配置的联机CA的主机名。

```
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
```

证书有效日期问题

当网络时间协议(NTP)无法正常工作时，证书有效日期出现问题。此检查由CES在启动时执行，并在NGINX日志中观察到。

```
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
```

证书模板配置错误

服务参数中名称的拼写错误将导致故障。CAPF和NGINX日志中不会记录任何错误，因此需要检查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身份验证超时

以下截图显示CES EST客户端在初始certsrv身份验证过程中，在默认计时器10秒后超时。

```
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 28
(Operation timed out after 10000 milliseconds with 0 bytes received)

nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

注意：CSCvo58656和CSCvf83629都与CES身份验证超时相关。

CES注册超时

CES EST客户端在身份验证成功后超时，但正在等待对注册请求的响应。

```
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
```

已知问题说明

CSCvo28048 CAPF服务不再列在RTMT收集文件菜单中

CSCvo58656 CAPF Online CA needs选项可配置RA和CA之间的最大连接超时

CSCvf83629 EST服务器在注册期间获取EST_ERR_HTTP_WRITE

相关信息

- 技术支持和文档 - Cisco Systems