أستكشاف أخطاء CAPF Online CA وإصلاحها

المحتويات

المقدمة

يصف هذا المستند أستكشاف أخطاء وظيفة وكيل المرجع المصدق (CAPF) وإصلاحها بميزة التسجيل والتجديد التلقائي. ويشار إلى هذه الميزة أيضا باسم CAPF Online CA.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الشهادات
- أمان مدير الاتصالات الموحدة (CUCM) من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 12.5 من CUCM حيث تم إدخال ميزة CAPF Online CA في CUCM 12.5.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة على مكونات الميزة

سلطة التسجيل

RA هو مرجع في شبكة تتحقق من طلبات المستخدم للحصول على شهادة رقمية وتأمر المرجع المصدق (CA) بإصدار الشهادة. تعد وحدات الوصول عن بعد (RA) جزءا من البنية الأساسية للمفتاح العام (PKI).

التسجيل عبر النقل الآمن (EST)

EST هو بروتوكول معرف في طلب التعليق (RFC) 7030 لتسجيل الشهادة للعملاء الذين يستخدمون رسائل إدارة الشهادات عبر رسائل CMS (CMC) عبر أمان طبقة النقل (TLS) وبروتوكول نقل النص التشعبي (HTTP). يستخدم EST نموذج عميل/خادم حيث يرسل عميل EST طلبات التسجيل ويرسل خادم EST استجابات مع النتائج.

ليب إيست

LibEST هي مكتبة تنفيذ Cisco ل EST. يسمح LibEST بتوفير شهادات X509 على أجهزة المستخدم النهائي وأجهزة البنية الأساسية للشبكة. يتم تنفيذ هذه المكتبة بواسطة CiscoEST و CiscoRA.

Engine-X (NGINX)

NGINX هو خادم ويب ووكيل عكسي مشابه ل Apache. يتم إستخدام NGINX لاتصال HTTP بين CAPF و CES بالإضافة إلى الاتصال بين CES وخدمة تسجيل الويب CA. عندما يعمل libEST في وضع الخادم، يلزم توفر خادم ويب لمعالجة طلبات TCP نيابة عن libEST.

خدمة تسجيل الشهادة (CES)

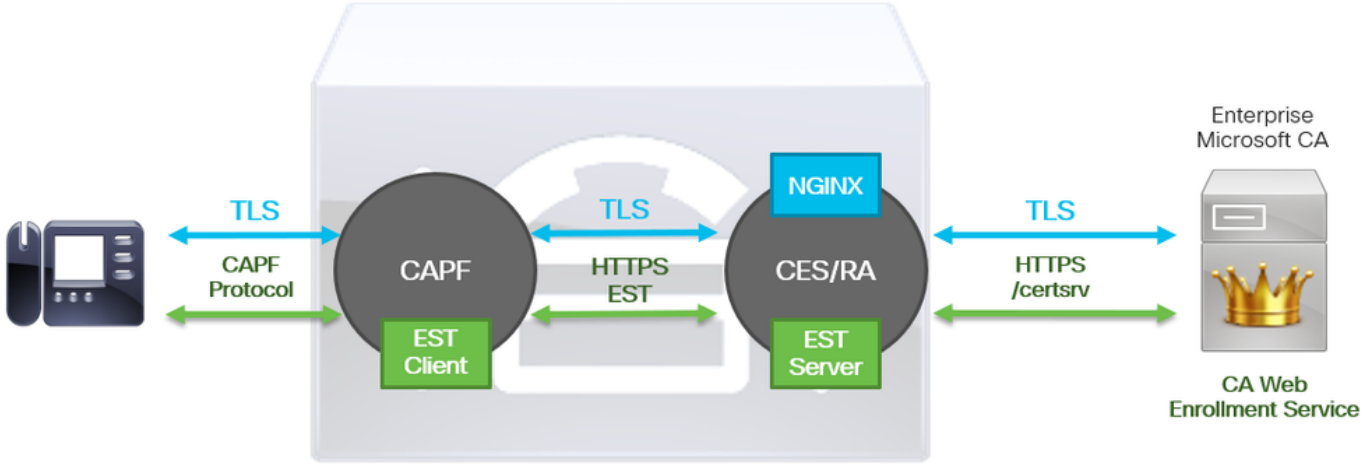
CES هي الخدمة في CUCM التي تعمل كRA بين خدمة CAPF و CA. ويشار إلى CES أيضا باسم CiscoRA، أو ببساطة RA. يستخدم CES NGINX كخادم ويب الخاص به لأن CES يقوم بتطبيق libEST في وضع الخادم ليعمل كRA.

وظيفة وكيل جهة منح الشهادة (CAPF)

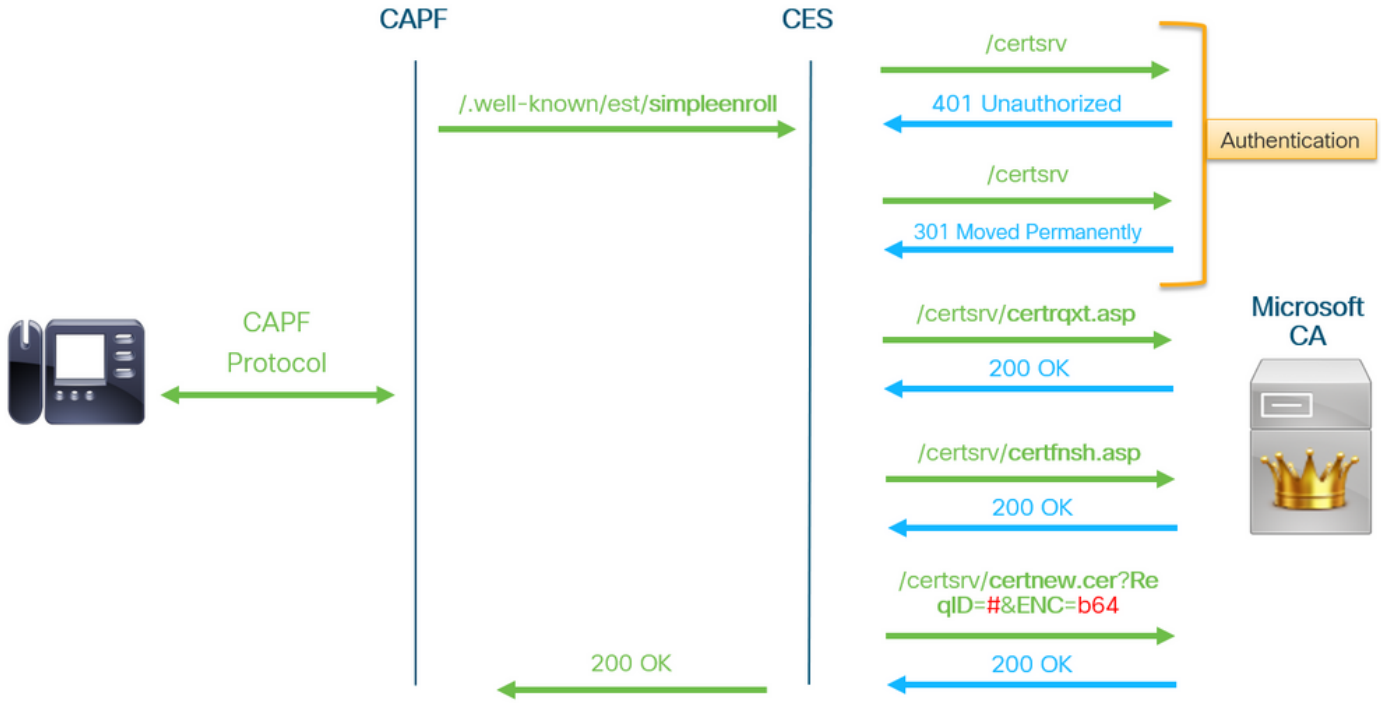
CAPF هي خدمة CUCM والتي تتفاعل مع الهواتف عند تنفيذ طلبات تسجيل الشهادة. ويتفاعل CAPF مع CES نيابة عن الهواتف. في نموذج المميزة هذا يقوم CAPF بتطبيق libEST في وضع العميل لتسجيل شهادات الهواتف من خلال CES.

وباختصار، فيما يلي كيفية تنفيذ كل مكون:

1. يرسل الهاتف طلب شهادة إلى CAPF
2. يطبق CAPF CiscoEST (وضع العميل) للاتصال ب CES
3. يطبق CES CiscoRA (وضع الخادم) لمعالجة طلبات EST Client والاستجابة لها
4. تتصل CES/CiscoRA بخدمة تسجيل ويب CA عبر HTTPS



الرسم التخطيطي لتدفق الرسائل



شرح تدفق الرسائل

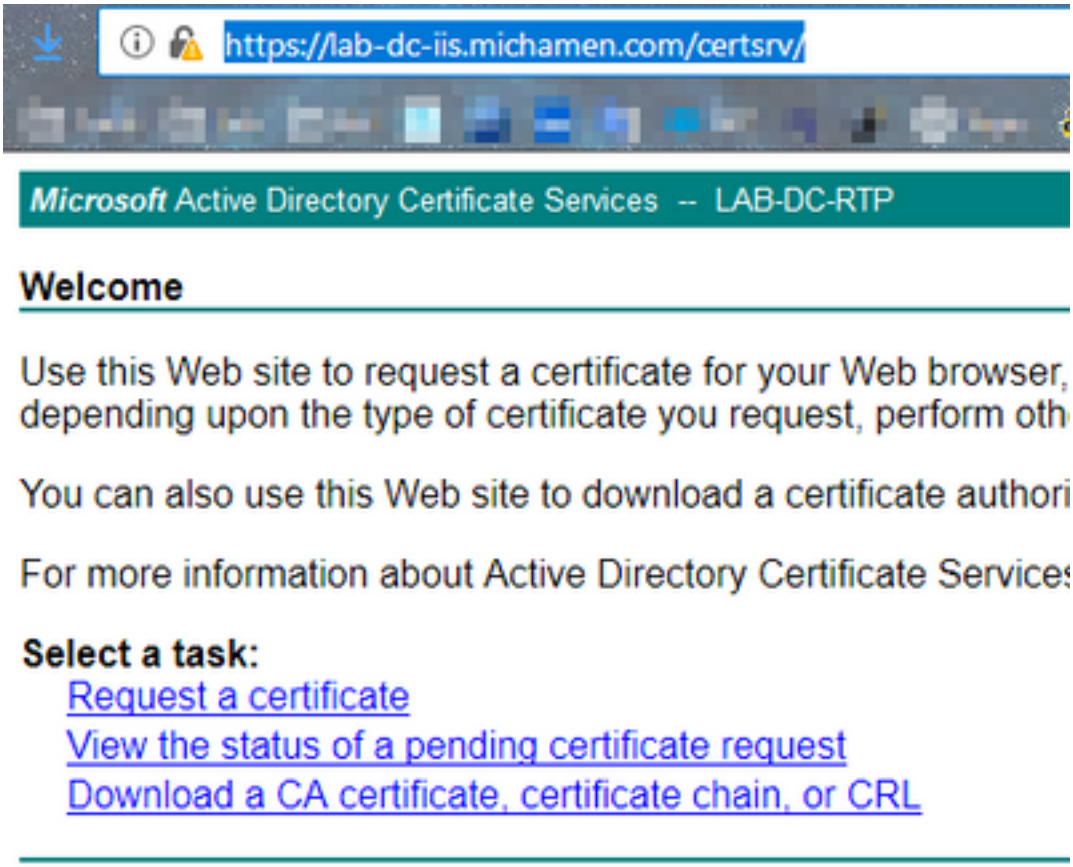
/.well-known/est/simpleenroll

يستخدم عميل EST عنوان URL هذا لإرسال إستدعاء API الذي يطلب تسجيل الشهادة من خادم EST. بمجرد أن يتلقى خادم EST إستدعاء API، فإنه سيبدأ عملية تسجيل الشهادة التي تتضمن اتصال HTTPS بخدمة تسجيل الويب الخاصة ب CA. إذا نجحت عملية التسجيل، واستلم خادم EST الشهادة الجديدة، فستتابع CAPF تحميل الشهادة وتقديمها مرة أخرى إلى هاتف IP.

/certsrv

يتم إستخدام عنوان URL **/certsrv** من قبل عميل EST للمصادقة على جلسة عمل وبدء تشغيلها باستخدام CA.

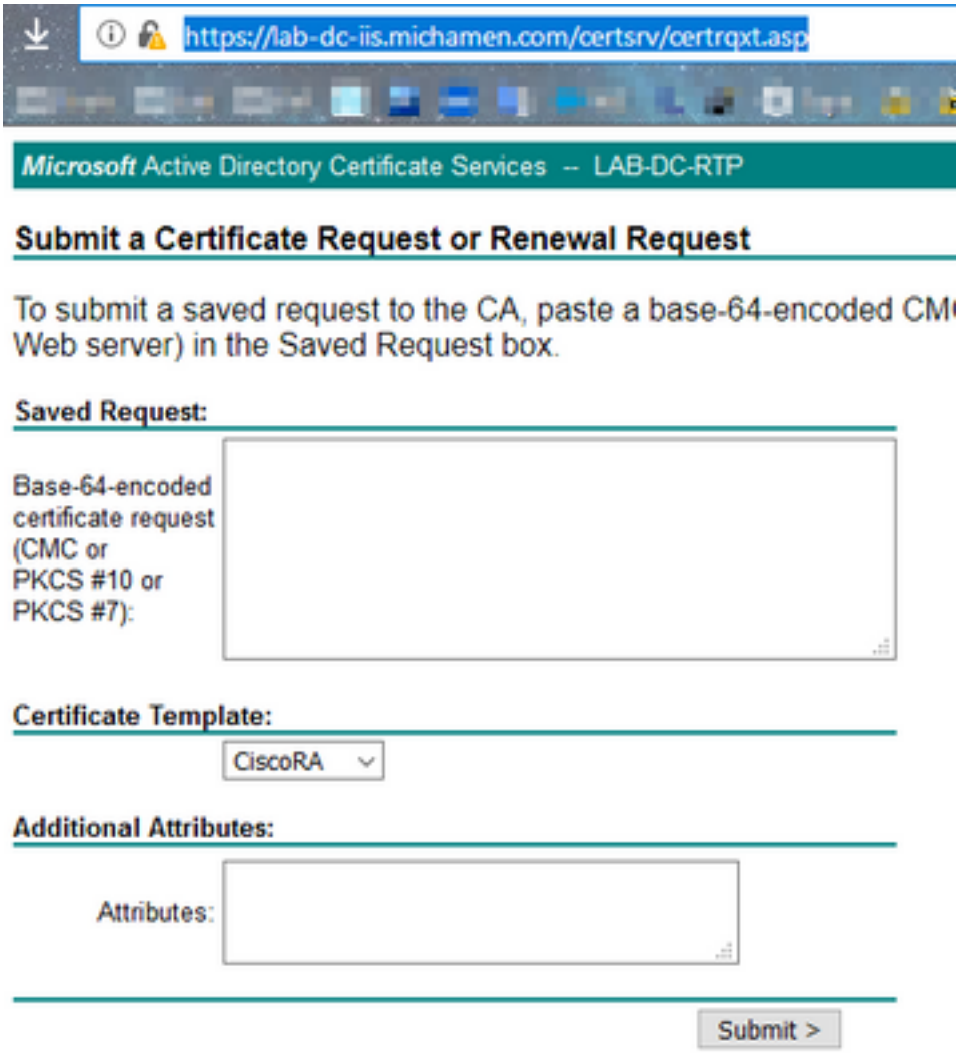
الصورة أدناه هي مثال على عنوان URL **/certsrv** من مستعرض ويب. هذه هي صفحة تنزيل "خدمات الشهادات".



/certsrv/certrqxt.asp

يتم إستخدام عنوان URL **/certsrv/certrqxt.asp** لبدء طلب شهادة جديدة. يستخدم عميل EST **/certsrv/certrqxt.asp** لإرسال CSR، واسم قالب الشهادة، وأي سمات مطلوبة.

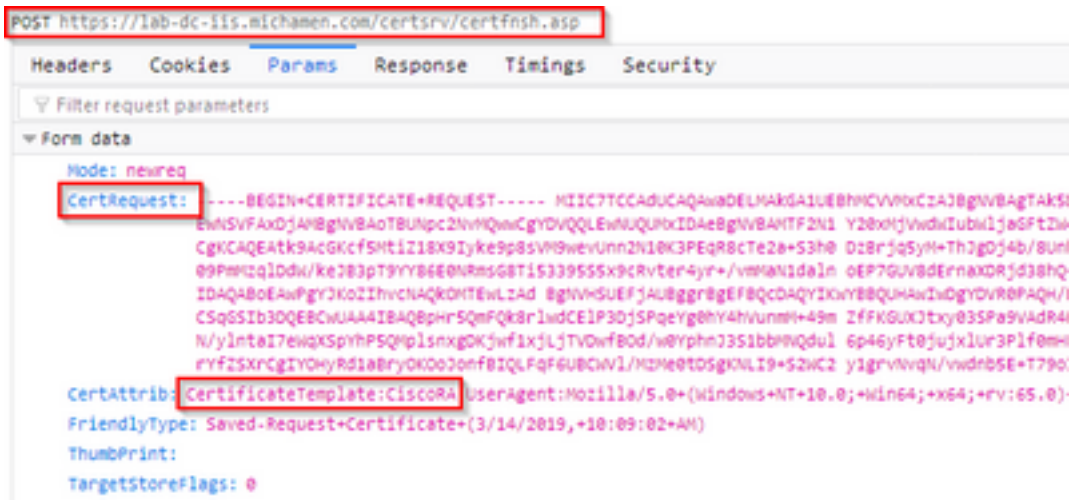
الصورة أدناه هي مثال على **/certsrv/certrqxt.asp** من مستعرض ويب.



/certsrv/certfnsh.asp

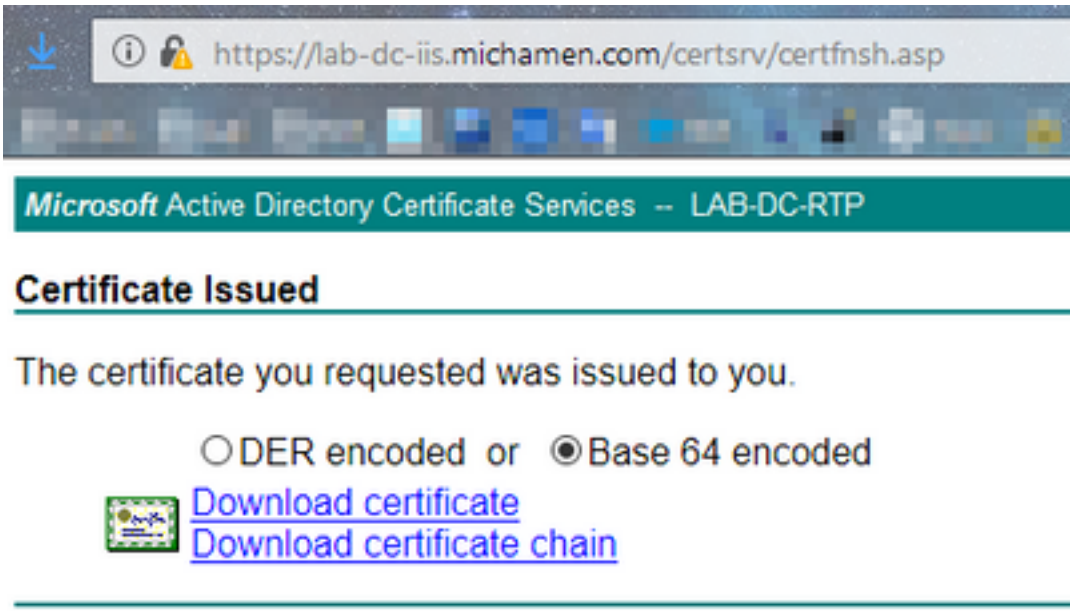
يتم إستخدام عنوان URL **/certsrv/certfnsh.asp** لإرسال البيانات الخاصة بطلب الشهادة، والتي تتضمن CSR واسم قالب الشهادة وأي سمات مطلوبة. لعرض الإرسال، أستخدم **أدوات المطور** الخاصة بالمستعرض لفتح وحدة تحكم المستعرض قبل إرسال البيانات عبر صفحة *certqxt.asp*.

الصورة أدناه هي مثال للبيانات المعروضة في وحدة تحكم المستعرض.

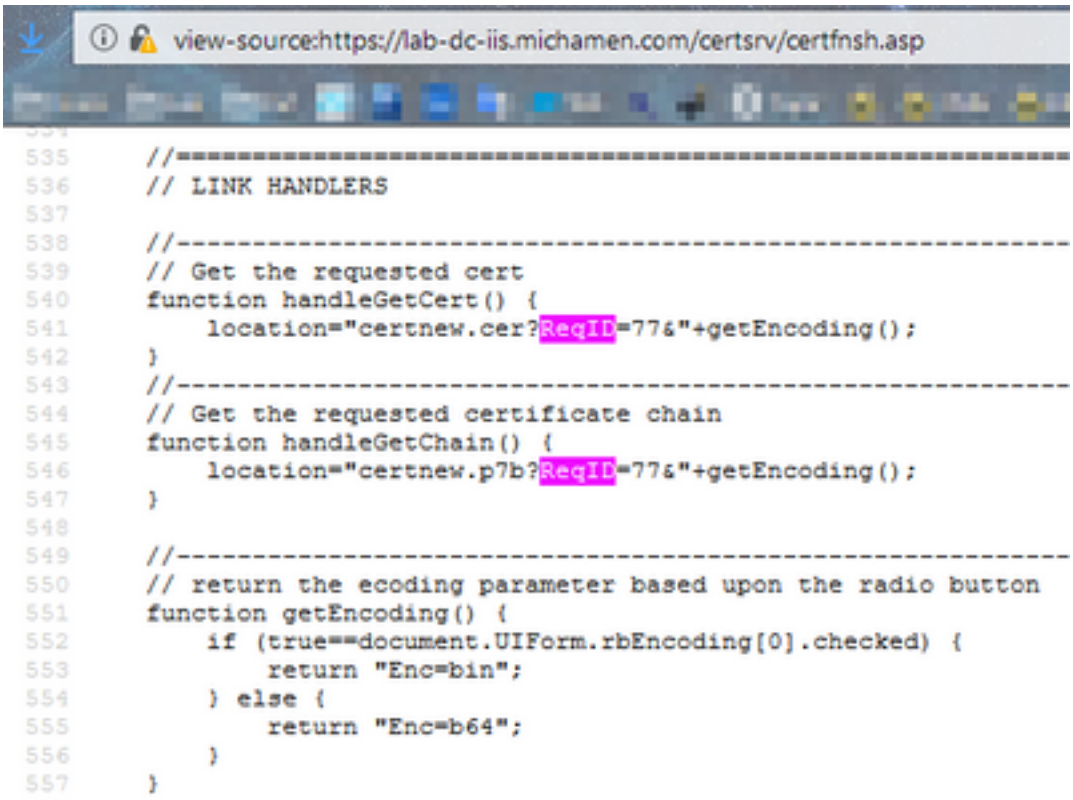


تتضمن إجابة الإرسال من **/certsrv/certfnsh.asp** معرف الطلب للشهادة الصادرة عن المرجع

المصدق. يتم عرض معرف الطلب في مستعرض ويب عند فحص كود مصدر الصفحة.



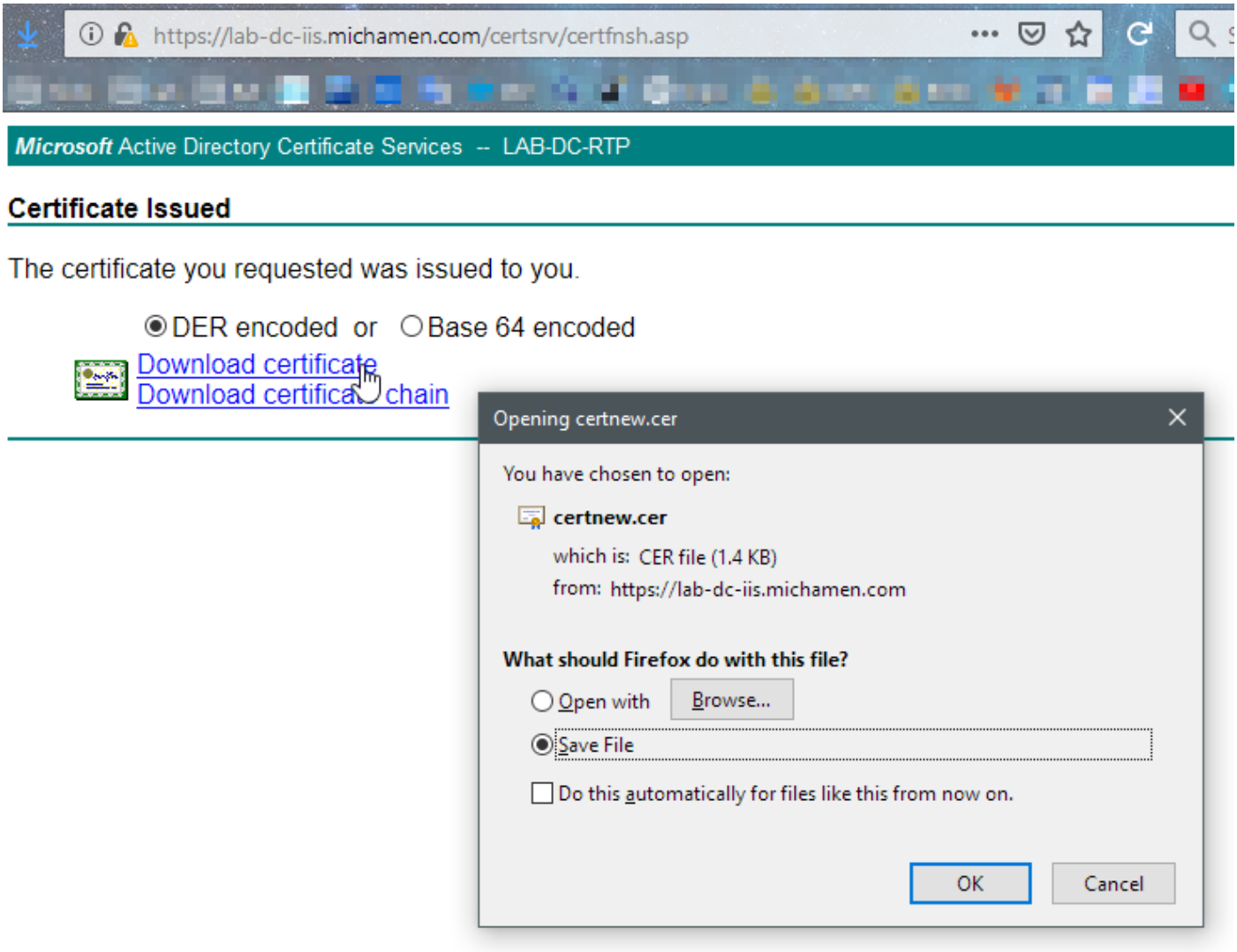
تلميح: البحث في مصدر الصفحة عن "ReqID"



/certsrv/certnew.cer

عند هذه النقطة، يكون عميل EST على علم بمعرف الطلب للشهادة الجديدة. يستخدم عميل EST **/certsrv/certnew.cer** لتمرير معرف الطلب وترميز الملف كمعلمات لتنزيل ملف الشهادة مع ملحق **.cer**.

وهذا يعادل ما يحدث في المستعرض لديك عند النقر فوق إرتباط **تنزيل الشهادة**.



لعرض محدد موقع المعلومات (URL) الخاص بالطلب والمعلمات، أستخدم وحدة تحكم المستعرض.

ملاحظة: يحدد المستعرض **سلة** لمعلمة الترميز في حالة تحديد ترميز DER؛ ومع ذلك، سيظهر ترميز Base64 ك b64.

المسارات/السجلات ذات الصلة لاستكشاف الأخطاء وإصلاحها

تساعد هذه السجلات في عزل معظم المشكلات.

سجلات CAPF

تتضمن سجلات CAPF التفاعلات مع الهواتف والحد الأدنى من تسجيل نشاط CiscoEST.

ملاحظة: تتوفر هذه السجلات للمجموعة عبر واجهة سطر الأوامر (CLI) أو أداة مراقبة الوقت الفعلي (RTMT). بسبب CSCvo28048 CAPF قد يظهر بين قائمة الخدمات في RTMT.

سجلات CiscoRA

غالبا ما يتم الإشارة إلى سجلات CiscoRA على أنها سجلات CES. تحتوي سجلات CiscoRA على نشاط بدء التشغيل الأولي ل CES وتعرض الأخطاء التي قد تحدث أثناء حدوث المصادقة مع CA.إذا تجحت المصادقة الأولية مع CA، فلن يتم تسجيل النشاط اللاحق في عمليات تسجيل الهاتف هنا. لذلك، تعمل سجلات CiscoRA كنقطة أولية جيدة لاستكشاف الأخطاء وإصلاحها.

ملاحظة: لا يمكن تجميع هذه السجلات إلا عبر واجهة سطر الأوامر (CLI) عند إنشاء هذه المستندات.

NGINX Error.log

NGINX error.log هو السجل الأكثر فائدة لهذه المهمة لأنه يسجل كل النشاط أثناء البدء بالإضافة إلى أي تفاعلات HTTP بين NGINX و CA جانبا؛ والذي يتضمن رموز الأخطاء التي تم إرجاعها من CA بالإضافة إلى تلك التي تم إنشاؤها بواسطة CiscoRA بعد معالجة الطلب.

ملاحظة: في وقت إنشاء هذا المستند، لا توجد طريقة لجمع هذه السجلات حتى من واجهة سطر الأوامر. يمكن تنزيل هذه السجلات فقط باستخدام حساب دعم عن بعد (جذر).

سجلات خادم ويب CA

تعد سجلات خادم ويب CA هامة لأنها تعرض أي نشاط HTTP بما في ذلك عناوين URL الخاصة بالطلب ورموز الاستجابة ومدة الاستجابة وحجم الاستجابة. يمكنك إستخدام هذه السجلات لربط التفاعلات بين CiscoRA و CA.

ملاحظة: سجلات خادم ويب ل CA في سياق هذا المستند هي سجلات MS IIS. إذا كانت ترخيص CA الأخرى مدعومة في المستقبل، فقد يكون لها ملفات سجل مختلفة تعمل كسجلات خادم ويب CA

مواقع ملفات السجل

سجلات CAPF:

- من الجذر: /var/log/active/cm/trace/capf/sdi/capf<*number*>.txt
- من واجهة سطر الأوامر (CLI): الحصول على ملف بتنسيق ActiveMog cm/trace/capf/sdi/capf*

ملاحظة: قم بتعيين مستوى تتبع CAPF إلى "مفصل" ثم أعد تشغيل خدمة CAPF قبل إجراء الاختبار.

Cisco RA:

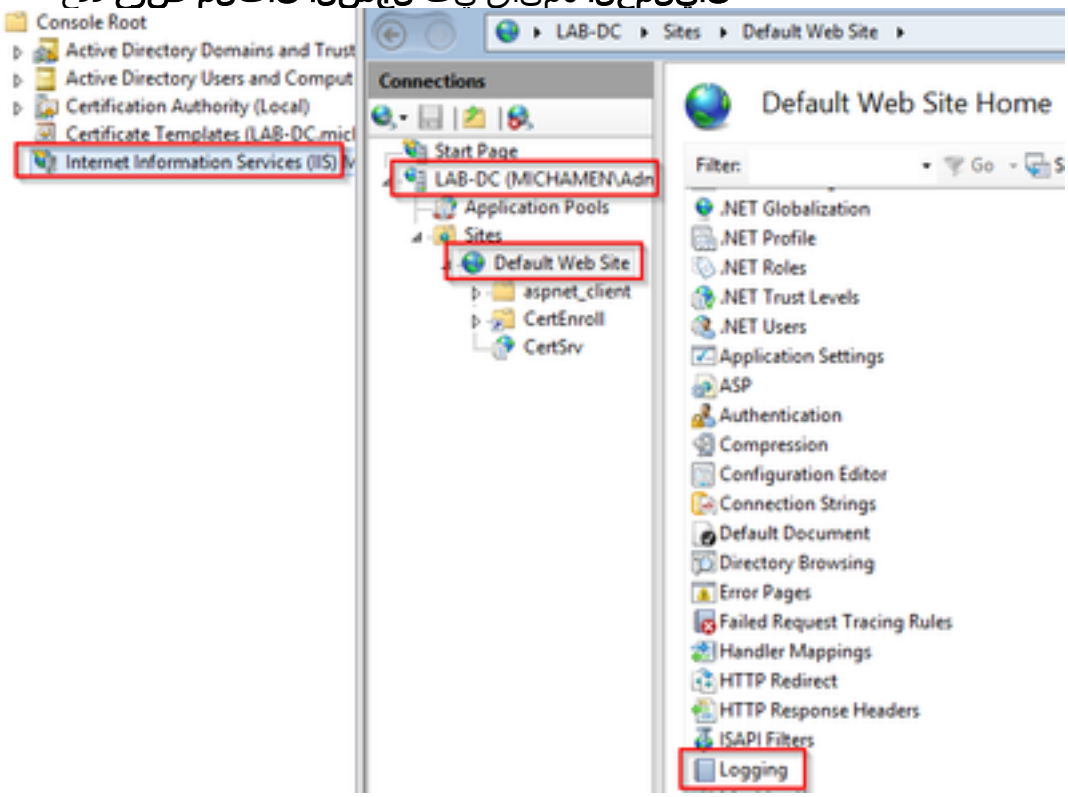
- من الجذر: /var/log/active/cm/trace/capf/sdi/nginx<*number*>.txt
- من واجهة سطر الأوامر (CLI): الحصول على ملف بتنسيق ActiveMog cm/trace/capf/sdi/nginx*

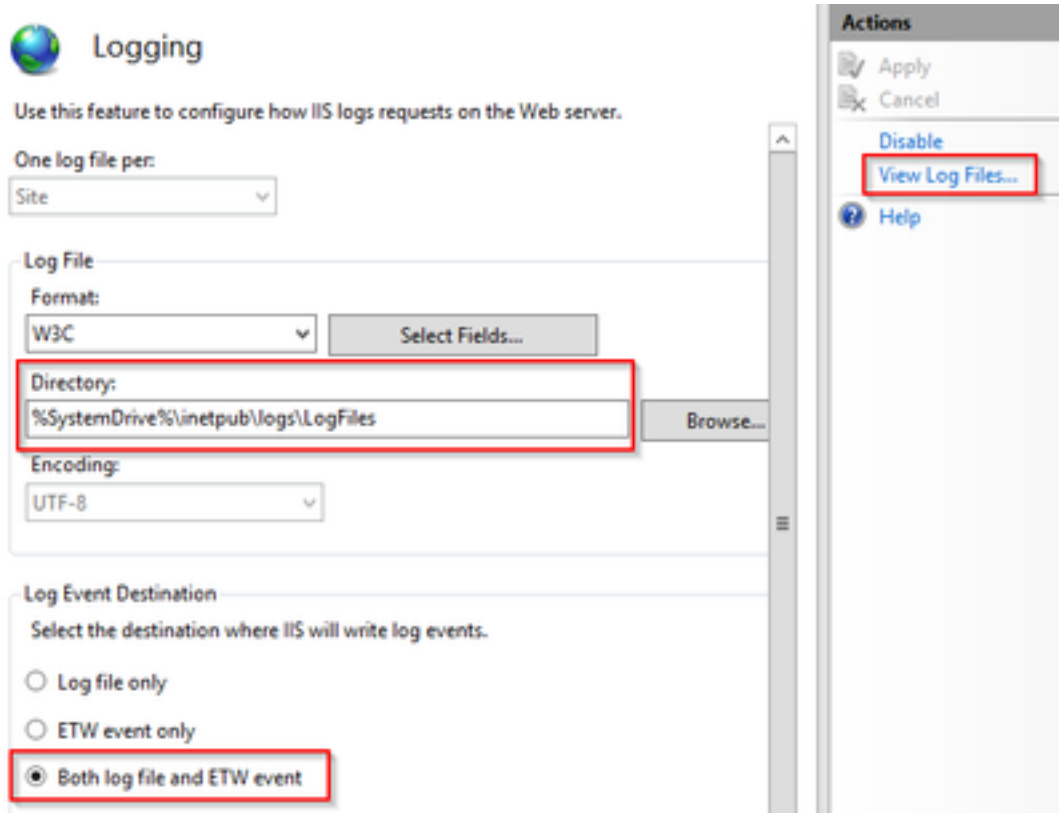
سجل أخطاء NGINX:

- من الجذر: /usr/local/thirdparty/nginx/install/logs/error.log
- غير متوفر من واجهة سطر الأوامر (CLI)

سجل MS IIS:

- فتح MMC
- حدد الأداة الإضافية **لخدمات معلومات الإنترنت (IIS)**
- انقر على اسم الخادم
- انقر فوق **موقع ويب الافتراضي**
- انقر نقرا مزدوجا فوق **التسجيل** للاطلاع على خيارات التسجيل
- حدد **عرض ملفات السجل** في قائمة **العمليات**





مثال سجل تحليل

يتم تشغيل الخدمات بشكل طبيعي

يتم بدء تشغيل CES كما هو موضح في سجل NGINX

ال تجمع معلومات كثيرة من هذا السجل. تظهر سلسلة الشهادات الكاملة المحملة في مخزن الثقة الخاص بها هنا ووحدة لحاوية الويب في حين أن الأخرى ل 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
```

يف NGINX error.log حضوم وه امك CES ليغشت ءدب متي

يف دامتعالا تانايبو ةداهشلا بلاق نيوكت مادختساب لوخدلا ليجست ةظحالم متي
انه ةزجوملا ةميلعتلا:

```
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
```

انه ةصاصقلا يف قدصملا عجرملا تاداهش ةلسلس عاجرتسإ ةظحالم متي:

```
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
```

تانايب عم هسفن URL مادختسإ نكمي .certnew.p7b فلم ىلع لوصحلا متي ،بلطلا حاجن دنع
بيو ضرعتسم نم certnew.p7b فلم ىلع لوصحلل بلاقلا دامتعا.

IIS تالجس يف حضوم وه امك (CES) لسلستلا تافلم ماظن ليغشت ءدب

لجسلا ةظحالم اضيأ متي.NGINX أطخ يف اهتيؤر مت يتلا CES ليغشت ءدب ثادحأ سفن
متيس هنأل نييفاضإ HTTP GET نيبلط IIS تالجس نمضتت ،كلذ عمو ؛IIS تالجس ىلع
بلطلا ىلع ةقداصملا درجمبو ؛401 ةباجتسإ لالخ نم بيو مداخ لبق نم لوألا بلطلا ضارتعا
متيس هداعإ ةيجوت هيجوتلا مادختساب ةباجتسإ 301:

```
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 تالجس يف حضوم وه امك CAPF ليغشت ءدب

مع معظم ما يحدث في سجلات CAPF الخاصة بعدة تشغيل CES يبدو نفس ما يحدث في السجلات الأخرى، ولكن ستلاحظ خدمة CAPF التي تكتشف الطريقة والتكوين لـ CA عبر الإنترنت:

```
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
```

الملاحظة المهمة التالية من السجلات هي عندما تقوم خدمة CAPF بتهيئة عميل EST الخاص بها.

```
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!!
```

عملية تثبيت LSC للهاتف

سجلات CAPF

يوصى بجمع جميع السجلات اللازمة وبدء التحليل باستعراض سجلات CAPF. وهذا يتيح لنا معرفة المرجع الزمني لهاتف معين.

يبدو الجزء الأولي من إرسال الإشارات مماثلا لطرق CAPF الأخرى باستثناء أن عميل EST الذي يعمل في خدمة CAPF سيقوم بالتسجيل مع CES قرب نهاية مربع الحوار (بعد توفير CSR بواسطة الهاتف).

```
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
```

بمجرد إسترداد CES للشهادة الموقعة على الهاتف، يتم تحويل الشهادة إلى تنسيق DER قبل توفيرها إلى الهاتف.

```
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
```

تتولى خدمة CAPF مرة أخرى وتحميل CSR من المكان الذي تمت كتابته إليه في المقطع السابق. ثم تقوم خدمة CAPF LSC الموقع إلى الهاتف. في نفس الوقت يتم أعلاه (/tmp/capf/cert/). حذف CSR للهاتف.

```
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
```

سجلات IIS

يعرض القصاصة أدناه الأحداث الموجودة في سجلات IIS لخطوات تثبيت LSC للهاتف كما هو موضح أعلاه.

```
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
```

المشكلات الشائعة

عندما يكون هناك خطأ في CES جانب، يتوقع أن يرى وه إنتاج مثل القصاصة أدناه في CAPF سجل. تأكد من فحص السجلات الأخرى لمتابعة تضييق المشكلة.

```
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
```

شهادة مرجع مصدق مفوقود في سلسلة مصدري شهادة هوية IIS

عندما ال تكون الشهادة الجذر وأ الشهادة الوسيطة، الموجودة في سلسلة الشهادات، موثوق بها من قبل CES، يطبع الخطأ "إسترداد سلسلة شهادة CA من CA" في سجالت NGINX.

```
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
```

خادم ويب يقدم شهادة موقعة ذاتيا

تم دعم إستخدام الشهادة الموقعة ذاتيا على IIS وسيالحاظ العمل حتى إذا تم تحميله ال كأمانة CAPF على CUCM. القصاصة أدناه من ال nginx سجل وهو يعرض ما يالحاظ عندما ال iis يستعمل شهادة ذاتية التوقيع.

```
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
```

عدم التطابق مع اسم مضيف URL والاسم الشائع

تطابق الاسم الشائع لشهادة IIS (lab-dc) مع FQDN لخادم URL الخاص بخدمة تسجيل ويب ال CA. للتحقق من صحة الشهادة التي تنتج FQDN لخادم عنوان URL يجب أن يطابق الاسم الشائع على الشهادة المستخدمة من قبل CA.

```
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
```

مشكلة في تحليل DNS

يتعذر على CiscoRA حل اسم المضيف ل CA عبر الإنترنت الذي تم تكوينه في معلمات الخدمة.

```
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
```

إصدار تواريخ صالحية الشهادة

عند عدم عمل بروتوكول وقت الشبكة (NTP) بشكل صحيح تحدث مشاكل في تواريخ الشهادة. يتم إجراء هذا الفحص بواسطة CES عند بدء التشغيل ويتم ملاحظته في سجلات NGINX.

```
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
```

تكوين قالب الشهادة غير صحيح

سيؤدي خطأ مطبعي في اسم الخادم لعملية التسجيل إلى حدوث حالات فشل. لن يتم تسجيل أي أخطاء في سجلات NGINX وأ CAPF لذلك يجب التحقق من 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
```

مهلة مصادقة CES

يظهر ال snipped أدناه وقت انتهاء عميل CES EST بعد المؤقت الافتراضي من 10 ثانية أثناء محاولة المصادقة الأولية لعميل CERTSRV.

```
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
```

ملاحظة: يتعلق CSCvo58656 وCSCvf83629 بكل امهم بمهلة مصادقة CES.

مهلة تسجيل CES

انتهت مهلة عميل CES EST بعد مصادقة ناجحة ولكن أثناء انتظار إستجابة لطلب تسجيل.

```
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
```

المحاذير المعروفة

RTMT لم تعد تدعم CSCvo28048 CAPF مدرجة في قائمة تجميع ملفات

يحتاج CSCvo58656 CAPF Online CA إلى خيار تكوين الحد الأقصى لمهلة الاتصال بين RA و CA

CSCvf83629 EST لا يحصل على EST_ERR_HTTP_WRITE أثناء التسجيل

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).