

# Resolución de problemas de CA en línea CAPF

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción general de los componentes de funciones](#)

[Autoridad de registro \(RA\)](#)

[Inscripción en transporte seguro \(EST\)](#)

[libEST](#)

[Motor-X \(NGINX\)](#)

[Servicio de inscripción de certificados \(CES\)](#)

[Función de proxy de autoridad de certificados \(CAPF\)](#)

[Diagrama de flujo de mensajes](#)

[Explicación de flujo de mensajes](#)

[/.well-known/est/simpleenroll](#)

[/certsrv](#)

[/certsrv/certrqxt.asp](#)

[/certsrv/certfnsh.asp](#)

[/certsrv/certnew.cer](#)

[Registros/seguimientos relevantes para la resolución de problemas](#)

[Registros CAPF](#)

[Registros de CiscoRA](#)

[NGINX error.log](#)

[Registros de CA Web Server](#)

[Ubicaciones del archivo de registro](#)

[Registros CAPF:](#)

[Cisco RA:](#)

[Registro De Errores Nginx:](#)

[Registro MS IIS:](#)

[Ejemplo de análisis de registro](#)

[Servicios que se inician normalmente](#)

[Inicio de CES tal y como se ve en el registro de NGINX](#)

[CES Starting Up \(Inicio de CES\) como se ve en NGINX error.log](#)

[CES que se inicia como se ve en los registros IIS](#)

[Inicio de CAPF como se ve en los registros CAPF](#)

[Operación de Instalación de LSC del Teléfono](#)

[Registros CAPF](#)

[Registros IIS](#)

[Problemas comunes](#)

[Falta el certificado de CA en la cadena del emisor del certificado de identidad de IIS](#)

[Servidor Web que presenta un certificado firmado automáticamente](#)

[Falta de coincidencia con el nombre de host de URL y el nombre común](#)

[Problema de resolución DNS](#)

[Problema con las Fechas de Validez del Certificado](#)

[Error de configuración de la plantilla de certificado](#)

[Tiempo de espera de autenticación CES](#)

[Tiempo de espera de inscripción CES](#)

[Advertencias conocidas](#)

[Información Relacionada](#)

## Introducción

Este documento describe la solución de problemas para la función de renovación e inscripción automáticas de la función de proxy de la autoridad certificadora (CAPF). Esta función también se conoce como CAPF Online CA.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados
- Seguridad de Cisco Unified Communications Manager (CUCM)

### Componentes Utilizados

La información de este documento se basa en la versión 12.5 de CUCM, ya que la función CAPF Online CA se introdujo en CUCM 12.5.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Descripción general de los componentes de funciones

### Autoridad de registro (RA)

RA es una autoridad de una red que verifica las solicitudes de los usuarios de un certificado digital y le indica a la autoridad de certificación (CA) que emita el certificado. Las RA forman parte de una infraestructura de clave pública (PKI).

### Inscripción en transporte seguro (EST)

EST es un protocolo definido en la solicitud de comentario (RFC) 7030 para la inscripción de certificados para clientes que utilizan mensajes de administración de certificados sobre CMS (CMC) a través de seguridad de la capa de transporte (TLS) y protocolo de transferencia de hipertexto (HTTP). EST utiliza un modelo cliente/servidor donde el cliente EST envía solicitudes

de inscripción y el servidor EST envía respuestas con los resultados.

## libEST

libEST es la biblioteca para la implementación de EST por parte de Cisco. libEST permite aprovisionar certificados X509 en dispositivos de usuario final y dispositivos de infraestructura de red. CiscoEST y CiscoRA implementan esta biblioteca.

## Motor-X (NGINX)

NGINX es un servidor web y proxy inverso similar a Apache. NGINX se utiliza para la comunicación HTTP entre CAPF y CES, así como para la comunicación entre CES y el servicio de inscripción web de CA. Cuando libEST funciona en modo de servidor, se necesita un servidor web para manejar las solicitudes TCP en nombre de libEST.

## Servicio de inscripción de certificados (CES)

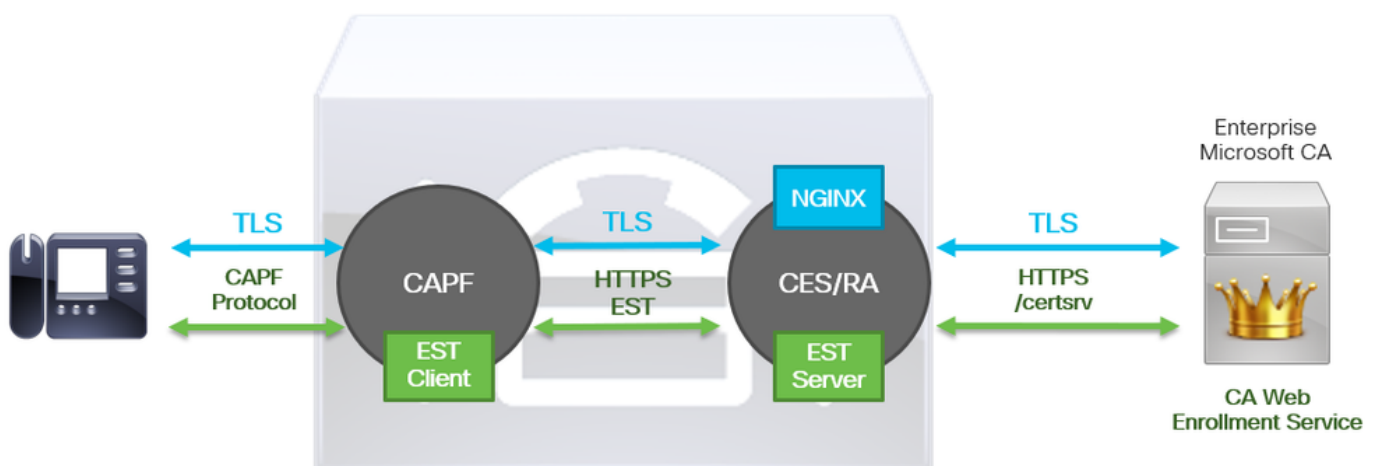
CES es el servicio en CUCM que actúa como RA entre el servicio CAPF y la CA. CES también se denomina CiscoRA o simplemente RA. CES utiliza NGINX como servidor Web porque CES implementa libEST en el modo de servidor para actuar como RA.

## Función de proxy de autoridad de certificados (CAPF)

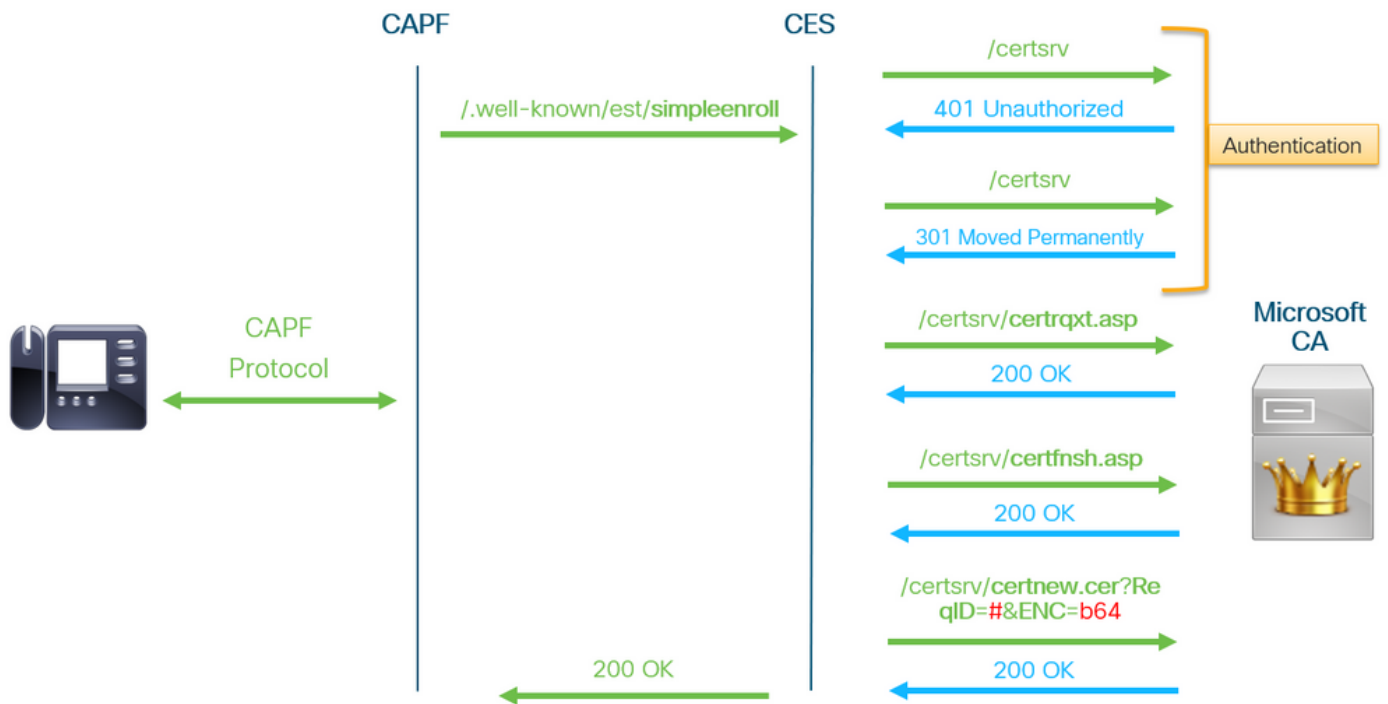
CAPF es un servicio de CUCM con el que los teléfonos interactúan al realizar solicitudes de inscripción de certificados. CAPF interactúa con el CES en nombre de los teléfonos. En esta función, CAPF implementa libEST en el modo cliente para registrar los certificados de los teléfonos a través de CES.

En resumen, se explica cómo se implementa cada componente:

1. El teléfono envía una solicitud de certificado a CAPF
2. CAPF implementa CiscoEST (modo cliente) para comunicarse con CES
3. CES implementa CiscoRA (modo servidor) para procesar y responder a las solicitudes del cliente EST
4. CES/CiscoRA se comunica con el servicio de inscripción web de la CA a través de HTTPS



# Diagrama de flujo de mensajes



## Explicación de flujo de mensajes

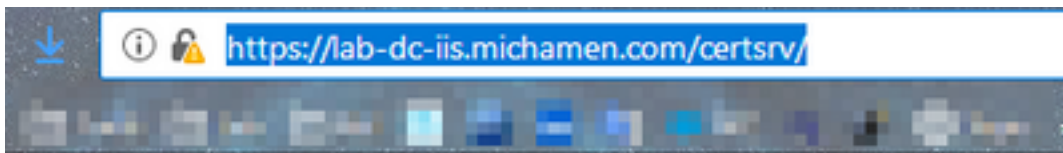
### `/.well-known/est/simpleenroll`

El cliente EST utiliza esta URL para enviar una llamada API que solicita la inscripción de certificados del servidor EST. Una vez que el servidor EST recibe la llamada de la API, iniciará el proceso de inscripción de certificados, que incluye la comunicación HTTPS con el servicio de inscripción web de la CA. Si el proceso de inscripción es exitoso y el servidor EST recibe el nuevo certificado, CAPF procederá a cargar el certificado y lo enviará de vuelta al teléfono IP.

### `/certsrv`

El cliente EST utiliza la URL `/certsrv` para autenticar e iniciar una sesión con la CA.

La siguiente imagen es un ejemplo de la URL `/certsrv` de un navegador web. Esta es la página de inicio de Servicios de Certificate Server.



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 other tasks.

You can also use this Web site to download a certificate authority certificate.

For more information about Active Directory Certificate Services, see the help topics.

### 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**

La URL **/certsrv/certrqxt.asp** se utiliza para iniciar la solicitud de un nuevo certificado. El cliente EST utiliza **/certsrv/certrqxt.asp** para enviar la CSR, el nombre de la plantilla de certificado y los atributos deseados.

La siguiente imagen es un ejemplo de **/certsrv/certrqxt.asp** desde un navegador web.

↓ ⓘ <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:

Submit >

### /certsrv/certifnsh.asp

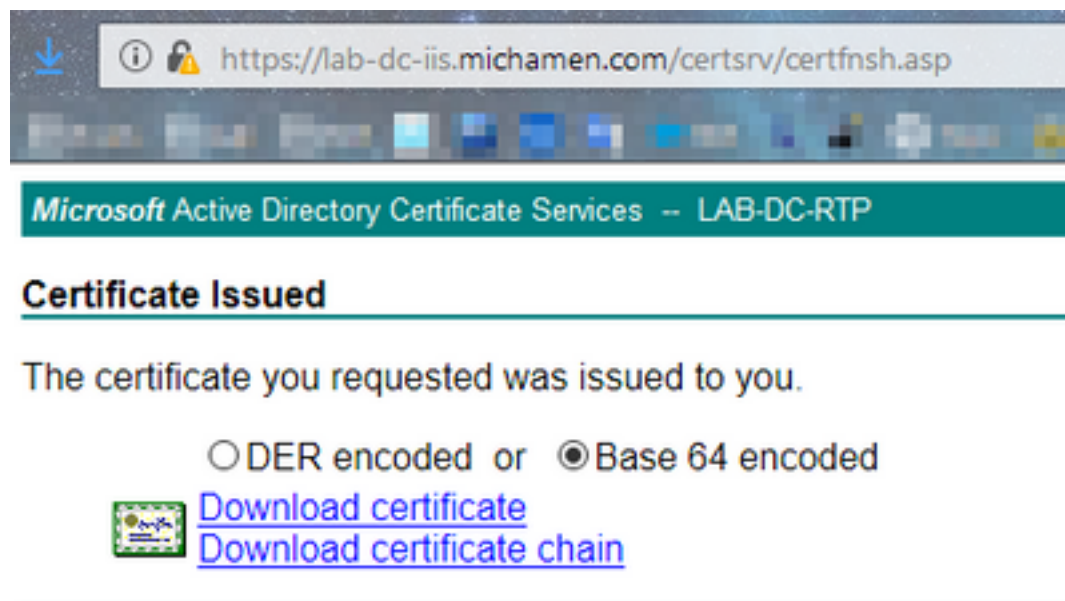
La URL `/certsrv/certifnsh.asp` se utiliza para enviar datos para la solicitud de certificado; que incluye el CSR, el nombre de la plantilla de certificado y los atributos deseados. Para ver el envío, utilice **Developer Tools** para abrir la consola del explorador antes de que los datos se envíen a través de la página `certrqxt.asp`.

La siguiente imagen es un ejemplo de los datos mostrados en la consola del explorador.

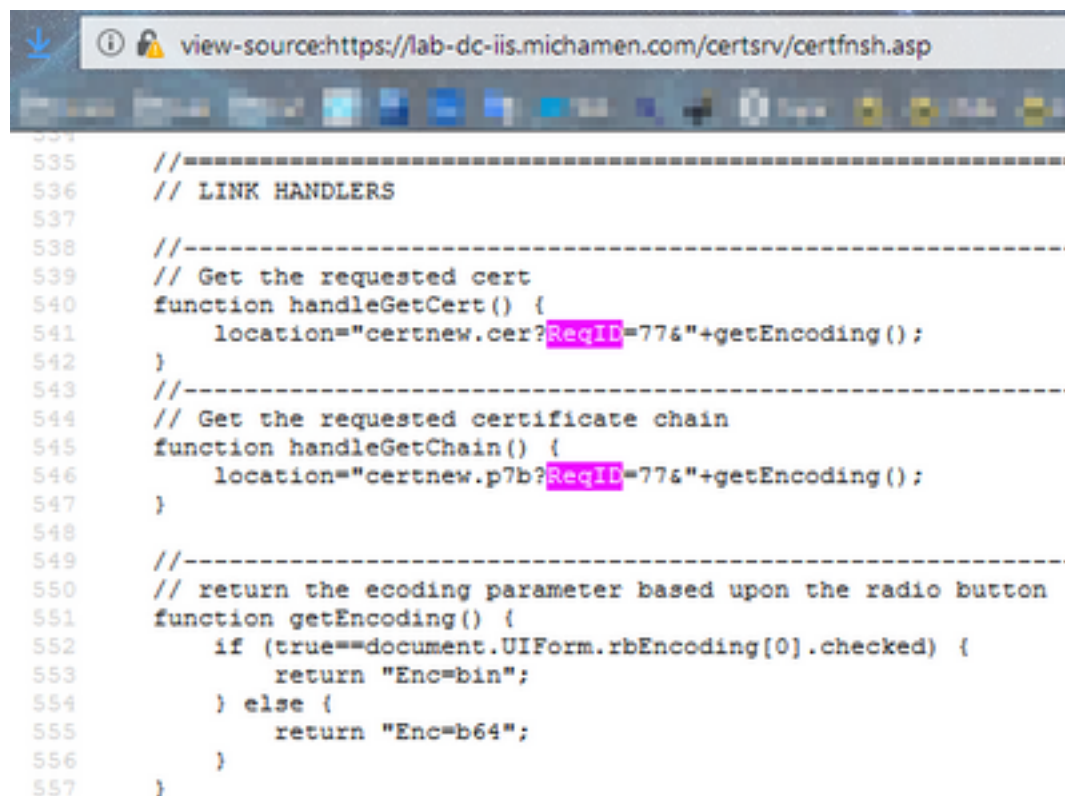
```
POST https://lab-dc-iis.michamen.com/certsrv/certifnsh.asp
Headers Cookies Params Response Timings Security
Filter request parameters
Form data
Mode: newreq
CertRequest: -----BEGIN+CERTIFICATE+REQUEST----- MIIC7TCCAdUCAQAwBDELMAKGA1UEBHMVb3R0LWVudDIzLWVudC5FTDZl
CgkCAQEAtk9AcGKcfshtIzI8X9Iyke9p8sVp9wevUunn2N10K3PEqR8cTe2a+S3h0 D18rjaSyM+ThJg0j4b/8unl
09Pmzqlddx/keJ83pT9YBEE0NRmsG8T15339555x9cRvter4yr+/vM0N1daIn oEP7GUv8dErnAXDRj538HQ
IDAQABoEAWPgy3ko2IhvcNAQkOHTeWZAd BgNVHSUEFjAUBgggr8gEFBQcDAQYIKwYBBQUHwIwDgyDVR0PAQH/
CSQGSIB3DQEBCwUAA4IBAQBpHR5QmFQk8r1wdCElP3DjSPqeYg8hY4hVunMH+49m ZfFKGUXJtxy03SPa9VAdR4I
N/yintaI7ewqXspYhP5QmPlsnxgDKjwf1xJLjTVdWfBod/w0rphn73S1bbWQdu1 6p46yFt0jujx1ur3P1f0mH
rYfZ5XrcgIY0hyrd1aBry0K0002onf8IQLFqF6u0wV1/M2Me0T05GKNI9+S2WC2 y1grvVqN/vwdrb5E+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
```

La respuesta de envío de `/certsrv/certifnsh.asp` incluye la ID de solicitud del certificado emitido por

la CA. La ID de solicitud se muestra en un explorador Web cuando se inspecciona el código fuente de la página.



**Consejo:** Buscar el origen de la página para "ReqID"



**/certsrv/certnew.cer**

En este punto, el cliente EST es consciente del ID de solicitud para el nuevo certificado. El cliente EST utiliza **/certsrv/certnew.cer** para pasar el ID de solicitud y la codificación de archivo como parámetros para descargar el archivo de certificado con la extensión **.cer**.


Esto equivale a lo que sucede en su navegador cuando hace clic en el enlace **Descargar certificado**.

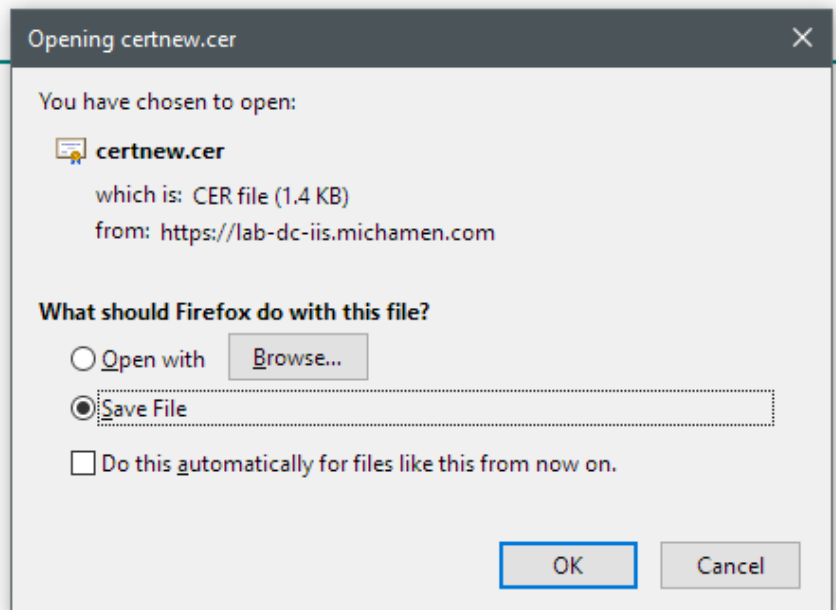


## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)  
[Download certificate chain](#)



Para ver la dirección URL y los parámetros de la solicitud, utilice la consola del explorador.

**Nota:** El explorador especifica **bin** para el parámetro de codificación si se selecciona la codificación DER; sin embargo, la codificación Base64 se mostrará como b64.



## Registros/seguimientos relevantes para la resolución de problemas

Estos registros ayudan a aislar la mayoría de los problemas.

### Registros CAPF



Los registros CAPF incluyen interacciones con teléfonos y registro mínimo de la actividad CiscoEST.

**Nota:** Estos registros están disponibles para su recopilación a través de la interfaz de línea de comandos (CLI) o la herramienta de supervisión en tiempo real (RTMT). Debido a [CSCvo28048](#) CAPF no puede aparecer entre la lista de servicios en RTMT.

## Registros de CiscoRA

Los registros de CiscoRA suelen denominarse registros de CES. Los registros de CiscoRA contienen la actividad de inicio inicial de CES y muestran los errores que pueden surgir mientras se produce la autenticación con la CA. Si la autenticación inicial con la CA es correcta, la actividad subsiguiente para las inscripciones del teléfono no se registra aquí. Por lo tanto, los registros de CiscoRA sirven como un buen punto inicial para resolver problemas.

**Nota:** Estos registros sólo se pueden recopilar a través de la CLI a partir de esta creación de documentos.

## NGINX error.log

NGINX error.log es el registro más útil para esta función ya que registra toda la actividad durante el inicio, así como cualquier interacción HTTP entre NGINX y el lado CA; que incluye los códigos de error devueltos por la CA así como los generados por CiscoRA después de procesar la solicitud.

**Nota:** En el momento de crear este documento, no hay forma de recopilar estos registros ni siquiera desde CLI. Estos registros sólo se pueden descargar mediante una cuenta de soporte remoto (root).

## Registros de CA Web Server

Los registros de CA Web Server son importantes, ya que muestran cualquier actividad HTTP, incluidas las URL de solicitud, los códigos de respuesta, la duración de respuesta y el tamaño de respuesta. Puede utilizar estos registros para correlacionar las interacciones entre CiscoRA y la CA.

**Nota:** Los registros de CA Web Server en el contexto de este documento son los registros de MS IIS. Si se admiten otras CA web en el futuro, es posible que tengan archivos de registro diferentes que sirvan como registros del servidor web de la CA

## Ubicaciones del archivo de registro

### Registros CAPF:

- De la raíz: `/var/log/active/cm/trace/capf/sdi/capf<number>.txt`
- Desde CLI: `file get avelog cm/trace/capf/sdi/capf*`

**Nota:** Establezca el nivel de seguimiento CAPF en "Detallado" y reinicie el servicio CAPF antes de realizar la prueba.

## Cisco RA:

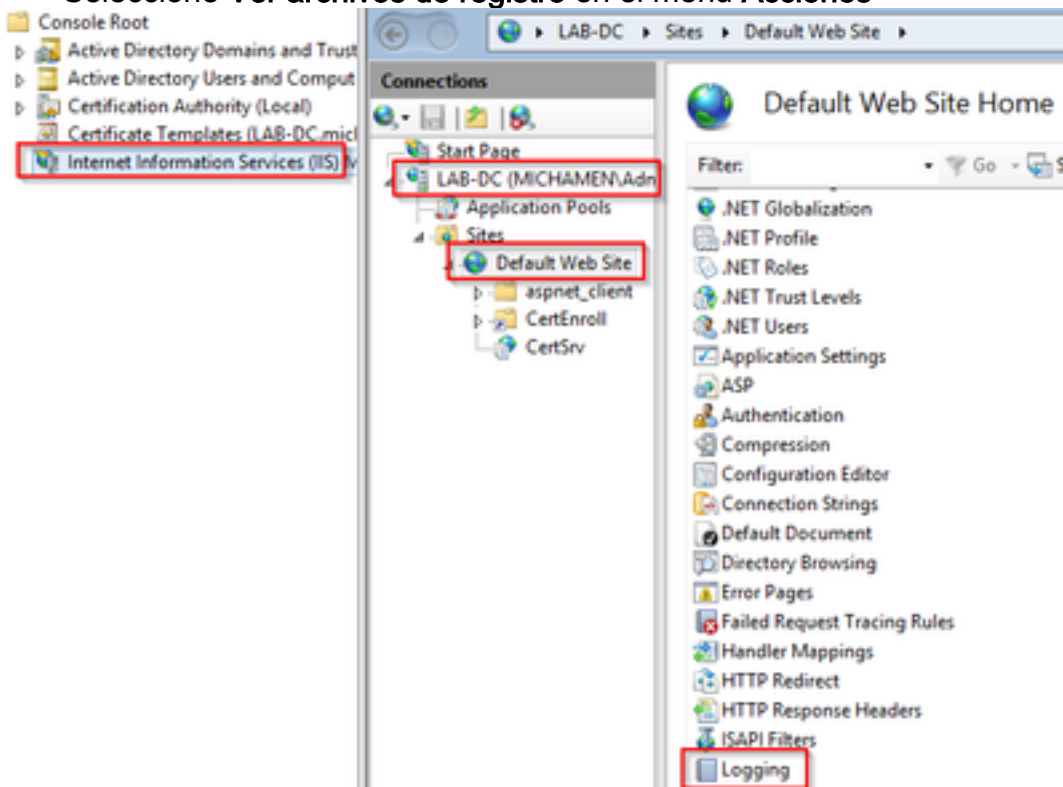
- De la raíz: `/var/log/active/cm/trace/capf/sdi/nginx<number>.txt`
- Desde CLI: `file get activelog cm/trace/capf/sdi/nginx*`

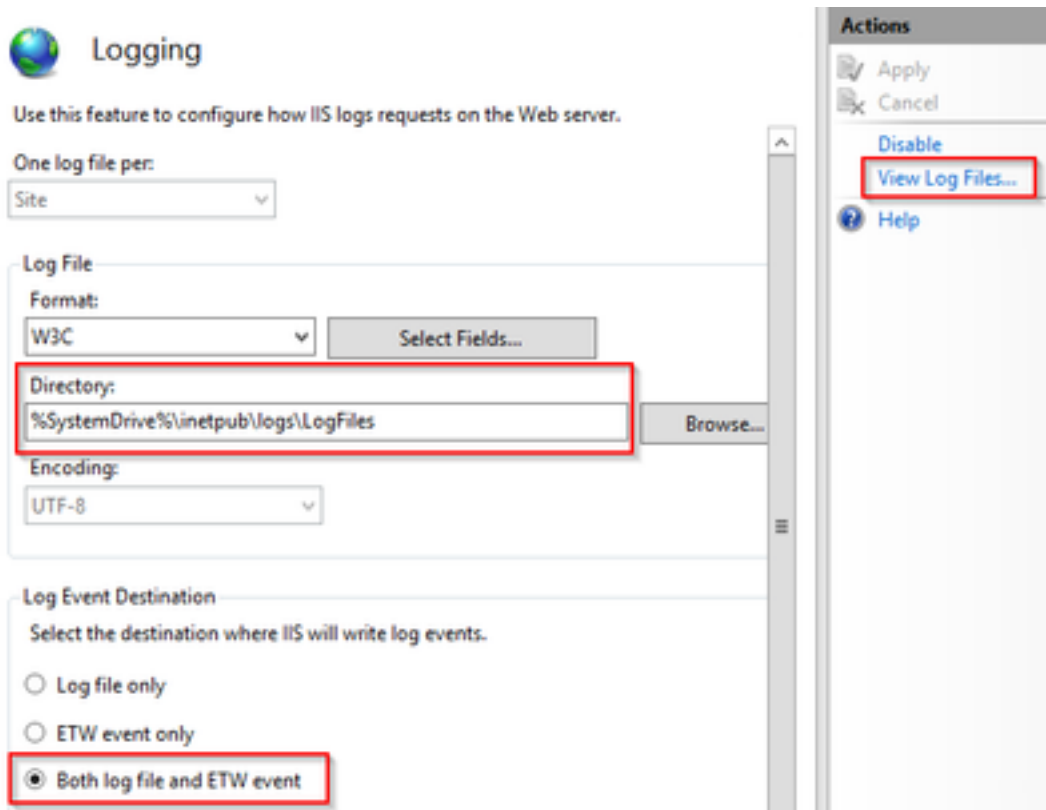
## Registro De Errores Nginx:

- De la raíz: `/usr/local/thirdparty/nginx/install/logs/error.log`
- No disponible desde CLI

## Registro MS IIS:

- Abrir MMC
- Seleccione el complemento **Servicios de Internet Information Server (IIS)**
- Haga clic en el nombre del servidor
- Haga clic en **Sitio Web predeterminado**
- Haga doble clic en **Registro** para ver las opciones de registro
- Seleccione **Ver archivos de registro** en el menú **Acciones**





## Ejemplo de análisis de registro

### Servicios que se inician normalmente

### Inicio de CES tal y como se ve en el registro de NGINX

Se recopila poca información de este registro. La cadena de certificados completa que se carga en su almacén de confianza se ve aquí y una es para el contenedor web mientras que la otra es para 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] ssl_init_cert_store: Adding cert to store (/O=Cisco/CN=ACT2 SUDI CA)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco
Manufacturing CA)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Manufacturing CA
SHA2)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco Root CA
2048)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Root CA M2)
nginx: [warn] ssl_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][ssl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco/CN=ACT2 SUDI
CA)
***EST [INFO][ssl_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 Comenzando como se ve en el error NGINX.log

El inicio de sesión con la configuración de la plantilla de certificado y las credenciales se observa en el fragmento de código aquí:

```

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

```

La recuperación de la cadena de certificados de CA se observa en el fragmento de código aquí:

```

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

```

Cuando la solicitud se realiza correctamente, se obtiene el archivo certnew.p7b. La misma URL con las credenciales de plantilla se puede utilizar para obtener el archivo certnew.p7b de un navegador web.

## Inicio de CES tal como se ve en los registros IIS

Los mismos eventos de inicio de CES que se ven en el error.log de NGINX también se observan en los registros de IIS; sin embargo, los registros IIS incluyen 2 solicitudes GET HTTP más porque el servidor Web desafiará la primera solicitud mediante una respuesta 401; y una vez autenticado, un pedido será redirigido usando una respuesta 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

```

## Inicio de CAPF tal como se ve en los registros CAPF

La mayor parte de lo que ocurre en los registros CAPF para CES que se inician parece lo mismo que en los otros registros; pero observará que el servicio CAPF detecta el método y la configuración para la CA en línea:

```
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
```

La siguiente observación importante de los registros es cuando el servicio CAPF se inicializa como cliente EST.

```
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!!
```

## Operación de Instalación de LSC del Teléfono

### Registros CAPF

Se recomienda recolectar todos los registros necesarios e iniciar el análisis con una revisión de los registros CAPF. Esto nos permite conocer la referencia horaria de un teléfono específico.

La parte inicial de la señalización se ve igual que con otros métodos CAPF, excepto que el cliente EST que se ejecuta en el servicio CAPF realizará la inscripción con CES hacia el final del diálogo (después de que el teléfono haya proporcionado la CSR).

```

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

```

Una vez que el CES ha recuperado el certificado firmado del teléfono, el certificado se convierte en formato DER antes de que se proporcione al teléfono.

```

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

```

El servicio CAPF toma el control de nuevo y carga el CSR desde la ubicación a la que se escribió en el fragmento anterior (/tmp/capf/cert/). A continuación, el servicio CAPF proporciona el LSC firmado al teléfono. Al mismo tiempo, se elimina la CSR del teléfono.

```

14:05:05.289 |<--findAndPost
14:05:05.289 |-->debug
14:05:05.289 |   debug added 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

```

## Registros IIS

El siguiente fragmento de código muestra los eventos en los registros de IIS para los pasos de instalación de LSC de un teléfono, como se explicó anteriormente.

```
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
```

## Problemas comunes

Siempre que haya un error en el lado de CES, se espera que vea la salida como el fragmento de abajo en los registros CAPF. Asegúrese de verificar otros registros para continuar reduciendo el problema.

```
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 added 10 to readset
12:38:04.779 |<--debug
```

**Falta el certificado de CA en la cadena del emisor del certificado de identidad de IIS**



Cuando CES no confía en un certificado raíz o un certificado intermedio, que está en la cadena de certificados, el error "No se puede recuperar la cadena de certificados de CA de CA" se imprime en los registros de 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
```

## Servidor Web que presenta un certificado firmado automáticamente

No se admite el uso de un certificado autofirmado en IIS y anotará el trabajo incluso si se carga como CAPF-trust en CUCM. El fragmento siguiente proviene de los registros nginx y muestra lo que se observa cuando IIS utiliza un certificado autofirmado.

```
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
```

## Falta de coincidencia con el nombre de host de URL y el nombre común

El nombre común (lab-dc) del certificado de IIS no coincide con el FQDN dentro de la dirección URL del servicio de suscripción Web de la CA. Para que la validación de certificados se realice correctamente con el FQDN dentro de la URL, debe coincidir con el nombre común del certificado utilizado por la 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
```

## Problema de resolución DNS

CiscoRA no puede resolver el nombre de host de la CA en línea configurada en los parámetros de servicio.

```
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
```

## Problema con las Fechas de Validez del Certificado

Cuando el protocolo de tiempo de red (NTP) no funciona correctamente, se producen problemas con las fechas de validez de los certificados. Este control es realizado por CES al inicio y se observa en los registros de 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
```

## Error de configuración de la plantilla de certificado

Un error en el nombre dentro de los parámetros de servicio causará fallas. No se registrarán errores en los registros CAPF ni NGINX, por lo que es necesario verificar el registro de errores NGINX.

```
***EST [INFO][est_enroll_auth:356]--> TLS: no peer certificate
2019/02/27 16:53:28 [warn] 3187#0: *2 openssl_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
```

## Tiempo de espera de autenticación CES

El siguiente fragmento muestra el tiempo de espera del cliente CES EST después del temporizador predeterminado de 10 segundos durante el proceso inicial de autenticación 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
```

**Nota:** [CSCvo58656](#) y [CSCvf83629](#) ambos pertenecen al tiempo de espera de autenticación CES.

## Tiempo de espera de inscripción CES

El tiempo de espera del cliente CES EST después de una autenticación exitosa pero mientras espera una respuesta a una solicitud de inscripción.

```
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
```

## Advertencias conocidas

El servicio [CSCvo28048](#) CAPF ya no aparece en el menú RTMT Collect Files .

[CSCvo58656](#) CAPF CA Online necesita la opción para configurar el tiempo de espera máximo de conexión entre RA y CA

[CSCvf83629](#) EST Server obtiene EST\_ERR\_HTTP\_WRITE durante la inscripción

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)