Troubleshooting de CAPF Online CA

Contents

Introduction

Este documento descreve a solução de problemas para o recurso de Registro e Renovação Automáticos da Função de Proxy da Autoridade de Certificação (CAPF). Esse recurso também é chamado de CAPF Online CA.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados
- Segurança do Cisco Unified Communications Manager (CUCM)

Componentes Utilizados

As informações neste documento são baseadas na versão 12.5 do CUCM, pois o recurso CAPF Online CA foi introduzido no 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.

Visão geral dos componentes do recurso

Autoridade de registro (RA)

O RA é uma autoridade em uma rede que verifica as solicitações dos usuários por um certificado digital e instrui a autoridade de certificação (CA) a emitir o certificado. Os RAs fazem parte de uma infraestrutura de chave pública (PKI).

Inscrição no Secure Transport (EST)

EST é um protocolo definido na solicitação de comentário (RFC - Request for Comment) 7030 para inscrição de certificado para clientes que usam mensagens de Gerenciamento de Certificado sobre CMS (CMC - Certificate Management over CMS) sobre TLS (Transport Layer Security) e HTTP (HyperText Transfer Protocol). O EST usa um modelo cliente/servidor em que o cliente

EST envia solicitações de inscrição e o servidor EST envia respostas com os resultados.

libEST

libEST é a biblioteca para a implementação do EST pela Cisco. libEST permite que os certificados X509 sejam provisionados em dispositivos de usuário final e dispositivos de infraestrutura de rede. Esta biblioteca é implementada pelo CiscoEST e CiscoRA.

Engine-X (NGINX)

O NGINX é um servidor Web e proxy reverso semelhantes ao Apache. O NGINX é usado para comunicação HTTP entre CAPF e CES, bem como comunicação entre CES e o CA Web Enrollment Service. Quando a libEST opera no modo de servidor, um servidor web é necessário para processar solicitações TCP em nome da libEST.

Serviço de inscrição de certificado (CES)

CES é o serviço no CUCM que atua como o RA entre o serviço CAPF e a CA. O CES também é conhecido como CiscoRA ou simplesmente RA. O CES usa o NGINX como servidor Web porque o CES implementa o libEST no modo de servidor para atuar como RA.

Função de proxy da autoridade de certificação (CAPF)

CAPF é um serviço CUCM com o qual os telefones interagem ao executar solicitações de registro de certificado. O CAPF interage com o CES em nome dos telefones. Neste modelo de recurso, o CAPF implementa o libEST no modo cliente para inscrever os certificados dos telefones através do CES.

Em resumo, aqui está como cada componente é implementado:

1. O telefone envia uma solicitação de certificado ao CAPF
2. O CAPF implementa o CiscoEST (modo cliente) para se comunicar com o CES
3. O CES implementa o CiscoRA (modo servidor) para processar e responder às solicitações do cliente EST
4. CES/CiscoRA se comunica com o serviço de inscrição na Web da CA via HTTPS

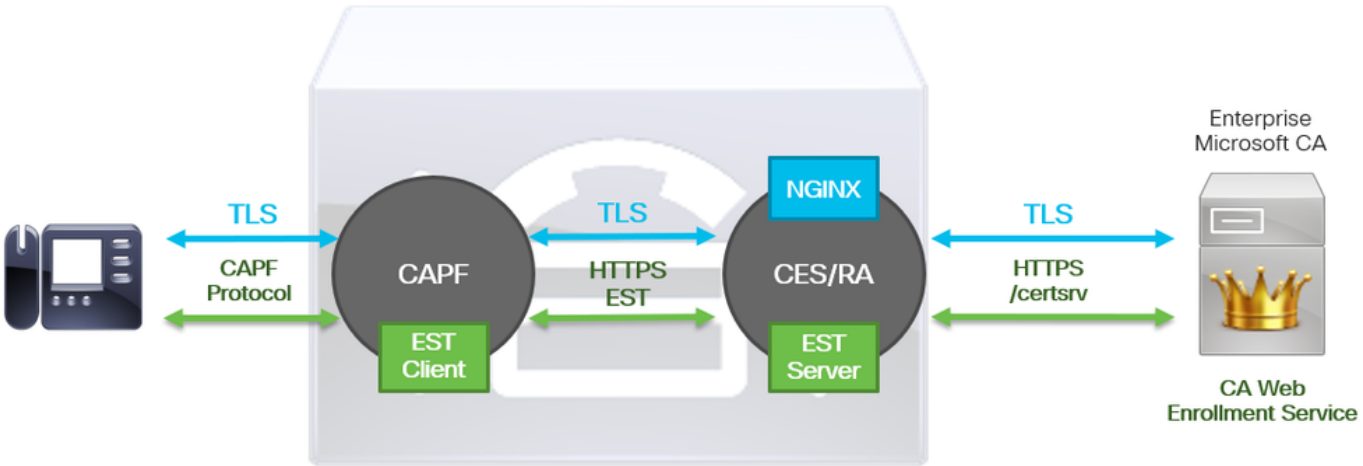
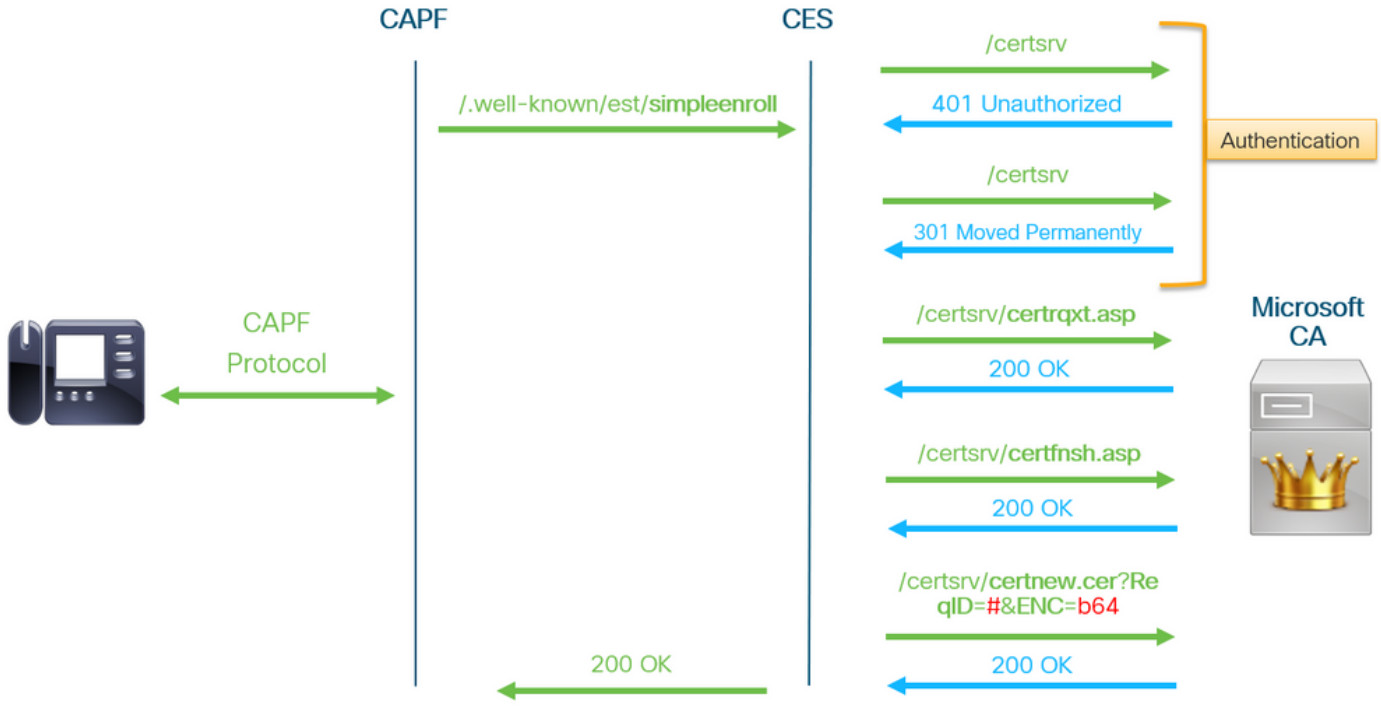


Diagrama de fluxo de mensagem



Explicação do fluxo de mensagem

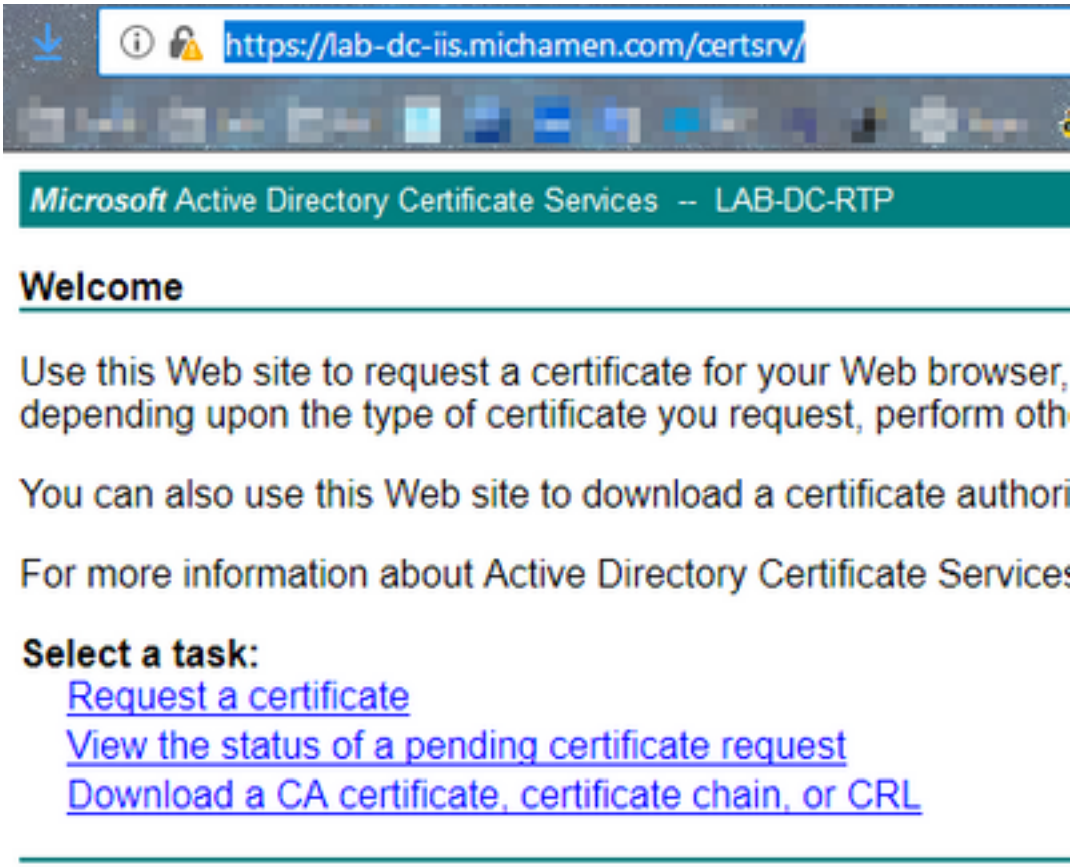
/.well-known/est/simpleenroll

O cliente EST usa este URL para enviar uma chamada de API que solicita a inscrição de certificado do servidor EST. Quando o servidor EST receber a chamada de API, ele iniciará o processo de inscrição de certificado que inclui a comunicação HTTPS com o serviço de inscrição na Web da CA. Se o processo de inscrição for bem-sucedido, e o servidor EST receber o novo certificado, o CAPF continuará a carregar o certificado e devolvê-lo ao telefone IP.

/certsrv

A URL **/certsrv** é usada pelo cliente EST para autenticar e iniciar uma sessão com a CA.

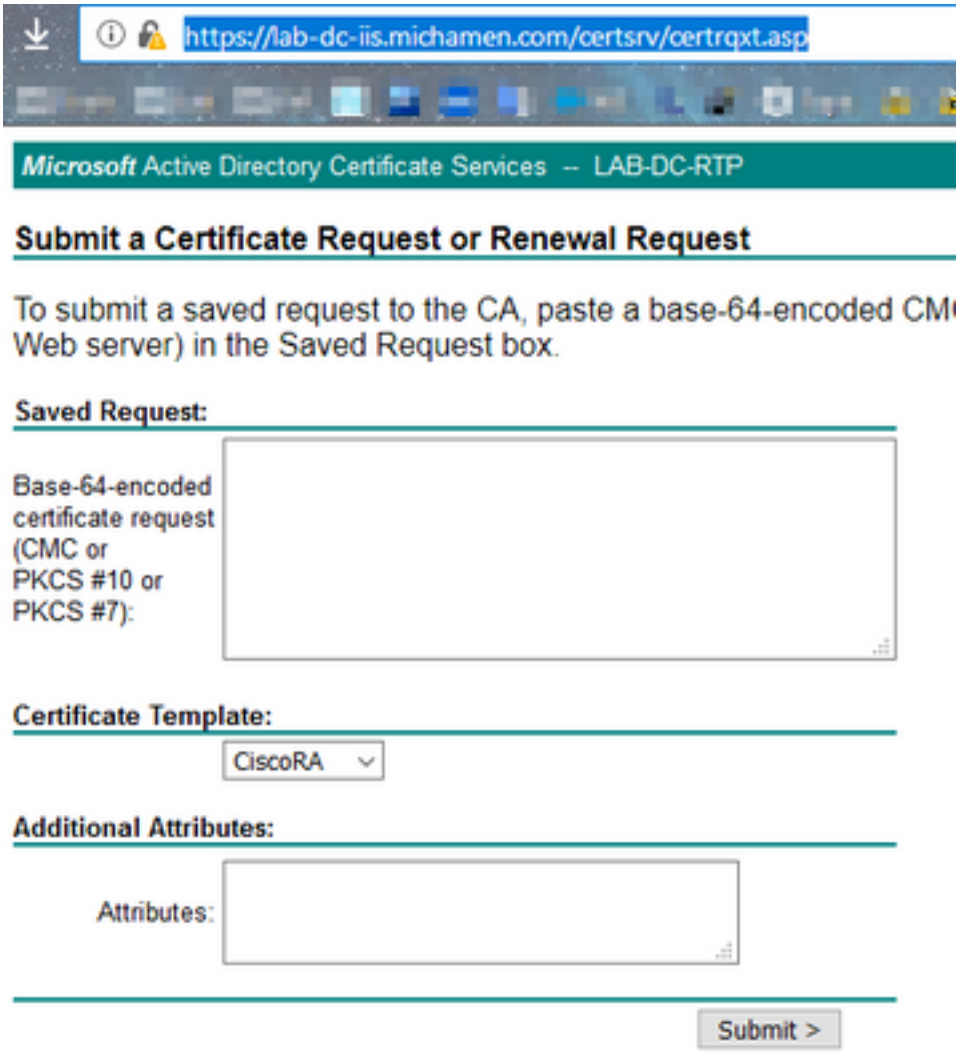
A imagem abaixo é um exemplo de **/certsrv** URL de um navegador da Web. Esta é a página inicial dos Serviços de Certificado.



/certsrv/certrqxt.asp

O URL **/certsrv/certrqxt.asp** é usado para iniciar a solicitação de um novo certificado. O cliente EST usa **/certsrv/certrqxt.asp** para enviar o CSR, o nome do modelo de certificado e todos os atributos desejados.

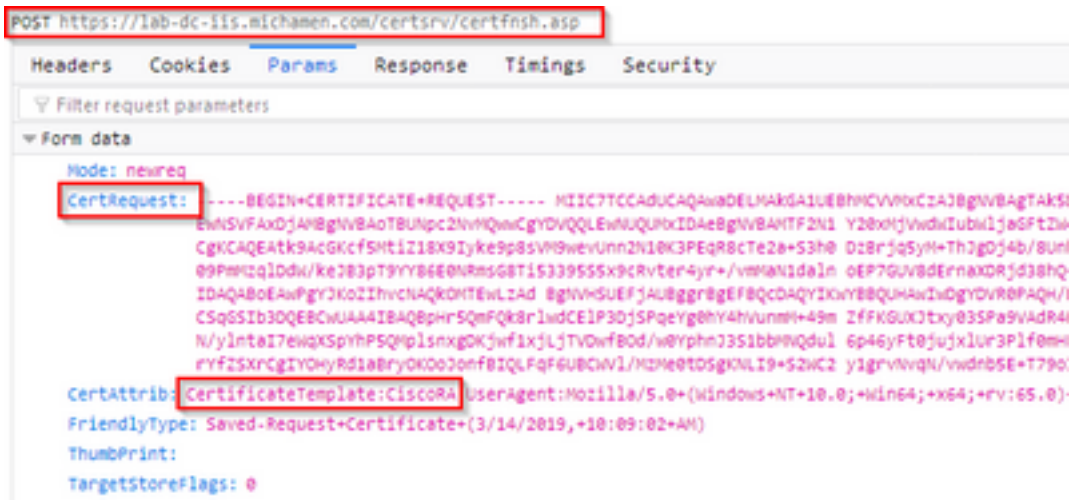
A imagem abaixo é um exemplo de **/certsrv/certrqxt.asp** de um navegador da Web.



/certsrv/certfnsh.asp

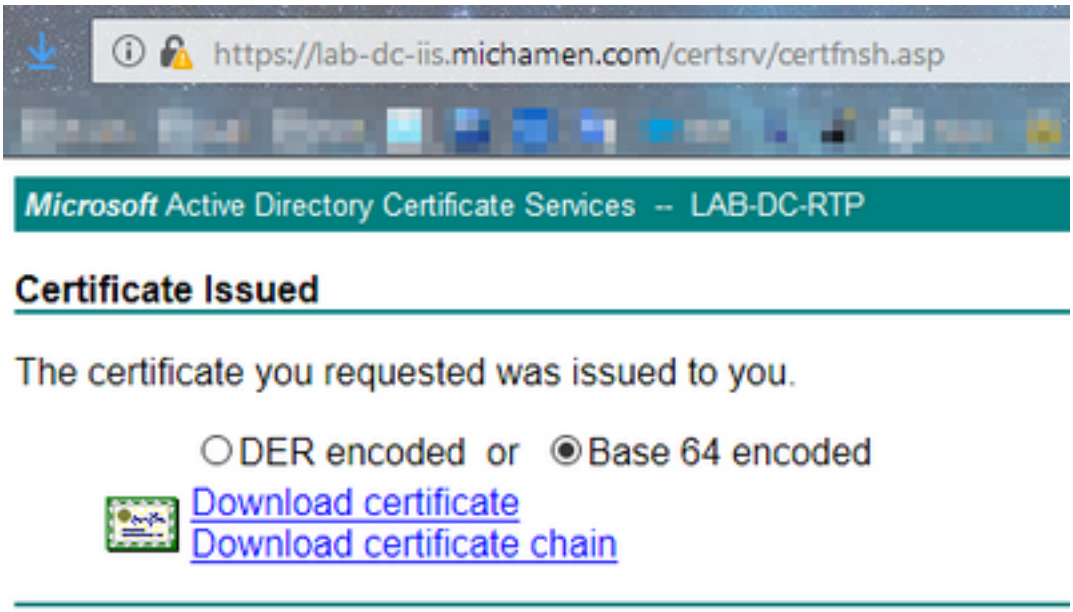
O URL **/certsrv/certfnsh.asp** é utilizado para enviar dados para a solicitação de certificado; que inclui o CSR, o nome do modelo de certificado e todos os atributos desejados. Para visualizar o envio, use as **Ferramentas de desenvolvedor** do navegador para abrir o console do navegador antes que os dados sejam enviados através da página *certrqxt.asp*.

A imagem abaixo é um exemplo dos dados exibidos no console do navegador.

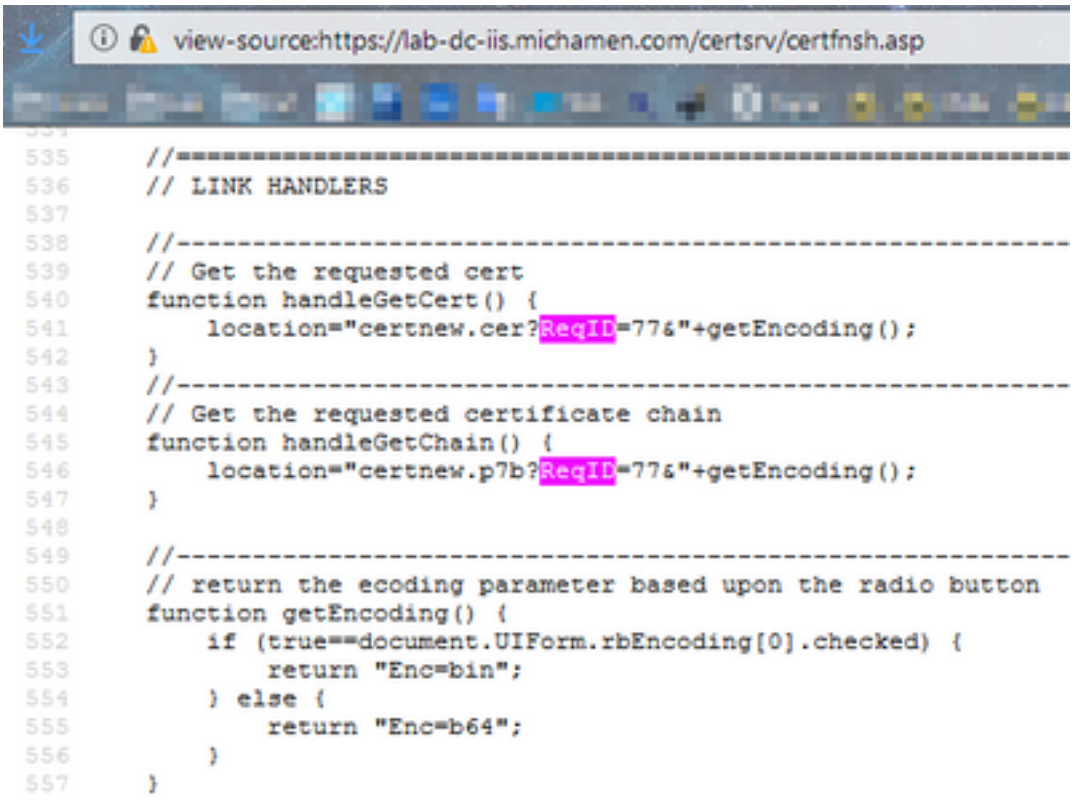


A resposta de envio de **/certsrv/certfnsh.asp** inclui a ID de solicitação do certificado emitido pela

CA. A ID da solicitação é vista em um navegador da Web quando o código-fonte da página é inspecionado.



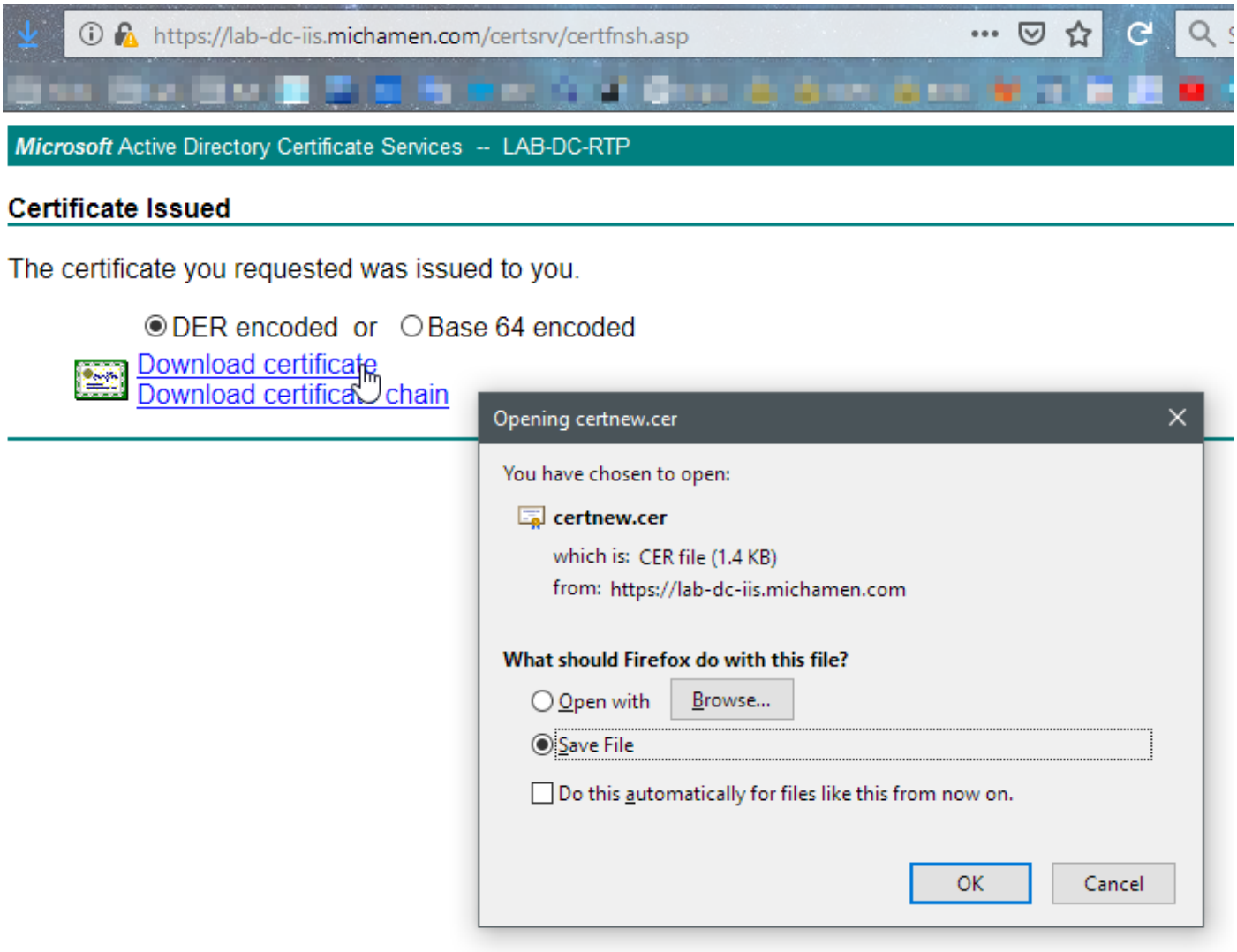
Tip: Procure "ReqID" na origem da página



/certsrv/certnew.cer

Neste ponto, o cliente EST está ciente da ID de solicitação do novo certificado. O cliente EST usa **/certsrv/certnew.cer** para passar a ID de solicitação e a codificação de arquivo como parâmetros para baixar o arquivo de certificado com a extensão **.cer**.

Isso equivale ao que acontece no seu navegador quando você clica no link **Download Certificate**.



Para exibir a URL e os parâmetros da solicitação, use o console do navegador.

> **Note**: O navegador especifica **bin** para o parâmetro de codificação se a codificação DER estiver selecionada; entretanto, a codificação Base64 será exibida como b64.

Rastreamentos/registros relevantes para solução de problemas

Esses registros ajudam no isolamento da maioria dos problemas.

Logs CAPF

Os registros CAPF incluem interações com telefones e registro mínimo da atividade CiscoEST.

Note: Esses registros estão disponíveis para coleta via CLI (Command Line Interface, interface de linha de comando) ou RTMT (Real Time Monitoring Tool, ferramenta de monitoramento em tempo real). Devido ao CSCvo28048, o CAPF pode não ser mostrado entre a lista de serviços na RTMT.

Logs CiscoRA

Os registros CiscoRA são frequentemente chamados de registros CES. Os registros do CiscoRA contêm a atividade inicial de inicialização do CES e exibem erros que podem surgir enquanto ocorre a autenticação com a CA.Se a autenticação inicial com a CA for bem-sucedida, a atividade subsequente para as inscrições do telefone não é registrada aqui. Portanto, os registros do CiscoRA servem como um bom ponto inicial para solucionar problemas.

Note: Esses registros só podem ser coletados via CLI a partir dessa criação de documentos.

erro de NGINX.log

NGINX error.log é o log mais útil para esse recurso, pois registra todas as atividades durante a inicialização, bem como todas as interações HTTP entre o NGINX e o lado CA; que inclui códigos de erro retornados da CA, bem como os gerados pelo CiscoRA após o processamento da solicitação.

Note: No momento da criação deste documento, não há como coletar esses registros mesmo da CLI. Esses registros só podem ser baixados usando uma conta de suporte remoto (raiz).

Registros do servidor Web da AC

Os registros do Servidor Web da CA são importantes, pois exibem qualquer atividade HTTP, incluindo URLs de solicitação, códigos de resposta, duração da resposta e tamanho da resposta. Você pode usar esses logs para correlacionar interações entre o CiscoRA e a CA.

Note: Os logs do CA Web Server no contexto deste documento são os logs do MS IIS. Se outras ACs da Web forem suportadas no futuro, elas poderão ter arquivos de log diferentes que servem como logs do CA Web Server

Locais dos arquivos de log

Registros CAPF:

- Da raiz: /var/log/ative/cm/trace/capf/sdi/capf<*number*>.txt
- Da CLI: arquivo get ativelog cm/trace/capf/sdi/capf*

Note: Defina o nível de rastreamento CAPF como "Detalhado" e reinicie o serviço CAPF antes de executar o teste.

RA da Cisco:

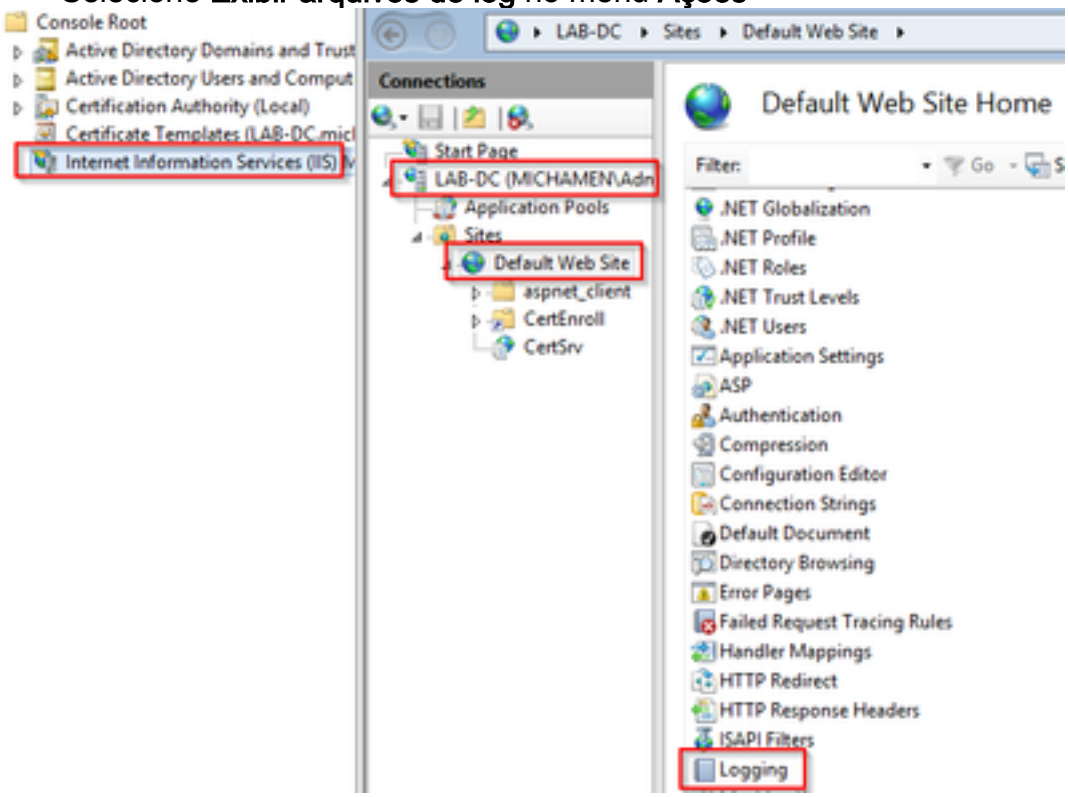
- Da raiz: /var/log/ative/cm/trace/capf/sdi/nginx<*number*>.txt
- Da CLI: file get ativelog cm/trace/capf/sdi/nginx*

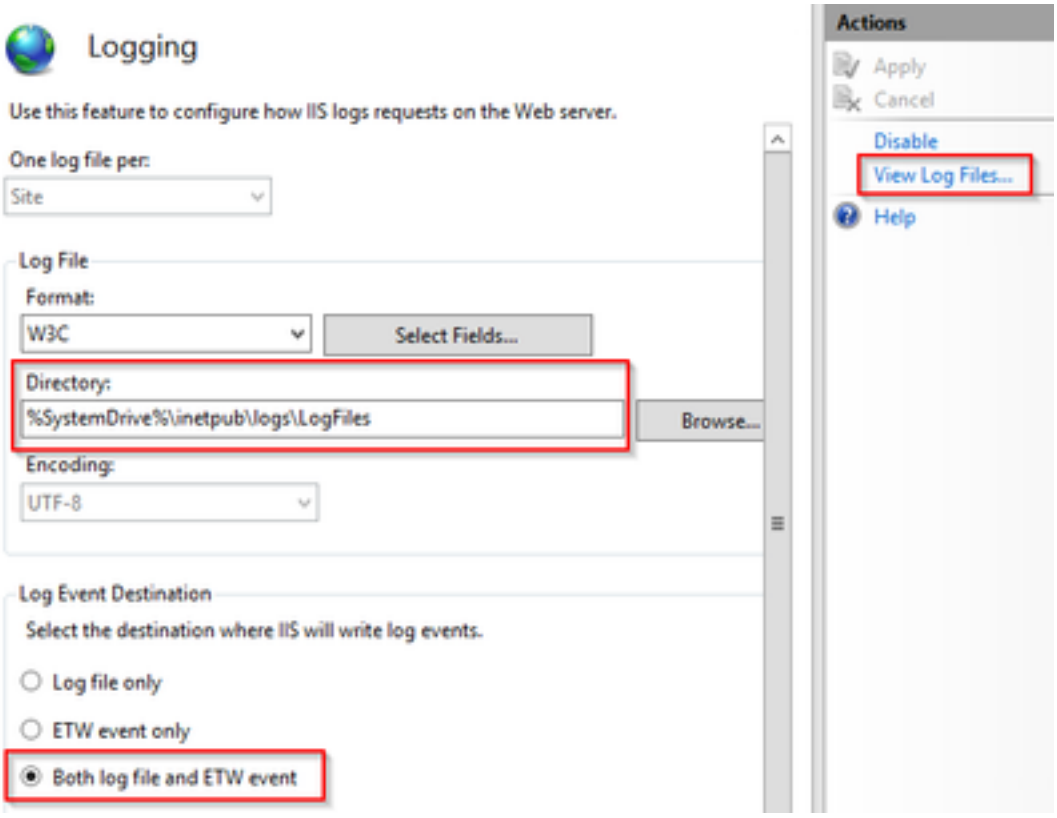
Nginx Error Log (Registro de Erros do Nginx):

- Da raiz: /usr/local/thirdparty/nginx/install/logs/error.log
- Não disponível na CLI

Log do MS IIS:

- Abrir MMC
- Selecione o snap-in **Internet Information Services (IIS)**
- Clique no nome do servidor
- Clique em **Web Site Predefinido**
- Clique duas vezes em **Log** para ver as opções de registro
- Selecione **Exibir arquivos de log** no menu **Ações**





Exemplo de análise de log

Serviços que iniciam normalmente

CES Startup como visto no registro do NGINX

Poucas informações são coletadas desse registro. A cadeia completa de certificados carregada em seu repositório confiável é vista aqui e uma é para o contêiner da Web enquanto a outra é 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] 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 Startup como visto no erro NGINX.log

O login usando a configuração e as credenciais do modelo de certificado é observado no trecho aqui:

```
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
```

A recuperação da cadeia de certificados CA é observada no trecho aqui:

```
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
```

Quando a solicitação é bem-sucedida, o arquivo certnew.p7b é obtido. O mesmo URL com as credenciais do modelo pode ser usado para obter o arquivo certnew.p7b de um navegador da Web.

CES iniciando conforme visto nos registros do IIS

Os mesmos eventos de inicialização CES vistos no arquivo de erro do NGINX.log também são observados nos registros do IIS; no entanto, os registros do IIS incluem mais 2 solicitações HTTP GET, pois a primeira solicitação será desafiada pelo servidor Web por meio de uma resposta 401; e uma vez autenticado, um pedido será redirecionado utilizando uma resposta 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 Starting Up (CAPF iniciando) conforme visto nos registros CAPF

A maior parte do que ocorre na inicialização dos registros CAPF para CES parece igual ao que ocorre nos outros registros; mas você perceberá que o serviço CAPF está detectando o método e a configuração para CA on-line:

```
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
```

A próxima observação importante dos registros é quando o serviço CAPF inicializa seu 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!!
```

Operação de instalação do LSC do telefone

Logs CAPF

Érecomendável coletar todos os registros necessários e iniciar a análise com uma revisão dos registros CAPF. Isso nos permite saber a referência de hora de um telefone específico.

A parte inicial da sinalização tem a mesma aparência de outros métodos CAPF, exceto que o cliente EST em execução no serviço CAPF executará a inscrição com CES no final da caixa de diálogo (depois que o CSR tiver sido fornecido pelo telefone).

```
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
```

Depois que o CES recuperou o certificado assinado do telefone, o certificado é convertido no formato DER antes de ser fornecido ao telefone.

```
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
```

O serviço CAPF assume novamente e carrega o CSR a partir do local onde foi gravado no trecho acima (/tmp/capf/cert/). O serviço CAPF fornece o LSC assinado ao telefone. Ao mesmo tempo, o CSR do telefone é excluído.

```
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
```

Logs do IIS

O trecho abaixo exibe os eventos nos registros do IIS para as etapas de instalação do LSC de um telefone, como explicado acima.

```
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 comuns

Sempre que houver um erro no lado CES, é esperado que ele veja a saída como o trecho abaixo nos registros CAPF. Verifique outros registros para continuar a reduzir o 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 addded 10 to readset
12:38:04.779 |<--debug
```

Falta certificado CA na cadeia de emissor do certificado de identidade IIS

Quando um certificado raiz ou um certificado intermediário, que está na cadeia de certificados, não é confiável pelo CES, o erro "Unable to recover CA Cert chain from CA" é impresso nos registros iniciais.

```
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 apresenta um certificado com assinatura automática

O uso de um certificado autoassinado no IIS não é suportado e observará o trabalho mesmo se carregado como CAPF-trust no CUCM. O snippet abaixo é dos registros iniciais e exibe o que é observado quando o IIS está usando um certificado autoassinado.

```
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
```

Incompatibilidade com o nome de host da URL e o nome comum

O Nome Comum do certificado IIS (lab-dc) não corresponde ao FQDN dentro da URL do serviço de Inscrição na Web da AC. Para que a validação do certificado seja bem-sucedida, o FQDN dentro da URL deve corresponder ao Nome Comum no certificado usado pela 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 resolução de DNS

O CiscoRA não consegue resolver o nome de host da CA on-line configurada nos parâmetros de serviço.

```
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 com datas de validade do certificado

Quando o Network Time Protocol (NTP) não está funcionando, problemas com datas de validade do certificado ocorrem. Essa verificação é realizada pelo CES na inicialização e é observada nos registros do 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
```

Erro de configuração do modelo de certificado

Um erro de digitação no nome dentro dos parâmetros de serviço causará falhas. Nenhum erro será registrado nos registros CAPF ou NGINX, portanto é necessário verificar o arquivo 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
```

Tempo limite de autenticação CES

O snipped abaixo mostra o tempo limite do cliente EST CES após o temporizador padrão de 10 segundos durante o processo de autenticação inicial do 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
```

Note: CSCvo58656 e CSCvf83629 pertencem ao tempo limite de autenticação CES.

Tempo limite de inscrição CES

Tempo limite do cliente EST CES após uma autenticação bem-sucedida, mas enquanto espera por uma resposta a uma solicitação de inscrição.

```
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
```

Caveats conhecidos

O serviço CSCvo28048 CAPF não está mais listado no menu RTMT Collect Files

CSCvo58656 CAPF A CA online precisa de opção para configurar o tempo limite máximo de conexão entre RA e CA

CSCvf83629 EST Server obtendo EST_ERR_HTTP_WRITE durante a inscrição

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems