Dépannage de CAPF Online CA

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Présentation des composants de la fonction
Autorité d'enregistrement (RA)
Inscription sur le transport sécurisé (EST)
libEST
Engine-X (NGINX)
Service d'inscription de certificat (CES)
Fonction de proxy d'autorité de certification (CAPF)
Diagramme de flux de messages
Explication du flux de messages
/.well-known/est/simpleenroll
/certsrv
/certsrv/certrqxt.asp
/certsrv/certfnsh.asp
/certsrv/certnew.cer
Suivis/journaux pertinents pour le dépannage
Journaux CAPF
Journaux CiscoRA
Erreur NGINX.log
Journaux du serveur Web AC
Emplacement des fichiers journaux
Journaux CAPF :
Cisco RA :
Journal d'erreurs Nginx :
Journal IIS MS :
Exemple d'analyse de journal
Services démarrant normalement
CES Démarrage tel qu'indiqué dans le journal NGINX
CES Démarrage tel qu'indiqué dans le fichier error.log de NGINX
CES Démarrage tel qu'il apparaît dans les journaux IIS
Démarrage du protocole CAPF tel qu'il apparaît dans les journaux CAPF
Opération d'installation LSC du téléphone
Journaux CAPF
Journaux IIS
Problèmes courants
Certificat CA manquant dans la chaîne d'émetteurs du certificat d'identité IIS
Serveur Web présentant un certificat auto-signé

Incompatibilité avec le nom d'hôte de l'URL et le nom commun
Problème de résolution DNS
Problème avec les dates de validité du certificat
Erreur de configuration du modèle de certificat
Délai d'authentification CES
Délai d'inscription CES
Caveats connus
Informations connexes

Introduction

Ce document décrit le dépannage de la fonction CAPF (Certificate Authority Proxy Function) d'inscription et de renouvellement automatiques. Cette fonctionnalité est également appelée CA CAPF Online.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats
- Sécurité de Cisco Unified Communications Manager (CUCM)

Components Used

Les informations de ce document sont basées sur CUCM version 12.5, car la fonctionnalité CAPF Online CA a été introduite dans CUCM version 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.

Présentation des composants de la fonction

Autorité d'enregistrement (RA)

RA est une autorité d'un réseau qui vérifie les demandes d'un certificat numérique de l'utilisateur et demande à l'autorité de certification d'émettre le certificat. Les AR font partie d’une infrastructure à clé publique (ICP).

Inscription sur le transport sécurisé (EST)

EST est un protocole défini dans la requête de commentaire (RFC) 7030 pour l'inscription de certificats pour les clients qui utilisent des messages CMS (Certificate Management over CMS) sur TLS (Transport Layer Security) et HTTP (HyperText Transfer Protocol). L'EST utilise un modèle client/serveur où le client EST envoie des demandes d'inscription et le serveur EST envoie

des réponses avec les résultats.

libEST

libEST est la bibliothèque pour la mise en oeuvre d'EST par Cisco. libEST permet de provisionner des certificats X509 sur des périphériques d'utilisateur final et d'infrastructure réseau. Cette bibliothèque est mise en oeuvre par CiscoEST et CiscoRA.

Engine-X (NGINX)

NGINX est un serveur web et un proxy inverse similaire à Apache. NGINX est utilisé pour la communication HTTP entre CAPF et CES ainsi que pour la communication entre CES et le service d'inscription Web CA. Lorsque libEST fonctionne en mode serveur, un serveur Web est nécessaire pour traiter les requêtes TCP pour le compte de libEST.

Service d'inscription de certificat (CES)

CES est le service sur CUCM qui agit comme RA entre le service CAPF et l'autorité de certification. CES est également appelé CiscoRA, ou simplement RA. CES utilise NGINX comme serveur Web car CES implémente la libEST en mode serveur afin d'agir en tant que RA.

Fonction de proxy d'autorité de certification (CAPF)

CAPF est un service CUCM avec lequel les téléphones interagissent lors de l'exécution de demandes d'inscription de certificat. Le protocole CAPF interagit avec la CES au nom des téléphones. Dans ce modèle de fonctionnalité, CAPF implémente libEST en mode client pour inscrire les certificats des téléphones via CES.

En résumé, voici comment chaque composant est mis en oeuvre :

1. Le téléphone envoie une demande de certificat au protocole CAPF
2. CAPF implémente CiscoEST (mode client) pour communiquer avec CES
3. CES implémente CiscoRA (mode serveur) pour traiter et répondre aux demandes du client EST
4. CES/CiscoRA communique avec le service d'inscription Web de l'Autorité de certification via HTTPS

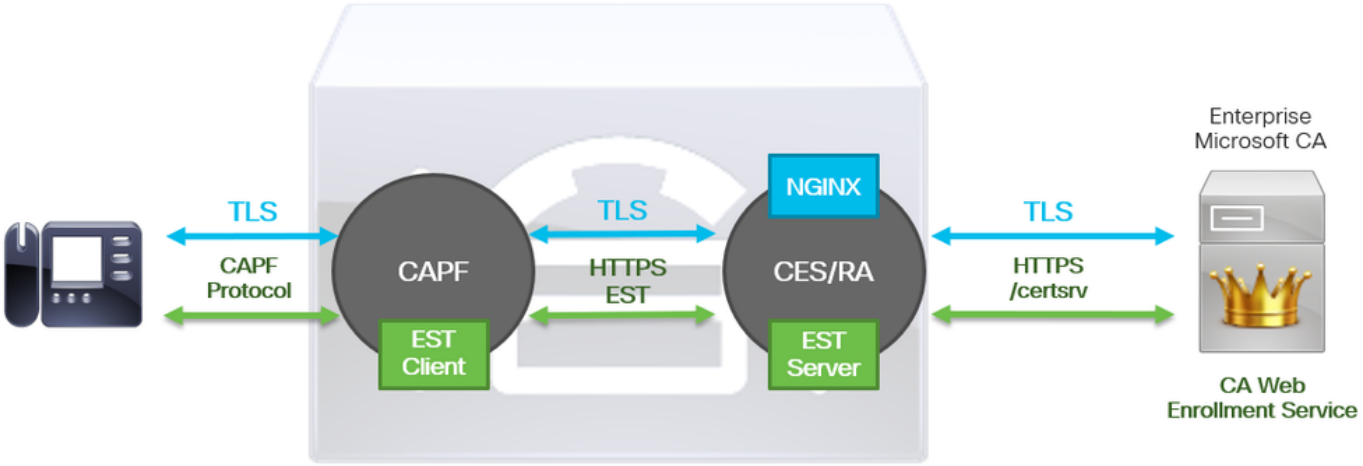
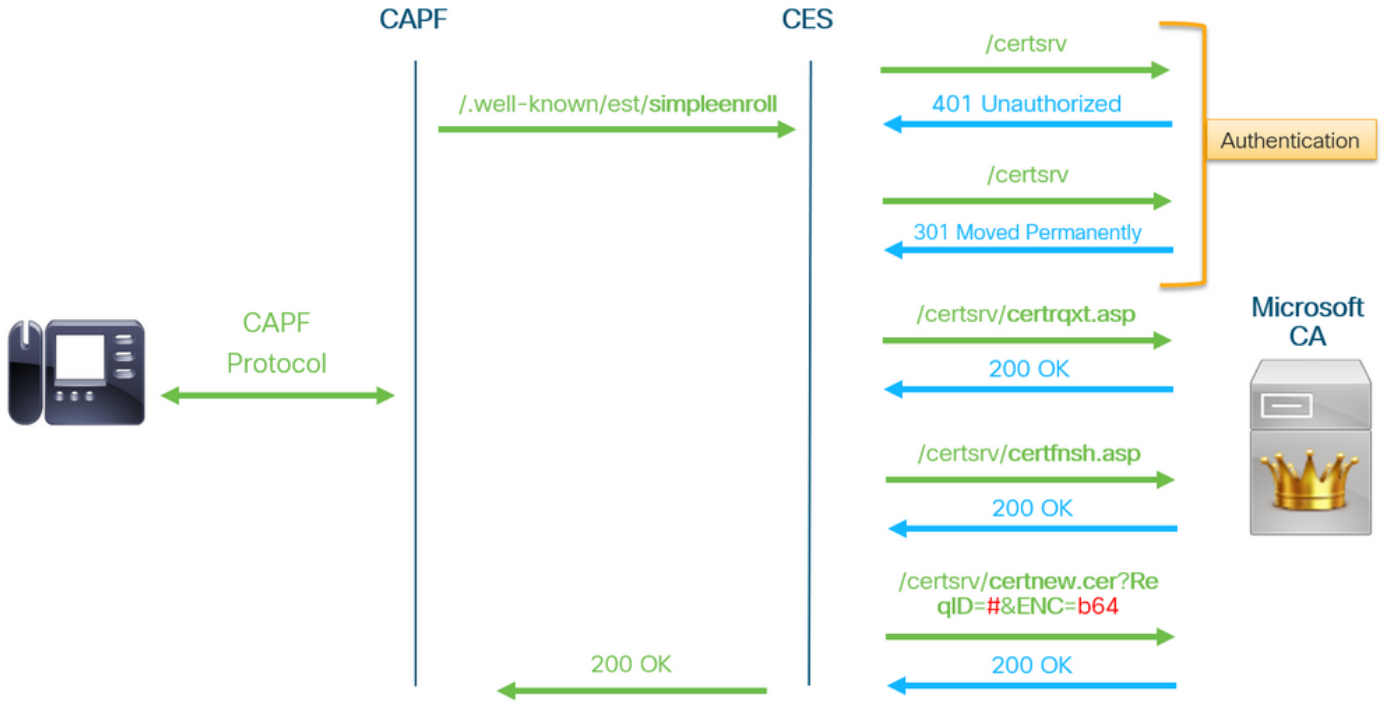


Diagramme de flux de messages



Explication du flux de messages

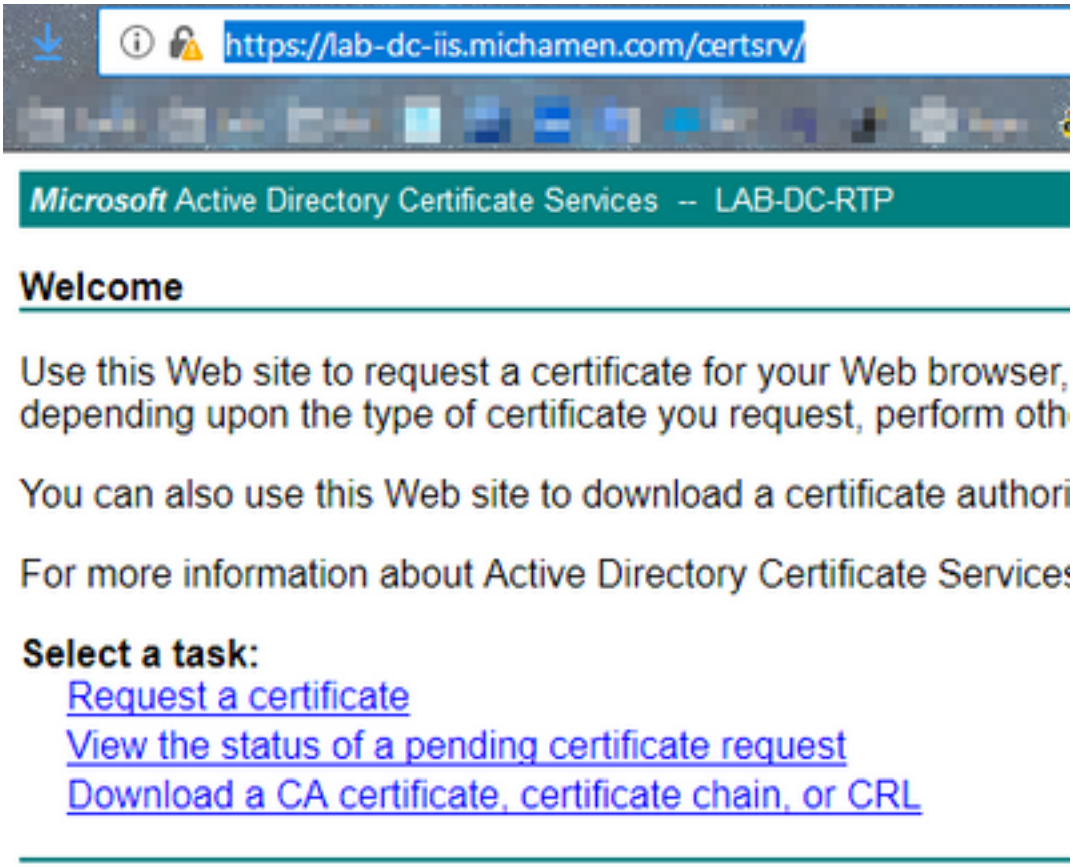
/.well-known/est/simpleenroll

Le client EST utilise cette URL pour envoyer un appel API qui demande l'inscription du certificat à partir du serveur EST. Une fois que le serveur EST reçoit l'appel API, il démarre le processus d'inscription de certificat qui inclut la communication HTTPS avec le service d'inscription Web de l'Autorité de certification. Si le processus d'inscription réussit et que le serveur EST reçoit le nouveau certificat, le protocole CAPF va charger le certificat et le renvoyer au téléphone IP.

/certsrv

L'URL **/certsrv** est utilisée par le client EST pour authentifier et démarrer une session avec l'autorité de certification.

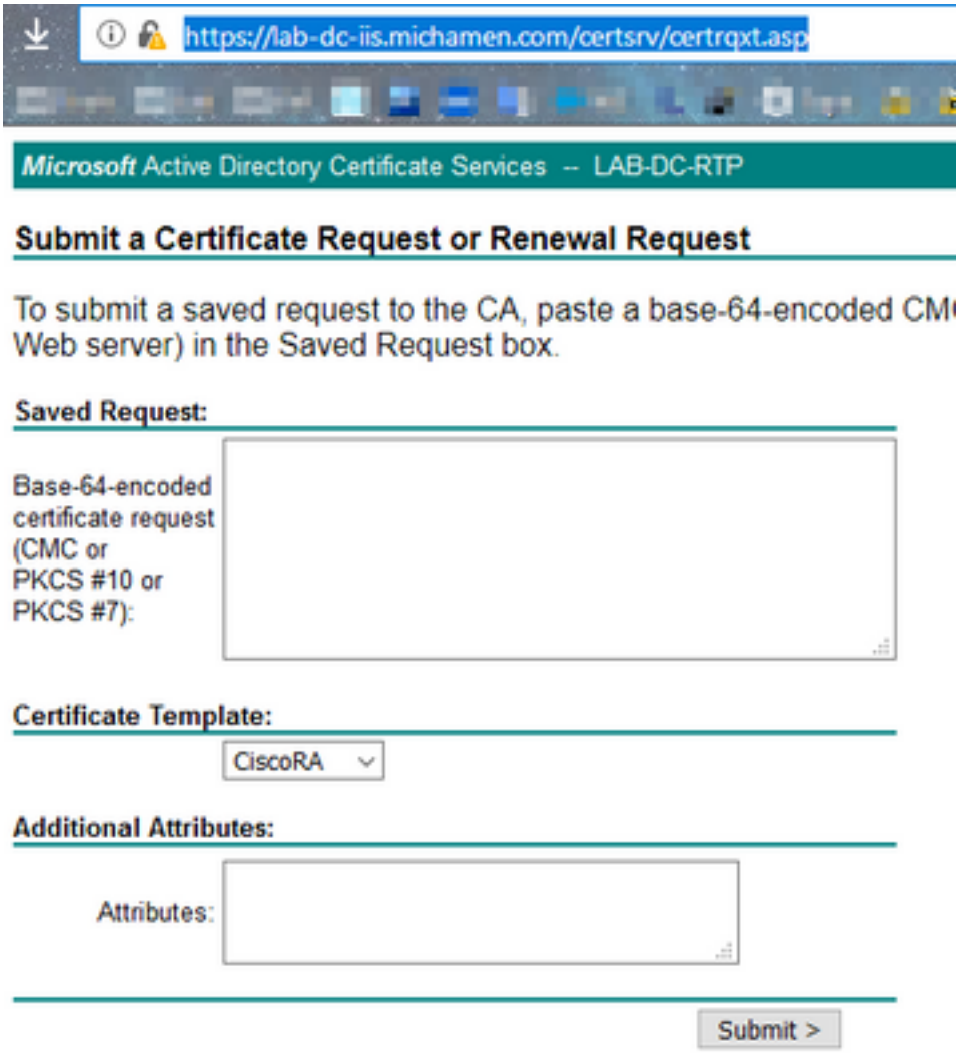
L'image ci-dessous est un exemple d'URL **/certsrv** à partir d'un navigateur Web. Il s'agit de la page de renvoi des services de certificats.



/certsrv/certrqxt.asp

L'URL **/certsrv/certrqxt.asp** est utilisée pour lancer la demande de nouveau certificat. Le client EST utilise **/certsrv/certrqxt.asp** pour envoyer le CSR, le nom du modèle de certificat et tous les attributs souhaités.

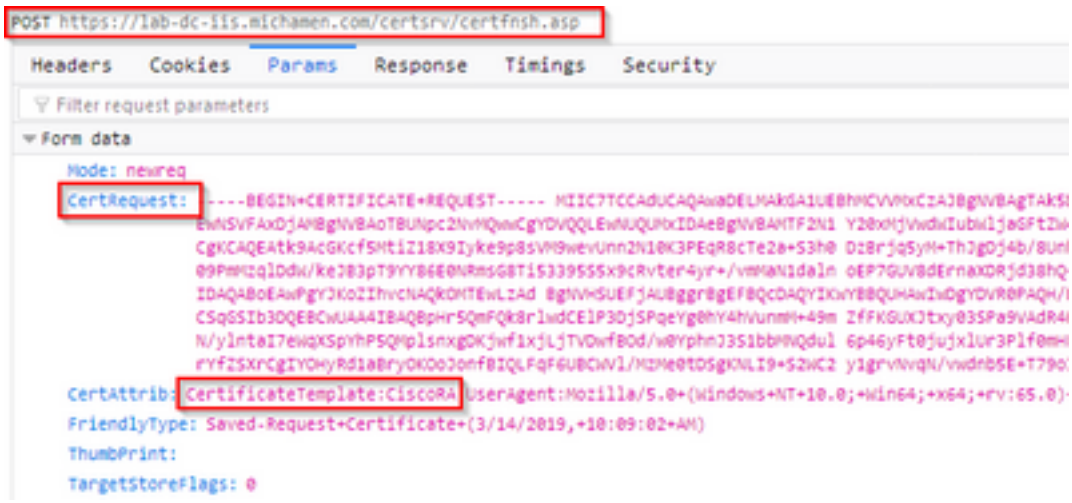
L'image ci-dessous est un exemple de **/certsrv/certrqxt.asp** à partir d'un navigateur Web.



/certsrv/certfnsh.asp

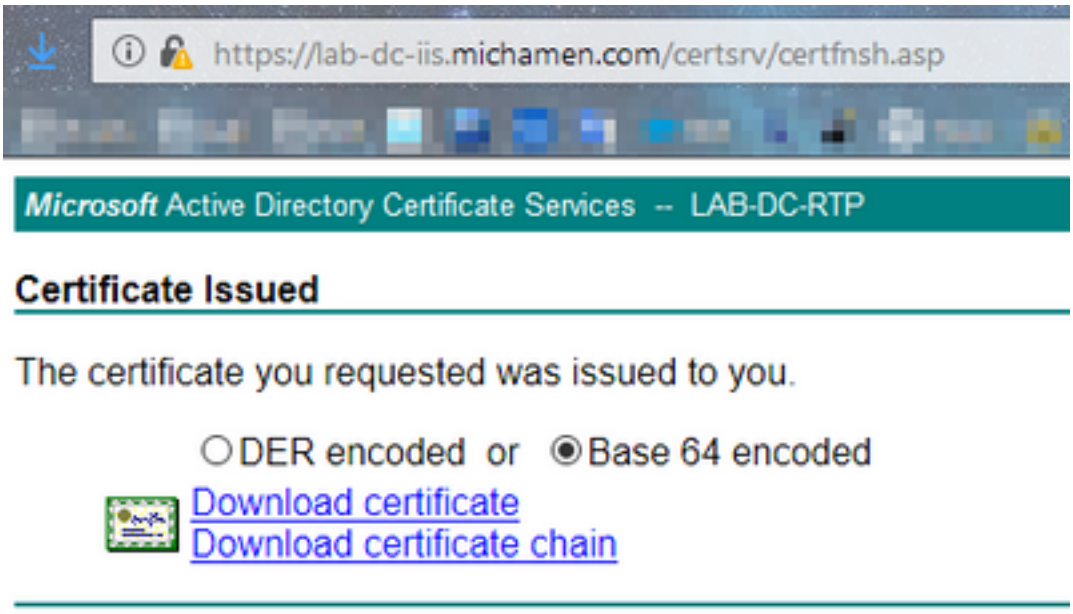
L'URL **/certsrv/certfnsh.asp** est utilisée pour soumettre des données pour la demande de certificat ; qui inclut le CSR, le nom du modèle de certificat et tous les attributs souhaités. Pour afficher l'envoi, utilisez les **outils de développement** du navigateur pour ouvrir la console du navigateur avant que les données ne soient envoyées via la page *certrqxt.asp*.

L'image ci-dessous est un exemple des données affichées dans la console du navigateur.

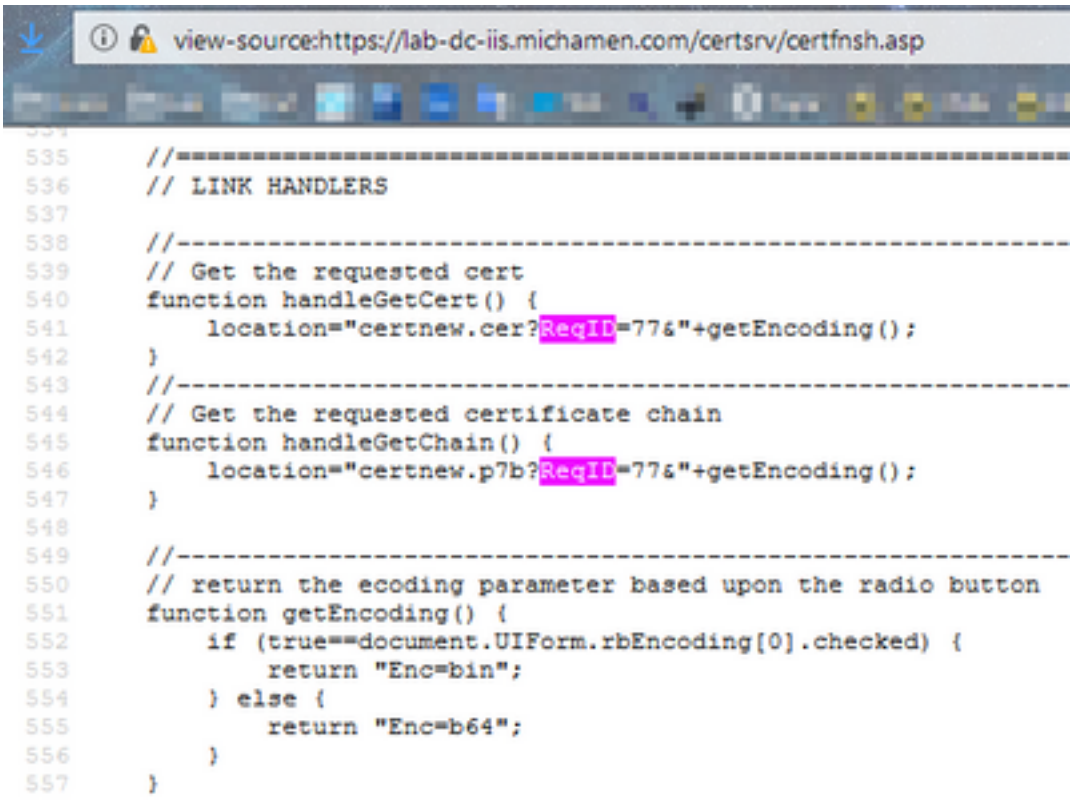


La réponse de la soumission de **/certsrv/certfnsh.asp** inclut l'ID de demande du certificat émis par

l'AC. L'ID de demande est affiché dans un navigateur Web lorsque le code source de la page est inspecté.



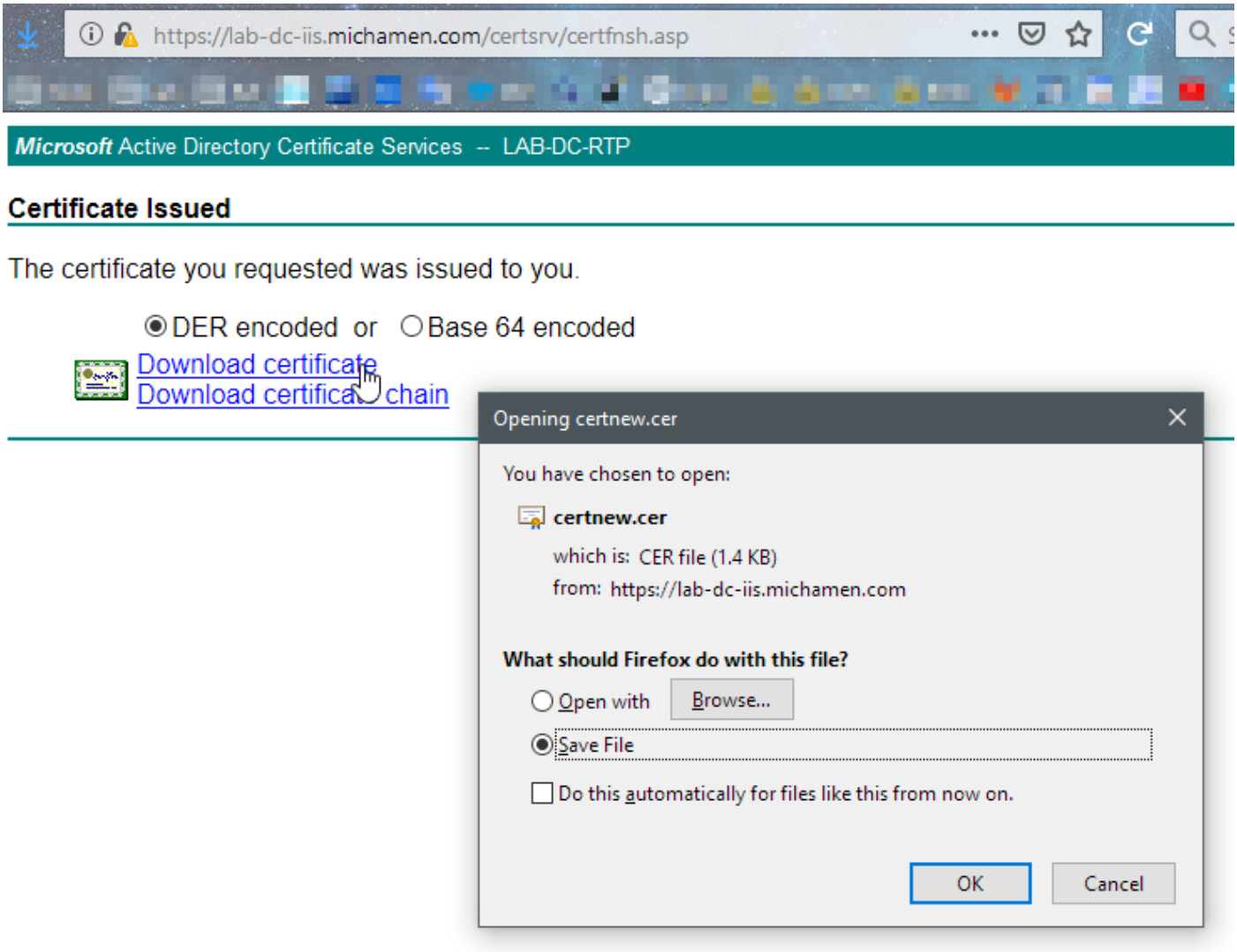
Astuce : Rechercher dans la source de la page “ ” ReqID



/certsrv/certnew.cer

Àce stade, le client EST connaît l'ID de demande du nouveau certificat. Le client EST utilise **/certsrv/certnew.cer** pour transmettre l'ID de demande et le codage de fichier comme paramètres pour télécharger le fichier de certificat avec l'extension **.cer**.

Cela équivaut à ce qui se passe dans votre navigateur lorsque vous cliquez sur le lien **Télécharger le certificat**.



Pour afficher l'URL et les paramètres de la demande, utilisez la console du navigateur.

> **Note**: Le navigateur spécifie **bin** pour le paramètre de codage si le codage DER est sélectionné ; cependant, le codage Base64 s'affichera sous la forme b64.

Suivis/journaux pertinents pour le dépannage

Ces journaux aident à isoler la plupart des problèmes.

Journaux CAPF

Les journaux CAPF incluent les interactions avec les téléphones et la journalisation minimale de l'activité CiscoEST.

Note: Ces journaux peuvent être collectés via l'interface de ligne de commande (CLI) ou l'outil de surveillance en temps réel (RTMT). En raison de CSCvo28048 CAPF peut ne pas apparaître dans la liste des services dans RTMT.

Journaux CiscoRA

Les journaux CiscoRA sont souvent appelés journaux CES. Les journaux CiscoRA contiennent l'activité initiale de démarrage CES et affichent les erreurs qui peuvent survenir lors de l'authentification avec l'autorité de certification.Si l'authentification initiale avec l'autorité de certification réussit, l'activité suivante pour les inscriptions téléphoniques n'est pas connectée ici. Par conséquent, les journaux CiscoRA constituent un bon point de départ pour le dépannage des problèmes.

Note: Ces journaux ne peuvent être collectés que via l'interface de ligne de commande à partir de la création de ces documents.

Erreur NGINX.log

Le fichier error.log de NGINX est le journal le plus utile pour cette fonctionnalité, car il enregistre toutes les activités au démarrage ainsi que toutes les interactions HTTP entre NGINX et le côté CA ; qui inclut les codes d'erreur retournés par l'autorité de certification ainsi que ceux générés par CiscoRA après le traitement de la demande.

Note: Au moment de la création de ce document, il n'y a aucun moyen de collecter ces journaux même à partir de l'interface de ligne de commande. Ces journaux ne peuvent être téléchargés qu'à l'aide d'un compte de support distant (root).

Journaux du serveur Web AC

Les journaux du serveur Web AC sont importants car ils affichent toute activité HTTP, y compris les URL de demande, les codes de réponse, la durée de réponse et la taille de réponse. Vous pouvez utiliser ces journaux pour corréler les interactions entre CiscoRA et l'autorité de certification.

Note: Les journaux du serveur Web AC dans le contexte de ce document sont les journaux IIS MS. Si d'autres autorités de certification Web sont prises en charge dans le futur, elles peuvent avoir différents fichiers journaux qui servent de journaux du serveur Web AC

Emplacement des fichiers journaux

Journaux CAPF :

- De la racine : /var/log/active/cm/trace/capf/sdi/capf< *numéro*>.txt
- Àpartir de CLI : fichier get activelog cm/trace/capf/sdi/capf*

Note: Définissez le niveau de suivi CAPF sur “ ” détaillée et redémarrez le service CAPF

avant d'effectuer le test.

Cisco RA :

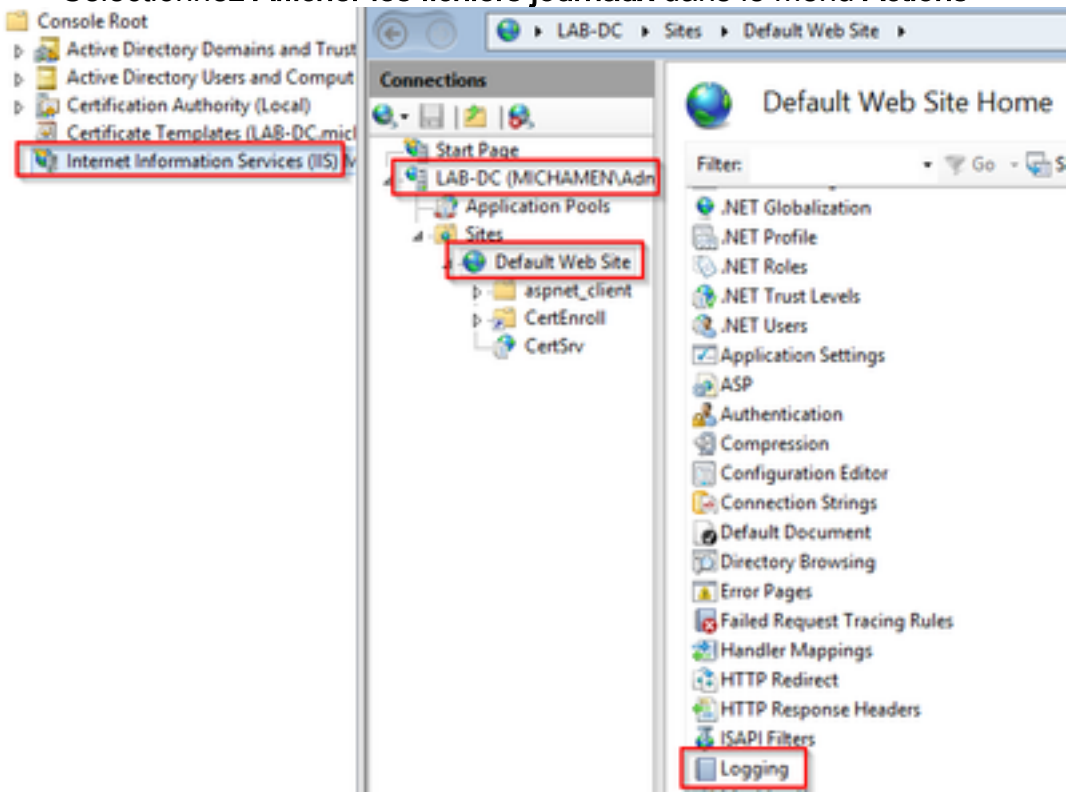
- De la racine : /var/log/active/cm/trace/capf/sdi/nginx< *numéro*>.txt
- Àpartir de CLI : fichier get activelog cm/trace/capf/sdi/nginx*

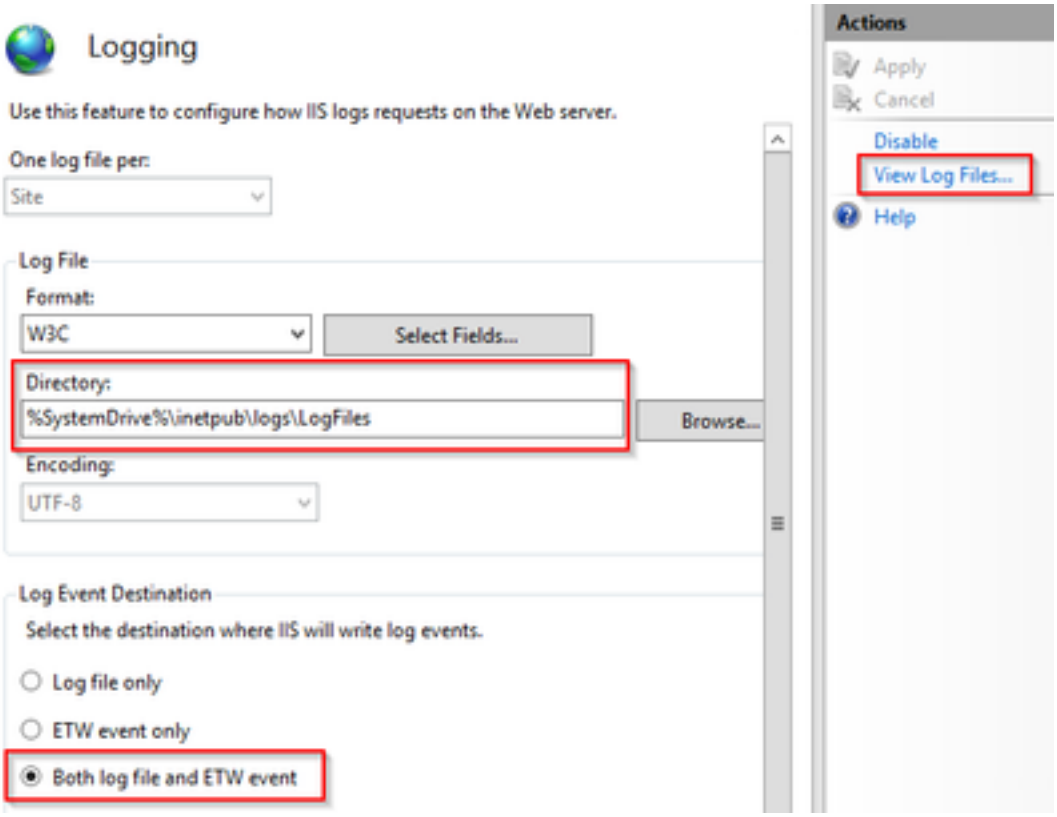
Journal d'erreurs Nginx :

- De la racine : /usr/local/thirdparty/nginx/install/logs/error.log
- Non disponible à partir de CLI

Journal IIS MS :

- Ouvrir MMC
- Sélectionnez le composant logiciel enfichable **IIS (Internet Information Services)**.
- Cliquez sur le nom du serveur
- Cliquez sur **Site Web par défaut**
- Double-cliquez sur **Journalisation** pour afficher les options de journalisation
- Sélectionnez **Afficher les fichiers journaux** dans le menu **Actions**





Exemple d'analyse de journal

Services démarrant normalement

CES Démarrage tel qu'indiqué dans le journal NGINX

Peu d'informations sont recueillies à partir de ce journal. La chaîne de certificats complète chargée dans son magasin de confiance est visible ici et l'une concerne le conteneur Web tandis que l'autre concerne 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 Démarrage comme indiqué dans le fichier error.log NGINX

La connexion à l'aide de la configuration et des informations d'identification du modèle de certificat est observée dans l'extrait ici :

```
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 récupération de la chaîne de certificats CA est observée dans l'extrait ici :

```
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
```

Lorsque la demande est acceptée, le fichier certnew.p7b est obtenu. La même URL avec les informations d'identification du modèle peut être utilisée pour obtenir le fichier certnew.p7b à partir d'un navigateur Web.

Démarrage de CES comme indiqué dans les journaux IIS

Les mêmes événements de démarrage CES vus dans le fichier error.log de NGINX sont également observés dans les journaux IIS ; cependant, les journaux IIS incluent 2 requêtes HTTP GET supplémentaires, car la première requête sera contestée par le serveur Web via une réponse 401 ; et une fois authentifié, une demande sera redirigée à l'aide d'une réponse 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
```

Démarrage de CAPF tel qu'il apparaît dans les journaux CAPF

La plupart de ce qui se passe dans les journaux CAPF pour le démarrage de CES ressemble à ce qui se passe dans les autres journaux ; mais vous remarquerez que le service CAPF détecte la méthode et la configuration de l'autorité de certification en ligne :

```
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 prochaine observation importante des journaux est quand le service CAPF initialise son client 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!!
```

Opération d'installation LSC du téléphone

Journaux CAPF

Il est recommandé de collecter tous les journaux nécessaires et de commencer l'analyse en examinant les journaux CAPF. Cela nous permet de connaître la référence temporelle d'un téléphone spécifique.

La partie initiale de la signalisation est identique à celle des autres méthodes CAPF, à l'exception du client EST exécuté dans le service CAPF qui effectue l'inscription avec CES vers la fin de la boîte de dialogue (une fois que le CSR a été fourni par le téléphone).

```
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
```

Une fois que le service CES a récupéré le certificat signé du téléphone, le certificat est converti au format DER avant d'être fourni au téléphone.

```
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
```

Le service CAPF reprend le relais et charge le CSR à partir de l'emplacement où il a été écrit dans l'extrait ci-dessus (/tmp/capf/cert/). Le service CAPF fournit ensuite le LSC signé au téléphone. En même temps, le CSR du téléphone est supprimé.

```
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
```

Journaux IIS

L'extrait ci-dessous affiche les événements des journaux IIS pour les étapes d'installation LSC d'un téléphone, comme expliqué ci-dessus.

```
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
```

Problèmes courants

Chaque fois qu'il y a une erreur dans le côté CES, il est attendu qu'il voit des résultats comme l'extrait ci-dessous dans les journaux CAPF. Vérifiez les autres journaux pour continuer à réduire le problème.

```
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
```

Certificat CA manquant dans la chaîne d'émetteurs du certificat d'identité IIS

Lorsqu'un certificat racine ou un certificat intermédiaire, qui se trouve dans la chaîne de certificats, n'est pas approuvé par CES, l'erreur « Impossible de récupérer la chaîne de certificats CA à partir de CA » est imprimée dans les journaux 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
```

Serveur Web présentant un certificat auto-signé

L'utilisation d'un certificat auto-signé sur IIS n'est pas prise en charge et notera le travail même si téléchargé en tant que CAPF-trust sur CUCM. L'extrait ci-dessous provient des journaux nginx et affiche ce qui est observé lorsque IIS utilise un certificat auto-signé.

```
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
```

Incompatibilité avec le nom d'hôte de l'URL et le nom commun

Le nom commun (lab-dc) du certificat IIS ne correspond pas au nom de domaine complet dans l'URL du service d'inscription Web de l'Autorité de certification. Pour que la validation du certificat réussisse, le nom de domaine complet à l'intérieur de l'URL doit correspondre au nom commun du certificat utilisé par l'autorité de certification.

```
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
```

Problème de résolution DNS

CiscoRA ne peut pas résoudre le nom d'hôte de l'autorité de certification en ligne configuré dans les paramètres de service.

```
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
```

Problème avec les dates de validité du certificat

Lorsque le protocole NTP (Network Time Protocol) ne fonctionne pas correctement, des problèmes de dates de validité des certificats se produisent. Cette vérification est effectuée par CES au démarrage et elle est observée dans les journaux 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
```

Erreur de configuration du modèle de certificat

Une faute de frappe dans le nom des paramètres de service entraîne des échecs. Aucune erreur ne sera consignée dans les journaux CAPF ou NGINX. Il est donc nécessaire de vérifier le fichier error.log de NGINX.

```
***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
```

Délai d'authentification CES

Le résumé ci-dessous montre le délai d'expiration du client CES EST après le minuteur par défaut de 10 secondes pendant le processus d'authentification Certsrv initial.

```
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 et CSCvf83629 se rapportent tous deux au délai d'expiration de l'authentification CES.

Délai d'inscription CES

Le client CES EST expire après une authentification réussie, mais en attendant une réponse à une demande d'inscription.

```
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 connus

CSCvo28048 Service CAPF non répertorié dans le menu RTMT Collect Files

CSCvo58656 CAPF Online CA a besoin d'une option pour configurer le délai de connexion maximal entre RA et CA

CSCvf83629 EST Server obtient EST_ERR_HTTP_WRITE lors de l'inscription

Informations connexes

- Support et documentation techniques - Cisco Systems