Dépannage de l'échec d'installation de fichiers PKCS#12 avec des algorithmes PBE non conformes FIPS

Contenu

Introduction

Ce document décrit comment dépanner l'échec d'installation d'un fichier PKCS (Public Key Cryptography Standards)#12 avec des algorithmes PBE (Password-Based Encryption) conformes à la norme FIPS (Federal Information Processing Standard) via Cisco Firepower Management Center (FMC). Il explique une procédure pour l'identifier et pour créer un nouveau bundle compatible avec OpenSSL.

Informations générales

La solution Cisco Firepower Threat Defense (FTD) prend en charge la conformité avec la norme FIPS 140 lorsque vous activez le mode Common Criteria (CC) ou Unified Capabilities Authorized Products List (UCAP) sur un périphérique géré. Cette configuration fait partie d'une stratégie de paramètres de plate-forme FMC. Une fois appliquée, la commande **fips enable** apparaît dans la sortie **show running-config** de FTD.

PKCS#12 définit un format de fichier utilisé pour regrouper une clé privée et le certificat d'identité respectif. Il est également possible d'inclure tout certificat racine ou intermédiaire appartenant à la chaîne de validation. Les algorithmes PBE protègent les parties des certificats et des clés privées du fichier PKCS#12. En raison de la combinaison du schéma d'authentification des messages (MD2/MD5/SHA1) et du schéma de chiffrement (RC2/RC4/DES), il existe plusieurs algorithmes PBE, mais le seul qui est compatible FIPS est PBE-SHA1-3DES.

> **Note**: Pour en savoir plus sur FIPS dans les produits Cisco, accédez à FIPS 140.

> **Note**: Pour en savoir plus sur les normes de certification de sécurité disponibles pour FTD et FMC, accédez au chapitre **Security Certifications Compliance** du Guide de configuration FMC.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Infrastructure à clé publique (PKI)
- OpenSSL

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- FMCv - 6.5.0.4 (build 57)
- FTDv - 6.5.0 (build 115)

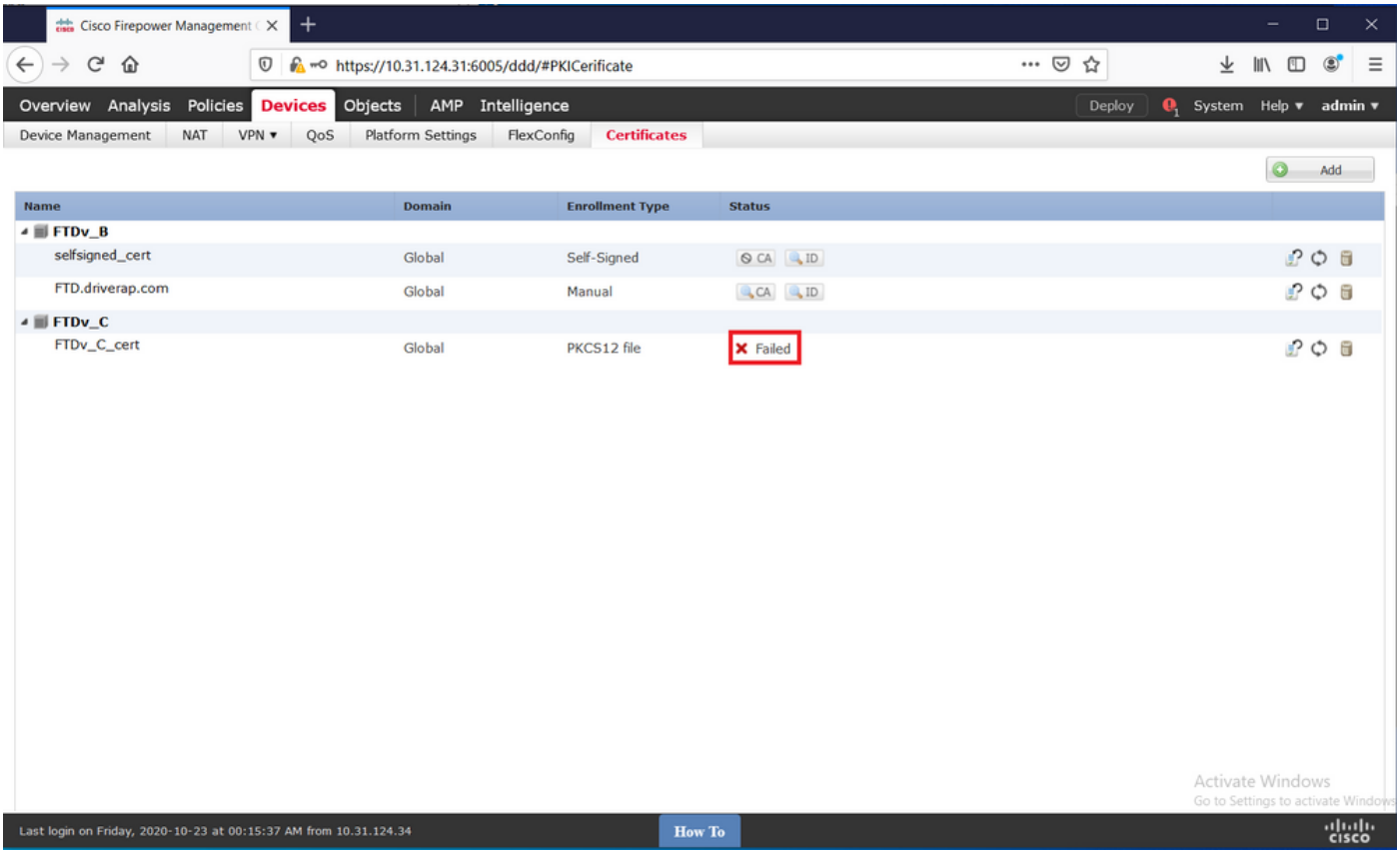
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

> **Note**: L'approche décrite dans ce document peut être mise en oeuvre sur toute autre plate-forme présentant un problème similaire, par exemple, un dispositif de sécurité adaptatif (ASA) Cisco, car le problème est que le certificat n'est pas conforme FIPS.

> **Note**: Ce document ne traite pas de la condition dans laquelle les composants PKCS#12 eux-mêmes ne sont pas conformes pour toute autre raison, comme la longueur de clé Rivest, Shamir, Adleman (RSA) ou l'algorithme de signature utilisé pour signer le certificat d'identité. Dans de tels cas, les certificats doivent être redélivrés pour être conformes à la norme FIPS.

Problème

Lorsque le mode FIPS est activé dans FTD, l'installation du certificat peut échouer si les algorithmes PBE utilisés pour protéger le fichier PKCS#12 ne sont pas compatibles FIPS.



Note: Trouvez une procédure pas à pas pour installer un fichier PKCS#12 à l'aide du FMC dans la section **Inscription PKCS12** de l'installation et du renouvellement des certificats sur FTD géré par FMC.

Si l'installation du certificat échoue pour cette raison, les débogages PKI impriment l'erreur ci-dessous :

```
firepower# debug crypto ca 14
firepower# show debug
debug crypto ca enabled at level 14
Conditional debug filters:
Conditional debug features:

firepower# PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[4]: Error unpacking pkcs7 encrypted data
PKI[1]: error:060A60A3:digital envelope routines:FIPS_CIPHERINIT:disabled for fips in fips_enc.c
line 143.
PKI[1]: error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen failure in evp_pbe.c
line 203.
PKI[1]: error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error in
p12_decr.c line 93.
PKI[1]: error:2306A075:PKCS12 routines:PKCS12_item_decrypt_d2i:pkcs12 pbe crypt error in
p12_decr.c line 145.
PKI[4]: pkcs7 encryption algorithm may not be fips compliant
PKI[4]: Error unpacking pkcs12 struct to extract keys and certs
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list is NULL
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
```

```
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
```

Vous pouvez également confirmer avec OpenSSL que le PKCS#12 présent inclut des algorithmes PBE FIPS non conformes.

```
OpenSSL> pkcs12 -info -in ftdv_C_.p12 -noout
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
```

Dans la sortie précédente, il y a deux algorithmes PBE, pbeWithSHA1And40BitRC2-CBC et pbeWithSHA1And3-KeyTripleDES-CBC, qui protègent respectivement les certificats et la clé privée. Le premier n'est pas conforme FIPS.

Solution

La solution consiste à configurer l'algorithme PBE-SHA1-3DES pour la protection des certificats et des clés privées. Dans l'exemple ci-dessus, seul l'algorithme de certificat doit être modifié. Premièrement, vous devez obtenir la version Privacy-Enhanced Mail (PEM) du fichier PKCS#12 d'origine à l'aide d'OpenSSL.

```
OpenSSL> pkcs12 -in ftdv_C_.p12 -out ftdv_C_.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Enfin, vous devez utiliser la commande ci-dessous avec l'algorithme PBE compatible FIPS à l'aide du fichier PEM obtenu à l'étape précédente pour générer un tout nouveau fichier PKCS#12 :

```
OpenSSL> pkcs12 -certpbe PBE-SHA1-3DES -export -in ftdv_C_.pem -out ftdv_C_FIPS_compliant.p12
Enter pass phrase for ftdv_C_.pem:
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'
```

> **Note**: Si l'algorithme de protection de la clé privée doit également être modifié, vous pouvez ajouter le mot clé **-keypbe** suivi de **PBE-SHA1-3DES** à la même commande : **pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out *<fichier de certificat PKCS12>***.

Vérification

Utilisez la même commande OpenSSL pour obtenir des informations sur la structure de fichiers PKCS#12 afin de confirmer que les algorithmes FIPS sont utilisés :

```
OpenSSL> pkcs12 -info -in ftdv_C_FIPS_compliant.p12 -noout
```

```
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
```

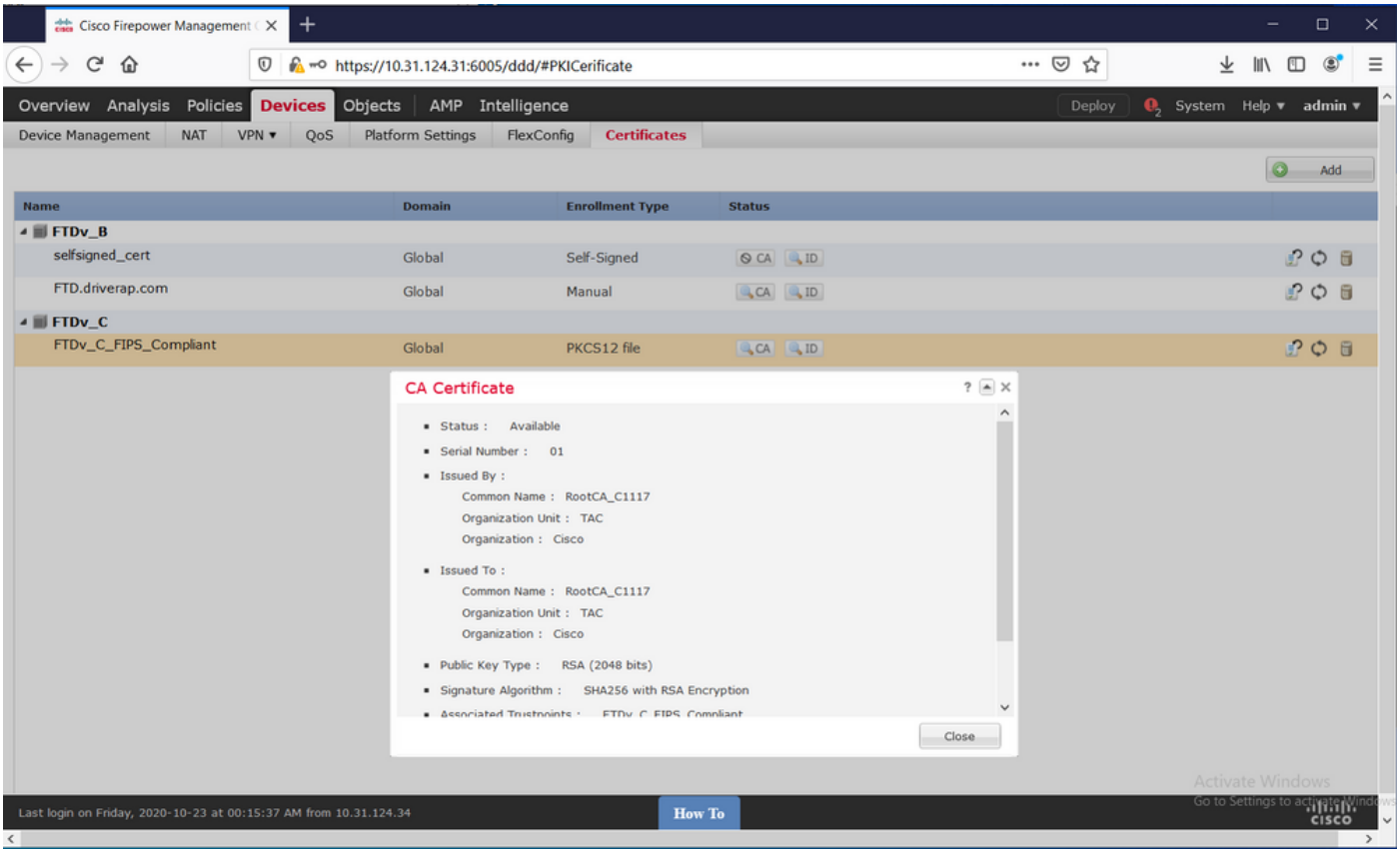
Maintenant, les débogages PKI affichent le résultat ci-dessous lorsque l'installation du certificat réussit.

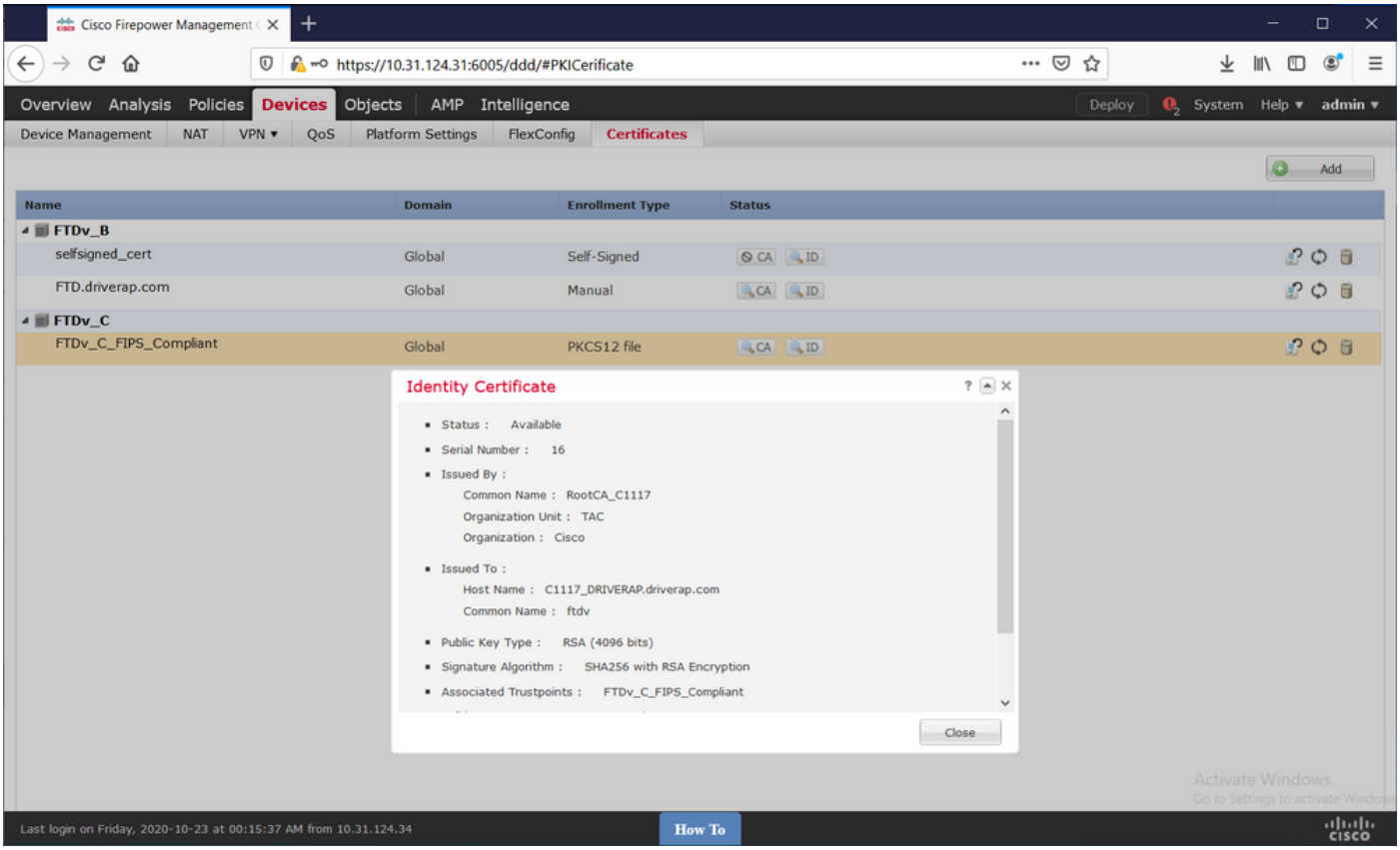
```
PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_key, pki_ossl_pkcs12.c:1252
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[14]: compare_key_ids, pki_ossl_pkcs12.c:1150
PKI[12]: transfer_p12_contents_to_asa, pki_ossl_pkcs12.c:375
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list is NULL

CRYPTO_PKI: examining router cert:
CRYPTO_PKI: issuerName=/O=Cisco/OU=TAC/CN=RootCA_C1117
CRYPTO_PKI: subjectname=/CN=ftdv/unstructuredName=C1117_DRIVERAP.driverap.com
CRYPTO_PKI: key type is RSAPKI[13]: GetKeyUsage, pki_ossl_pkcs12.c:278

CRYPTO_PKI: bitValue of ET_KEY_USAGE = a0
CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
CRYPTO_PKI: adding RSA Keypair
CRYPTO_PKI: adding as a router certificate.
CRYPTO_PKI: InsertCertData: subject name =

30 3b 31 0d 30 0b 06 03 55 04 03 13 04 66 74 64 76 31 2a 30
28 06 09 2a 86 48 86 f7 0d 01 09 02 16 1b 43 31 31 31 37 5f
44 52 49 56 45 52 41 50 2e 64 72 69 76 65 72 61 70 2e 63 6f
6d
CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: serial number = 16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty,
pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
```

```
PKI[9]: Starting to build the PKI cache
PKI[4]: No identity cert found for TP: FTDv_C_FIPS_Compliant
PKI[4]: Failed to cache certificate chain for the trustpoint FTDv_C_FIPS_Compliant or none
available
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[4]: Failed to retrieve trusted issuers list or no trustpoint configured
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_add_sync_record, pki_ossl_pkcs12.c:144
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: ID cert in trustpoint FTDv_C_FIPS_Compliant successfully validated with CA cert.

CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

CRYPTO_PKI: trustpoint FTDv_C_FIPS_Compliant authentication status = 0

CRYPTO_PKI: InsertCertData: subject name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: serial number = 01 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
17 9d 0e b0 15 9d cd a2 5a 01 95 bf c6 8c 4f 2e | ........Z.....O.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty,
pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
PKI[9]: Starting to build the PKI cache

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.
PKI[7]: Get Certificate Chain: number of certs returned=2
PKI[13]: CERT_GetDNbyBuffer, vpn3k_cert_api.c:993
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[7]: Built trustpoint cache for FTDv_C_FIPS_Compliant
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[9]: Added 1 issuer hashes to cache.
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_free_sync_record, pki_ossl_pkcs12.c:113
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
```

```
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI: certificate data
<omitted output>
CRYPTO_PKI: status = 0: failed to get extension from cert

CRYPTO_PKI: certificate data
<omitted output>
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
```

Enfin, le FMC affiche les certificats d'autorité de certification et d'identité disponibles :




Cisco Firepower Management
https://10.31.124.31:6005/ddd/#PKICerificate
Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates
Add
Name Domain Enrollment Type Status
FTDv_B
selfsigned_cert Global Self-Signed CA ID
FTD.driverap.com Global Manual CA ID
FTDv_C
FTDv_C_FIPS_Compliant Global PKCS12 file CA ID
Identity Certificate
Status : Available
Serial Number : 16
Issued By :
Common Name : RootCA_C1117
Organization Unit : TAC
Organization : Cisco
Issued To :
Host Name : C1117_DRIVERAP.driverap.com
Common Name : ftdv
Public Key Type : RSA (4096 bits)
Signature Algorithm : SHA256 with RSA Encryption
Associated Trustpoints : FTDv_C_FIPS_Compliant
Close
Activate Windows
Last login on Friday, 2020-10-23 at 00:15:37 AM from 10.31.124.34
How To