Renouvellement du certificat CA Sftunnel FMC pour la connectivité FTD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Problème
  - Que se passe-t-il après la date de péremption ?
  - Comment vérifier rapidement si le certificat a expiré ou quand il expire ?
  - Comment être averti à l'avenir de l'expiration prochaine d'un certificat ?
- Solution 1 - Le certificat n'a pas encore expiré (scénario idéal)
  - Approche recommandée
- Solution 2 - Le certificat a déjà expiré
  - FTD toujours connectés via sftunnel
  - Les FTD ne sont plus connectés via sftunnel
    - Approche recommandée
    - Approche manuelle
- Annexe
  - Certificats utilisés dans FMC HA

Introduction

Ce document décrit le renouvellement du certificat de l'autorité de certification (CA) sftunnel du Centre de gestion Firepower (FMC) en relation avec la connectivité FTD (Firepower Threat Defense).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense
- Centre de gestion Firepower
- Infrastructures à clé publique (PKI)

Composants utilisés

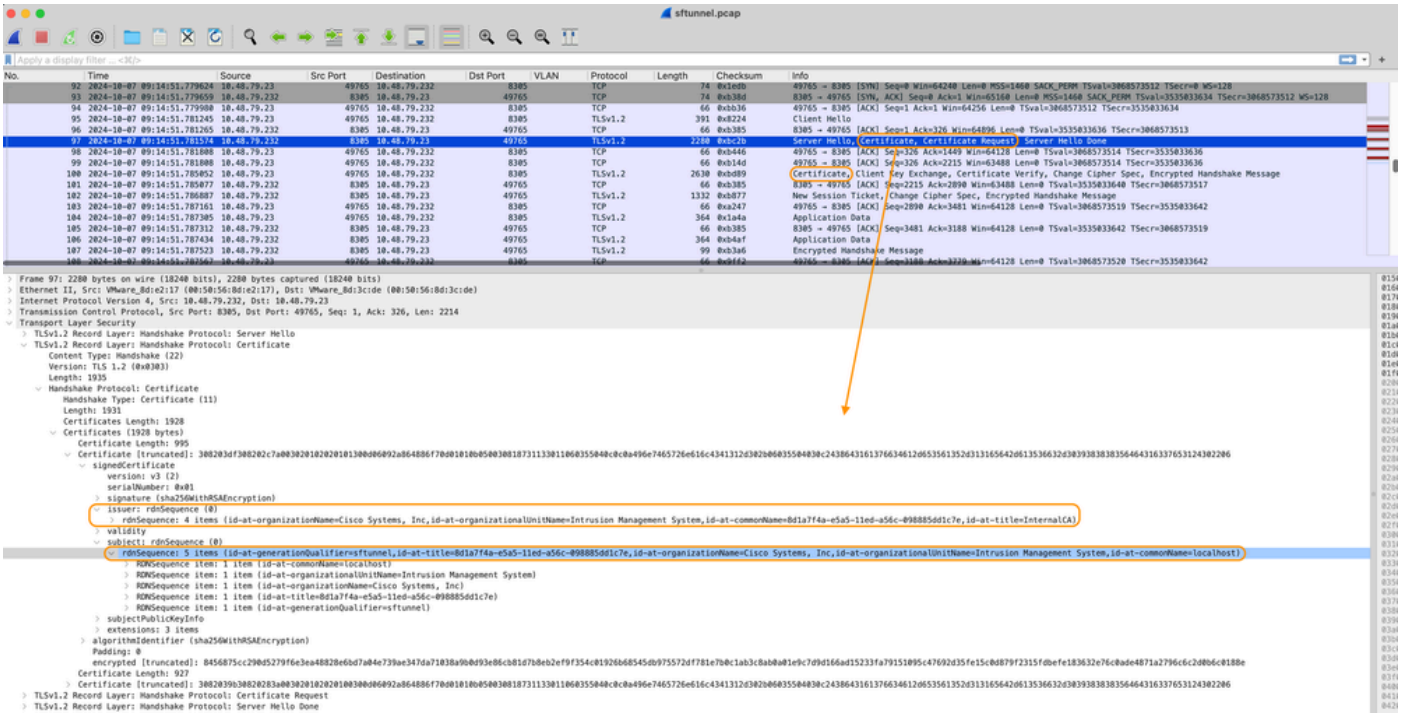
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

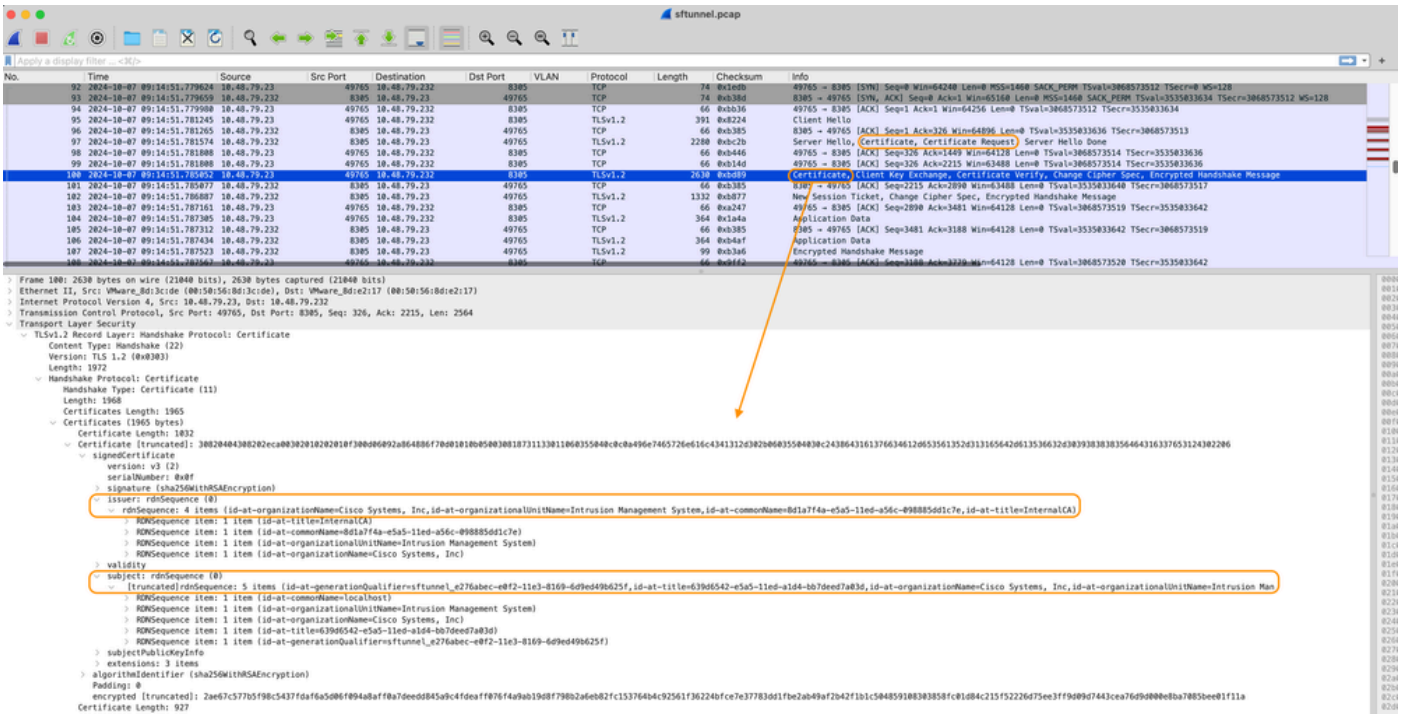
Informations générales

FMC et FTD communiquent entre eux via sftunnel (tunnel Sourcefire). Cette communication utilise des certificats pour sécuriser la conversation sur une session TLS. Plus d'informations sur le sftunnel et comment il s'établit peuvent être trouvées sur ce lien.

À partir de la capture de paquets, vous pouvez voir que le FMC (10.48.79.232 dans cet exemple) et le FTD (10.48.79.23) échangent des certificats entre eux. Ils le font afin de valider qu'ils parlent avec le bon appareil et qu'il n'y a pas d'écoute électronique ou d'attaque Man-In-The-Middle (MITM). La communication est chiffrée à l'aide de ces certificats et seule la partie qui a la clé privée associée pour ce certificat est en mesure de le déchiffrer à nouveau.



Certificat_exchange_server_cert



Certificat_change_client_cert

Vous pouvez voir que les certificats sont signés par la même autorité de certification (CA) interne (émetteur) qui est configurée sur le système FMC. La configuration est définie sur le FMC sur le fichier /etc/sf/sftunnel.conf qui contient quelque chose comme :

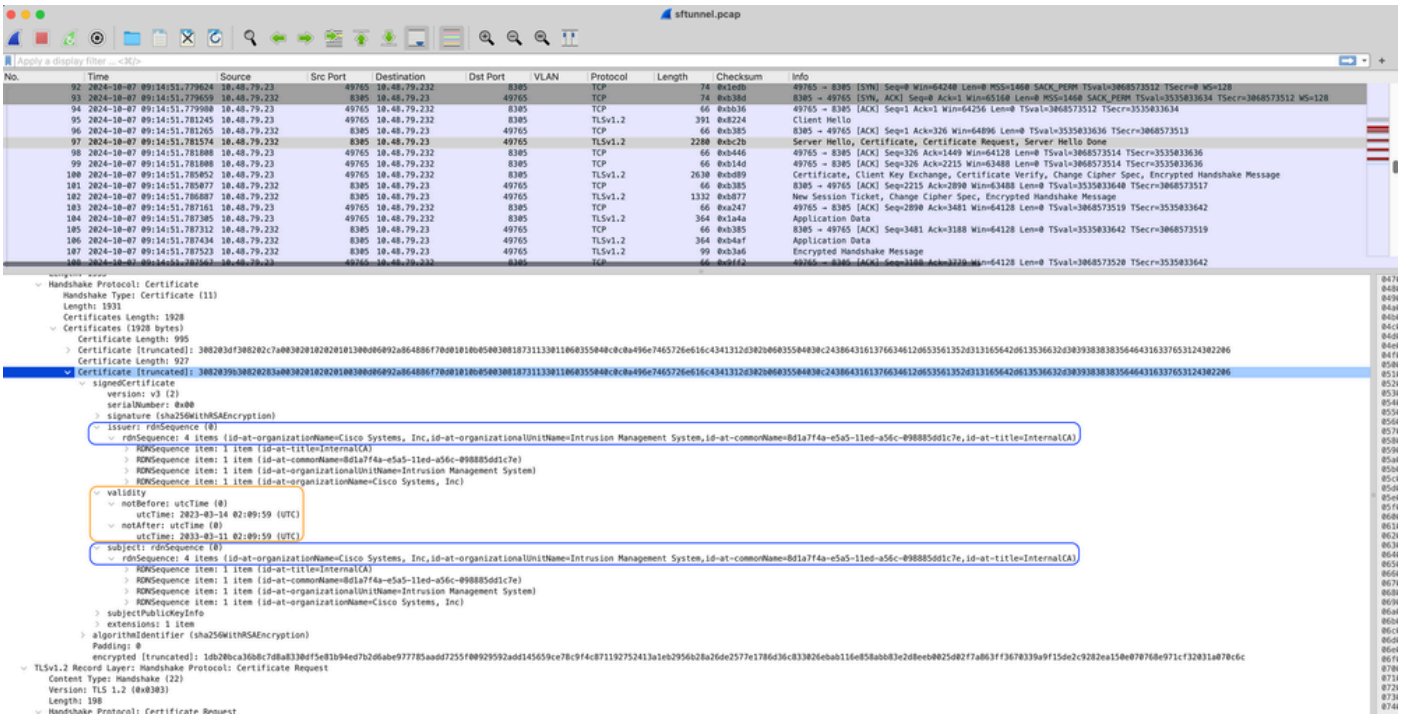
```
proxyssl {
  proxy_cert   /etc/sf/keys/sftunnel-cert.pem;              ---> Certificate provided by FMC to FTD f
  proxy_key    /etc/sf/keys/sftunnel-key.pem;
  proxy_cacert /etc/sf/ca_root/cacert.pem;                  ---> CA certificate (InternalCA)
  proxy_crl    /etc/sf/ca_root/crl.pem;
  proxy_cipher 1;
  proxy_tls_version TLSv1.2;
};
```

Indique l'autorité de certification utilisée pour signer tous les certificats pour sftunnel (à la fois le FTD et le FMC) et le certificat utilisé par le FMC pour envoyer à tous les FTD. Ce certificat est signé par l'autorité de certification interne.

Lorsque le FTD s'enregistre auprès du FMC, le FMC crée également un certificat à transmettre au périphérique FTD qui est utilisé pour la communication ultérieure sur le sftunnel. Ce certificat est également signé par le même certificat CA interne. Sur FMC, vous pouvez trouver ce certificat (et la clé privée) sous /var/sf/peers/<UUID-FTD-device> et potentiellement sous le dossier certs_push et est appelé sftunnel-cert.pem (sftunnel-key.pem pour la clé privée). Sur FTD, vous pouvez trouver ceux sous /var/sf/peers/<UUID-FMC-device> avec la même convention d'attribution de noms.

Cependant, chaque certificat a également une période de validité à des fins de sécurité. Lors de l'inspection du certificat InternalCA, nous pouvons également voir la période de validité qui est de

10 ans pour le FMC InternalCA comme indiqué dans la capture de paquets.

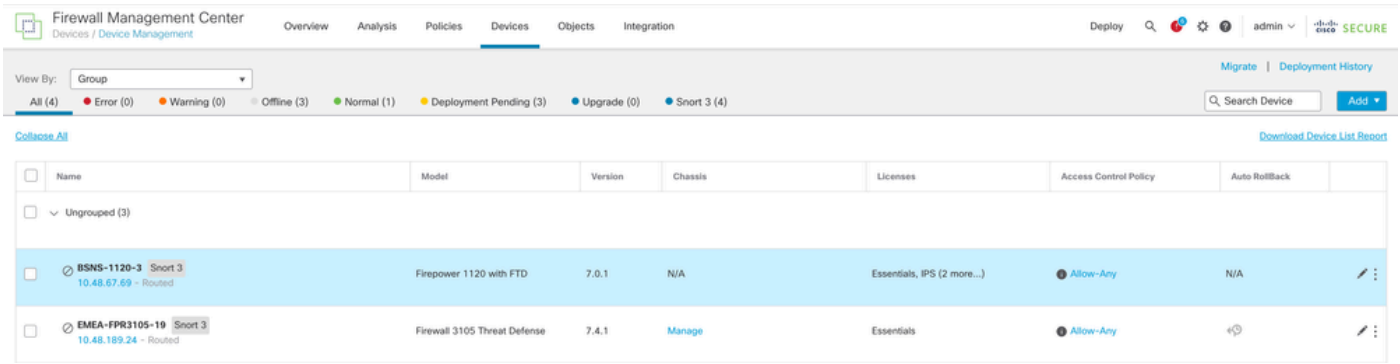


FMC-InternalCA_valid

Problème

Le certificat FMC InternalCA n'est valide que pour 10 ans. Après le délai d'expiration, le système distant ne fait plus confiance à ce certificat (ainsi qu'aux certificats signés par lui) et cela entraîne des problèmes de communication sftunnel entre les périphériques FTD et FMC (ainsi que la communication FMC HA). Cela signifie également que plusieurs fonctionnalités clés telles que les événements de connexion, les recherches de programmes malveillants, les règles basées sur l'identité, les déploiements de politiques et bien d'autres choses ne fonctionnent pas.

Les périphériques s'affichent comme désactivés sur l'interface utilisateur FMC sous l'onglet Périphériques > Gestion des périphériques lorsque le sftunnel n'est pas connecté. Le problème lié à cette expiration est suivi sur l'ID de bogue Cisco CSCwd08098. Notez bien que tous les systèmes sont affectés, même lorsque vous exécutez une version fixe du défaut. Vous trouverez plus d'informations sur ce correctif dans la section Solution.



Disabled-devices

Le FMC n’actualise pas automatiquement l’autorité de certification et ne republie pas les certificats sur les périphériques FTD. Et il n'y a pas non plus d'alerte d'intégrité FMC qui indique que le certificat expire. L'ID de bogue Cisco CSCwd08448 est suivi à cet égard pour fournir une alerte de santé sur l'interface utilisateur FMC à l'avenir.

Que se passe-t-il après la date de péremption ?

Au départ, rien ne se passe et les canaux de communication sftunnel continuent à fonctionner comme avant. Cependant, lorsque la communication sftunnel entre les périphériques FMC et FTD est interrompue et qu'il tente de rétablir la connexion, elle échoue et vous pouvez observer des lignes de journal sur le fichier journal des messages qui pointent vers l'expiration du certificat. Notez que la communication sftunnel (utilisée pour la synchronisation haute disponibilité (HA)) entre le FMC principal et le FMC secondaire est également potentiellement affectée, comme décrit dans cette section.

Lignes de journal du périphérique FTD de /ngfw/var/log/messages :

```
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [INFO] Initiating IPv4 connection
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [INFO] Wait to connect to 8305 (IP
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [INFO] Connected to 10.10.200.31 f
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [ERROR] -Error with certificate at
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [ERROR]   issuer   = /title=Interna
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [ERROR]   subject  = /title=Interna
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [ERROR]   err 10:certificate has ex
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [ERROR] SSL_renegotiate error: 1:
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [ERROR] Connect:SSL handshake faile
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [WARN] SSL Verification status: ce
```

Lignes de journal du périphérique FMC à partir de /var/log/messages :

```
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [INFO] VERIFY ssl_verify_callback_in
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [ERROR] SSL_renegotiate error: 1: er
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [INFO] establishConnectionUtil: Faile
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [ERROR] establishSSLConnection: Unabl
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [ERROR] establishSSLConnection: ret_
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [ERROR] establishSSLConnection: iret
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [ERROR] establishSSLConnection: Faile
```

La communication sftunnel peut être interrompue pour diverses raisons :

- Perte de communication en raison d'une perte de connectivité réseau (éventuellement temporaire)
- Redémarrage de FTD ou FMC

- Celles attendues : redémarrage manuel, mises à niveau, redémarrage manuel du processus sftunnel sur FMC ou FTD (par exemple par pmtool restartbyid sftunnel)
- Des inattendues : tracebacks, coupure de courant

Étant donné le grand nombre de possibilités qui peuvent interrompre la communication sftunnel, il est fortement conseillé de corriger la situation le plus rapidement possible, même lorsque tous les périphériques FTD sont actuellement correctement connectés malgré l'expiration du certificat.

Comment vérifier rapidement si le certificat a expiré ou quand il expire ?

Le plus simple est d'exécuter ces commandes sur la session FMC SSH :

```
expert
sudo su
cd /etc/sf/ca_root
openssl x509 -dates -noout -in cacert.pem
```

Vous voyez ainsi les éléments Validité du certificat. La partie principale pertinente ici est le "notAfter" qui montre que le certificat ici est valable jusqu'au 5 octobre 2034.

```
root@firepower:/Volume/home/admin# openssl x509 -dates -in /etc/sf/ca_root/cacert.pem
notBefore=Oct  7 12:16:56 2024 GMT
notAfter=Oct  5 12:16:56 2034 GMT
```

NonAprès

Si vous préférez exécuter une seule commande qui vous donne immédiatement le nombre de jours pendant lesquels le certificat est toujours valide, vous pouvez utiliser ceci :

```
CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -enddate -noout -in "$CERT_PATH" | cu
```

Un exemple de configuration où le certificat est encore valide pendant plusieurs années est affiché.

```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS + THIRTY_
DAYS_SECONDS)); DAYS_LEFT=$(( (EXPIRY_DATE_SECONDS - CURRENT_DATE_SECONDS) / (24*60*60) )); if [ "$EXPIRY_DATE
_SECONDS" -le "$CURRENT_DATE_SECONDS" ]; then DAYS_EXPIRED=$(( (CURRENT_DATE_SECONDS - EXPIRY_DATE_SECONDS) /
(24*60*60) )); echo -e "\nThe certificate has expired $DAYS_EXPIRED days ago.\nIn case the sftunnel communicat
ion with the FTD is not yet lost, you need to take action immediately in renewing the certificate.\n"; elif [
"$EXPIRY_DATE_SECONDS" -le "$EXPIRY_THRESHOLD" ]; then echo -e "\nThe certificate will expire within the next
30 days!\nIt is ONLY valid for $DAYS_LEFT more days.\nIt is recommended to take action in renewing the certifi
cate as quickly as possible.\n"; else echo -e "\nThe certificate is valid for more than 30 days.\nIt is valid
for $DAYS_LEFT more days.\nThere is no immediate need to perform action but this depends on how far the expiry
 date is in the future.\n"; fi

The certificate is valid for more than 30 days.
It is valid for 3649 more days.
There is no immediate need to perform action but this depends on how far the expiry date is in the future.

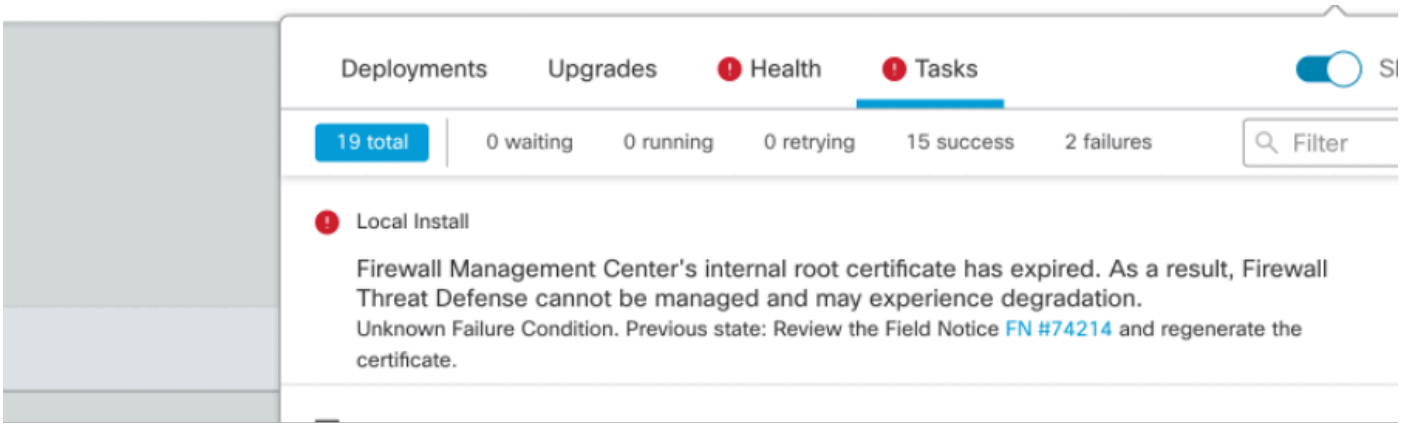
root@fmcv72-stejanss:/Volume/home/admin#
```

Certificate_expiry_validation_command

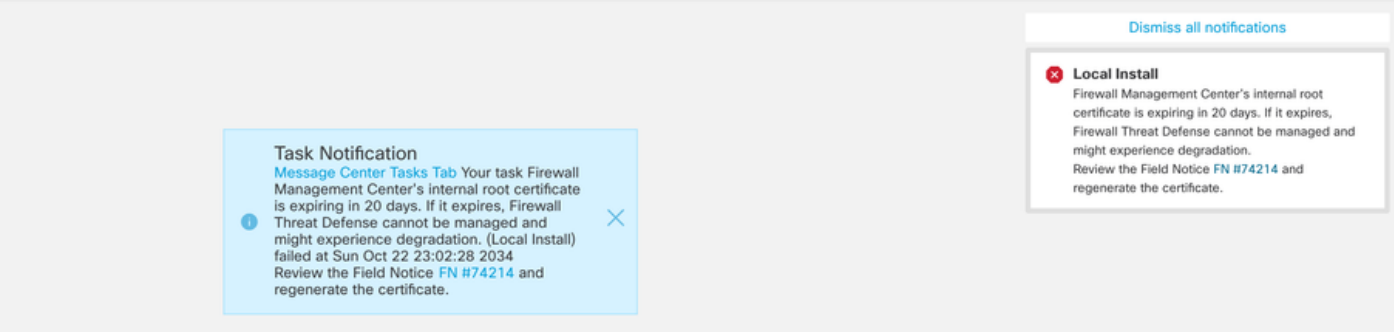
Comment être averti à l'avenir de l'expiration prochaine d'un certificat ?

Avec les mises à jour récentes de VDB (399 ou plus), vous êtes automatiquement alerté lorsque votre certificat expire dans les 90 jours. Par conséquent, vous n'avez pas besoin d'effectuer un suivi manuel vous-même, car vous êtes alerté lorsque vous approchez du délai d'expiration. Il apparaît ensuite sur la page Web de FMC sous deux formes. Les deux méthodes font référence à la page d'avis de champ.

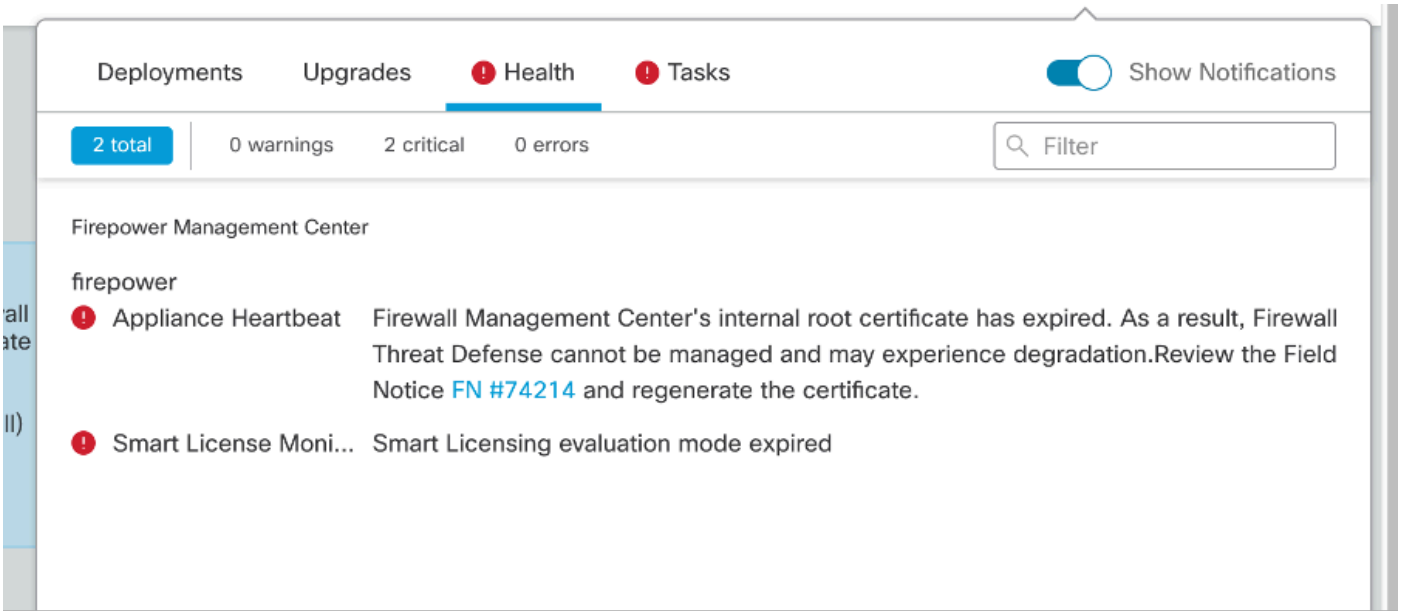
La première méthode est via l'onglet Tâche. Ce message est rémanent et disponible pour l'utilisateur, sauf s'il est explicitement fermé. La fenêtre contextuelle de notification s'affiche également et est disponible jusqu'à ce que l'utilisateur la ferme explicitement. Il s'affiche toujours comme une erreur.



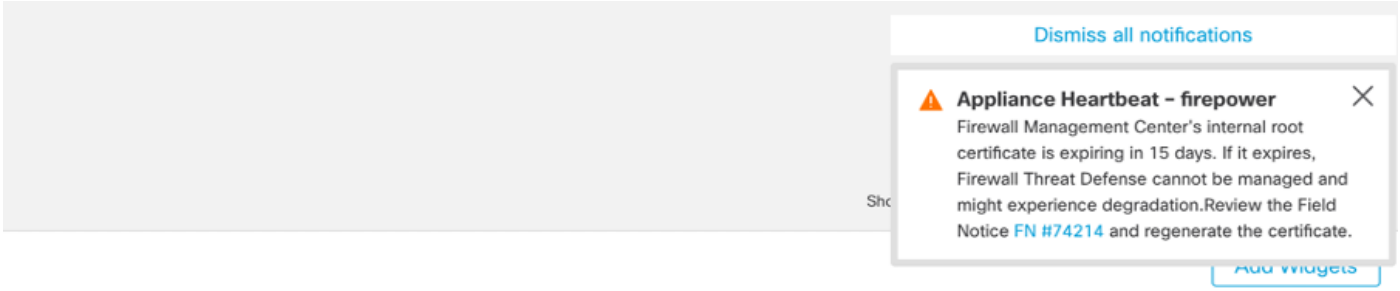
Notification d'expiration sur l'onglet Tâche



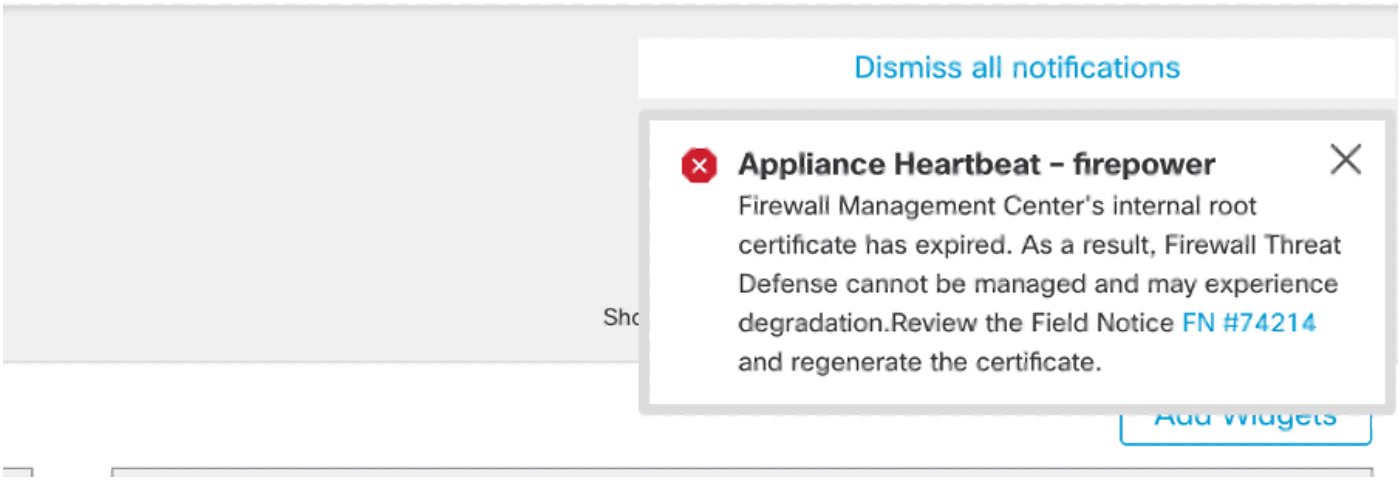
La deuxième méthode est via Health Alert. Cela apparaît dans l'onglet Health (Intégrité), mais cela n'est pas rémanent et remplace ou supprime lorsque le moniteur d'intégrité est exécuté, qui par défaut est toutes les 5 minutes. Il affiche également une fenêtre contextuelle de notification qui doit être explicitement fermée par l'utilisateur. Cela peut apparaître à la fois comme une erreur (lorsqu'il est arrivé à expiration) et comme un avertissement (lorsqu'il va expirer).



Notification d'expiration sur l'onglet Intégrité



Notification d'avertissement dans la fenêtre contextuelle Alerte d'intégrité



Notification d'erreur dans la fenêtre contextuelle Alerte d'intégrité

Solution 1 - Le certificat n'a pas encore expiré (scénario idéal)

C'est la meilleure situation car, selon l'expiration du certificat, nous avons encore le temps. Soit nous adoptons l'approche entièrement automatisée (recommandée) qui dépend de la version FMC, soit nous adoptons une approche plus manuelle qui nécessite l'intervention du TAC.

Approche recommandée

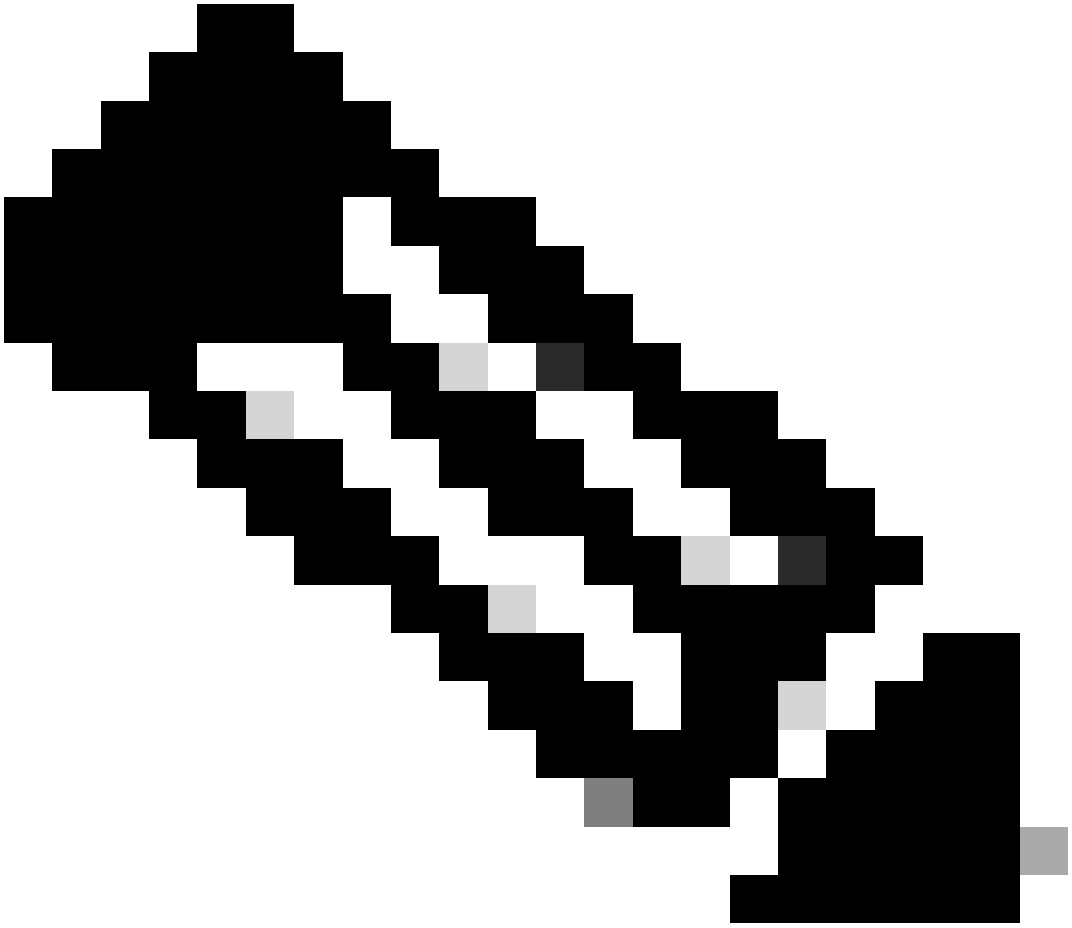
Il s'agit d'une situation dans laquelle aucun temps d'arrêt et un minimum d'opérations manuelles sont prévus dans des circonstances normales.

Avant de continuer, vous devez installer le correctif logiciel correspondant à votre version spécifique, comme indiqué ici. L'avantage ici est que ces correctifs ne nécessitent pas un redémarrage du FMC et donc une éventuelle rupture de la communication sftunnel lorsque le certificat a déjà expiré. Les correctifs disponibles (les liens de téléchargement sont pour FMC virtuel, pour FMC matériel regardez sur les pages de téléchargement appropriées pour les versions) sont :

- 7.0.0 - 7.0.6: Correctif FK - 7.0.6.99-9
- 7.1.x : pas de version fixe en fin de maintenance logicielle
- 7.2.0 - 7.2.9: Hotfix FZ - 7.2.9.99-4
- 7.3.x : HotFix AE - 7.3.1.99-4
- 7.4.0 - 7.4.2: Hotfix AO - 7.4.2.99-5
- 7.6.0 : Correctif B - 7.6.0.99-5

Une fois le correctif installé, le FMC contient maintenant le script generate_certs.pl qui :

1. Régénère la CA interne
2. Recrée les certificats sftunnel signés par cette nouvelle autorité de certification interne
3. Diffuse les nouveaux certificats sftunnel et les clés privées vers les périphériques FTD respectifs (et FMC secondaire le cas échéant) (lorsque le sftunnel est opérationnel)



Remarque : Le script generate_certs.pl vérifie actuellement si des opérations critiques sont en cours d'exécution. Si ce n'est pas le cas, son exécution échoue.

Les opérations critiques peuvent être : Agent Smart non enregistré ou enregistrement en cours, Tâche de sauvegarde/restauration en cours, Tâche de mise à jour SRU en cours, Tâche de mise à jour VDB en cours, Tâche de domaine en cours, Opération HA en cours ou Mise à niveau en cours d'exécution.

Par conséquent, vous ne pouvez pas exécuter ce script lorsque vous utilisez uniquement des licences classiques sur votre FMC (ou que l'une des opérations répertoriées doit être terminée en premier), auquel cas vous devez contacter le TAC Cisco pour contourner cette vérification, régénérer les certificats, puis annuler le contournement à nouveau.

Il est donc recommandé (si possible) de :

1. Installez le correctif logiciel correspondant à votre version de train
2. Effectuez une sauvegarde sur le FMC

3. Validez toutes les connexions sftunnel actuelles en utilisant le script sftunnel_status.pl sur le FMC (à partir du mode expert)
4. Exécutez le script en mode expert en utilisant generate_certs.pl
5. Examiner le résultat pour vérifier si des opérations manuelles sont nécessaires (lorsque les périphériques ne sont pas connectés au FMC) [expliqué plus loin]
6. Exécutez sftunnel_status.pl à partir du FMC pour valider que toutes les connexions sftunnel fonctionnent correctement

```
root@fmcv72-stejanss:/Volume/home/admin# generate_certs.pl
setting log file to /var/log/sf/sfca_generation.log

You are about to generate new certificates for FMC and devices.
After successful cert generation, device specific certs will be pushed automatically
If the connection between FMC and a device is down, user needs to copy the certificates onto the device manually
For more details on disconnected devices, use sftunnel_status.pl
Do you want to continue? [yes/no]:yes

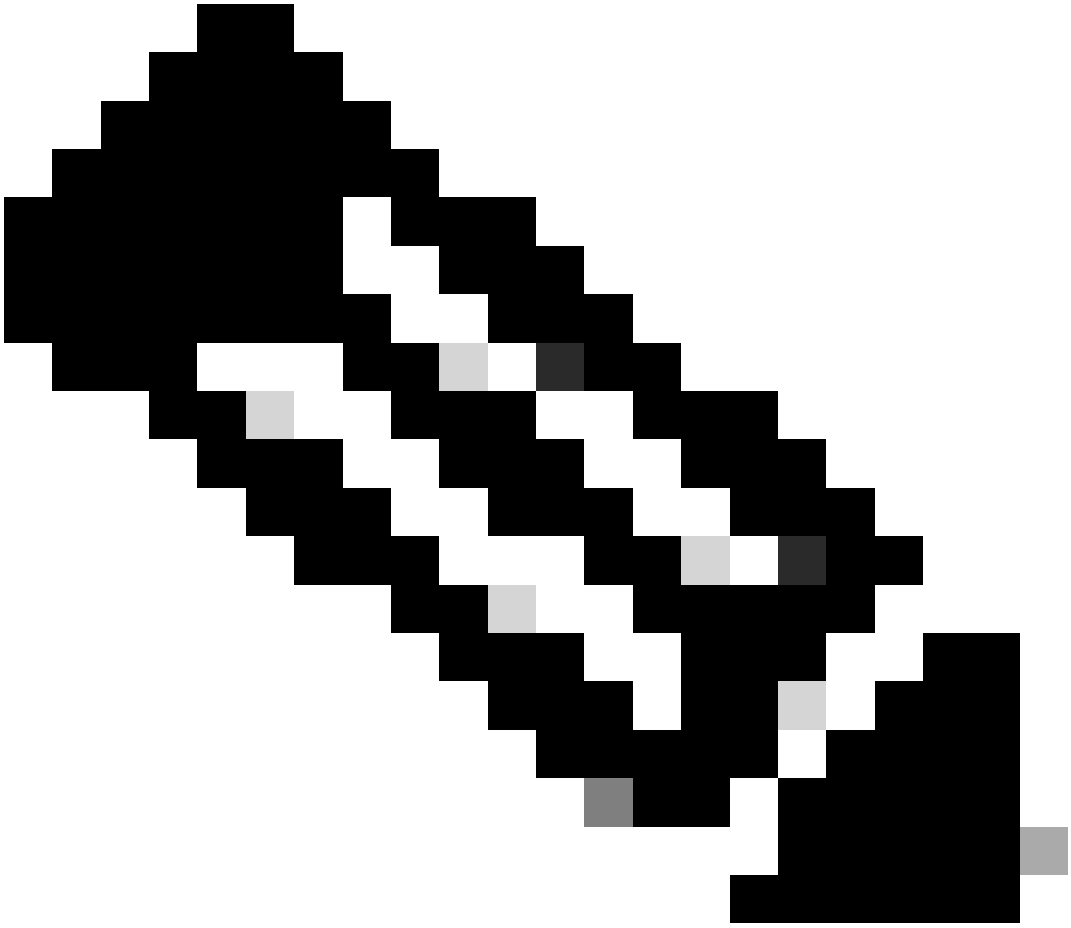
Current ca_root expires in 3646 days - at Oct  9 10:12:50 2034 GMT
Do you want to continue? [yes/no]:yes

Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem

Some files were failed to be pushed to remote peers. For more details check /var/tmp/certs/1728915794/FAILED_PUSH

Scalars leaked: 1
root@fmcv72-stejanss:/Volume/home/admin#
```

Script Generate_certs.pl



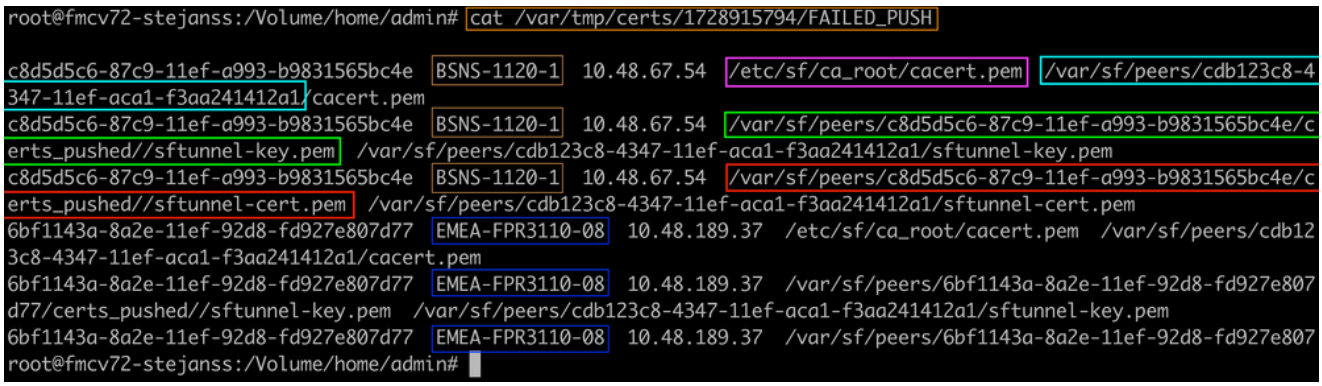
Remarque : Lorsque FMC est exécuté en haute disponibilité (HA), vous devez d'abord effectuer l'opération sur le noeud principal, puis sur le noeud secondaire, car il utilise ces certificats pour communiquer entre les noeuds FMC. L'autorité de certification interne sur les deux noeuds FMC est différente, de sorte qu'ils ont des délais d'expiration différents. Vous pouvez trouver plus d'informations sur les certificats dans FMC HA sur cette section.

Dans l'exemple ici, vous voyez qu'il crée un fichier journal sur /var/log/sf/sfca_generation.log, indique d'utiliser sftunnel_status.pl, indique l'heure d'expiration sur l'InternalCA et indique pour toute défaillance sur elle. Ici, par exemple, il n'a pas réussi à transmettre les certificats au périphérique BSNS-1120-1 et au périphérique EMEA-FPR3110-08, ce qui est attendu parce que le sftunnel était désactivé pour ces périphériques.

Afin de corriger le sftunnel pour les connexions défaillantes, vous exécutez les étapes suivantes :

1. Sur l'interface de ligne de commande de FMC, ouvrez le fichier FAILED_PUSH en utilisant

cat /var/tmp/certs/1728303362/FAILED_PUSH (la valeur du nombre représente l'heure unix, vérifiez donc le résultat de la commande précédente dans votre système) qui a le format suivant : FTD_UUID FTD_NAME FTD_IP SOURCE_PATH_ON_FMC DESTINATION_PATH_ON_FTD



ECHEC_POUSSÉE

2. Transférez ces nouveaux certificats (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) du FMC vers les périphériques FTD
   ===Approche automatique===

   L'installation du correctif fournit également les scripts copy_sftunnel_certs.py et copy_sftunnel_certs_jumpserver.py qui automatisent le transfert des différents certificats vers les systèmes pour lesquels le sftunnel n'était pas activé pendant la régénération des certificats. Cela peut également être utilisé pour les systèmes qui avaient une connexion sftunnel interrompue parce que le certificat a déjà expiré.

   Vous pouvez utiliser le script copy_sftunnel_certs.py quand le FMC lui-même a un accès SSH aux différents systèmes FTD (et potentiellement au FMC secondaire le cas échéant). Si ce n'est pas le cas, vous pouvez télécharger le script (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) du FMC vers un serveur de saut qui a un accès SSH à la fois aux FMC et aux périphériques FTD et exécuter le script Python à partir de là. Si cela n'est pas possible, suggérez d'exécuter l'approche manuelle indiquée ci-dessous. Les exemples suivants montrent le script copy_sftunnel_certs.py utilisé, mais les étapes sont les mêmes pour le script copy_sftunnel_certs_jumpserver.py.

   A. Créez un fichier CSV sur le FMC (ou serveur de saut) qui contient les informations de périphérique (nom_périphérique, adresse IP, nom_utilisateur_admin, mot_de_passe_admin) utilisées pour établir la connexion SSH.

   Lorsque vous exécutez ceci à partir d'un serveur distant comme un serveur de saut pour le FMC principal, assurez-vous d'ajouter dans les détails du FMC principal comme la première entrée suivie par tous les FTD gérés et FMC secondaire. Lorsque vous exécutez ceci à partir d'un serveur distant comme un serveur de saut pour le FMC secondaire, assurez-vous d'ajouter dans les détails du FMC secondaire comme première entrée suivie de tous les FTD

gérés. Vous trouverez plus d'informations sur les certificats dans FMC HA dans cette section.

i. Créez un fichier à l'aide de vi devices.csv.

```
root@firepower:/Volume/home/admin# vi devices.csv
```

périphériques vi.csv

ii. Cela ouvre le fichier vide (non affiché) et vous remplissez les détails comme indiqué après avoir utilisé i letter sur le clavier pour passer en mode INTERACTIF (vu en bas de l'écran).



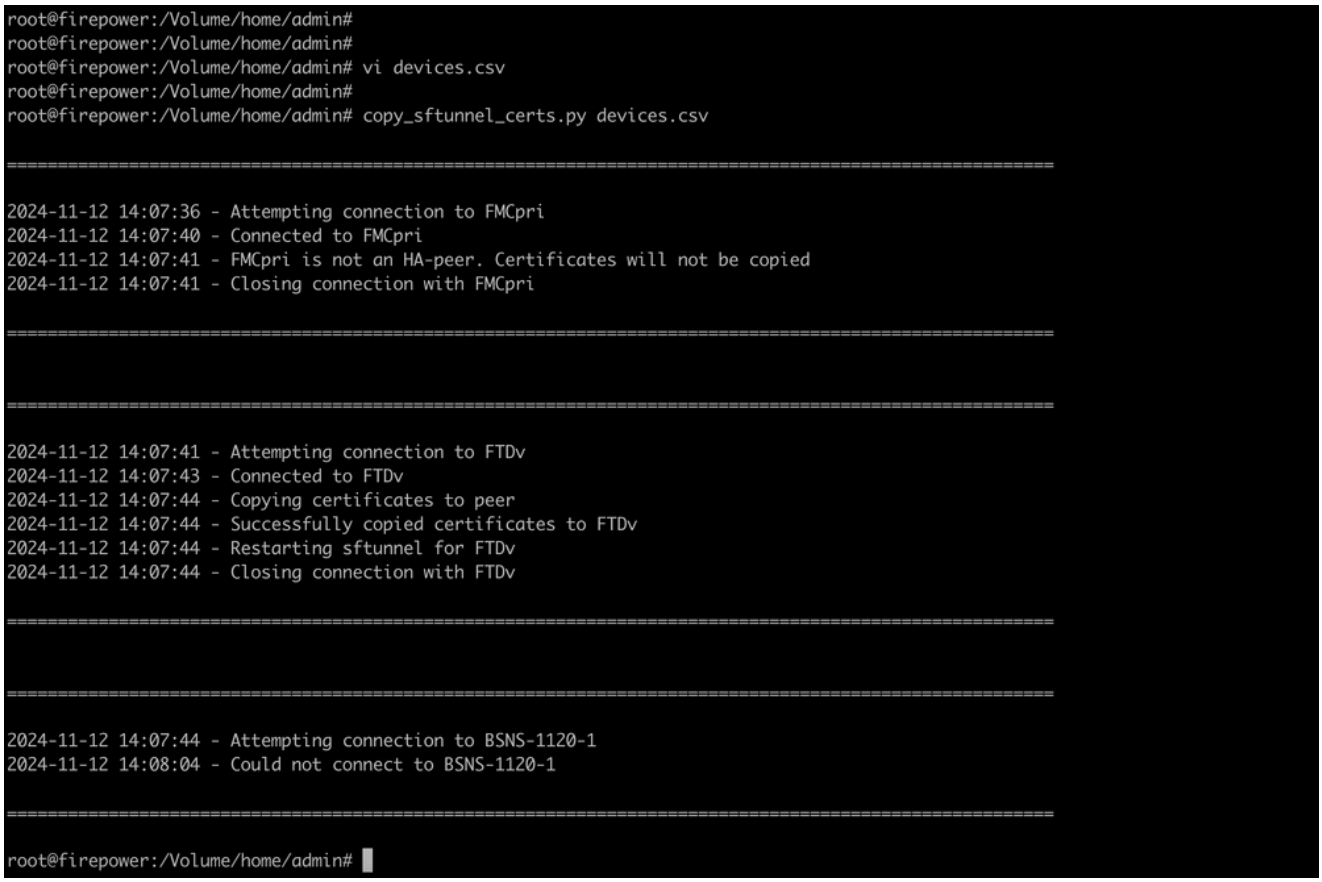
devices.csv, exemple

iii. Une fois terminé, vous fermez et enregistrez le fichier en utilisant ESC suivi de :wq et puis Enter.



Enregistrez les périphériques.csv

B. Exécutez le script (à partir de la racine en utilisant sudo) avec copy_sftunnel_certs.py devices.csv et il vous montre le résultat. Ici, il montre que le certificat vers FTDv a été correctement envoyé et que pour BSNS-1120-1, il n'a pas pu établir la connexion SSH au périphérique.



copy_sftunnel_certs.py devices.csv

===Approche manuelle===

1. Imprimez (cat) la sortie de chacun des fichiers pour chaque FTD (ou FMC secondaire dans HA) affecté (cacert.pem / sftunnel-key.pem (non affiché complètement à des fins de sécurité) / sftunnel-cert.pem) sur l'interface de ligne de commande FMC en copiant l'emplacement du fichier à partir de la sortie précédente (fichier FAILED_PUSH).

```
root@fmcv72-stejanss:/Volume/home/admin# cat /etc/sf/ca_root/cacert.pem
-----BEGIN CERTIFICATE-----
MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwgYcxEzARBgNVBAwMCkludGVybmFs
Q0ExJDAiBgNVBAsMG0ludHJ1c2lvbiBNYW5hZ2VtZW50IFN5c3RlbTEtMCsGA1UE
AwwkY2RiMTIzYzgtNDM0Ny0xMWVmLWFjYTEtZjNhYTI0MTQxMmExMRswGQYDVQQK
DBJDaXNjbyBTeXN0ZW1zLCBJbmMwHhcNMjQxMDE0MTQyMzI4WhcNMzQxMDEyMTQy
MzI4WjCBhzETMBEGA1UEDAwKSW50ZXJuYWxDQTEkMCIGA1UECwwbSW50cnVzaW9u
IE1hbmFnZW1lbnQgU3lzdGVtMS0wKwYDVQQDDCRjZGIxMjNjOC00MzQ3LTExZWYt
YWNhMS1mM2FhMjQxNDEyYTExGzAZBgNVBAoMEkNpc2NvIFN5c3RlbXMsIEluYzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMmUav8kVukF
xiV917W4d7/CYBb4pd1KiMOijAEp3wqxmdpDUQ4KBDWnC5+p8dg+XK7AspOW36CD
mdpRwRfqM7J51txEUyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6VlQl+aRlAPCF
7UYpMgFPh3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXnL6Jn3rfoKbF0M77
xUtiMeC05O4buhfzSltAm5J0bFuXMcPYq1N+t137rl/1etwHzmjVkE7g/rfNv0yO
N+4m8i5QRN0BoghtZO+Y/PudToSX0VmKh5Sq/i1MvOYBZEIM3Dx+Gb/DQYBWLEUC
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAY2EVhEoylDdlWSu2ewdehthBtI6Q5x7e
UD187bbowmTJsdlOOLVGgYoU5qUFDh3NAqSxrDHEu/NsLUbrRiA30RI8WEA1o/S6
J3Q1F3hJJFOqSrlIx/ST72jgL2o87ixhRIzreB/+26rHo5nns2r2tFss61KBltWN
nRZnSIYAwYhqGCjH9quiZpfDJ3N83oREGX+xflYqFim5h3rFwk0J2q6YtaBJAuwg
0bldXGnrnWuIIV/xbOcwKbrALmtanhgGXyqT/pMYrjwlI1xVLl6/PrMTV29WcQcA
IVBnyzhS4ER9sYIKB5V6MK4r2gJDG1t47E3RYnstyGx8hlzRvzHz2w==
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

cacert.pem

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed//sftunnel-key.pem
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDcy5A0xZ5N22qD
```

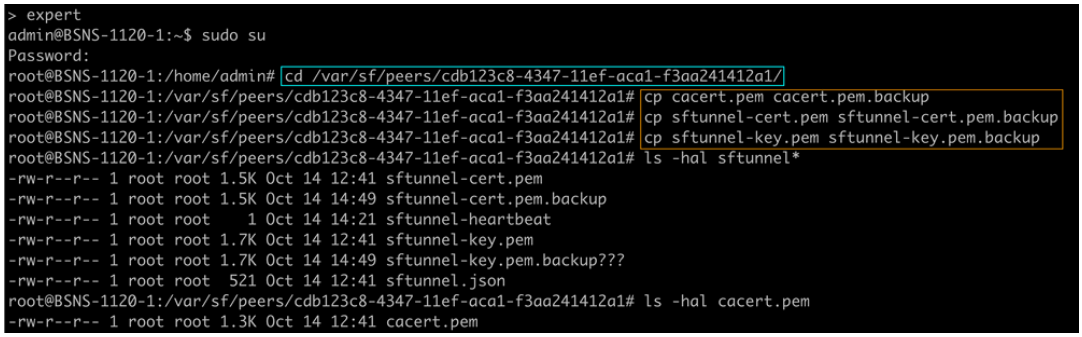
sftunnel-key.pem

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed//sftunnel-cert.pem
-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIBDTANBgkqhkiG9w0BAQsFADCBhzETMBEGA1UEDAwKSW50
ZXJuYWxDQTEkMCIGA1UECwwbSW50cnVzaW9uIE1hbmFnZW1lbnQgU3lzdGVtMS0w
KwYDVQQDDCRjZGIxMjNjOC00MzQ3LTExZWYtYWNhMS1mM2FhMjQxNDEyYTExGzAZ
BgNVBAoMEkNpc2NvIFN5c3RlbXMsIEluYzAeFw0yNDEwMTMxNDIzMzFaFw0zNDEw
MTIxNDIzMzFaMIGZMRIwEAYDVQQDDAlsb2NhbGhvc3QxJDAiBgNVBAsMG0ludHJ1
c2lvbiBNYW5hZ2VtZW50IFN5c3RlbTEbMBkGA1UECgwSQ2lzY28gU3lzdGVtcywg
SW5jMS0wKwYDVQQMDCRjOGQ1ZDVjNi04N2M5LTExZWYtYTk5My1iOTgzMTU2NWJj
NGUxETAPBgNVBCwMCHNmdHVubmVsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA3MuQNMWeTdtqg2k52FKHY2dQJEHc0mdUc/YOKniUUa45iAdLBv0X8l9y
lQFPFdlurv4mYxgDoBDCzoZLLiRBeaaXcZnowoqmatvOMtMyL0ITNTL+5G/KiyCr
gsz2ub03avXW/cbC2WZQGat0kQ/4Fb+LC5dnX2KA5H7m1rsOWNWEKFspn/Y2UYGb
Zdi3bZz5wy5YHGGFQ8KKO4v4mksSu02b+AWfIgOe1EaSwv5K+Wa0ssj6keaCkYfA
TP1sEiYkytFdE0f2s8mXfSfLbK+8hI+jWqAN/QOa3D9gHD8gErPHgLDBm30Tqp8s
kRf5JEIsU5HHwlvT0FKbhWEW069O6QIDAQABo0IwQDAJBgNVHRMEAjAAMBQGA1Ud
EQQNMAuCCWxvY2FsaG9zdDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
DQYJKoZIhvcNAQELBQADggEBAAHHAjwZHXG1nA+jAxGIaL6T/L2oYCDxuB3tcNKW
ZViILv11OcUNYIvC/w7JbKllUTLbit0aH01ff4lcv0q6uk+SL7cAuAIcXodP1EQo
ERz4E13a0MNNnvi5dT/a2fhIxzimhIq7P3zTMuKknVyblg0RqG7q8SxyEL5AT8Iy
beuhcg6+7LZcIw29/pTzCnycIrzBhBVK2ZcQ9vYtBXxDCaZGK17lnYiEpK4Qifne
9A2tQQecypKRRA5d60uttEmVvpHCgMtGrC6OKb5h5SPO0Ze1rGWDoV9eTj1NJis0
+J+WXE06VApIl7aYKWXXhHLGF7n+esy1GaZ3Djn44mMkn8I=
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

sftunnel-cert.pem

2. Ouvrez l'interface de ligne de commande FTD (ou FMC secondaire dans FMC HA) de chaque FTD respectif en mode expert avec les privilèges root via sudo su et renouvelez les certificats avec la procédure suivante.
    1. Recherchez l'emplacement indiqué sur la surbrillance bleu clair de la sortie FAILED_PUSH (cd/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1 ici par exemple, mais il est différent pour chaque FTD).
    2. Effectuer des sauvegardes des fichiers existants.

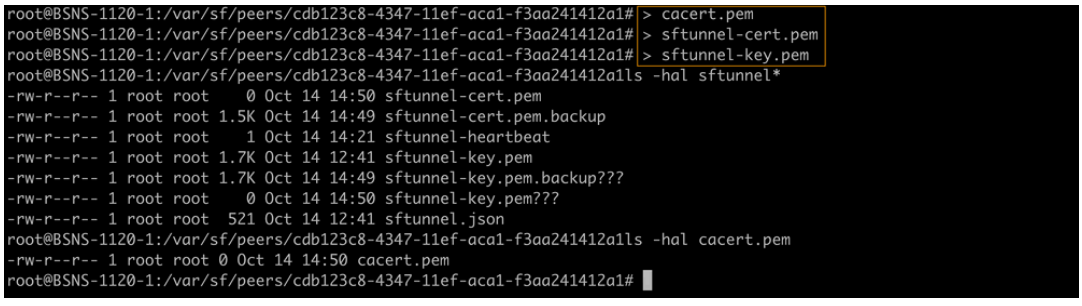
```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```



Effectuer des sauvegardes des certificats actuels

    3. Videz les fichiers afin que nous puissions y écrire du nouveau contenu.

```
> cacert.pem
> sftunnel-cert.pem
> sftunnel-key.pem
```



Contenu vide des fichiers de certificats existants

    4. Écrivez le nouveau contenu (à partir de la sortie FMC) dans chacun des fichiers individuellement en utilisant vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (commande séparée par fichier - les captures d'écran ne montrent cela que pour cacert.pem mais doivent être répétées pour

sftunnel-cert.pem et sftunnel-key.pem).

vi cacert.pem

1. Appuyez sur i pour passer en mode interactif (après avoir entré la commande vi et vu un fichier vide).
2. Copiez et collez l'intégralité du contenu (y compris -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----) dans le fichier.



Copier le contenu en vi (mode INSERT)

3. Fermez le fichier et écrivez-le avec ESC suivi de :wq, puis entrez.



Échap suivi de : wq pour écrire dans le fichier

1. Vérifiez que les autorisations correctes (chmod 644) et les propriétaires (chown root:root) sont définis pour chaque fichier à l'aide de la commande ls -hal. Ceci est correctement défini en fait lorsque nous mettons à jour le fichier existant.

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal
total 68K
drwxr-xr-x 4 root root 4.0K Oct 14 15:01 .
drwxr-xr-x 3 root root 4.0K Oct 14 15:01 ..
-rw-r--r-- 1 root root    0 Oct 14 12:42 LIGHT_REGISTRATION
-rw-r--r-- 1 root root    0 Oct 14 12:42 LIGHT_UNREGISTRATION
-rw-r--r-- 1 root root 2.0K Oct 14 12:45 LL-caCert.pem
-rw-r--r-- 1 root root 2.2K Oct 14 12:45 LL-cert.pem
-rw-r--r-- 1 root root 3.2K Oct 14 12:45 LL-key.pem
-rw-r--r-- 1 root root 1.3K Oct 14 14:55 cacert.pem
-rw-r--r-- 1 root root 1.3K Oct 14 14:49 cacert.pem.backup
-rw-r--r-- 1 root root 2.3K Oct 14 12:41 ims.conf
-rw-r--r-- 1 root root  221 Oct 14 12:41 peer_flags.json
drwxr-xr-x 3 root root   19 Oct 14 12:42 proxy_config
-rw-r--r-- 1 root root 1.2K Oct 14 12:42 sfipproxy.conf.json
-rw-r--r-- 1 root root 1.4K Oct 14 14:59 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root    1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 15:01 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root    0 Oct 14 14:50 sftunnel-key.pem???
-rw-r--r-- 1 root root  521 Oct 14 12:41 sftunnel.json
-rw-r--r-- 1 root root    5 Oct 14 12:48 sw_version
drwxr-xr-x 6 root root   90 Oct 14 12:42 sync2
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#
```

Tous les fichiers de certificat mis à jour avec les propriétaires et autorisations de droits

3. Redémarrez le sftunnel sur chaque FTD respectif (ou FMC secondaire dans FMC HA) où le sftunnel n'était pas opérationnel pour que les modifications dans le certificat prennent effet avec la commande pmtool restartbyid sftunnel

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# pmtool restartbyid sftunnel
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#
```

pmtool restartbyid sftunnel

3. Vérifiez que tous les FTD (et FMC secondaire) sont correctement connectés maintenant en utilisant la sortie sftunnel_status.pl

Solution 2 - Le certificat a déjà expiré

Dans cette situation, nous avons deux scénarios différents. Soit toutes les connexions sftunnel sont toujours opérationnelles, soit elles ne le sont plus (ou ne le sont plus partiellement).

FTD toujours connectés via sftunnel

Nous pouvons appliquer la même procédure que celle indiquée dans la section Certificat non encore expiré (scénario idéal) - Approche recommandée.

Cependant, ne mettez PAS à niveau ou ne redémarrez PAS le FMC (ou tout FTD) dans cette situation, car il déconnecte toutes les connexions sftunnel et nous devons exécuter manuellement toutes les mises à jour de certificat sur chaque FTD (et FMC secondaire comme décrit dans cette section). La seule exception à celle-ci, sont les versions de correctifs répertoriées car elles ne nécessitent pas de redémarrage du FMC.

Les tunnels restent connectés et les certificats sont remplacés sur chacun des FTD (et FMC secondaire lorsqu'il est dans FMC HA). Dans le cas où certains certificats ne seraient pas remplis, il vous invite avec ceux qui ont échoué et vous devez adopter l'approche manuelle comme indiqué précédemment sur la section précédente.

Les FTD ne sont plus connectés via sftunnel

Approche recommandée

Nous pouvons appliquer la même procédure que celle indiquée dans la section Certificat non encore expiré (scénario idéal) - Approche recommandée. Dans ce scénario, le nouveau certificat est généré sur le FMC, mais ne peut pas être copié sur les périphériques, car le tunnel est déjà arrêté. Ce processus peut être automatisé avec les scripts copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py

Si tous les périphériques FTD sont déconnectés du FMC, nous pouvons mettre à niveau le FMC dans cette situation car il n'a pas d'impact sur les connexions sftunnel. Si certains périphériques sont toujours connectés via sftunnel, alors sachez que la mise à niveau du FMC ferme toutes les connexions sftunnel et qu'elles ne se réactivent pas en raison de l'expiration du certificat. L'avantage de la mise à niveau ici serait qu'elle vous fournit une bonne orientation sur les fichiers de certificat qui doivent être transférés à chacun des FTD (et FMC secondaire quand dans FMC HA).

Approche manuelle

Dans cette situation, vous pouvez alors exécuter le script generate_certs.pl à partir du FMC qui génère les nouveaux certificats mais vous devez quand même les pousser vers chacun des FTD (et FMC secondaire comme décrit dans cette section) périphériques manuellement. En fonction de la quantité de périphériques, cette opération est faisable ou peut s'avérer fastidieuse. Cependant, lors de l'utilisation des scripts copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py, ceci est hautement automatisé.

Annexe

Certificats utilisés dans FMC HA

La communication entre les FMC principal et secondaire dans une paire haute disponibilité se produit également sur le sftunnel, de la même manière qu'un FMC qui communique sur les périphériques FTD. Les éléments de certificat (cacert.pem / sftunnel-cert.pem / sftunnel-key.pem) sont stockés sur le FMC au même endroit sous /var/sf/peers/<UUID-FMC>. Cependant, c'est

toujours le FMC principal qui agit en tant que gestionnaire du FMC secondaire. De cette façon, le FMC secondaire est comme un dispositif FTD du point de vue du FMC primaire. Par conséquent, vous ne voyez le certificat que sur le FMC secondaire et non sur les fichiers sur le FMC principal sur le dossier /var/sf/peers/.

Souvent, votre FMC secondaire a été créé à une date ultérieure à votre FMC principal et ainsi l'autorité de certification interne peut toujours être valide et pas encore expiré contrairement à votre FMC principal. Par conséquent, un changement de rôle manuel du FMC actif pourrait être une option pour minimiser l'impact dans les situations où le FMC secondaire aurait encore un certificat valide et donc des communications sftunnel associées avec tous les FTD. Cela vous permettrait ensuite de déployer des configurations pendant que vous préparez également le correctif ou la mise à jour sur le certificat du FMC principal. Cependant, la communication entre les deux périphériques FMC peut également être interrompue lorsque le sftunnel est arrêté après l'expiration du certificat du FMC principal.

Dans le processus de renouvellement des certificats, il existe deux scénarios différents :

1. Le certificat CA FMC principal a expiré : comme le FMC secondaire est considéré comme un FTD pour le FMC principal, le renouvellement de certificat doit diffuser les certificats mis à jour créés sur le FMC principal non seulement vers les périphériques FTD, mais également vers le FMC secondaire.

2. Le certificat CA FMC secondaire a expiré : dans cette situation, les seules mises à jour de certificat requises sont celles des périphériques FTD. Parce que la communication sftunnel entre les deux FMC dans HA est basée sur le certificat principal de l'autorité de certification FMC.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.