為FTD連線續訂FMC Sftunnel CA憑證

目錄

簡介

本檔案介紹有關Firepower威脅防禦(FTD)連線的Firepower管理中心(FMC)Sftunnel憑證授權單位(CA)憑證的續訂。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower威脅防禦
- Firepower管理中心
- 公開金鑰基礎架構 (PKI)

採用元件

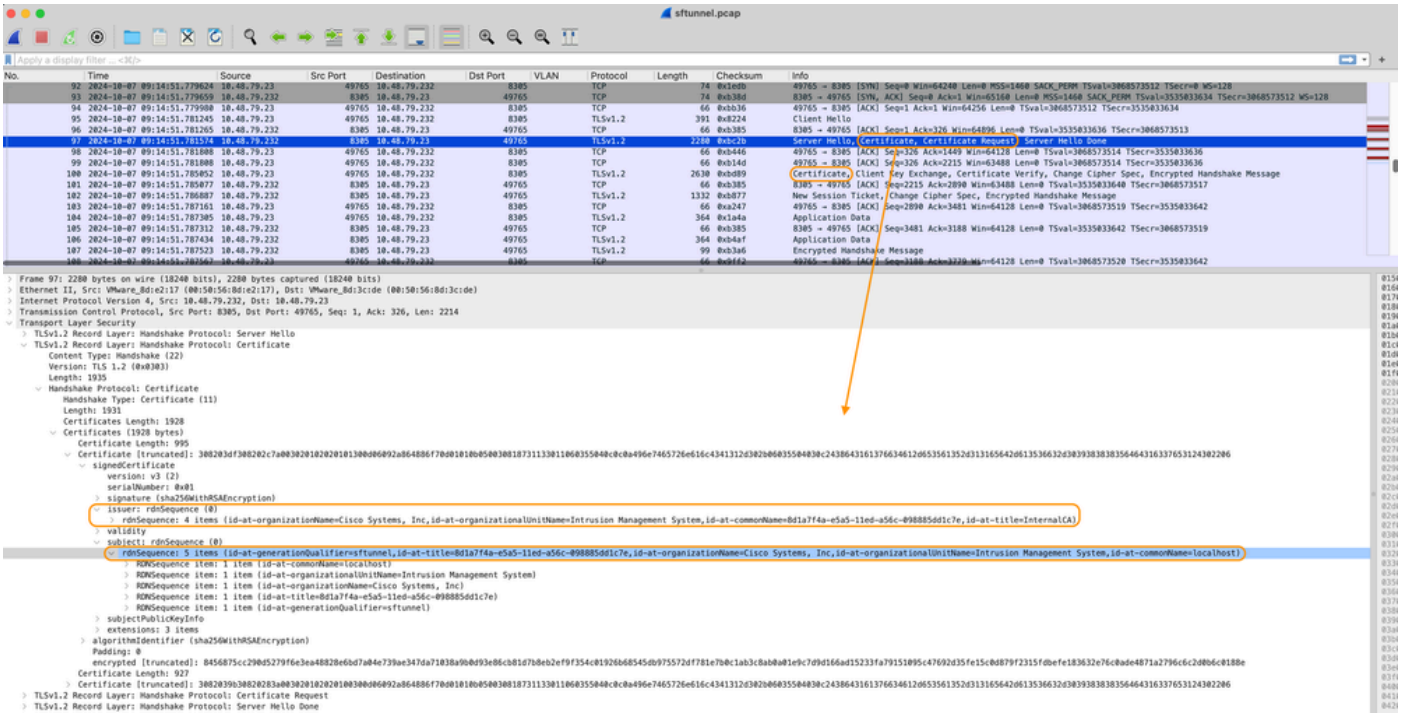
本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

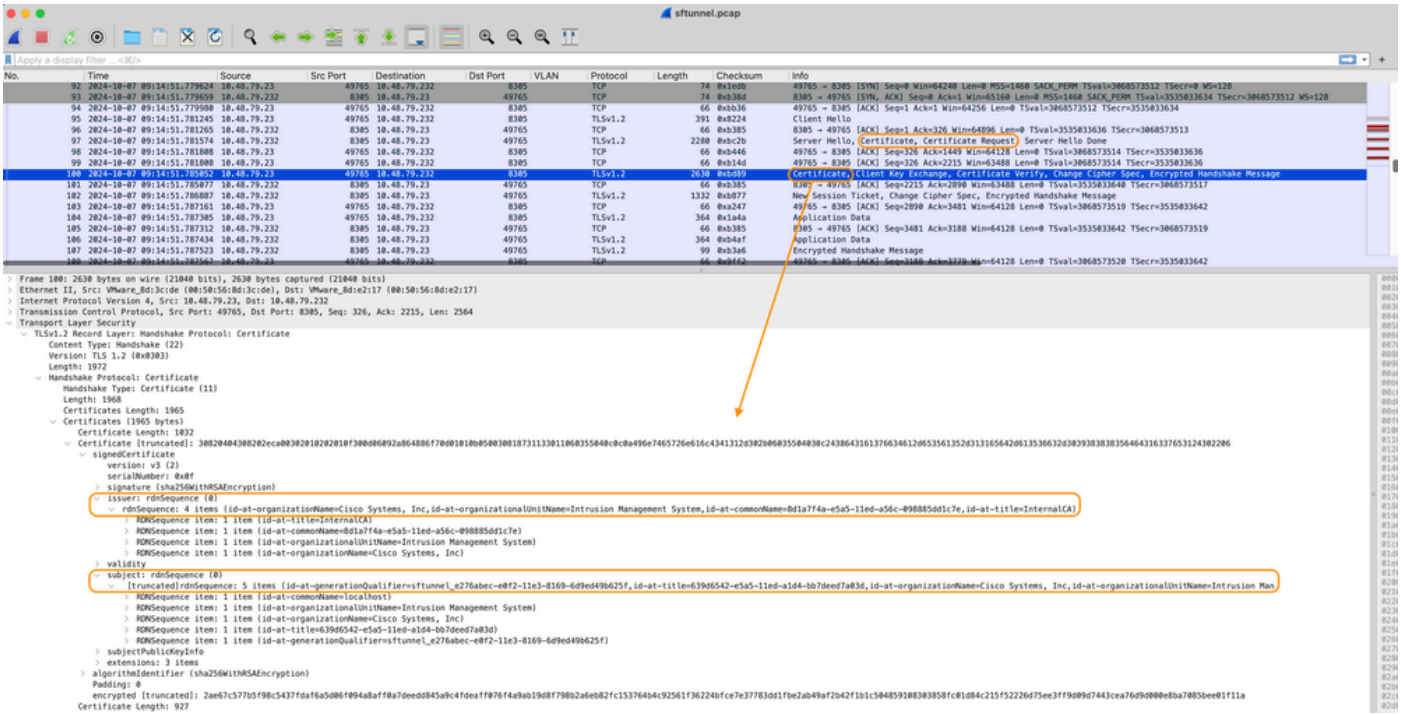
背景資訊

FMC和FTD會通過sftunnel(Sourcefire tunnel)彼此通訊。 此通訊使用證書來確保TLS會話中的會話安全。有關sftunnel及其如何建立的詳細資訊，可在該連結上找到。

透過封包擷取，您可以看到FMC（本範例中為10.48.79.232）和FTD(10.48.79.23)正在相互交換憑證。他們這樣做是為了驗證他們是否與正確的裝置進行了通訊，以及是否不存在竊聽或中間人(MITM)攻擊。使用這些證書對通訊進行加密，只有擁有該證書的關聯私鑰的一方才能再次對其進行解密。



Certificate_exchange_server_cert



Certificate_exchange_client_cert

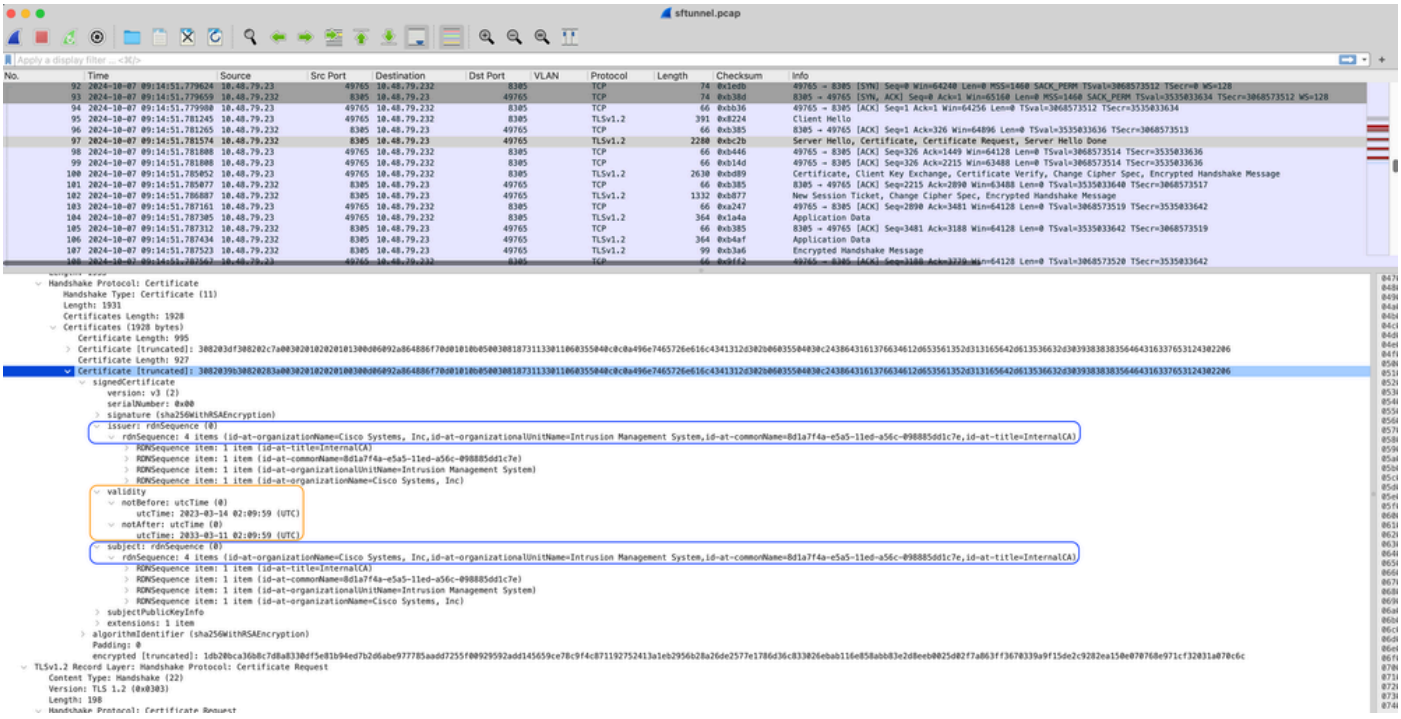
您可以看到憑證是由在FMC系統上建立的同一InternalCA(Issuer)憑證授權單位(CA)簽署。配置在/etc/sf/sftunnel.conf檔案上的FMC中定義，該檔案包含以下內容：

```
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;
};
```

這表示用於簽署sftunnel（FTD和FMC一）的所有憑證的CA，以及FMC用於傳送給所有FTD的憑證。此證書由InternalCA簽名。

當FTD註冊到FMC時，FMC也會建立一個憑證以推送到FTD裝置，該憑證用於sftunnel上的進一步通訊。此證書也由同一內部CA證書簽名。在FMC上，您可以在/var/sf/peers/<UUID-FTD-device>下找到證書（和私鑰），也可能在certs_pused資料夾下，稱為sftunnel-cert.pem(對於私鑰，sftunnel-key.pem)。 在FTD上，可以找到在/var/sf/peers/<UUID-FMC-device>下使用相同命名約定的路由器。

但是，出於安全考慮，每個證書也有一個有效期。檢查InternalCA憑證時，我們可以看到封包擷取中所示的FMC InternalCA的有效期為10年。

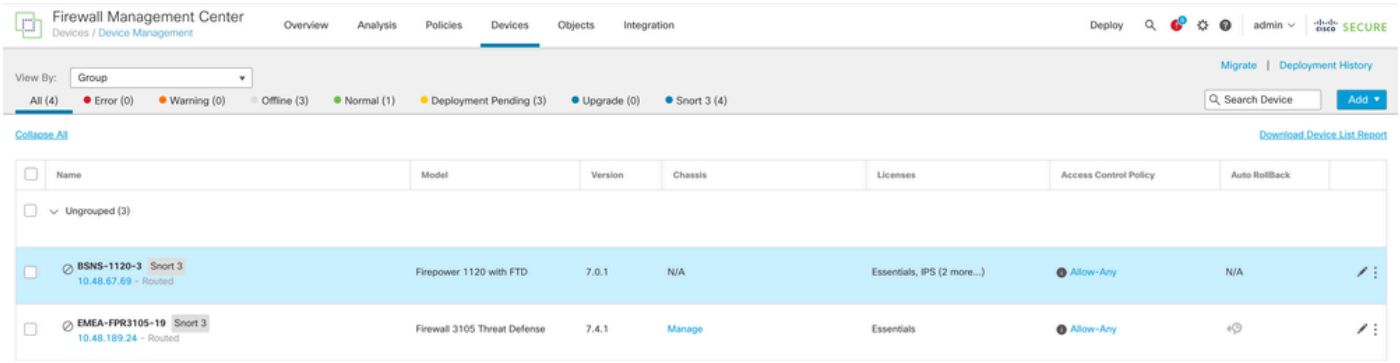


FMC-InternalCA_validity

問題

FMC InternalCA證書的有效期僅為10年。到期時間過後，遠端系統不再信任此證書（以及由其簽名的證書），這將導致FTD和FMC裝置之間的隧道通訊問題。這也意味著一些關鍵功能（如連線事件、惡意軟體查詢、基於身份的規則、策略部署以及許多其他功能）無法正常工作。

當sftunnel未連線時，裝置在Devices > Device Management頁籤下的FMC UI中顯示為已禁用。在思科錯誤ID CSCwd08098上，會追蹤與此過期時間相關的問題。雖然請注意，即使您執行的是錯誤的固定版本，所有系統仍會受到影響。有關此修補程式的更多資訊，請參閱解決方案部分。



已禁用裝置

FMC不會自動刷新CA並將憑證重新發佈到FTD裝置。此外，也沒有指示證書到期的FMC運行狀況警報。在此方面跟蹤思科錯誤ID CSCwd08448，以便將來在FMC UI上提供運行狀況警報。

到期日期後會發生什麼？

一開始什麼也沒發生，而sftunnel通訊通道繼續像以前一樣運行。但是，當FMC和FTD裝置之間的sftunnel通訊中斷並嘗試重新建立連線時，它確實會失敗，並且您可以觀察消息日誌檔案中指向證書到期的日誌行。

來自FTD裝置的/ngfw/var/log/messages的日誌行:

```
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 e
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 fail
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [WARN] SSL Verification status: ce
```

來自FMC裝置的日誌行，來自/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: Fail
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl [ERROR] establishSSLConnection: Unab
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: Fail
```

Sftunnel通訊可能由於多種原因而中斷：

- 由於網路連線丟失而丟失通訊（可能只是暫時的）
- 重新啟動FTD或FMC
  - 預期的：在FMC或FTD上手動重新啟動、升級、手動重新啟動sftunnel程式（例如通過pmtool restartbyid sftunnel）
  - 意外的：回溯，斷電

由於有太多可能性會中斷sftunnel通訊，因此強烈建議儘快糾正情況，即使目前所有FTD裝置都已正確連線（儘管憑證已過期）。

如何快速驗證憑證是否已到期或何時到期？

最簡單的方法是在FMC SSH會話上運行以下命令：

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

此處顯示憑證的「有效性」元素。此處的主要相關部分是「notAfter」，它表明此證書有效期至2034年10月5日。

```
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
```

NotAfter

如果您偏好立即執行單一命令，並給予您憑證仍然有效的天數，則可使用以下命令：

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

此處範例顯示憑證仍然有效多年的設定專案。

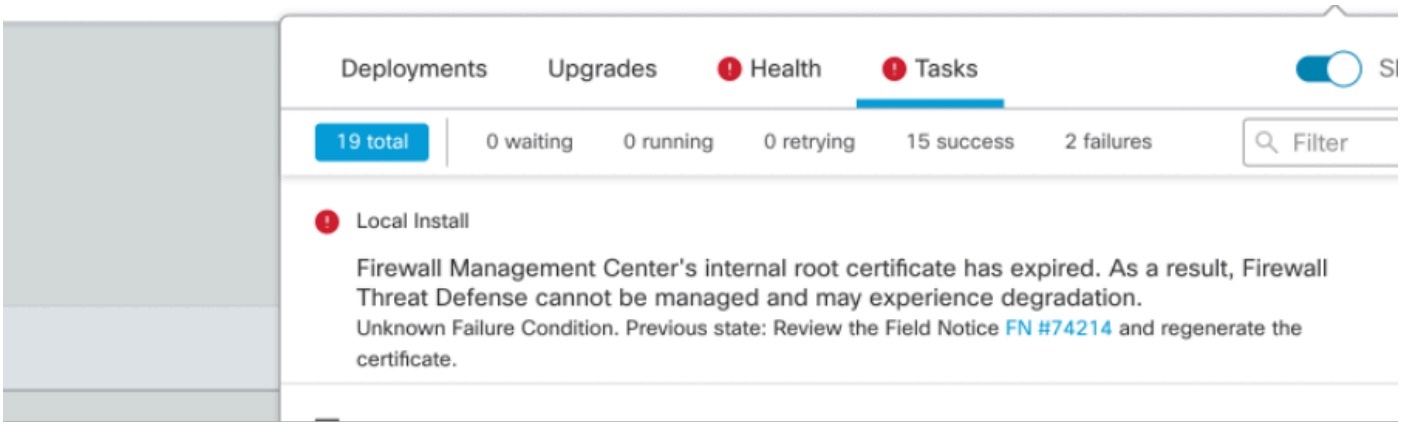
```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS + THIRTY_
DAYS_SECONDS)); DAYS_LEFT=$(( (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_expire_validation_command

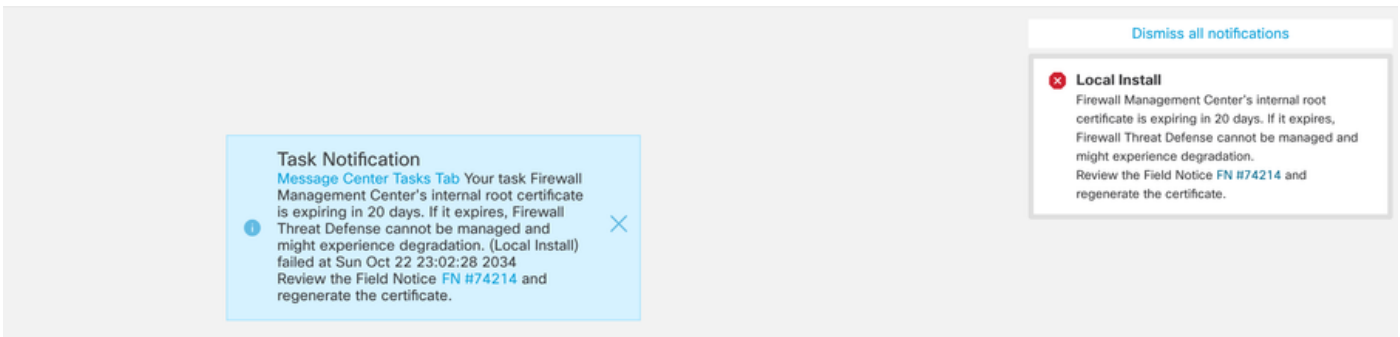
以後如何獲得有關即將到期的證書的通知？

使用最近的VDB更新（399或更高），當證書在90天內到期時，系統會自動通知您。因此，您自己無需手動跟蹤，因為當您接近到期時間時會收到警報。然後，它以兩種形式顯示在FMC網頁上。這兩種方式均請參閱現場通知頁面。

第一種方法是通過Task Tab。此消息是粘性的，除非明確關閉，否則使用者可以使用它。通知也會彈出，直到使用者明確關閉時才可用。它始終顯示為錯誤。

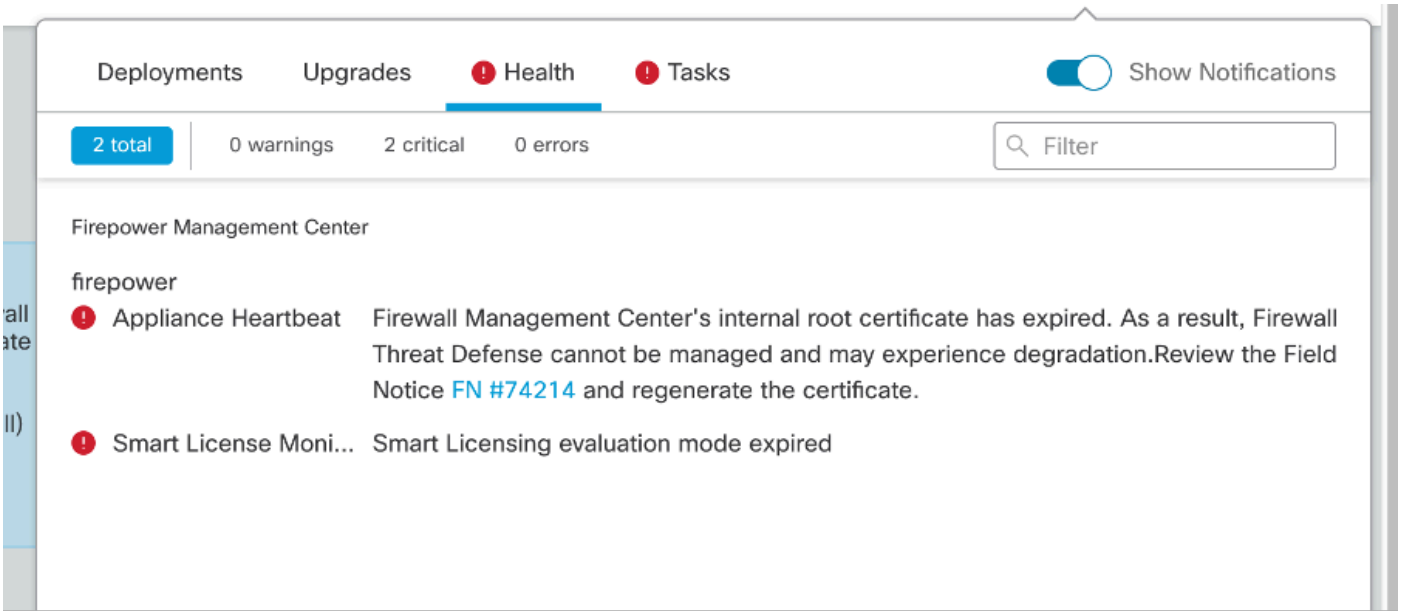


「任務」頁籤上的到期通知

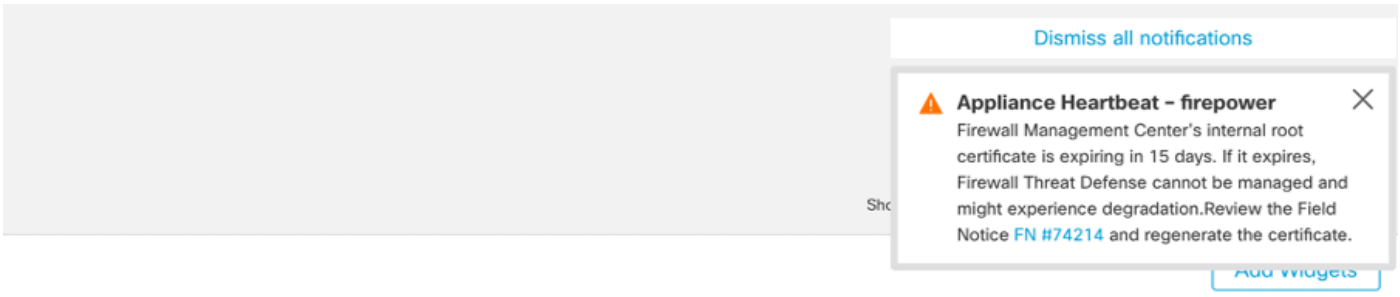


第二種方法是通過Health Alert。這顯示在運行狀況頁籤中，但這不是粘滯狀態，在運行運行狀況監視器時替換或刪除該資訊，預設情況下，運行狀況監視器每5分鐘運行一次。它還顯示一個通知彈出

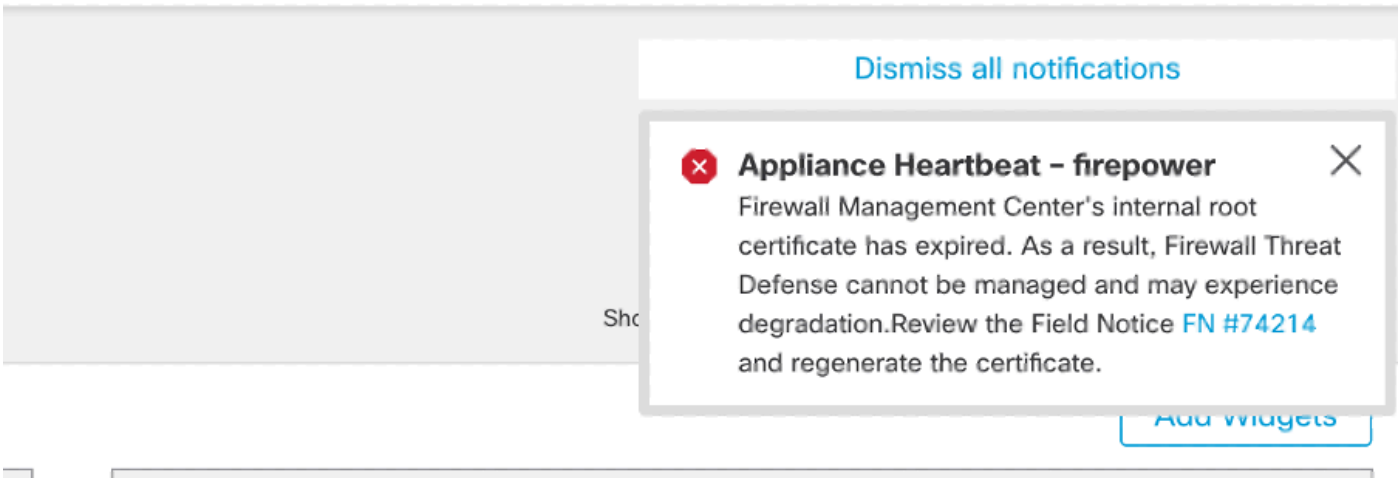
視窗，使用者需要顯式關閉該視窗。這可以同時顯示為錯誤（過期時）和警告（即將過期時）。



「健康」頁籤上的到期通知



健康警報彈出時的警告通知



出現健康警報彈出錯誤通知

解決方案1 — 證書尚未過期（理想情況）

這是最佳情況，因為根據證書到期時間，我們還有時間。我們要麼採用依賴於FMC版本的全自動方法（推薦），要麼採取需要TAC互動的更手動的方法。

推薦的方法

這種情況下，正常情況下預計不會出現停機時間和最少的人工操作。

在繼續操作之前，您必須按此處所列安裝特定版本的修補程式。此處的好處是，這些修補程式不要求重新啟動FMC，因此當證書過期時，可能會中斷sftunnel通訊。可用的修補程式包括：

- 7.0.0 - 7.0.6 :修補程式FK - 7.0.6.99-9
- 7.1.x :軟體維護結束時無固定版本
- 7.2.0 - 7.2.9 :修補程式FZ - 7.2.9.99-4
- 7.3.x :修補程式AE - 7.3.1.99-4
- 7.4.0 - 7.4.2 :修補程式AO - 7.4.2.99-5
- 7.6.0 :修補程式B - 7.6.0.99-5

安裝修補程式後，FMC現在應包含generate_certs.pl指令碼：

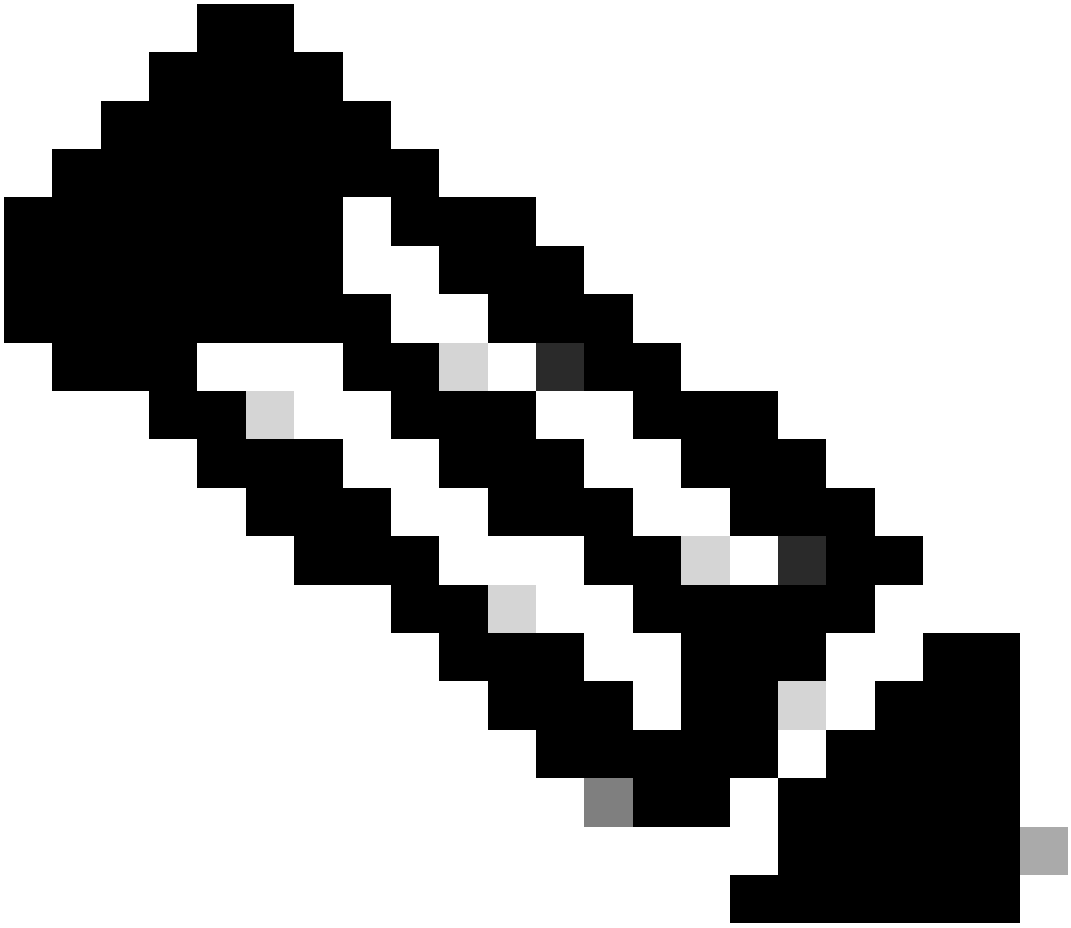
1. 重新生成內部CA
2. 重新建立由此新的InternalCA簽名的sftunnel證書
3. 將新的sftunnel憑證和私鑰推送到各自的FTD裝置（當sftunnel運作時）

因此，建議（如果可能）：

1. 安裝上面適用的修補程式
2. 對FMC進行備份
3. 在FMC上使用sftunnel_status.pl腳本驗證所有當前的sftunnel連線(從專家模式)
4. 使用generate_certs.pl從專家模式運行指令碼
5. 檢查結果以驗證是否需要任何手動操作（當裝置未連線到FMC時）[下面將進一步說明]
6. 從FMC運行sftunnel_status.pl，以驗證所有sftunnel連線是否運行正常

```
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#
```

Generate_certs.pl指令碼



附註：當在High-Availability(HA)中運行FMC時，您需要先在主節點上執行操作，然後在輔助節點上執行操作，因為它使用這些證書並在FMC節點之間進行通訊。兩個FMC節點上的InternalCA不同。

在此處的示例中，您看到它在/var/log/sf/sfca_generation.log上建立日誌檔案，指示使用sftunnel_status.pl，指示InternalCA上的到期時間並指示其上的任何故障。例如，它未能將證書推送到裝置BSNS-1120-1和EMEA-FPR3110-08裝置，這是預期的，因為這些裝置的sftunnel已關閉。

為了更正失敗連線的sftunnel，請運行以下步驟：

1. 在FMC CLI上，使用cat /var/tmp/certs/1728303362/FAILED_PUSH（number值代表unix時間，因此請檢查系統中上一個命令的輸出）開啟FAILED_PUSH檔案，該檔案採用以下格式：FTD_UUID FTD_NAME FTD_IP SOURCE_PATH_ON_FMC DESTINATION_PATH_ON_FTD

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/tmp/certs/1728915794/FAILED_PUSH

c8d5d5c6-87c9-11ef-a993-b9831565bc4e  BSNS-1120-1  10.48.67.54  /etc/sf/ca_root/cacert.pem  /var/sf/peers/cdb123c8-4
347-11ef-aca1-f3aa241412a1/cacert.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e  BSNS-1120-1  10.48.67.54  /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/c
erts_pushed//sftunnel-key.pem  /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e  BSNS-1120-1  10.48.67.54  /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/c
erts_pushed//sftunnel-cert.pem  /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77  EMEA-FPR3110-08  10.48.189.37  /etc/sf/ca_root/cacert.pem  /var/sf/peers/cdb12
3c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77  EMEA-FPR3110-08  10.48.189.37  /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807
d77/certs_pushed//sftunnel-key.pem  /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77  EMEA-FPR3110-08  10.48.189.37  /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807
root@fmcv72-stejanss:/Volume/home/admin#
```

FAILED_PUSH

2. 透過這些新憑證(cacert.pem / sftunnel-key.pem / sftunnel-cert.pem)從FMC傳輸至FTD裝置
<u>===自動方法===</u>

該修補程式安裝還提供了copy_sftunnel_certs.py和copy_sftunnel_certs_jumpserver.py指令碼，這些指令碼可將各種證書自動傳輸到在重新生成證書時未啟動sftunnel的系統。這也可用於由於證書已過期而導致sftunnel連線斷開的系統。

當FMC本身擁有對各種FTD系統的SSH存取權時，可以使用copy_sftunnel_certs.py指令碼。如果情況並非如此，您可以將指令碼(/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py)從FMC下載到具有SSH訪問FMC和FTD裝置的跳轉伺服器，並從那裡運行Python指令碼。如果同樣不可能，則建議運行下文所示的手動方法。以下示例顯示正在使用的copy_sftunnel_certs.py指令碼，但copy_sftunnel_certs_jumpserver.py指令碼的步驟相同。

A.在FMC（或跳轉伺服器）上建立一個CSV檔案，該檔案包含用於建立SSH連線的裝置資訊（裝置名稱、IP地址、管理員使用者名稱、管理員密碼）。

當您從遠端伺服器（如主FMC的跳轉伺服器）運行此命令時，請確保在主FMC詳細資訊中新增第一個條目，後跟所有託管FTD和輔助FMC。當您從遠端伺服器（如輔助FMC的跳轉伺服器）運行此命令時，請確保將輔助FMC詳細資訊新增為第一個條目，後跟所有託管FTD。

i.使用vi devices.csv建立檔案。

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

vi devices.csv

二。這將開啟空檔案（未顯示），並在您使用鍵盤上的i letter進入互動模式（在螢幕底部看到）後填寫詳細資訊，如圖所示。

devices.csv示例

三。完全完成後，可使用ESC並按:wq和Enter鍵關閉並儲存檔案。

B.使用copy_sftunnel_certs.py devices.csv運行指令碼(使用sudo從根目錄中)，並顯示結果。此處顯示已正確推送到FTDv的憑證，且對於BSNS-1120-1，無法建立到裝置的SSH連線。

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

================================================================================================

2024-11-12 14:07:36 - Attempting connection to FMCpri
2024-11-12 14:07:40 - Connected to FMCpri
2024-11-12 14:07:41 - FMCpri is not an HA-peer. Certificates will not be copied
2024-11-12 14:07:41 - Closing connection with FMCpri

================================================================================================



================================================================================================

2024-11-12 14:07:41 - Attempting connection to FTDv
2024-11-12 14:07:43 - Connected to FTDv
2024-11-12 14:07:44 - Copying certificates to peer
2024-11-12 14:07:44 - Successfully copied certificates to FTDv
2024-11-12 14:07:44 - Restarting sftunnel for FTDv
2024-11-12 14:07:44 - Closing connection with FTDv

================================================================================================



================================================================================================

2024-11-12 14:07:44 - Attempting connection to BSNS-1120-1
2024-11-12 14:08:04 - Could not connect to BSNS-1120-1

================================================================================================

root@firepower:/Volume/home/admin#
```

copy_sftunnel_certs.py devices.csv

<u>===手動方法===</u>

1. 從先前的輸出（FAILED_PUSH檔案）中複製檔案位置，在FMC CLI上列印每個受影響的FTD(cacert.pem / sftunnel-key.pem（未出於安全目的完整顯示）/ sftunnel-cert.pem)的輸出(cat)。

```
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
```

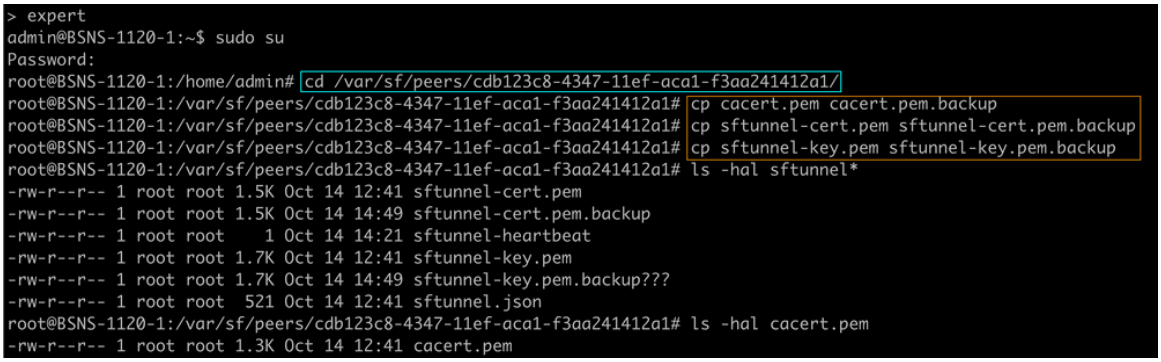
sftunnel-key.pem

```
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. 透過sudo su在expert模式下開啟每個相應FTD的FTD CLI，並依照下一個程式續訂憑證。
    1. 瀏覽至FAILED_PUSH輸出中淺藍色突出顯示區域上顯示的位置(例如，cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1，但每個FTD的顯示位置不同)。
    2. 備份現有檔案。

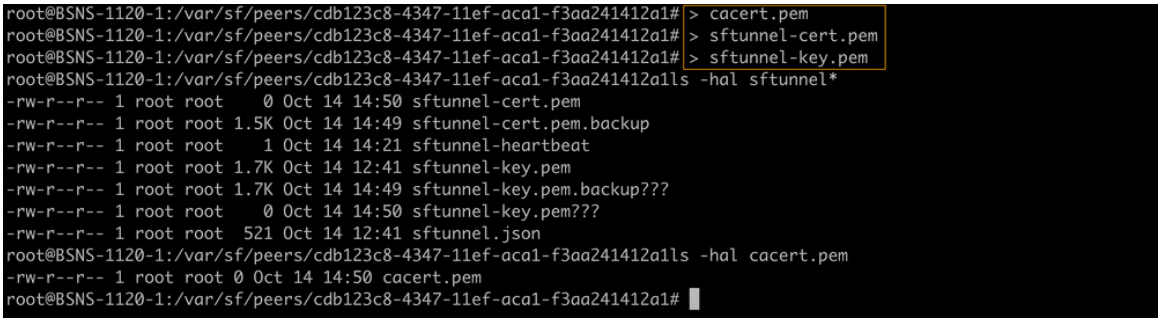
```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```



備份當前證書

    3. 清空檔案，以便我們在其中寫入新內容。

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



現有證書檔案的內容為空

    4. 使用vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem （每個檔案的單獨命令 — 螢幕截圖僅對cacert.pem顯示此資訊，但對sftunnel-cert.pem和sftunnel-key.pem需要重複此資訊），在每個檔案中單獨寫入新內容（來自FMC輸出）。

vi cacert.pem

1. 按i進入互動模式（輸入vi命令後，您會看到一個空檔案）。
2. 複製貼上檔案中的整-----內容-----包括-----BEGIN CERTIFICATE-----和(END CERTIFICATE))。

在vi（插入模式）中複製內容

3. 關閉並使用ESC後跟：wq寫入檔案，然後輸入。

ESC後跟：wq以寫入檔案

5. 使用ls -hal驗證是否為每份檔案設定了正確的許可權(chmod 644)和擁有者(chown root:root)。實際上在更新現有檔案時已正確設定。

```
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#
```

所有證書檔案已更新，具有適當的所有者和許可權

3. 在每個FTD上（其中sftunnel無法運作）重新啟動sftunnel，使憑證的變更通過指令生效
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. 使用sftunnel_status.pl輸出驗證所有FTD現在是否已正確連線

解決方案2 — 證書已過期

在這種情況下，我們面臨兩種不同的情形。所有sftunnel連線都仍然可以運行或者不再運行（或者不完整）。

FTD仍透過sftunnel連線

我們可以應用「證書尚未過期(理想情況) — 推薦方法」一節中說明的相同步驟。

但是在這種情況下，請勿升級或重新啟動FMC（或任何FTD），因為它會斷開所有sftunnel連線，且我們需要手動在每個FTD上執行所有憑證更新。唯一例外是列出的修補程式版本，因為它們不

需要重新啟動FMC。

通道會保持連線狀態，且會在每個FTD上交換憑證。如果某些證書無法填充，則會提示您填充失敗的證書，您需要採取上節前面所提到的手動方法。

FTD不再通過sftunnel連線

推薦的方法

我們可以應用「證書尚未過期(理想情況) — 推薦方法」一節中說明的相同步驟。在此案例中，新憑證將產生於FMC上，但無法複製到裝置上，因為通道已關閉。可以使用copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py指令碼自動執行此過程

如果所有FTD裝置都從FMC斷開，我們可以在此情況下升級FMC，因為它對sftunnel連線沒有影響。如果仍有一些裝置通過sftunnel連線，則請注意，FMC的升級會關閉所有sftunnel連線，並且由於證書過期，它們不會再次出現。此處的升級好處在於，它確實能提供需要傳輸至各個FTD的憑證檔案的良好指南。

手動方法

在這種情況下，接著您可以從FMC執行generate_certs.pl 指令碼，此指令碼將產生新憑證，但您仍需要手動將它們推送到各個FTD裝置。根據裝置數量，這是可行或繁瑣的任務。但是，使用copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py指令碼時，此操作高度自動化。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。