为FTD连接续订FMC Sftunnel CA证书

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

问题

- 到期日期后会发生什么情况？
- 如何快速验证证书是否过期或何时过期？
- 以后如何获得有关即将到期的证书的通知？

解决方案1 — 证书尚未过期（理想情况）

- 推荐的方法

解决方案2 — 证书已过期

- FTD仍通过sftunnel连接
- FTD不再通过sftunnel连接
  - 推荐的方法
  - 手动方法

Appendix

- FMC HA中使用的证书

简介

本文档介绍与Firepower威胁防御(FTD)连接相关的Firepower管理中心(FMC)sftunnel Certificate Authority(CA)证书的续订。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower威胁防御
- Firepower 管理中心
- 公用密钥基础结构 (PKI)

使用的组件

本文档不限于特定的软件和硬件版本。

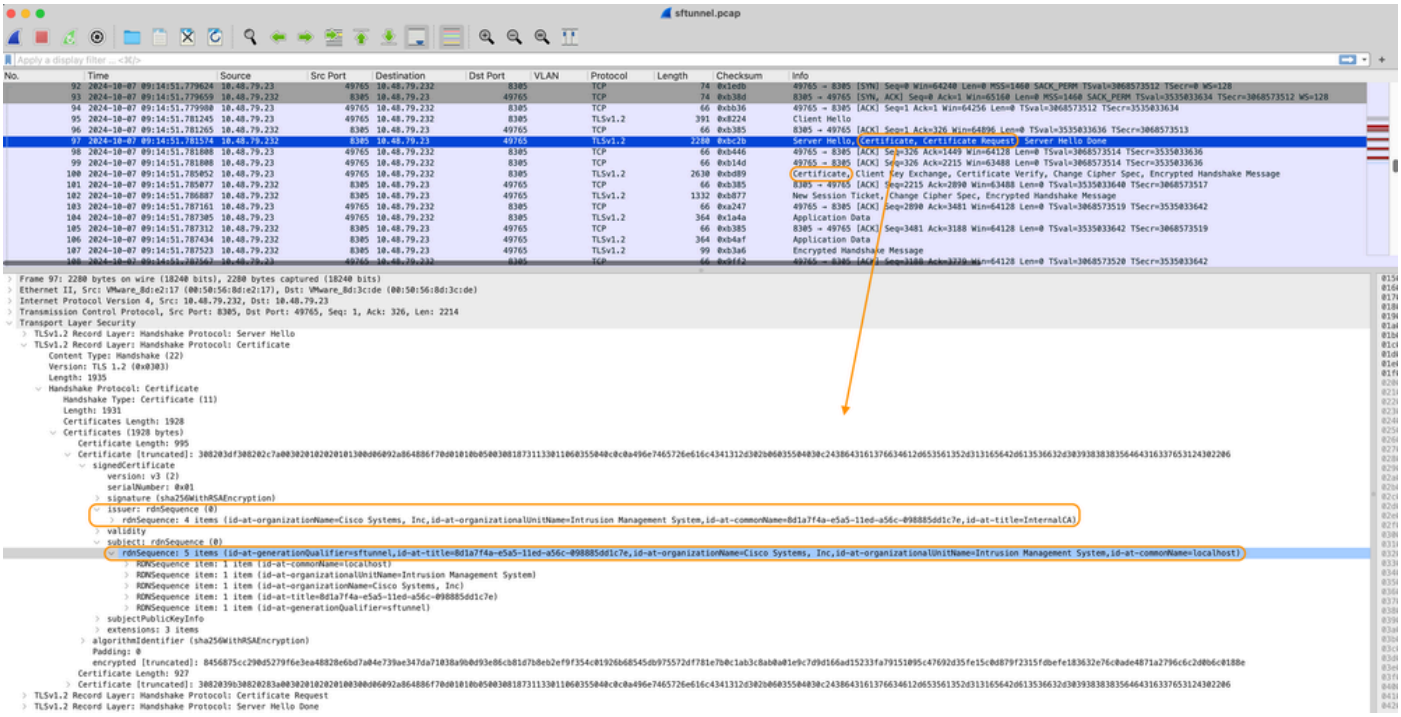
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

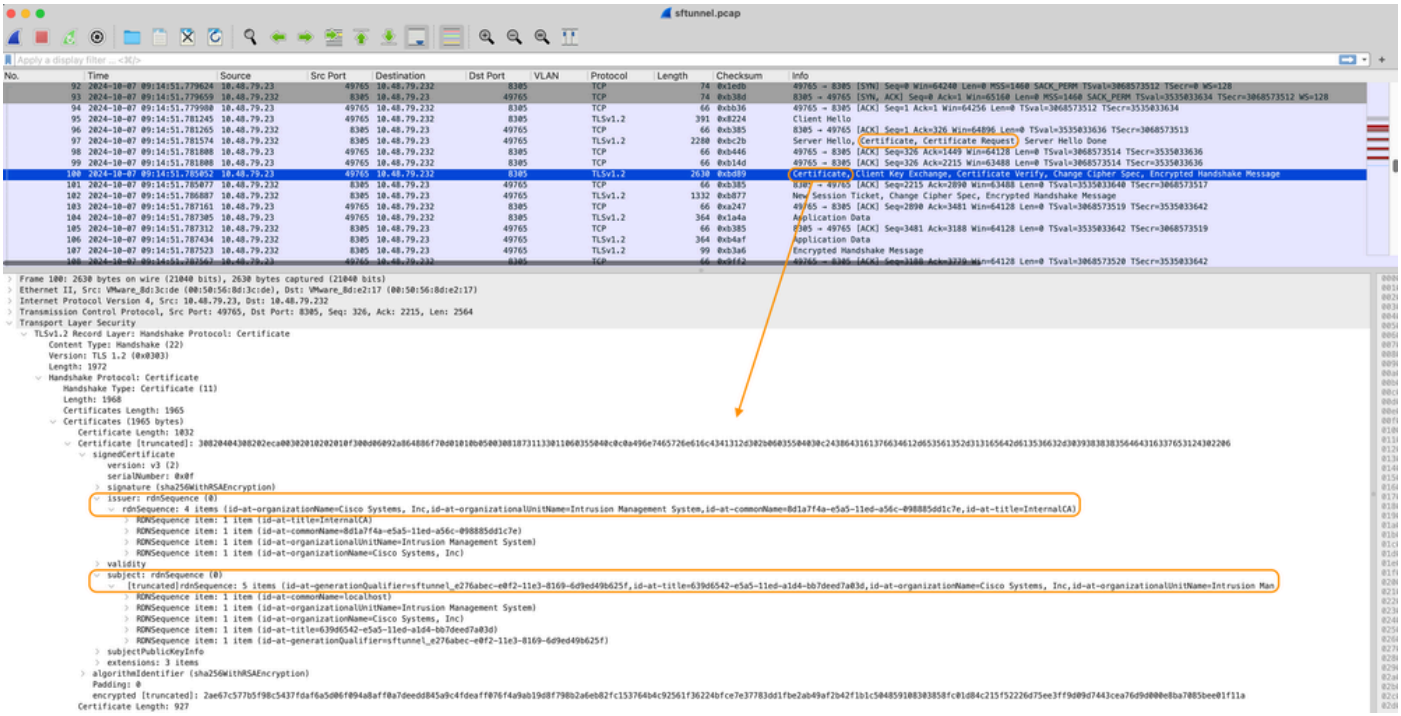
背景信息

FMC和FTD通过sftunnel（Sourcefire隧道）相互通信。 此通信使用证书来确保TLS会话中的会话安全。有关sftunnel及其如何建立的详细信息，可在此链接上找到。

通过数据包捕获，您可以看到FMC（本例中为10.48.79.232）和FTD(10.48.79.23)正在相互交换证书。他们这样做是为了验证他们是否与正确的设备通信，以及不存在窃听或中间人(MITM)攻击。使用那些证书对通信进行加密，只有拥有该证书的关联私钥的一方才能再次解密该证书。



Certificate_exchange_server_cert



Certificate_exchange_client_cert

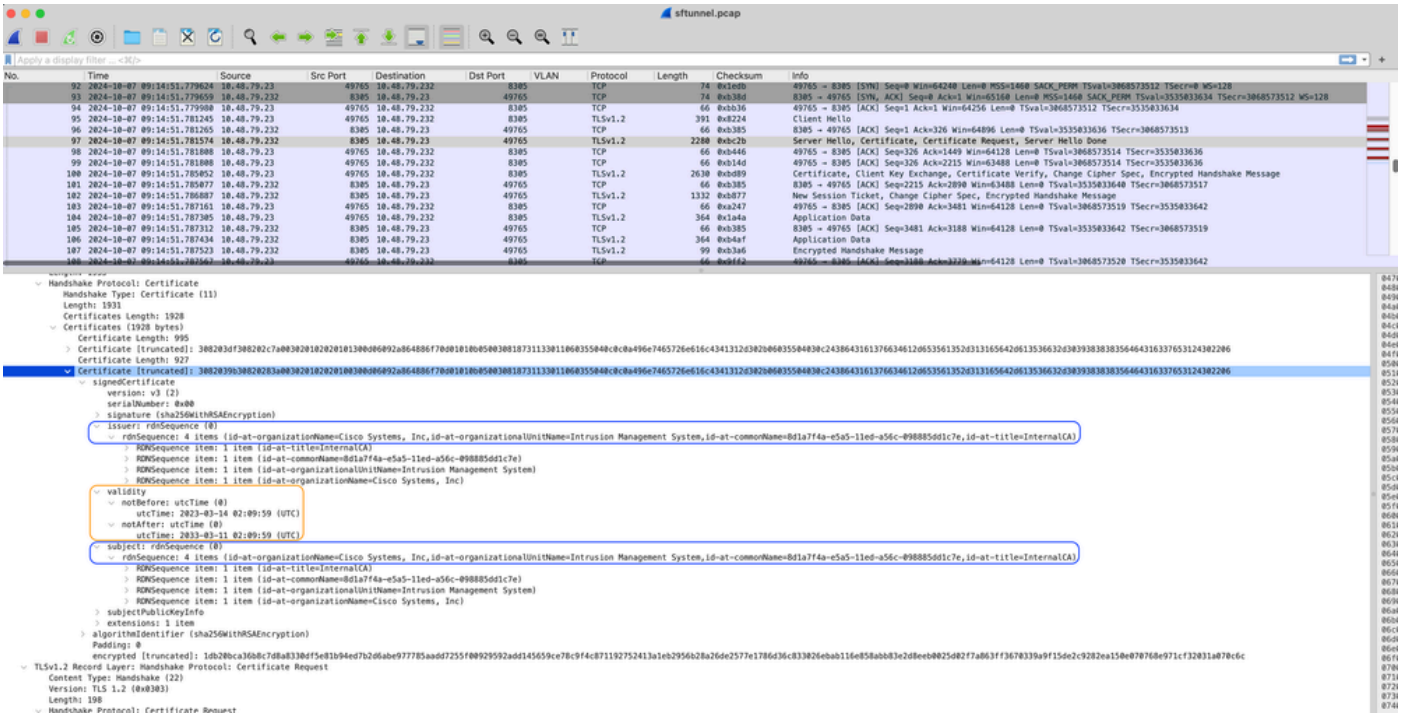
您可以看到证书由FMC系统上设置的相同InternalCA(Issuer)证书颁发机构(CA)签名。在/etc/sf/sftunnel.conf文件上的FMC上定义配置，该文件包含以下内容：

```
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;
};
```

这表示用于签署sftunnel（FTD和FMC one）的所有证书的CA，以及FMC用于发送到所有FTD的证书。此证书由InternalCA签名。

当FTD注册到FMC时，FMC还会创建证书以推送到FTD设备，用于在sftunnel上进行进一步通信。此证书也由同一内部CA证书签名。在FMC上，可以在/var/sf/peers/<UUID-FTD-device>下和可能在certs_pushed文件夹下找到证书（和私钥），该文件夹名为sftunnel-cert.pem(对于私钥，sftunnel-key.pem)。 在FTD上，您可以找到那些在/var/sf/peers/<UUID-FMC-device>下使用相同命名约定的FTD。

但是，出于安全考虑，每个证书也有一个有效期。在检查InternalCA证书时，我们还可以看到数据包捕获所显示的FMC InternalCA的有效期（10年）。

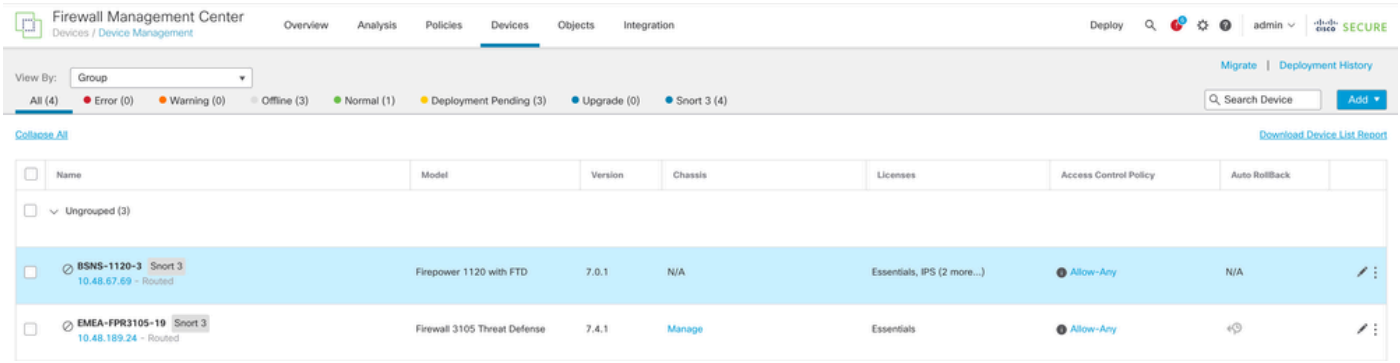


FMC-InternalCA_validity

问题

FMC InternalCA证书有效期仅为10年。到期后，远程系统不再信任此证书（以及由其签名的证书），这将导致FTD和FMC设备之间的sftunnel通信问题（以及FMC HA通信）。 这也意味着连接事件、恶意软件查找、基于身份的规则、策略部署等多项关键功能无法正常工作。

当sftunnel未连接时，设备在FMC UI的Devices > Device Management选项卡下显示为禁用。思科漏洞ID CSCwd08098会跟踪与此到期相关的问题。请注意，即使您运行了缺陷的固定版本，所有系统都会受到影响。有关此修补程序的更多信息，请参阅解决方案部分。



已禁用设备

FMC不会自动刷新CA并将证书重新发布到FTD设备。此外，也没有指示证书到期的FMC运行状况警报。在此方面跟踪思科漏洞ID CSCwd08448，以便将来在FMC UI上提供运行状况警报。

到期日期后会发生什么情况？

最初什么都没有发生，并且sftunnel通信通道继续像以前一样运行。但是，当FMC和FTD设备之间的sftunnel通信中断并尝试重新建立连接时，它确实会失败，并且您可以观察消息日志文件中指向证书到期的日志行。请注意，主要和辅助FMC之间的sftunnel通信(用于高可用性(HA)同步)也可能受到影响，如本节所述。

来自/ngfw/var/log/messages的FTD设备的日志行:

```
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
```

从/var/log/messages的FMC设备的日志行:

```
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通信可能会因各种原因中断：

- 由于网络连接中断而丢失通信（可能只是暂时的）
- 重新启动FTD或FMC
  - 期望值：在FMC或FTD上手动重新启动、升级、手动重新启动sftunnel进程（例如，通过pmtool restartbyid sftunnel）
  - 意外的：回溯，断电

由于有如此多的可能性可以中断sftunnel通信，因此强烈建议尽快纠正这种情况，即使当前所有FTD设备都已正确连接（尽管证书已过期）。

如何快速验证证书是否过期或何时过期？

最简单的方法是在FMC SSH会话上运行以下命令：

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

这将为您显示证书的有效性元素。此处的主要相关部分是“notAfter”，表明此处的证书有效期至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

如果您希望运行一个命令，立即向您提供证书仍然有效的天数，则可以使用此命令：

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

显示了一个设置示例，其中证书仍然多年有效。

```
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.

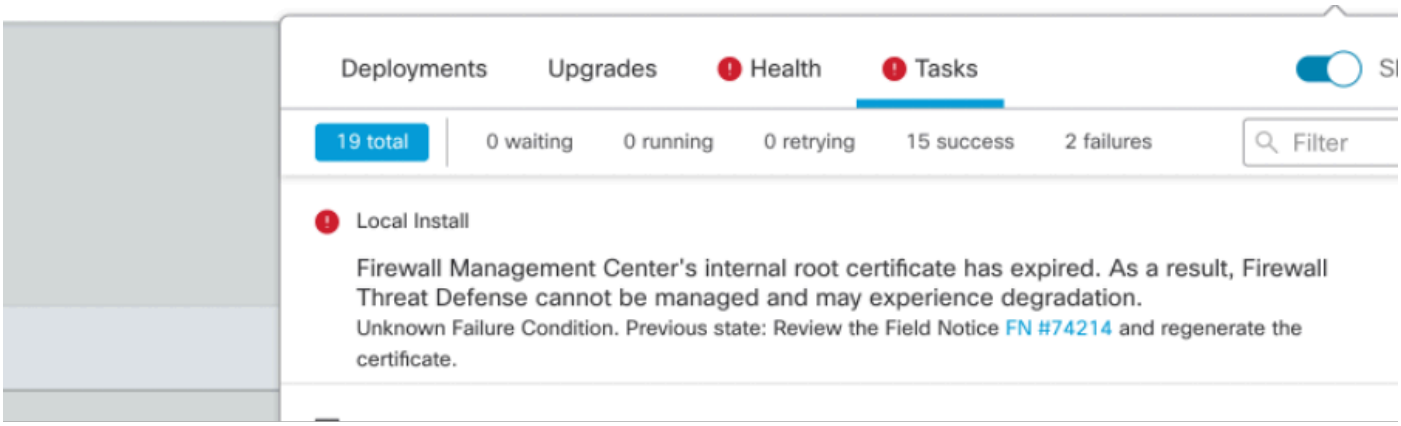
root@fmcv72-stejanss:/Volume/home/admin#
```

Certificate_expire_validation_command

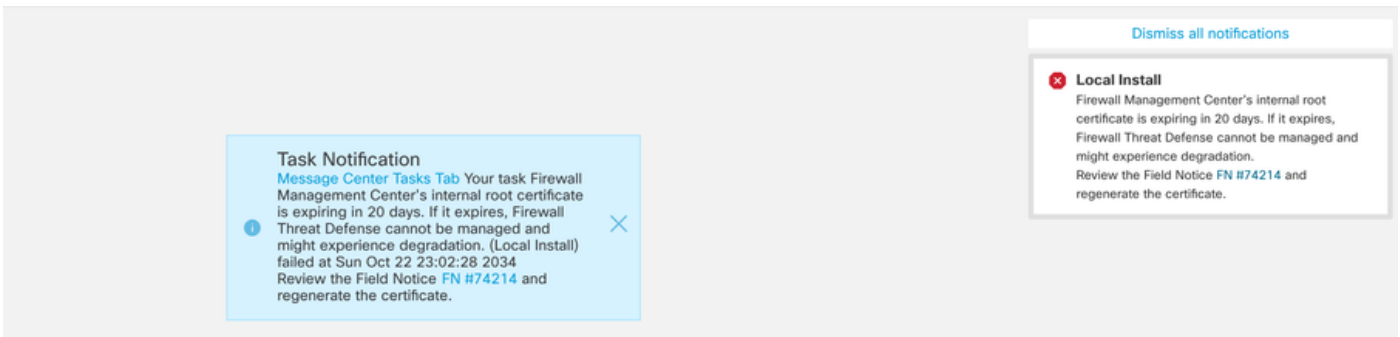
以后如何获得有关即将到期的证书的通知？

使用最近的VDB更新（399或更高），证书在90天内到期时会自动向您发出警报。因此，您自己无需手动跟踪，因为当您接近到期时间时会收到警报。然后，FMC网页上会显示两种表格。这两种方式均请参阅现场通知页面。

第一种方法是通过Task选项卡。此消息为粘滞消息，除非明确关闭，否则用户可以使用它。通知弹出窗口也会显示，在用户明确关闭之前一直可用。它始终显示为错误。

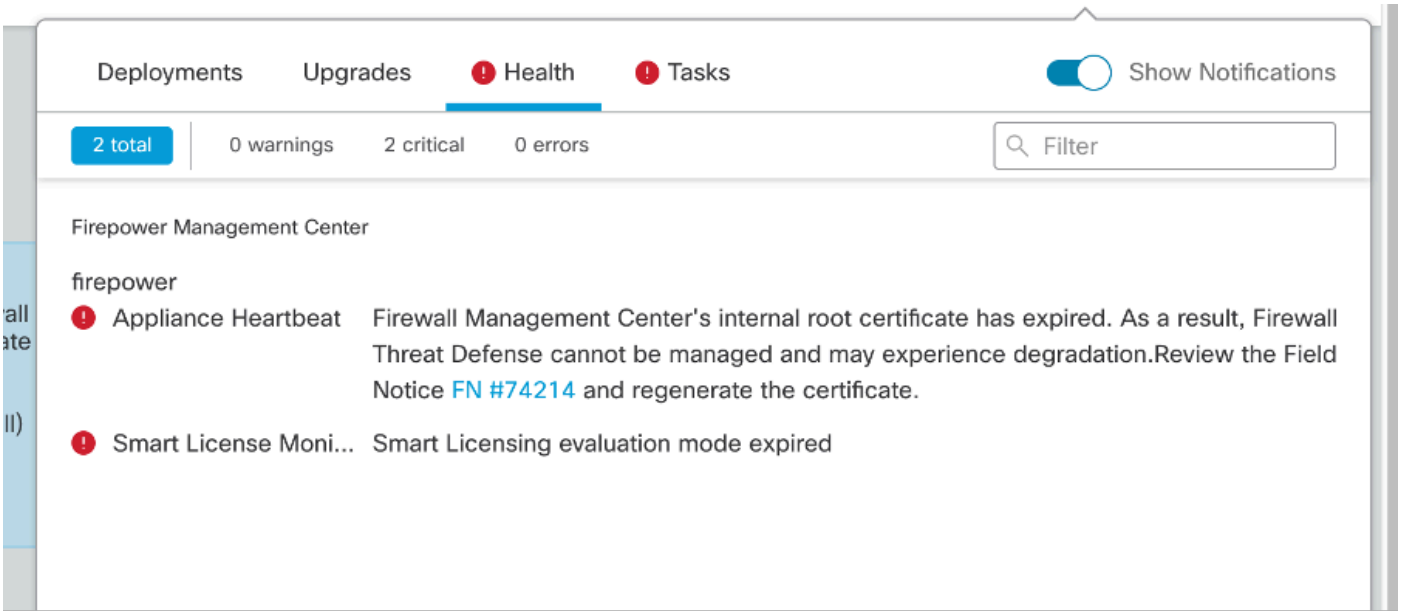


“任务”选项卡上的到期通知

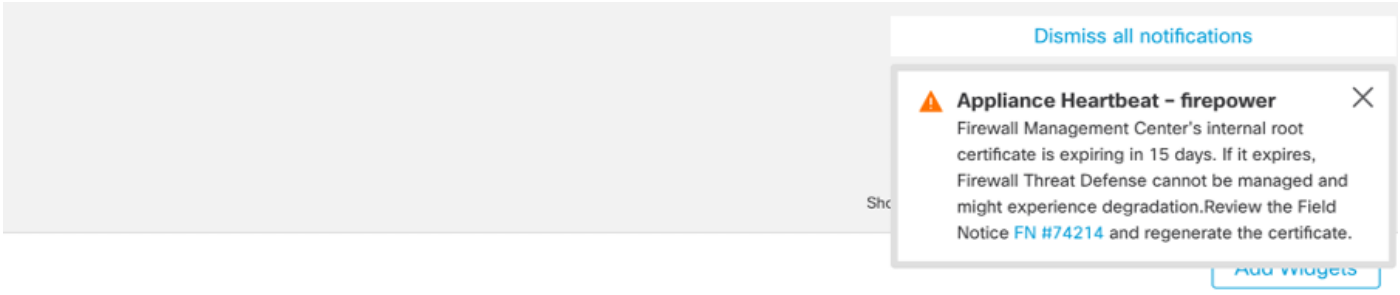


第二种方法是通过Health Alert。这在Health选项卡中显示，但这不是粘滞的，并在运行运行状况监控器时替换或删除，默认情况下，运行状况监控器每5分钟运行一次。它还显示一个通知弹出窗口

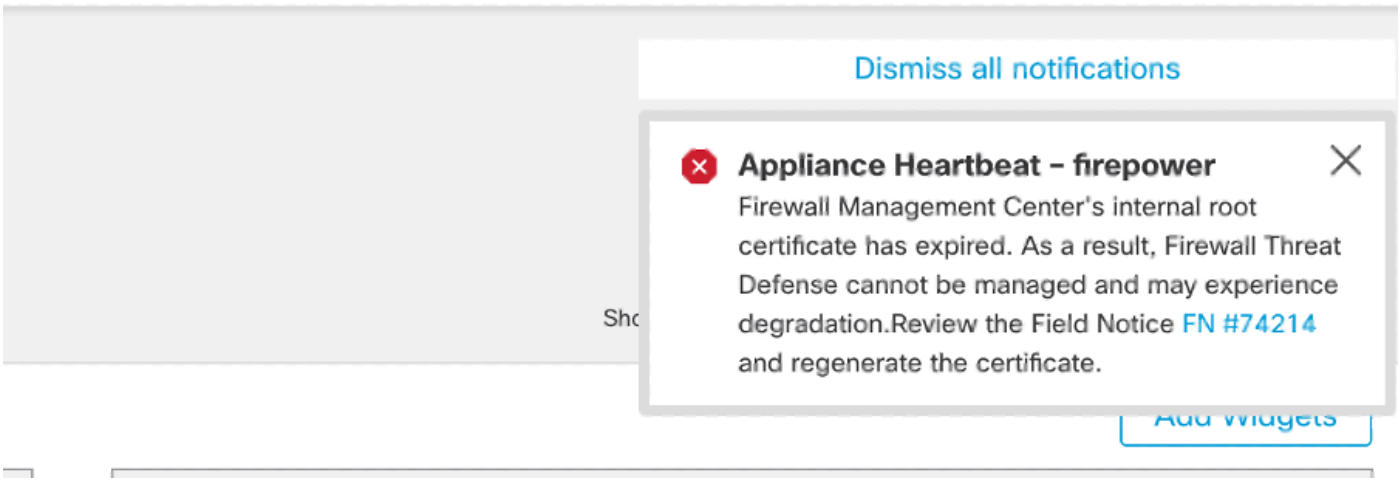
，用户需要明确关闭该窗口。这可以同时显示为错误（过期时）和警告（即将过期时）。



“运行状况”(Health)选项卡上的到期通知



弹出运行状况警报时的警告通知



出现运行状况警报弹出时的错误通知

解决方案1 — 证书尚未过期（理想情况）

这是最佳情况，因为根据证书到期时间，我们还有时间。要么我们采用依赖FMC版本的全自动方法（推荐），要么我们采用需要TAC交互的更手动的方法。

推荐的方法

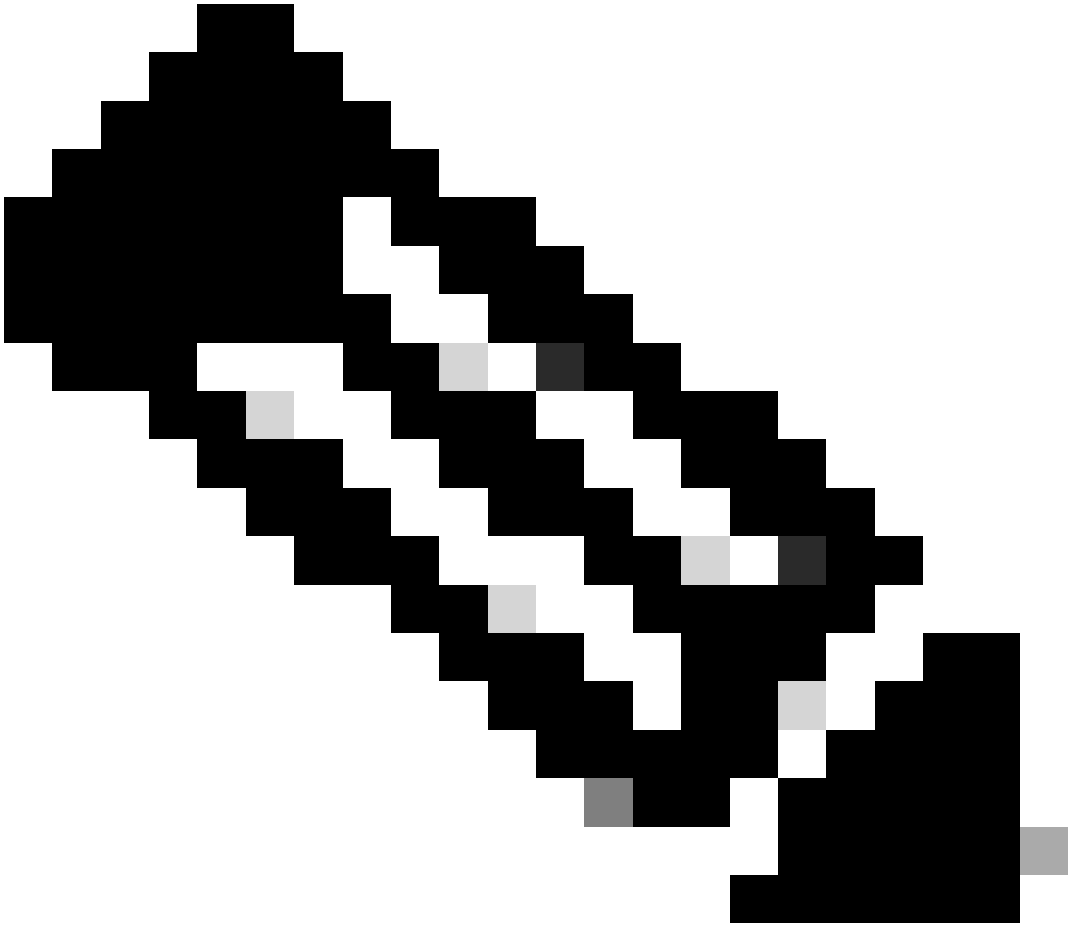
这是正常情况下预期没有停机时间和最少手动操作量的情况。

在继续操作之前，必须安装适用于此处所列特定版本的修补程序。此处的好处是这些修补程序不需要重新启动FMC，因此当证书过期时，可能会中断sftunnel通信。可用的修补程序（下载链接适用于虚拟FMC，对于硬件FMC，请在相应版本的下载页面上查找）如下：

- 7.0.0 - 7.0.6:修补程序FK - 7.0.6.99-9
- 7.1.x :软件维护终止时无固定版本
- 7.2.0 - 7.2.9:修补程序FZ - 7.2.9.99-4
- 7.3.x:修补程序AE - 7.3.1.99-4
- 7.4.0 - 7.4.2:修补程序AO - 7.4.2.99-5
- 7.6.0 :修补程序B - 7.6.0.99-5

安装修补程序后，FMC现在包含generate_certs.pl脚本：

1. 重新生成InternalCA
2. 重新创建由此新的InternalCA签名的sftunnel证书
3. 将新的sftunnel证书和私钥推送到各自的FTD设备(以及辅助FMC（如果适用））（当sftunnel运行时）



注意：generate_certs.pl脚本当前检查关键操作是否正在运行。如果不是，则它无法运行。

关键操作可以是：智能代理未注册或注册正在进行中，备份/还原任务正在进行中，SRU更新任务正在进行中，VDB更新任务正在进行中，域任务正在进行中，高可用性操作正在进行或升级正在运行。

因此，如果您只在FMC上使用传统许可证（或列出的任何操作都需要首先完成），则无法运行此脚本，在这种情况下，您需要联系思科TAC以绕过此检查、重新生成证书，然后再次撤消绕行。

因此，建议（如果可能）：

1. 为您的版本系列安装适用的修补程序
2. 在FMC上进行备份
3. 在FMC上使用sftunnel_status.pl脚本验证所有当前sftunnel连接(从专家模式)
4. 使用generate_certs.pl从专家模式运行脚本
5. 检查结果以验证是否需要任何手动操作（当设备未连接到FMC时）[下面将进一步说明]

6. 从FMC运行sftunnel_status.pl，以验证所有sftunnel连接是否运行正常

```
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

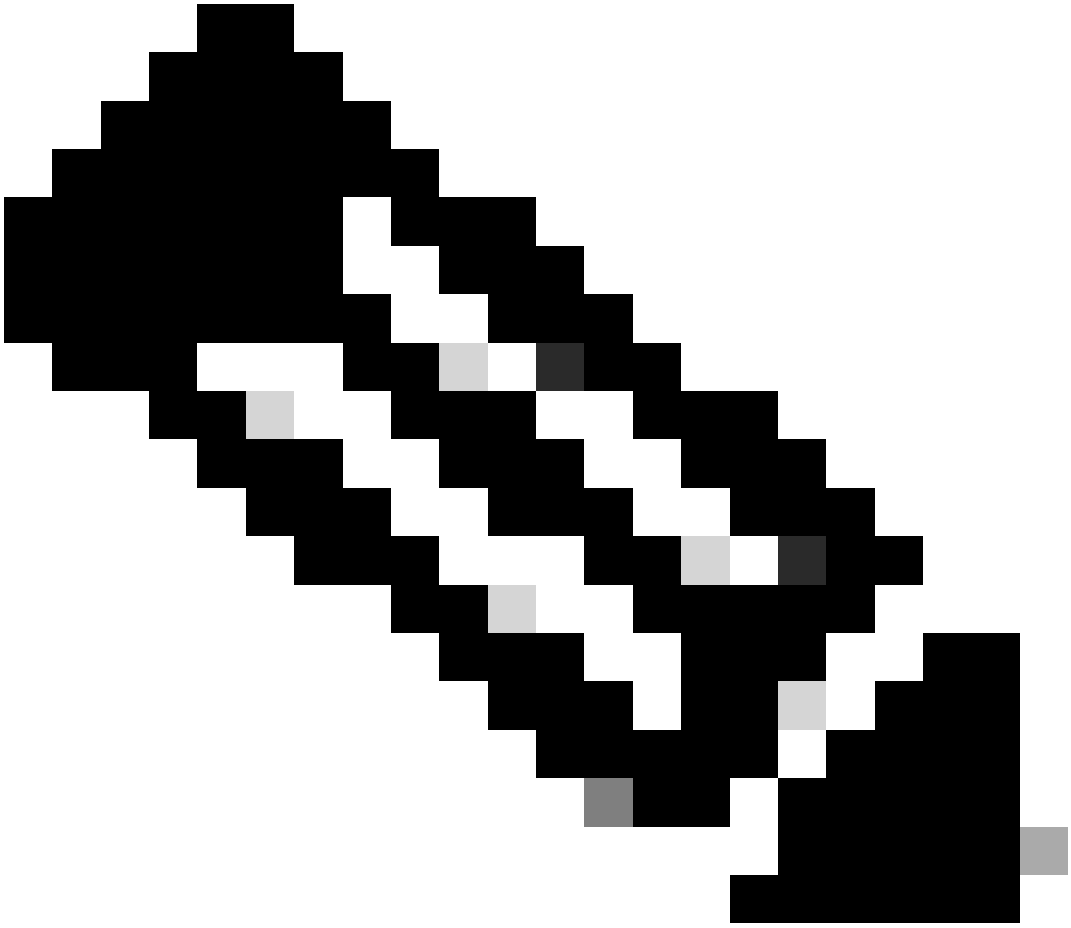
Current ca_root expires in 3646 days - at Oct  9 10:12:50 2034 GMT
Do you want to continue? [yes/no]:yes

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脚本



注意：当您让FMC在高可用性(HA)中运行时，您需要首先在主节点上执行操作，然后在辅助节点上执行操作，因为它使用这些证书并在FMC节点之间进行通信。两个FMC节点上的InternalCA不同，因此它们具有不同的到期时间。您可以在此部分找到有关FMC HA中证书的更多信息。

在此处的示例中，您看到它在/var/log/sf/sfca_generation.log上创建日志文件，指示使用sftunnel_status.pl，指示InternalCA上的到期时间并指示其上的任何故障。例如，它未能将证书推送到设备BSNS-1120-1和EMEA-FPR3110-08设备，这是预期结果，因为这些设备的sftunnel已关闭。

要更正失败连接的sftunnel，请运行以下步骤：

1. 在FMC CLI上，使用cat /var/tmp/certs/1728303362/FAILED_PUSH（number值表示unix时间，因此请检查系统中上一个命令的输出）打开FAILED_PUSH文件，此文件采用以下格式：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. 通过这些新证书(cacert.pem / sftunnel-key.pem / sftunnel-cert.pem)从FMC传输到FTD设备
   ===自动方法===

   修补程序安装还提供了copy_sftunnel_certs.py和copy_sftunnel_certs_jumpserver.py脚本，这些脚本可自动将各种证书传输到证书重新生成时未启动sftunnel的系统。这也可用于由于证书已过期而导致sftunnel连接中断的系统。

   当FMC本身拥有对各种FTD系统（可能还有辅助FMC，如果适用）的SSH访问权限时，可以使用copy_sftunnel_certs.py脚本。 如果情况并非如此，您可以将脚本(/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py)从FMC下载到具有SSH访问FMC和FTD设备的跳转服务器，并从那里运行Python脚本。如果也不可能这样做，则建议运行下面所示的手动方法。下面的示例显示正在使用的copy_sftunnel_certs.py脚本，但对于copy_sftunnel_certs_jumpserver.py脚本的步骤是相同的。

   A.在FMC（或跳转服务器）上创建包含用于建立SSH连接的设备信息（device_name、IP地址、admin_username、admin_password）的CSV文件。

   当您从远程服务器（如主FMC的跳转服务器）运行此时，请确保在主FMC详细信息中添加作为第一个条目，后跟所有托管FTD和辅助FMC。当您从远程服务器（如辅助FMC的跳转服务器）运行此时，请确保在辅助FMC详细信息中添加作为第一个条目，后跟所有托管FTD。有关FMC HA中证书的更多信息，请参阅本节。

   i.使用vi devices.csv创建文件。

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

vi devices.csv

二、这将打开空文件（未显示），当您使用键盘上的i letter进入INTERACTIVE模式（在屏幕底部看到）后，请填写详细信息，如下所示。



devices.csv示例

三。完全完成后，使用ESC并按:wq然后按Enter键关闭并保存文件。



保存设备.csv

B.使用copy_sftunnel_certs.py devices.csv运行脚本(使用sudo从根运行)，并显示结果。此处显示已正确推送到FTDv的证书，并且对于BSNS-1120-1，无法建立到设备的SSH连接。

```
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

===手动方法===

1. 通过从以前的输出（FAILED_PUSH文件）复制文件位置，在FMC CLI上打印(cat)受影响(cacert.pem / sftunnel-key.pem（出于安全目的未完全显示）/ sftunnel-cert.pem)的每个FTD（或HA中的辅助FMC）的每个文件的输出。

```
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. 通过sudo su在expert模式下打开每个相应FTD的FTD（或FMC HA中的辅助FMC）CLI，并使用sudo su的root权限更新证书。
    1. 从FAILED_PUSH输出浏览到浅蓝色突出显示区域上显示的位置(例如，cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1，但每个FTD不同)。
    2. 备份现有文件。

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

```
> expert
admin@BSNS-1120-1:~$ sudo su
Password:
root@BSNS-1120-1:/home/admin# cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp cacert.pem cacert.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp sftunnel-cert.pem sftunnel-cert.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp sftunnel-key.pem sftunnel-key.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal sftunnel*
-rw-r--r-- 1 root root 1.5K Oct 14 12:41 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 12:41 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  521 Oct 14 12:41 sftunnel.json
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal cacert.pem
-rw-r--r-- 1 root root 1.3K Oct 14 12:41 cacert.pem
```

备份当前证书

    3. 清空文件，以便我们可以在其中写入新内容。

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

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-cert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-key.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1ls -hal sftunnel*
-rw-r--r-- 1 root root    0 Oct 14 14:50 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 12:41 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
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1ls -hal cacert.pem
-rw-r--r-- 1 root root 0 Oct 14 14:50 cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#
```

现有证书文件的内容为空

    4. 使用vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem（每个文件的单独命令 — 屏幕截图仅对cacert.pem显示此内容，但对sftunnel-cert.pem和sftunnel-key.pem需要重复此内容），在每个文件中单独写入新内容（来自FMC输出）。

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# vi cacert.pem
```

vi cacert.pem

1. 按i进入交互模式（输入vi命令后，您会看到一个空文件）。
2. 复制粘贴文件中的整-----内容(-----BEGIN CERTIFICATE-----和-----END CERTIFICATE)。



在vi中复制内容（INSERT模式）

3. 关闭并使用ESC后跟:wq写入文件，然后输入。



ESC后跟：wq以写入文件

1. 使用ls -hal验证为每个文件设置了正确的权限(chmod 644)和所有者(chown root:root)。这实际上是在更新现有文件时设置的。

```
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#
```

使用正确的所有者和权限更新所有证书文件

3. 在每个FTD（或辅助FMC，在FMC HA中）上重新启动sftunnel，在该处sftunnel未运行，证书中的更改会通过命令生效 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输出验证所有FTD（和辅助FMC）现在是否已正确连接

解决方案2 — 证书已过期

在这种情况下，我们有两种不同的场景。所有sftunnel连接仍可运行，或者不再运行（或部分运行）。

FTD仍通过sftunnel连接

我们可以应用“证书尚未过期(理想情况) — 推荐方法”部分中所示的相同步骤。

但是，在这种情况下，请勿升级或重新启动FMC（或任何FTD），因为它会断开所有sftunnel连接，并且我们需要手动运行每个FTD上的所有证书更新(以及本部分介绍的辅助FMC)。 唯一例外是列

出的修补程序版本，因为它们不需要重新启动FMC。

隧道保持连接，证书在每个FTD（和辅助FMC，在FMC HA中）上替换。 如果某些证书无法填充，则会提示您填写失败的证书，您需要采取上节前面所提到的手动方法。

FTD不再通过sftunnel连接

推荐的方法

我们可以应用“证书尚未过期(理想情况) — 推荐方法”部分中所示的相同步骤。在此场景中，新证书确实在FMC上生成，但无法复制到设备，因为隧道已关闭。可以使用copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py脚本自动执行此过程

如果所有FTD设备都与FMC断开连接，我们可以在此情况下升级FMC，因为它对sftunnel连接没有影响。如果仍有一些设备通过sftunnel连接，则请注意FMC的升级会关闭所有sftunnel连接，并且由于证书过期，它们不会再次出现。此处的升级的好处是，它确实可以针对需要传输到每个FTD（以及使用FMC HA时的辅助FMC）的证书文件提供良好的指导。

手动方法

在这种情况下，您可以从FMC运行generate_certs.pl脚本，该脚本会生成新证书，但您仍需要手动将其推送到每个FTD(以及本节介绍的辅助FMC)设备。根据设备数量，这是可行或繁琐的任务。但是，使用copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py脚本时，此过程高度自动化。

Appendix

FMC HA中使用的证书

高可用性对中的主FMC和辅助FMC之间的通信也通过sftunnel进行，与通过FTD设备通信的FMC类似。证书元素(cacert.pem / sftunnel-cert.pem / sftunnel-key.pem)存储在FMC的同一位置/var/sf/peers/<UUID-FMC>下。但是，主FMC始终充当辅助FMC的管理器。这样，从主FMC的角度看，辅助FMC就像FTD设备。因此，您只能看到辅助FMC上的证书，而不能看到/var/sf/peers/folder上的主FMC上的文件。

通常，您的辅助FMC创建的时间晚于您的主要FMC，因此内部CA仍然有效，并且尚未过期，这与您的主要FMC不同。因此，在辅助FMC仍将具有有效证书并因此与所有FTD相关联的sftunnel通信的情况下，活动FMC的手动角色切换可以作为一种选项，以最大程度地减小影响。这样，您仍可以部署配置，同时还可以准备主FMC证书的修复或更新。但是，当主FMC的证书到期后sftunnel关闭时，两个FMC设备之间的通信也可能中断。

在证书续订过程中，有两种不同的场景：

1.主FMC CA证书已过期：由于辅助FMC被视为主要FMC的FTD，因此证书续订需要将在主要FMC上创建的更新证书推送到FTD设备上，而且需要将更新后的证书推送到辅助FMC上。

2.辅助FMC CA证书已过期：在这种情况下，需要的唯一证书更新是FTD设备的证书更新。因为HA中两个FMC之间的sftunnel通信基于主FMC CA证书。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。