從FMC和FTD下載檔案

目錄

簡介

必要條件

- 需求
- 採用元件

複製檔案

- 將檔案從FTD複製到FMC
- 將檔案從FMC複製到本地電腦
- 使用SCP複製
- 從GUI下載

簡介

本檔案介紹如何將記錄檔從Cisco Firepower管理中心(FMC)和Firepower威脅防禦(FTD)下載到本機電腦。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Firepower裝置
- 虛擬裝置型號

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。

複製檔案

將檔案從FTD複製到FMC

FMC上有一個安全複製協定(SCP)伺服器，因此檔案可以從FTD移到FMC。

```
root@FMC:~$ scp admin@<FTD ip>:<path to file> <path to local directory where to store>
```

一個常見的示例是將核心檔案從FTD移動到FMC。

在FTD上：

```
root@ciscoasa:/ngfw/var/common# ls -l
total 1557960
-rw-r--r-- 1 root root 23231 Sep 6 03:43 core_1482327396_Firepower-module1_snort_6
-rw------- 1 root root 560128000 Apr 26 01:47 core_1556242979_ciscoasa_snort_6.8777
-rw------- 1 root root 383381504 Aug 25 23:05 core_1566774281_ciscoasa_snort_11.31618
-rw------- 1 root root 69562368 Aug 25 23:05 core_1566774281_ciscoasa_snort_11.31620
-rw------- 1 root root 465424384 Aug 28 02:21 core_1566958444_ciscoasa_snort_6.18352
-rw------- 1 root root 116887552 Aug 28 02:18 core_1566958688_ciscoasa_snort_6.18340
-rw------- 1 root root 52338688 Aug 28 02:18 core_1566958689_ciscoasa_snort_6.18341
-rw------- 1 root root 465514496 Sep 2 02:20 core_1567390346_ciscoasa_snort_6.27631
-rw------- 1 root root 151572480 Sep 2 02:17 core_1567390618_ciscoasa_snort_6.27435
```

現在，將檔案傳輸到FMC:

```
root@FMC:/Volume/home/admin# scp admin@10.10.10.10:/ngfw/var/common/core_1567390618_ciscoasa_snort_6.27
```

注意：在scp命令上新增 — v以進行詳細日誌記錄，以進一步進行故障排除。

將檔案從FMC複製到本地電腦

使用SCP複製

FMC上有一個安全複製協定(SCP)伺服器，它使用可以從FMC移動到其他裝置的檔案。

```
root@FMC:~$ scp  <path to local directory where to store>  admin@<FMC ip>:<path to file>
```

一種常見方法是將核心檔案從FMC移動到本地案頭：

```
root@localMachine:/Volume/home/admin# scp admin@10.10.10.20:/var/common/core_1567390618_ciscoasa_snort_
```

WInSCP是一種常用的工具，通常在Windows上使用。此工具提供基於GUI的介面。

```
In FMC 6.4 and above, SCP to the FMC is not possible directly. For that, the following is needed(the be
```

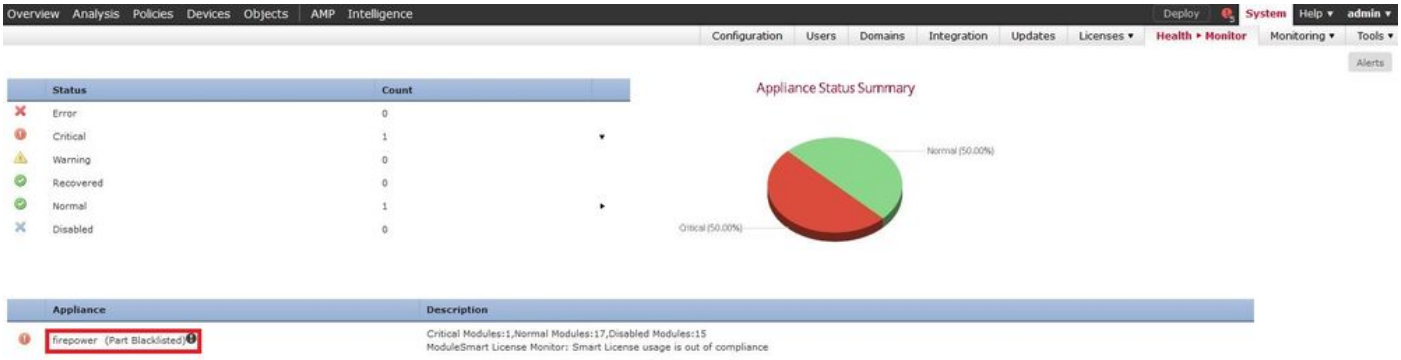
```
root@FMC:/Volume/home/admin# usermod --shell /bin/bash admin

After this SCP to the FMC will work. Once done, please remeber to rollback:

root@FMC:/Volume/home/admin# usermod --shell /usr/bin/clish admin
```

從GUI下載

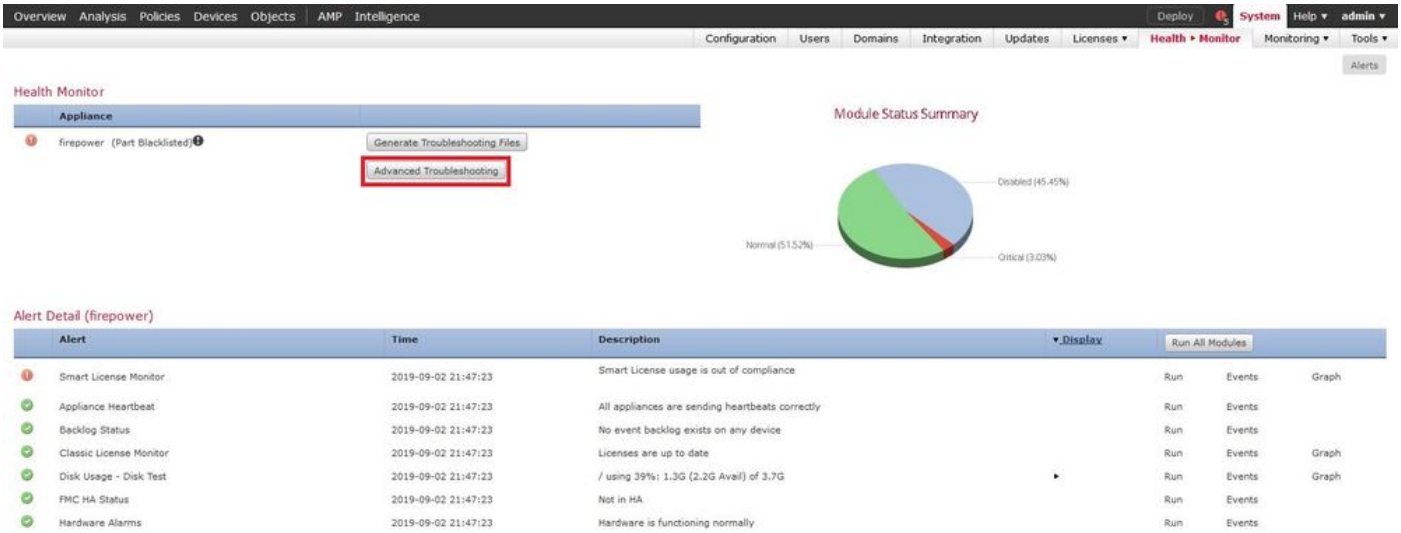
存在/var/common的檔案可從GUI下載。

```
If there are any file(s) and/or tcpdump generated on the FMC, please move to /var/common, so that it ca
```

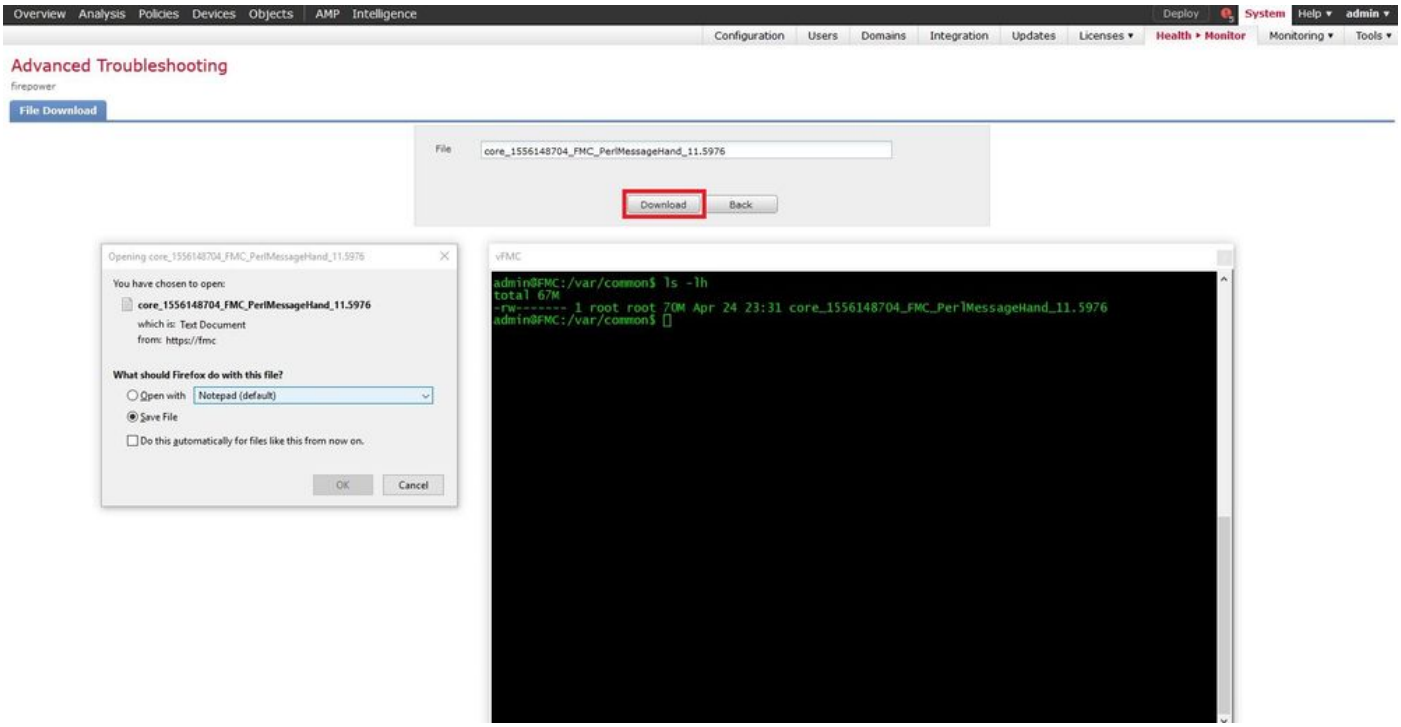
步驟 1.導覽至System > Health > Monitor，然後按一下需要下載檔案的感應器，如下圖所示：



步驟 2.導覽至System > Health > Monitor，然後按一下Advanced Troubleshooting，如下圖所示：



步驟 3.輸入檔案名稱，按一下「download」，如下圖所示：


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
Configuration Users Domains Integration Updates Licenses Health Monitor Monitoring Tools
Advanced Troubleshooting
firepower
File Download
File
core_1556148704_FMC_PerlMessageHand_11.5976
Download
Back
Opening core_1556148704_FMC_PerlMessageHand_11.5976
You have chosen to open:
core_1556148704_FMC_PerlMessageHand_11.5976
which is: Text Document
from: https://fmc
What should Firefox do with this file?
Open with
Notepad (default)
Save File
Do this automatically for files like this from now on.
OK
Cancel
vFMC
admin@FMC:/var/common$ ls -lh
total 67M
-rw------- 1 root root 70M Apr 24 23:31 core_1556148704_FMC_PerlMessageHand_11.5976
admin@FMC:/var/common$

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）。