從Firepower威脅防禦裝置收集核心檔案

目錄

簡介

本檔案介紹通過支援FTD軟體的所有平台收集FTD裝置的所有型別核心檔案的程式。當FTD上的進程遇到嚴重問題時，進程的運行記憶體的轉儲可以另存為核心檔案。為了確定故障的根本原因，思科技術支援可能會請求核心檔案。

針對FTD裝置，我們有兩種型別的核心檔案：Firepower核心和LINA核心檔案。

必要條件

需求

思科建議您瞭解以下產品：

- Firepower Management Center (FMC)
- Firepower裝置管理器(FDM)
- Firepower Threat Defense (FTD)
- Firepower可擴充作業系統(FXOS)

程式

Firepower處理核心檔案

FTD位於Firepower 2100、1000、ASA裝置和ISA 3000裝置中的Firepower核心檔案的位置

對於所有這些平台，可以通過此過程找到與所有firepower進程相關的核心檔案。

1.通過SSH或控制檯連線到裝置的CLI。

2.以專家模式進入。

```
> expert
admin@firepower:~$
```

3.成為超級使用者。

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```

4.導航至 /ngfw/var/common/ 核心檔案所在的資料夾。

```
root@firepower:/home/admin# cd /ngfw/var/common/
```

5.檢查該檔案的資料夾。

```
root@firepower:/ngfw/var/common# ls -l | grep -i core
total 21616
-rw-r--r-- 1 root root 22130788 Nov  6  2020 process.core.tar.gz
```

FTD位於Firepower 4100或9300中時Firepower核心檔案的位置

對於這兩個平台，core檔案可以位於兩個可能的路徑中，第一個路徑與上一節相同，第二個路徑可以通過此過程定位。

1.通過SSH或控制檯連線到裝置的CLI。

2.以專家模式進入。

```
> expert
admin@firepower:~$
```

3.成為超級使用者。

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```

4.導航至 /ngfw/var/data/cores/ 核心檔案所在的資料夾。

```
root@firepower:/home/admin# cd /ngfw/var/data/cores/
```

5.檢查該檔案的資料夾。

```
root@firepower:cores# ls -l | grep -i core
-rw-r--r-- 1 root root 27873115 Nov 17 15:01
core.snort.59095.1605625274.gz
-rw-r--r-- 1 root root 27856205 Nov 17 15:02
core.snort.59352.1605625368.gz
```

LINA處理核心檔案

FTD位於Firepower 1000、2100、4100和9300中時LINA核心檔案的位置

1.通過SSH或控制檯連線到裝置的CLI。

2.以專家模式進入。

```
> expert
admin@firepower:~$
```

3.成為超級使用者。

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```

4.導航至 /ngfw/var/data/cores/ 核心檔案所在的資料夾。

```
root@firepower:/home/admin# cd /ngfw/var/data/cores/
```

5.檢查該資料夾中的核心檔案。

```
root@firepower:/ngfw/var/data/cores# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49
core.lina.23228.1605628188.gz
```

如何使用FMC收集核心檔案

對於安裝了FTD的所有平台，應遵循以下步驟從裝置提取核心檔案。

1.對於Core Files位於 /ngfw/var/data/cores/ 需要把檔案移到 /ngfw/var/common/.

```
root@firepower:/ngfw/var/data/cores# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49 core.lina.23228.1605628188.gz
root@firepower:/ngfw/var/data/cores# mv core* /ngfw/var/common/
root@firepower:/ngfw/var/data/cores# cd /ngfw/var/common/
root@firepower:/ngfw/var/common# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49
core.lina.23228.1605628188.gz
```

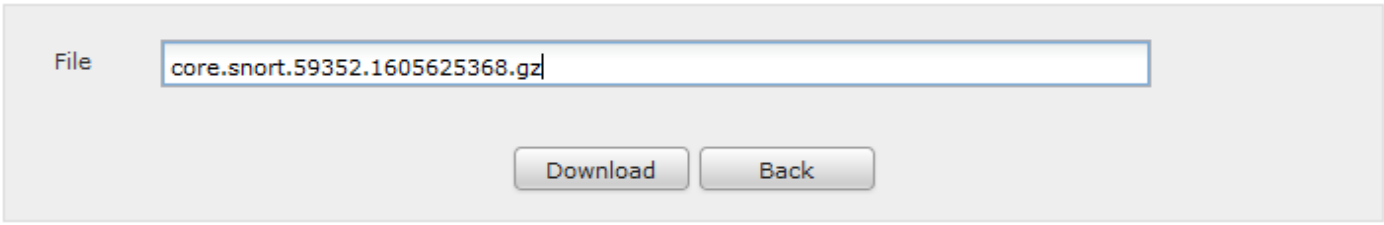
2.通過HTTPS訪問FMC，並進入**System > Health > Monitor**下。

3.選擇生成核心檔案的FTD。

4.選擇選項「高級故障排除」。

5.選擇選項「檔案下載」。

6.在搜尋欄上輸入將要下載的核心檔案的名稱，然後選擇「下載」選項。



7.下載後，將檔案上傳到SR進行分析。

如何使用FDM收集核心檔案

使用FDM時，不可能使用使用者介面收集特定檔案，相反，我們需要使用以下過程收集FTD的疑難解答檔案的核心檔案。

1.對於檔案位於以下位置的所有平台： /ngfw/var/common/ 和 /ngfw/var/data/cores/ 需要把檔案移到 /ngfw/var/log/.

```
root@firepower:cores# ls -l | grep -i core
-rw-r--r-- 1 root root 409612433 Nov 17 16:08 core.lina.3137.1605629317.gz
-rw-r--r-- 1 root root  27873115 Nov 17 15:01 core.snort.59095.1605625274.gz
-rw-r--r-- 1 root root  27856205 Nov 17 15:02 core.snort.59352.1605625368.gz
root@firepower:cores# mv core* /ngfw/var/log/
root@firepower:cores# cd /ngfw/var/log
root@firepower:log# ls -l | grep -i core
-rw-r--r-- 1 root root 409612433 Nov 17 16:08 core.lina.3137.1605629317.gz
-rw-r--r-- 1 root root  27873115 Nov 17 15:01 core.snort.59095.1605625274.gz
-rw-r--r-- 1 root root  27856205 Nov 17 15:02 core.snort.59352.1605625368.gz
```

2.使用FDM從FTD生成並下載疑難解答檔案。

使用FDM過程對檔案生成進行故障排除。

3.下載後，將檔案上傳到SR進行分析。