Firepower Threat Defenseデバイスからのコアファイルの収集

内容

概要

このドキュメントでは、FTDソフトウェアをサポートするすべてのプラットフォームを通じて、FTDデバイスのすべてのタイプのコアファイルを収集する手順について説明します。FTD上のプロセスで重大な問題が発生すると、プロセスの実行メモリのダンプをコアファイルとして保存できます。障害の根本原因を特定するために、シスコテクニカルサポートからコアファイルを要求されることがあります。

FTDデバイスには、FirepowerコアとLINAコアファイルの2種類のコアファイルがあります。

前提条件

要件

次の製品に関する知識があることが推奨されます。

- Firepower Management Center（FMC）
- Firepower Device Manager(FDM)
- Firepower Threat Defense(FTD)
- Firepower Extensible Operation System(FXOS)

手順

Firepowerプロセスのコアファイル

FTDがFirepower 2100、1000、ASAアプライアンス、およびISA 3000アプライアンスにあるときのFirepowerコアファイルの場所

これらのプラットフォームすべてについて、すべてのFirepowerプロセスに関連するコアファイルは、次の手順で検索できます。

1. SSHまたはコンソール経由でアプライアンスのCLIに接続します。

2.エキスパートモードで開始します。

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

3.ルートユーザになる。

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

4. /ngfw/var/common/ コアファイルがあるフォルダ。

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

5.ファイルのフォルダを確認します。

```
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がFirepower 4100または9300にある場合のFirepowerコアファイルの場所

これら2つのプラットフォームでは、コアファイルを2つの可能なパスに配置できます。最初のパスは前のセクションと同じで、2番目のパスはこの手順で配置できます。

1. SSHまたはコンソール経由でアプライアンスのCLIに接続します。

2.エキスパートモードで開始します。

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

3.ルートユーザになる。

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

4. /ngfw/var/data/cores/ コアファイルがあるフォルダ。

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

5.ファイルのフォルダを確認します。

```
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プロセスのコアファイル

FTDがFirepower 1000、2100、4100、および9300にある場合のLINAコアファイルの場所

1. SSHまたはコンソール経由でアプライアンスのCLIに接続します。

2.エキスパートモードで開始します。

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

3.ルートユーザになる。

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

4. /ngfw/var/data/cores/ コアファイルがあるフォルダ。

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

5.コアファイルのフォルダを確認します。

```
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
```

FMCを使用してコアファイルを収集する方法

FTDがインストールされているすべてのプラットフォームで、デバイスからコアファイルを抽出するには、次の手順に従う必要があります。

1.コアファイルが存在するすべてのプラットフォームについて /ngfw/var/data/cores/ ファイルを /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
```

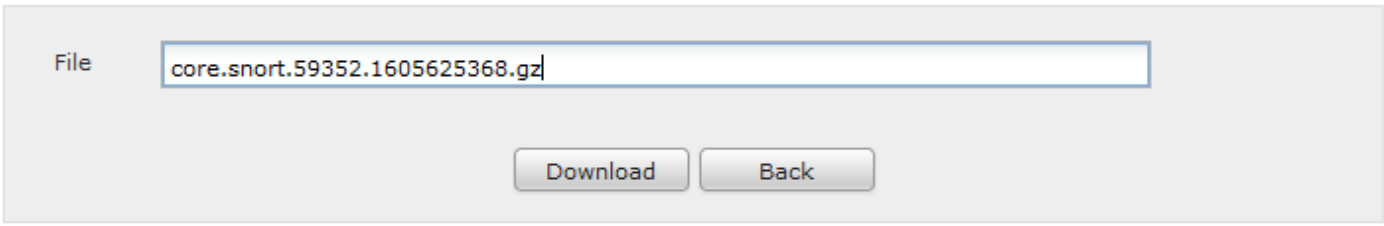
2. HTTPS経由でFMCにアクセスし、[System] > [Health] > [Monitor]の順に選択します。

3.コアファイルが生成されたFTDを選択します。

4. [Advanced Troubleshooting]オプションを選択します。

5. [File Download]オプションを選択します。

6.検索バーで、ダウンロードするコアファイルの名前を入力し、[Download]オプションを選択します。



7.ダウンロードしたら、分析のためにファイルをSRにアップロードします。

FDMを使用してコア・ファイルを収集する方法

FDMを使用する場合、ユーザー・インタフェースを使用して特定のファイルを収集することはできず、FTDのトラブルシューティング・ファイルとともにコア・ファイルを収集するには、次の手順を使用する必要があります。

1.ファイルが存在するすべてのプラットフォームについて /ngfw/var/common/ と /ngfw/var/data/cores/ ファイルを /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. FDMを使用して、FTDからトラブルシューティング・ファイルを生成してダウンロードします。

FDM手順を使用したファイル生成のトラブルシューティング。

3.ダウンロードしたら、分析のためにファイルをSRにアップロードします。