从Firepower威胁防御设备收集核心文件

目录

简介

本文档介绍通过支持FTD软件的所有平台收集FTD设备所有类型核心文件的过程。当FTD上的进程遇到严重问题时，该进程的运行内存转储可以另存为核心文件。为了确定故障的根本原因，思科技术支持可能会请求核心文件。

对于FTD设备，我们有两种类型的核心文件，Firepower核心和LINA核心文件。

先决条件

要求

思科建议您了解以下产品：

- Firepower管理中心(FMC)
- Firepower设备管理器(FDM)
- Firepower威胁防御(FTD)
- Firepower可扩展操作系统(FXOS)

步骤

Firepower处理核心文件

当FTD在Firepower 2100、1000、ASA设备和ISA 3000设备中时，Firepower核心文件的位置

对于所有这些平台，与所有firepower进程相关的核心文件都可以通过此程序找到。

1.通过SSH或控制台连接到设备的CLI。

2.进入专家模式。

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

3.成为根用户。

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

4.定位至 /ngfw/var/common/ 文件夹，核心文件所在的位置。

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

5.检查文件夹。

```
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
```

当FTD在Firepower 4100或9300中时Firepower核心文件的位置

对于这两个平台，核心文件可以位于两条可能的路径中，第一条路径与前一部分相同，第二条路径可以通过此过程进行定位。

1.通过SSH或控制台连接到设备的CLI。

2.进入专家模式。

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

3.成为根用户。

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

4.定位至 /ngfw/var/data/cores/ 文件夹，核心文件所在的位置。

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

5.检查文件夹。

```
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进程核心文件

当FTD在Firepower 1000、2100、4100和9300中时LINA核心文件的位置

1.通过SSH或控制台连接到设备的CLI。

2.进入专家模式。

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

3.成为根用户。

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

4.定位至 /ngfw/var/data/cores/ 文件夹，核心文件所在的位置。

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

5.检查文件夹以查找核心文件。

```
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收集核心文件

对于安装了FTD的所有平台，应按照此步骤从设备中提取核心文件。

1.对于核心文件位于 /ngfw/var/data/cores/ 需要在 /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
```

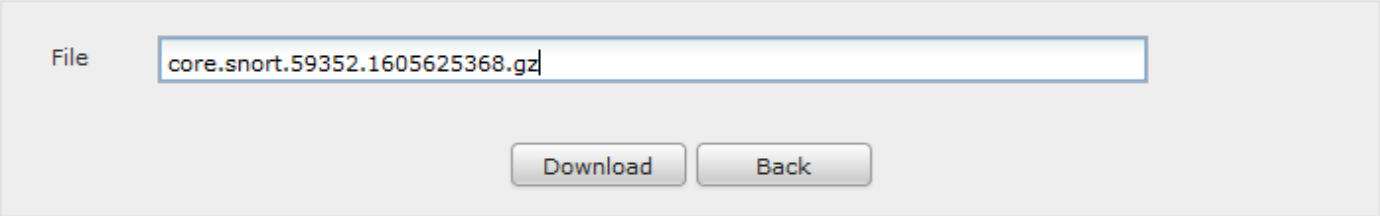
2.通过HTTPS访问FMC，并进入System > Health > Monitor下。

3.选择生成核心文件的FTD。

4.选择“高级故障排除”选项。

5.选择“文件下载”选项。

6.在搜索栏上，输入要下载的核心文件的名称并选择“下载”选项。



7.下载后，将文件上传到SR进行分析。

如何使用FDM收集核心文件

使用FDM时，无法使用用户界面收集特定文件，而是需要使用以下过程来收集包含FTD故障排除文件的核心文件。

1.对于文件所在的所有平台， /ngfw/var/common/ 和 /ngfw/var/data/cores/ 需要在 /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从FTD生成并下载故障排除文件。

使用FDM过程排除文件生成故障。

3.下载后，将文件上传到SR进行分析。