Sammlung von Kerndateien von einem FirePOWER Threat Defense-Gerät

Inhalt

Einführung

Dieses Dokument beschreibt das Verfahren zum Sammeln aller Arten von Core-Dateien für FTD-Geräte über alle Plattformen, die FTD-Software unterstützen. Wenn ein Prozess auf dem FTD auf ein kritisches Problem stößt, kann ein Speicherauszug des laufenden Prozessspeichers als Core-Datei gespeichert werden. Um die Ursache des Fehlers zu ermitteln, kann der technische Support von Cisco die Kerndateien anfordern.

Für FTD-Geräte gibt es zwei Arten von Core-Dateien: Firepower-Cores und LINA-Cores-Dateien.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über die folgenden Produkte verfügen:

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

Vorgehensweise

Firepower verarbeitet Kerndateien

Speicherort der Firepower Core-Dateien, wenn sich die FTD in Firepower 2100, 1000, ASA Appliance und ISA 3000 Appliance befindet

Für alle diese Plattformen können die Kerndateien für alle Firepower-Prozesse mit diesem Verfahren gefunden werden.

1. Stellen Sie über SSH oder Konsole eine Verbindung zur CLI der Einheit her.

2. Wechseln Sie in den Expertenmodus.

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

3. Werden Sie Root-Benutzer.

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

4. Navigieren Sie zum /ngfw/var/common/ Ordner, in dem sich die Kerndateien befinden.

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

5. Überprüfen Sie den Ordner auf die Datei.

```
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
```

Speicherort von Firepower Core-Dateien, wenn sich die FTD in Firepower 4100 oder 9300 befindet

Für diese beiden Plattformen können sich die Kerndateien in zwei möglichen Pfaden befinden, die erste ist die gleiche wie der vorherige Abschnitt, die zweite Pfad kann mit dieser Prozedur gefunden werden.

1. Stellen Sie über SSH oder Konsole eine Verbindung zur CLI der Einheit her.

2. Wechseln Sie in den Expertenmodus.

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

3. Werden Sie Root-Benutzer.

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

4. Navigieren Sie zum /ngfw/var/data/cores/ Ordner, in dem sich die Kerndateien befinden.

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

5. Überprüfen Sie den Ordner auf die Datei.

```
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 Process Core-Datei

Speicherort von LINA Core-Dateien, wenn sich die FTD in Firepower 1000, 2100, 4100 und 9300 befindet

1. Stellen Sie über SSH oder Konsole eine Verbindung zur CLI der Einheit her.

2. Wechseln Sie in den Expertenmodus.

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

3. Werden Sie Root-Benutzer.

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

4. Navigieren Sie zum /ngfw/var/data/cores/ Ordner, in dem sich die Kerndateien befinden.

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

5. Überprüfen Sie den Ordner auf die Kerndatei.

```
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
```

Sammeln der Core-Dateien mit dem FMC

Für alle Plattformen, auf denen FTD installiert ist, sollte dieses Verfahren befolgt werden, um die Kerndateien von den Geräten zu extrahieren.

1. Für alle Plattformen, auf denen sich die Core-Dateien unter /ngfw/var/data/cores/ müssen die Dateien unter /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
```

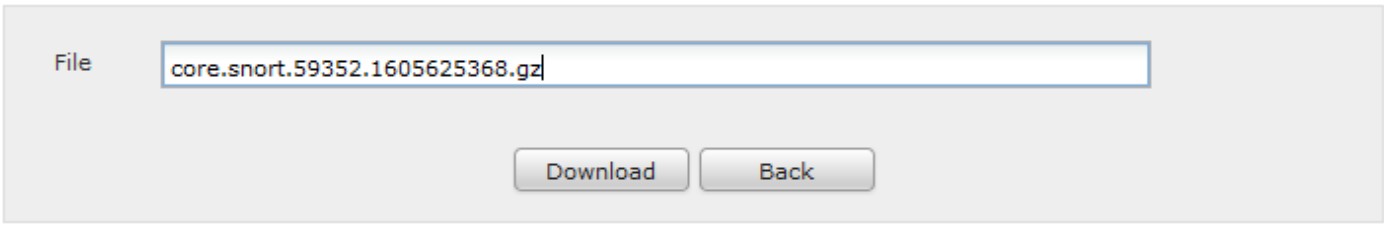
2. Zugriff auf das FMC über HTTPS und unter **System > Health > Monitor**.

3. Wählen Sie den FTD aus, in dem die Core-Dateien generiert wurden.

4. Wählen Sie die Option Erweiterte Fehlerbehebung aus.

5. Wählen Sie die Option Dateidownload aus.

6. Geben Sie in der Suchleiste den Namen der herunterzuladenden Core-Datei ein, und wählen Sie Download aus.



7. Laden Sie nach dem Herunterladen die Dateien zur Analyse in den SR hoch.

Sammeln der Core-Dateien mit FDM

Bei der Verwendung von FDM ist es nicht möglich, bestimmte Dateien über die Benutzeroberfläche zu sammeln. Stattdessen müssen wir die folgenden Verfahren verwenden, um die Core-Dateien mit den Fehlerbehebungsdateien der FTD zu sammeln.

1. Für alle Plattformen, auf denen sich die Dateien unter /ngfw/var/common/ und /ngfw/var/data/cores/ müssen die Dateien unter /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. Erstellen und Herunterladen der Fehlerbehebungsdateien aus der FTD mithilfe von FDM.

Fehlerbehebung bei der Dateigenerierung mithilfe der FDM-Prozedur.

3. Laden Sie die Datei nach dem Herunterladen zur Analyse in den SR hoch.