Raccolta di file di base da un dispositivo Firepower Threat Defense

Sommario

Introduzione

Questo documento descrive la procedura per raccogliere tutti i tipi di file di base per i dispositivi FTD attraverso tutte le piattaforme che supportano il software FTD. Quando un processo su FTD incontra un problema critico, un dump della memoria in esecuzione del processo può essere salvato come file di base. Per determinare la causa principale del problema, il supporto tecnico Cisco potrebbe richiedere i file di base.

Per i dispositivi FTD sono disponibili due tipi di file core, i core Firepower e i file core LINA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

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

Procedura

Firepower elabora i file di base

Posizione dei file di base di Firepower quando il FTD si trova in Firepower 2100, 1000, appliance ASA e appliance ISA 3000

Per tutte queste piattaforme i file di base relativi a tutti i processi firepower possono essere individuati con questa procedura.

1. Connettersi alla CLI dell'accessorio tramite SSH o console.

2. Accedere in modalità esperto.

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

3. Diventare un utente root.

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

4. Passare alla /ngfw/var/common/ , in cui si trovano i file di base.

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

5. Controllare la cartella del file.

```
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
```

Posizione dei file di base di Firepower quando il FTD è in Firepower 4100 o 9300

Per queste due piattaforme, i file di base possono trovarsi in due percorsi possibili, il primo è lo stesso della sezione precedente, il secondo percorso può essere individuato con questa procedura.

1. Connettersi alla CLI dell'accessorio tramite SSH o console.

2. Accedere in modalità esperto.

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

3. Diventare un utente root.

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

4. Passare alla /ngfw/var/data/cores/ , in cui si trovano i file di base.

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

5. Controllare la cartella del file.

```
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
```

File di base processo LINA

Percorso dei file di base LINA quando il FTD è in Firepower 1000, 2100, 4100 e 9300

1. Connettersi alla CLI dell'accessorio tramite SSH o console.

2. Accedere in modalità esperto.

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

3. Diventare un utente root.

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

4. Passare alla /ngfw/var/data/cores/ , in cui si trovano i file di base.

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

5. Controllare la cartella per il file di base.

```
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
```

Come raccogliere i file di base utilizzando FMC

Per tutte le piattaforme in cui è installato l'FTD, è necessario seguire questa procedura per estrarre i file di base dai dispositivi.

1. Per tutte le piattaforme in cui si trovano i file principali /ngfw/var/data/cores/ sarà necessario spostare i file in /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
```

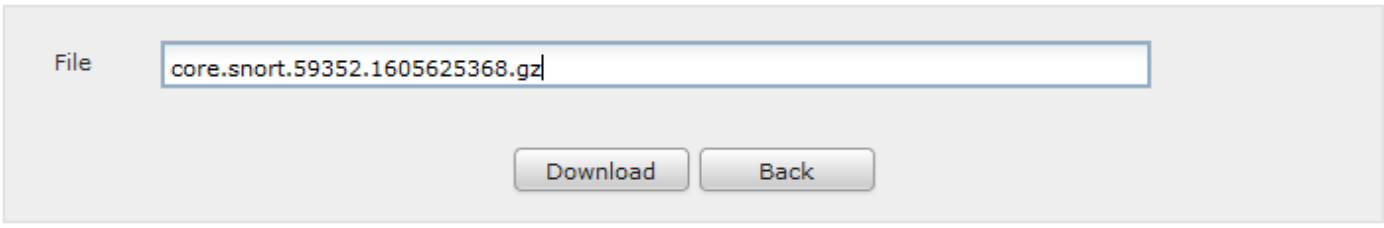
2. Accedere al CCP tramite HTTPS e andare in **Sistema > Integrità > Monitoraggio**.

3. Selezionare l'FTD in cui sono stati generati i file di base.

4. Selezionare l'opzione Advanced Troubleshooting.

5. Selezionare l'opzione File Download.

6. Sulla barra di ricerca, inserire il nome del Core File che verrà scaricato e selezionare l'opzione Download.



7. Una volta scaricato, caricare i file nella SR per analizzarli.

Come raccogliere i file di base utilizzando FDM

Quando si utilizza FDM, non è possibile raccogliere file specifici utilizzando l'interfaccia utente, è invece necessario utilizzare la seguente procedura per raccogliere i Core Files con i file di risoluzione dei problemi del FTD.

1. Per tutte le piattaforme in cui si trovano i file /ngfw/var/common/ e /ngfw/var/data/cores/ sarà necessario spostare i file in /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. Generare e scaricare i file di risoluzione dei problemi da FTD utilizzando FDM.

Risoluzione dei problemi relativi alla generazione di file mediante la procedura FDM.

3. Una volta scaricato, caricare il file nella SR per analizzarlo.