Collecte de fichiers principaux à partir d'un périphérique de défense contre les menaces Firepower

Contenu

Introduction

Ce document décrit la procédure de collecte de tous les types de fichiers principaux pour les périphériques FTD via toutes les plates-formes qui prennent en charge le logiciel FTD. Lorsqu'un processus sur le FTD rencontre un problème critique, un vidage de la mémoire en cours d'exécution du processus peut être enregistré en tant que fichier principal. Afin de déterminer la cause première de l'échec, l'assistance technique Cisco peut demander les fichiers principaux.

Pour les périphériques FTD, nous avons deux types de fichiers principaux : les coeurs Firepower et les coeurs LINA.

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez ces produits :

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

Procédure

Firepower traite les fichiers principaux

Emplacement des fichiers principaux Firepower lorsque le FTD se trouve dans Firepower 2100, 1000, l'appliance ASA et l'appliance ISA 3000

Pour toutes ces plates-formes, les fichiers principaux liés à tous les processus firepower peuvent être localisés avec cette procédure.

1. Connectez-vous à l'interface de ligne de commande de l'appliance via SSH ou la console.

2. Passez en mode expert.

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

3. Devenez utilisateur root.

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

4. Accédez à la /ngfw/var/common/ , où se trouvent les fichiers principaux.

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

5. Vérifiez le dossier du fichier.

```
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
```

Emplacement des fichiers principaux Firepower lorsque le FTD est dans Firepower 4100 ou 9300

Pour ces deux plates-formes, les fichiers principaux peuvent être localisés dans deux chemins possibles, le premier est identique à la section précédente, le second chemin peut être localisé avec cette procédure.

1. Connectez-vous à l'interface de ligne de commande de l'appliance via SSH ou la console.

2. Passez en mode expert.

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

3. Devenez utilisateur root.

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

4. Accédez à la /ngfw/var/data/cores/ , où se trouvent les fichiers principaux.

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

5. Vérifiez le dossier du fichier.

```
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
```

Fichier principal du processus LINA

Emplacement des fichiers principaux LINA lorsque le FTD se trouve dans Firepower 1000, 2100, 4100 et 9300

1. Connectez-vous à l'interface de ligne de commande de l'appliance via SSH ou la console.

2. Passez en mode expert.

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

3. Devenez utilisateur root.

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

4. Accédez à la /ngfw/var/data/cores/ , où se trouvent les fichiers principaux.

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

5. Vérifiez le dossier du fichier principal.

```
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
```

Comment collecter les fichiers principaux à l'aide de FMC

Pour toutes les plates-formes, où le FTD est installé, cette procédure doit être suivie pour extraire les fichiers principaux des périphériques.

1. Pour toutes les plates-formes sur lesquelles se trouvent les fichiers principaux /ngfw/var/data/cores/ devra déplacer les fichiers sous /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
```

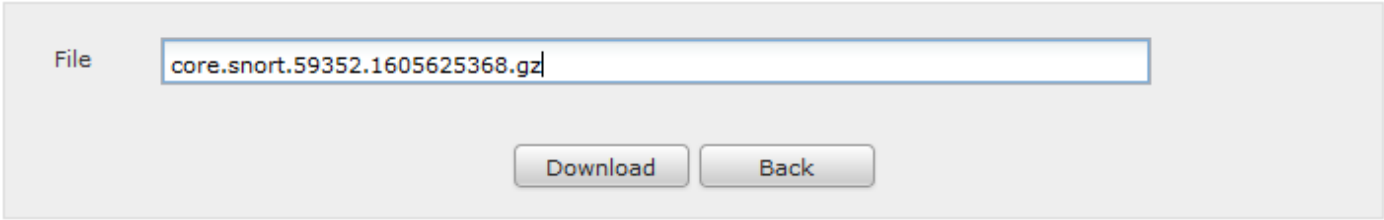
2. Accédez au FMC via HTTPS et passez sous **System > Health > Monitor**.

3. Sélectionnez le FTD où les fichiers principaux ont été générés.

4. Sélectionnez l'option Dépannage avancé.

5. Sélectionnez l'option Téléchargement de fichier.

6. Dans la barre de recherche, indiquez le nom du fichier principal qui sera téléchargé et sélectionnez l'option Télécharger.



7. Une fois téléchargé, téléchargez le ou les fichiers dans la demande de service pour analyse.

Comment collecter les fichiers principaux à l'aide de FDM

Lors de l'utilisation de FDM, il n'est pas possible de collecter des fichiers spécifiques à l'aide de l'interface utilisateur. Nous devons plutôt utiliser la procédure suivante pour collecter les fichiers principaux avec les fichiers de dépannage du FTD.

1. Pour toutes les plates-formes sur lesquelles se trouvent les fichiers /ngfw/var/common/ et /ngfw/var/data/cores/ devra déplacer les fichiers sous /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. Générez et téléchargez les fichiers de dépannage à partir du FTD à l'aide de FDM.

Dépannage de la génération de fichiers à l'aide de la procédure FDM.

3. Une fois téléchargé, téléchargez le fichier sur le SR pour analyse.