# Collecter les journaux pour les problèmes courants de Firepower

## Table des matières



## Introduction

Ce document décrit les journaux à collecter avant d'ouvrir un dossier TAC pour le dépannage des problèmes courants de Firepower.

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir connaissance des produits suivants :

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

## Collecter les journaux pour les problèmes courants de Firepower

### 1. Problème de basculement FTD inattendu

Informations à collecter avant d'ouvrir le dossier TAC pour résoudre le problème :

- Nom d'hôte et adresse IP de l'unité défaillante.
- Toute modification récente effectuée.
- Occurrence de l'événement : heure de l'événement et fuseau horaire.
- Connectivité par câble de basculement : directement connectée aux deux unités ou à tout périphérique intermédiaire (commutateur) situé entre les deux.
- Sortie de commande requise des deux unités :

show tech-support

show failover-history

show failover state

- Syslog pendant 10 minutes avant et après l'événement.
- Collecter le fichier de dépannage FTD.

Pour générer un fichier de dépannage, référez-vous à Dépannage des procédures de génération de fichier Firepower.

Pour ouvrir un dossier, reportez-vous à TAC SR.

Exemple : Comment exécuter des commandes depuis FTDv.

Connectez-vous à FTD SSH :

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.6.5 (build 13)
Cisco Firepower Threat Defense for VMWare v6.6.5 (build 81)

>
>
```

Exécutez les commandes à partir de clish :

```
> show tech-support                 <- - To display configuration of the device.
```

```
> show failover history             <- - To display failover Date/Time, what was the failover state an
```

```
> show failover state               <- - To display Last Failure Reason and Date/Time.
```

## 2. Problème d'interface utilisateur graphique FMC inaccessible

Informations à collecter avant d'ouvrir le dossier TAC pour résoudre le problème :

- Toute modification récente effectuée.
- Sortie de commande requise de FMC SSH :

état pmtool | interface utilisateur graphique grep -i

état pmtool | grep -E "Attente|désactivée|désactivée"

free -g

df -h

DBCheck.pl

peigné

- Lors de l'accès à l'interface utilisateur graphique du FMC, si un message d'erreur s'affiche, prenez une capture d'écran du message d'erreur.
- Lors de l'accès à l'interface utilisateur graphique FMC, vous devez collecter les résultats des commandes mentionnées :

manchon pour amorçage

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- Collecter le fichier de dépannage FMC.

Pour générer un fichier de dépannage, référez-vous à Dépannage des procédures de génération de fichier Firepower.

Pour ouvrir un dossier, reportez-vous à TAC SR.

Exemple : Comment exécuter des commandes à partir de FMCv.

Connectez-vous à FMC SSH :

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 175)
Cisco Firepower Management Center for VMware v7.0.1 (build 84)

>
> expert
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Exécutez les commandes à partir de la racine :

```
root@firepower:~# pmtool status | grep -i gui                  <- - To display all GUI services status.

root@firepower:~# pmtool status | grep -E "Wait|down|disabled" <- - To display services that are in wai

root@firepower:~# free -g                                      <- - To display Used and Free memory in

root@firepower:~# df -h                                        <- - To display Used and Free disk.

root@firepower:~# DBCheck.pl         <- - To display any error or warning in database.(Database Integri

root@firepower:~# top                <- - To display which processes cpu & memory utilisation.

root@firepower:~# pigtail gui        <- - To display GUI logs in real time.

root@firepower:~# cd /var/log/httpd/
root@firepower:/var/log/httpd# tail -f httpsd_access_log <- - To display GUI web server access logs in

root@firepower:~# cd /var/log/httpd/
root@firepower:/var/log/httpd# tail -f httpsd_error_log  <- - To display GUI web server error logs in r
```

Pour interrompre les journaux, entrez CTRL+C.

## 3. Problème d'échec de sauvegarde FMC

Informations à collecter avant d'ouvrir le dossier TAC pour résoudre le problème :

- Toute modification récente effectuée.
- Capture d'écran des messages d'erreur relatifs à l'échec de sauvegarde.
- La sauvegarde manuelle échoue-t-elle ou la sauvegarde planifiée/automatique échoue-t-elle ?
- Si la sauvegarde planifiée échoue, collectez l'occurrence d'événement : Heure et Fuseau

horaire.

- En cas d'échec de la sauvegarde manuelle, collectez les résultats de la commande tout en effectuant une sauvegarde manuelle :

tail -f /var/log/backup.log

- Collecter le fichier de dépannage FMC.

Pour générer un fichier de dépannage, référez-vous à Dépannage des procédures de génération de fichier Firepower.

Pour ouvrir un dossier, reportez-vous à TAC SR.

Exemple : exécution de commandes à partir de FMCv.

Connectez-vous à FMC SSH et exécutez la commande à partir de la racine :

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 175)
Cisco Firepower Management Center for VMware v7.0.1 (build 84)

>
> expert
admin@firepower:~$ sudo su -
Password:
Last login: Wed Sep  6 21:38:20 UTC 2023 on pts/0
root@firepower:~#
root@firepower:~# cd /var/log/
root@firepower:/var/log# tail -f backup.log                    <- - To display backup logs in real tim
```

Pour interrompre les journaux, entrez CTRL+C.

## 4. Échec du déploiement de la stratégie

- Toute modification récente effectuée.
- À quel pourcentage le déploiement de la stratégie échoue-t-il ?
- À partir de l'interface utilisateur graphique de FMC, prenez une capture d'écran des messages d'erreur relatifs à l'échec du déploiement et une transcription pour collecter l'ID de transaction :

Cliquez sur l'icône en regard de l'onglet Déployer, puis sur l'onglet Déploiement, puis sur l'onglet Afficher l'historique.

- Lors du déploiement de la stratégie, vous devez collecter le résultat des commandes mentionnées :

De FMC :

déploiement en queue de cochon

tail -f /var/log/sf/policy_deployment.log

À partir de FTD :

déploiement en queue de cochon

tail -f /ngfw/var/log/ngfwManager.log

tail -f /ngfw/var/log/sf/policy_deployment.log

- Collecter le fichier de dépannage FMC et FTD.

Pour générer un fichier de dépannage, référez-vous à Dépannage des procédures de génération de fichier Firepower.

Pour ouvrir un dossier, reportez-vous à TAC SR.

Exemple : exécution de commandes à partir de FMCv.

Connectez-vous à FMC SSH :

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 175)
Cisco Firepower Management Center for VMware v7.0.1 (build 84)

>
> expert
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~#
```

Exécutez les commandes à partir de la racine :

```
root@firepower:~# pigtail deploy                          <- - To display deployment logs in real tim
```

```
root@firepower:/# cd /var/log/sf
root@firepower:/var/log/sf# tail -f policy_deployment.log   <- - To display policy deployment logs in r
```

Exemple : Comment exécuter des commandes depuis FTDv.

Connectez-vous à FTD SSH :

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.6.5 (build 13)
Cisco Firepower Threat Defense for VMWare v6.6.5 (build 81)

>
> expert
admin@FTDA:~$ sudo su -
Password:
root@FTDA:~#
```

Exécutez les commandes à partir de la racine :

```
root@FTDA:~# pigtail deploy                  <- - To display deployment related logs in real time.
```

```
root@FTDA:~# cd /ngfw/var/log
root@FTDA:log# tail -f ngfwManager.log       <- - To display FTD to FMC communication related logs in r
```

```
root@firepower:/# cd /var/log/sf
root@firepower:/var/log/sf# tail -f policy_deployment.log   <- - To display policy deployment logs in r
```

Pour interrompre les journaux, entrez CTRL+C.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.