

# 收集Firepower常見問題的日誌

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[收集Firepower常見問題的日誌](#)

[1. FTD意外容錯移轉問題](#)

[2. FMC GUI無法訪問問題](#)

[3. FMC備份失敗問題](#)

[4.策略部署失敗](#)

## 簡介

本檔案介紹在開啟TAC案例以疑難排解Firepower常見問題之前要收集哪些日誌。

## 必要條件

### 需求

思科建議您瞭解以下產品：

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

## 收集Firepower常見問題的日誌

### 1. FTD意外容錯移轉問題

開啟TAC案例之前需要收集資訊以排解問題：

- 出現故障的裝置的主機名和IP地址。
- 最近所做的任何更改。
- 事件發生次數：事件的時間和時區。
- 故障轉移電纜連線：直接與兩台裝置或兩台裝置之間的任何中間裝置（交換機）連線。
- 兩個單元所需的命令輸出：

```
show tech-support
```

```
show failover-history
```

```
show failover state
```

- 事件發生前後保持10分鐘的系統日誌。
- 收集FTD疑難排解檔案。

要生成故障排除檔案，請參閱[排除Firepower檔案生成過程故障。](#)

若要建立案例，請參閱[TAC SR](#)。

範例：如何從FTDv執行命令。

登入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)
```

```
>
>
```

從clish運行命令：

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

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

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

## 2. FMC GUI無法訪問問題

開啟TAC案例之前需要收集資訊以排解問題：

- 最近所做的任何更改。
- FMC SSH所需的命令輸出：

```
pmtool狀態 | grep -i gui
```

```
pmtool狀態 | grep -E "等待|關閉|禁用"
```

```
free -g
```

df -h

DBCheck.pl

頂端

- 訪問FMC GUI時，如果出現任何錯誤消息，則獲取該錯誤消息的螢幕截圖。
- 訪問FMC GUI時，需要收集提到的命令輸出：

digtail gui

```
tail -f /var/log/httpd/httpsd_access_log
```

```
tail -f /var/log/httpd/httpsd_error_log
```

- 收集FMC故障排除檔案。

要生成故障排除檔案，請參閱[排除Firepower檔案生成過程故障。](#)

若要建立案例，請參閱[TAC SR](#)。

示例：如何從FMCv運行命令。

登入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:~#
```

從root運行命令：

```
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 wait
```

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

要中斷日誌，請輸入CTRL+C。

### 3. FMC備份失敗問題

開啟TAC案例之前需要收集資訊以排解問題：

- 最近所做的任何更改。
- 備份失敗的錯誤消息的螢幕快照。
- 手動備份失敗還是計畫/自動備份失敗？
- 如果定時備份失敗，請收集事件發生次數：時間和時區。
- 如果手動備份失敗，請在執行手動備份時收集命令輸出：

tail -f /var/log/backup.log

- 收集FMC故障排除檔案。

要生成故障排除檔案，請參閱[Firepower檔案生成過程故障排除](#)。

若要建立案例，請參閱[TAC SR](#)。

示例：如何從FMCv運行命令。

登入到FMC SSH並從根目錄運行命令：

```
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 time
```

要中斷日誌，請輸入CTRL+C。

#### 4.策略部署失敗

- 最近所做的任何更改。
- 策略部署失敗的百分比是多少。
- 在FMC GUI中，獲取部署失敗的錯誤消息的螢幕截圖，並記錄以收集事務ID:

點選Deploy頁籤旁邊的圖示，然後點選Deployment頁籤，然後點選Show History頁籤。

- 在執行策略部署時，需要收集提到的命令輸出：

在FMC上：

尾部部署

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

自FTD:

尾部部署

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

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

- 收集FMC和FTD疑難排解檔案。

要生成故障排除檔案，請參閱[Firepower檔案生成過程故障排除](#)。

若要建立案例，請參閱[TAC SR](#)。

示例：如何從FMCv運行命令。

登入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:~#
```

從root運行命令：

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

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

範例：如何從FTDv執行命令。

登入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:~#
```

從root運行命令：

```
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
```

要中斷日誌，請輸入CTRL+C。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。