# firepower 일반 문제에 대한 로그 수집

## 목차



## 소개

이 문서에서는 Firepower 일반 문제 해결을 위해 TAC 케이스를 열기 전에 수집할 로그에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 제품에 대해 알고 있는 것이 좋습니다.

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

## firepower 일반 문제에 대한 로그 수집

### 1. FTD 예기치 않은 장애 조치 문제

문제를 해결하기 위해 TAC 케이스를 열기 전에 정보를 수집해야 합니다.

- 실패한 유닛의 호스트 이름 및 IP 주소.
- 최근에 변경한 내용이 있습니다.
- 이벤트 발생: 이벤트의 시간 및 표준 시간대.
- 장애 조치 케이블 연결: 두 유닛 또는 그 사이의 중간 디바이스(스위치)에 직접 연결됩니다.
- 두 유닛에서 모두 명령 출력이 필요합니다.

show tech-support

장애 조치 기록 표시

장애 조치 상태 표시

- 이벤트 발생 전/후 10분 동안 Syslog를 생성합니다.
- FTD 문제 해결 파일을 수집합니다.

문제 해결 파일을 생성하려면 Firepower 파일 생성 절차 문제 해결을 참조하십시오.

케이스를 열려면 TAC SR을 참조하십시오.

예: FTDv에서 명령을 실행하는 방법

FTD SSH에 로그인합니다.

```
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)

>
>
```

clash에서 명령을 실행합니다.

```
> 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. FMC GUI에 액세스할 수 없는 문제

문제를 해결하기 위해 TAC 케이스를 열기 전에 정보를 수집해야 합니다.

- 최근에 변경한 내용이 있습니다.
- FMC SSH에서 필요한 명령 출력:

pmtool 상태 | grep -i gui

pmtool 상태 | grep -E "Wait|down|disabled"

자유 -g

df -h

DBCheck.pl

꼭대기

- FMC GUI에 액세스하는 동안 오류 메시지가 있으면 오류 메시지의 스크린샷을 만듭니다.
- FMC GUI에 액세스하는 동안 언급된 명령 출력을 수집해야 합니다.

피그테일 구이

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- FMC 문제 해결 파일을 수집합니다.

문제 해결 파일을 생성하려면 Firepower 파일 생성 절차 문제 해결을 참조하십시오.

케이스를 열려면 TAC SR을 참조하십시오.

예: FMCv에서 명령을 실행하는 방법.

FMC SSH에 로그인합니다.

```
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:~#
```

root에서 명령을 실행합니다.

```
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
```

로그를 중단하려면 CTRL+C를 입력합니다.

## 3. FMC 백업 실패 문제

문제를 해결하기 위해 TAC 케이스를 열기 전에 정보를 수집해야 합니다.

- 최근에 변경한 내용이 있습니다.
- 백업 실패에 대한 오류 메시지 스크린샷.
- 수동 백업이 실패합니까, 아니면 예약/자동 백업이 실패합니까?
- 예약된 백업이 실패한 경우 이벤트 발생(시간 및 시간대)을 수집합니다.
- 수동 백업이 실패할 경우 수동 백업을 수행하는 동안 명령 출력을 수집합니다.

tail -f /var/log/backup.log

- FMC 문제 해결 파일을 수집합니다.

문제 해결 파일을 생성하려면 Firepower 파일 생성 절차 문제 해결을 참조하십시오.

케이스를 열려면 TAC SR을 참조하십시오.

예: FMCv에서 명령을 실행하는 방법

FMC SSH에 로그인하고 루트에서 명령을 실행합니다.

```
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
```

로그를 중단하려면 CTRL+C를 입력합니다.

## 4. 정책 배포 실패

- 최근에 변경한 내용이 있습니다.
- 정책 구축에 실패하는 비율이 얼마나 됩니까?
- FMC GUI에서 구축 실패에 대한 오류 메시지와 트랜잭션 ID를 수집하는 기록을 스크린샷으로 캡처합니다.

Deploy(구축) 탭 옆의 아이콘을 클릭한 다음 Deployment(구축) 탭을 클릭하고 Show History(기록 표시) 탭을 클릭합니다.

- 정책 구축을 수행하는 동안 언급된 명령 출력을 수집해야 합니다.

FMC에서:

쇠머리오목눈이류

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

FTD에서:

쇠머리오목눈이류

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

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

- FMC 및 FTD 문제 해결 파일을 수집합니다.

문제 해결 파일을 생성하려면 Firepower 파일 생성 절차 문제 해결을 참조하십시오.

케이스를 열려면 TAC SR을 참조하십시오.

예: FMCv에서 명령을 실행하는 방법

FMC SSH에 로그인합니다.

```
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:~#
```

root에서 명령을 실행합니다.

```
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
```

예: FTDv에서 명령을 실행하는 방법

FTD SSH에 로그인합니다.

```
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:~#
```

root에서 명령을 실행합니다.

```
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
```

로그를 중단하려면 CTRL+C를 입력합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.