

# ASA 또는 FTD 예기치 않은 다시 로드 문제 해결

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[모든 플랫폼과 논리적 디바이스에 걸쳐 공통적으로 확인할 사항](#)

[디바이스\(논리적 또는 새시\)가 리부팅되었거나 충돌했는지 확인합니다.](#)

[ASA SoftwareLina\(FTD의 경우\) 충돌 시 Crashinfo 확인](#)

[ASA 플랫폼에서 확인할 사항](#)

[ASA 이미지를 실행하는 모든 ASA 플랫폼](#)

[실행 중인 FTD 이미지를 지원하는 ASA 플랫폼](#)

[firepower 플랫폼에서 확인할 사항](#)

[FP9300/FP4100 FXOS](#)

[FTD를 실행하는 FP9300/FP4100에서](#)

[ASA를 실행하는 FP9300/FP4100에서](#)

[FP2100 FXOS/ASA/FTD에서](#)

[FP1000 FXOS/ASA/FTD에서](#)

[코어 파일 다운로드](#)

[기타 확인 사항\(Firepower 4100 및 9300 플랫폼 관련\)](#)

[모듈 내의 코어 파일 보기](#)

[시스템 충돌과 관련된 알려진 버그](#)

---

## 소개

이 문서에서는 FTD(Firepower Threat Defense) 또는 ASA(Adaptive Security Appliance) 디바이스가 명백한 이유 없이 다시 로드되는 시나리오를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower 및 ASA 하드웨어 플랫폼의 기본 사항 이해
- firepower 플랫폼의 논리적 디바이스 이해

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 5500-X with ASA Software Version 9.x
- FTD 소프트웨어 버전 6.2.3 이상이 포함된 ASA 5500-X
- Firepower 1000, 1100, 2100, 4100, 9300 series with ASA Software Version 9. x
- Firepower 1000, 1100, 2100, 4100 및 9300 Series(FTD 소프트웨어 버전 6.2.3 이상)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

이 문서에서 디바이스는 ASA 또는 Firepower NGFW(Next-Generation Firewalls)를 말하며, Cisco Secure Firewalls로 브랜드화되어 ASA 또는 FTD 이미지를 논리적 디바이스로 실행합니다.

Cisco Secure Firewalls에는 다양한 하드웨어 및 소프트웨어 버전이 포함되어 있습니다. ASA 제품군에는 5500-X Series 방화벽이 포함되어 있으며 Firepower 제품군에는 FPR 1000, 2100, 4100 및 9300 Series 장치가 포함되어 있습니다. 이 문서에서는 앞서 언급한 모든 플랫폼에서 디바이스 또는 소프트웨어가 충돌한 레벨 및 충돌이 실제로 발생한 것인지 여부를 확인하기 위해 시작하는 접근 방식에 대해 설명합니다. 또한 충돌의 근본 원인을 찾기 위해 수집할 모든 아티팩트와 아티팩트를 찾을 위치 및 아티팩트를 사용하는 방법도 나열합니다.

## 모든 플랫폼과 논리적 디바이스에 걸쳐 공통적으로 확인할 사항

디바이스(논리적 또는 새시)가 리부팅되었거나 충돌했는지 확인합니다.


ASA의 경우 컨피그레이션 모드에서 명령을 사용하여 디바이스 업타임을 확인합니다. # show version | in Up

firepower 하드웨어에서 다음 명령을 사용하여 디바이스 가동 시간 및 새시 가동 시간(FXOS 레벨)을 확인합니다.

```
FP4100-3# connect fxos
FP4100-3(fxos)# show system uptime
```

```
System start time:      Thu Oct 31 22:50:09 2019
System uptime:         391 days, 19 hours, 30 minutes, 45 seconds
Kernel uptime:        391 days, 19 hours, 34 minutes, 34 seconds
Active supervisor uptime: 391 days, 19 hours, 30 minutes, 45 seconds
```

---

 참고: 문제가 발생한 시점부터 디바이스가 가동되는 것을 관찰하면 디바이스가 재부팅되었음을 확인할 수 있습니다.

---

갑작스러운 장치 재부팅으로 이어질 수 있는 전원 관련 문제가 있는지 확인 및 확인합니다.

가동 시간이 네트워크 다운타임의 타임스탬프와 관련이 없는 경우(또는 장애 조치 또는 클러스터에서 나가는 유닛), 이는 장치 다시 로드로 인해 문제가 발생하지 않았음을 의미하며 진단은 다른 방향으로 함께 이동해야 합니다.

## ASA SoftwareLina(FTD의 경우) 충돌 시 Crashinfo 확인


시스템 충돌은 시스템이 복구할 수 없는 오류를 감지하고 스스로 다시 시작된 상황입니다. 방화벽이 충돌하면 특수 텍스트 형식 파일인 `crashinfo` 파일을 클릭합니다. 이 파일은 충돌의 근본 원인 분석을 확인하는 데 도움이 되는 진단 정보 및 로그를 제공합니다. ASA의 경우 `crashinfo` 파일이 일반 텍스트 저장 위치 `Flash:` 에는 소프트웨어 버전, 수집된 데이터 등 기타 정보의 긴 목록과 함께 메모리 레지스터 내용이 포함되어 있습니다.

다음을 입력합니다. `show crashinfo` 명령을 실행할 수 있습니다 모든 텍스트 편집기 또는 ASA 콘솔 자체에서 출력을 볼 수 있습니다.

```
show flash | in crash
```

이 결과를 Service Request의 Cisco TAC(Technical Assistance Center)와 공유하면 내부 톨을 통해 해당 결과를 디코딩할 수 있습니다. 이 출력은 프로세스 및 스레드에 대한 유용한 정보를 제공하여 개발자가 충돌을 검토하고 디바이스 내의 다른 이벤트와 상호 연결할 수 있도록 합니다.

---

 **참고:** 일반적으로 `show tech-support` ASA 또는 Lina의 출력(FTD), `show crashinfo` 해당 출력에 이상적인 것입니다. 그러나 직접 를 실행하는 것과 비교하여 출력이 다르거나 불완전한 경우가 많습니다. `show crashinfo` 명령을 실행합니다. 따라서 항상 을 입력하는 것이 좋습니다. `show crashinfo` 명령을 실행할 수 있습니다

---

확인할 일반적인 세부사항 외에도 발생할 수 있는 다양한 수준의 충돌에 따라 수집할 추가 정보 및 아티팩트가 있습니다. ASA 플랫폼에서는 단일 수준의 충돌만 발생할 수 있습니다. 그러나 Firepower 플랫폼에는 논리적 디바이스(FTD 또는 ASA 소프트웨어) 레벨 충돌 또는 새시 레벨(FXOS) 충돌이 있을 수 있습니다.

가동 시간이 지나면 디바이스가 충돌한 것으로 확인되고 `coredump` 파일은 시스코 TAC의 추가 검토에 필요한 파일로 생성됩니다. 이 `coredump` 파일의 유형은 소프트웨어의 어떤 구성 요소가 충돌했는가에 따라 다를 수 있습니다. 이 `coredump` 또한 파일이 충돌한 구성 요소에 따라 디스크의 다른 디렉토리/부분에 저장됩니다.

## ASA 플랫폼에서 확인할 사항

ASA 플랫폼에는 ASA 또는 FTD가 될 수 있는 구성 요소가 하나만 있습니다.

ASA 이미지를 실행하는 모든 ASA 플랫폼

이 corefiles 충돌과 관련된 정보는 내부 플래시 드라이브의 disk0에 저장됩니다. 을(를) 확인하려면 corefiles, 을 입력합니다. dir disk0:/coredumpfsys 명령을 사용합니다:

```
<#root>
```

```
ciscoasa#
```

```
dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/
```

```
1071057 drwx 4096 23:14:58 Aug 30 2021 sysdebug
12 -rw- 87580218 04:49:23 Jun 04 2021
```

```
core_lina.1227726922.258.11.gz
```

```
11 drwx 16384 23:13:37 Aug 30 2021 lost+found
```

```
1 file(s) total size: 87580218 bytes
16106127360 bytes total (15749222400 bytes free/97% free)
```

다음을 입력합니다. show coredump filesystem 명령을 실행하여 coredump 파일 시스템 - 디스크 공간도 표시합니다. Firepower Threat Defense의 coredump 파일이 필요할 때 파일을 다운로드합니다. coredump 이전 항목을 제거할 수 있음 coredump(s) 현재 코어에 맞춥니다.

```
<#root>
```

```
ciscoasa# show coredump filesystem
```

```
Coredump Filesystem Size is 100 MB
```

```
Filesystem type is FAT for disk0
```

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/loop0	102182	75240	26942	74%	/mnt/disk0/coredumpfsys

```
Directory of disk0:/coredumpfsys/
```

```
246 -rwx 20205386 19:16:44 Nov 26 2021
```

```
core_lina.1227726922.258.11.gz
```

```
247 -rwx 36707919 19:21:56 Nov 26 2021
```

```
core_lina.1227727222.258.6.gz
```

```
248 -rwx 20130838 19:26:36 Nov 26 2021
```

```
core_lina.1227727518.258.11.gz
```

이 표시되지 않으면 coredump disk0에 있는 파일은 coredump 이(가) 활성화되지 않았으므로 이 항목에

대한 검토를 완료할 수 없습니다. 을(를) 활성화하려면 coredump 향후 발생 시 다음 명령을 입력합니다

```
ciscoasa(config)#coredump enable
```

WARNING: Enabling coredump on an ASA5505 platform will delay the reload of the system in the event of software forced reload. The exact time depends on the size of the coredump generated.

```
Proceed with coredump filesystem allocation of 60 MB
on 'disk0:' (Note this may take a while) ? [confirm]
```

```
Making coredump file system image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Coredump file system image created & mounted successfully
```

```
/dev/loop0 on /mnt/disk0/coredumpfsys type vfat
(rw, fmask=0022, dmask=0022, codepage=cp437, iocharset=iso8859-1)
```

## 실행 중인 FTD 이미지를 지원하는 ASA 플랫폼

ASA 플랫폼 5506-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X 및 ASA 5555-X는 FTD 이미지 실행과 차세대 방화벽을 지원합니다.

FTD 이미지를 실행하는 지원되는 모든 ASA 플랫폼에서 corefiles 이(가) 아래에 있습니다.

/var/data/cores 또는 /ngfw/var/data/cores Expert 모드를 사용합니다. 또한 Firepower Threat Defense disk0:/coredumpfsys lina flash의 디렉토리.

```
<#root>
```

```
root@firepower:/var/data/cores#
```

```
ls -l
```

```
total 59660
```

```
-rw-r--r-- 1 root root 4815651 Mar 14 17:07
```

```
core.SFDataCorrelato.2035.1552608478.gz
```

```
-rw-r--r-- 1 root root 56198339 Mar 14 16:47
```

```
core.lina.2113.1552607243.gz
```

```
root@firepower:/var/data/cores#
```

```
firepower# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
2498562 -rw- 56198339 23:47:26 Mar 14 2019
```

```
core.lina.2113.1552607243.gz
```

2498563 -rw- 4815651 00:07:58 Mar 15 2019

core.SFDataCorrelato.2035.1552608478.gz

2 file(s) total size: 61013990 bytes  
42949672960 bytes total (39523602432 bytes free/92% free)

## firepower 플랫폼에서 확인할 사항

firepower 플랫폼에는 두 가지 소프트웨어 구성 요소가 있습니다. 첫 번째는 새시 운영 체제인 FXOS이고, 두 번째는 ASA 또는 FTD가 될 수 있는 논리적 디바이스라고도 하는 앱 인스턴스입니다. 따라서 이를 다운로드할 위치를 확인하려면 어떤 부분이 충돌했는지 파악하는 것이 중요합니다.

corefiles

앱 인스턴스가 Firepower 1000/2000/4100 및 9300에서 충돌하면 충돌 정보 및 corefiles 항상 기본적으로 생성됩니다. 그러나 경우에 따라 코어 덤프를 비활성화할 수 있습니다.

4100/9300에서 코어 덤프가 활성화되었는지 확인하려면 다음 명령을 입력합니다.

```
connect module 1 console  
Firepower-module1>show platform coredumps
```

firepower 모듈 코어 덤프 사용 또는 사용 안 함:

시스템 충돌 시 문제 해결을 지원하거나 요청 시 Cisco TAC에 보내려면 Firepower 모듈에서 코어 덤프를 활성화합니다.

```
Firepower# connect module 1 console  
show coredump detail
```

명령 출력에는 현재 코어 덤프 상태 정보가 표시되며, 코어 덤프 압축의 활성화 여부가 포함됩니다.

<#root>

```
Firepower-module1>
```

```
show coredump detail
```

```
Configured status: ENABLED.  
ASA Coredump: ENABLED.  
Bootup status: ENABLED.  
Compress during crash: DISABLED.
```

이 `config coredump` 명령을 실행하여 코어 덤프를 활성화 또는 비활성화하고 충돌 중에 코어 덤프 압축을 활성화 또는 비활성화합니다.

- 다음을 입력합니다. `config coredump enable` 명령을 사용하여 크래시 중에 코어 덤프를 생성할 수 있습니다.
- 다음을 입력합니다. `config coredump disable` 명령을 사용하여 크래시 중에 코어 덤프 생성을 비활성화합니다.
- 다음을 입력합니다. `config coredump compress enable` 명령을 사용하여 코어 덤프의 압축을 활성화합니다.
- 다음을 입력합니다. `config coredump compress disable` 명령을 사용하여 코어 덤프 압축을 비활성화합니다.

다음 예에서는 코어 덤프를 활성화하는 방법을 보여 줍니다.

```
<#root>
```

```
Firepower-module1>
```

```
config coredump enable
```

```
Coredump enabled successfully.
```

```
ASA coredump enabled, do 'config coredump disableAsa' to disable
```


```
Firepower-module1>config coredump compress enable
```

```
WARNING: Enabling compression delays system reboot for several minutes after a system failure. Are you
```

```
y
```

```
Firepower-module1>
```

---

 참고: 코어 덤프 파일은 디스크 공간을 소비하며 공간이 부족하고 압축이 활성화되지 않으면 코어 덤프가 활성화된 경우에도 코어 덤프 파일이 저장되지 않습니다.

---

충돌 파일에 모든 데이터가 포함되어 있지 않을 수 있으므로 완전한 분석을 위해 충돌 파일과 코어 파일을 모두 업로드해야 합니다.

## FP9300/FP4100 FXOS

FP9300/FP4100에서 FXOS `corefiles` Firepower Threat Defense `local-mgmt cores` 디렉터리에 저장할 수 있습니다.

```
firepower-4110# connect local-mgmt
firepower-4110(local-mgmt)# dir cores
```

```
1 9337521 Apr 30 11:28:15 2016 1462040896_0x101_snm_log.5289.tar.gz
1 1067736 Oct 09 10:38:49 2017 1507570679_firepower-4110_BC01_MEZZ0101_mcp_log.122.tar.gz
1 798663 Oct 10 18:05:54 2017 1507683913_firepower-4110_BC01_MEZZ0101_mcp_log.122.tar.gz
1 348160 Feb 11 23:53:25 2019 core.21845
```

```
Usage for workspace://
3999125504 bytes total
```

```
64200704 bytes used
3730071552 bytes free
firepower-4110(local-mgmt)#
```

FXOS에서 로컬 컴퓨터로 코어 파일을 복사하려면 다음 명령을 입력합니다.

```
firepower-4110(local-mgmt)# copy workspace:/cores:/<file>.tar.gz scp://username@x.x.x.x
```

## FTD를 실행하는 FP9300/FP4100에서

FTD를 실행하는 FP9300/FP4100에서 `corefiles` 이(가) 아래에 있습니다. `/var/data/cores` 또는 `/ngfw/var/data/cores` Expert 모드를 사용합니다. 또한 Firepower Threat Defense `disk0:/coredumpfsys` `lina` flash의 디렉토리.

```
root@firepower:/var/data/cores# ls -l
total 59660
-rw-r--r-- 1 root root 4815651 Mar 14 17:07 core.SFDataCorrelato.2035.1552608478.gz
-rw-r--r-- 1 root root 56198339 Mar 14 16:47 core.lina.2113.1552607243.gz
root@firepower:/var/data/cores#
```

```
firepower# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
2498562 -rw- 56198339 23:47:26 Mar 14 2019 core.lina.2113.1552607243.gz
2498563 -rw- 4815651 00:07:58 Mar 15 2019 core.SFDataCorrelato.2035.1552608478.gz
```

```
2 file(s) total size: 61013990 bytes
42949672960 bytes total (39523602432 bytes free/92% free)
```

## ASA를 실행하는 FP9300/FP4100에서

ASA를 실행하는 FP9300/FP4100에서 `corefiles` Firepower Threat Defense `disk0:/coredumpfsys` 디렉토리에 저장할 수 있습니다.

```
<#root>
```

```
asa#
```

```
dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/
```

```
11 drwx 16384 17:34:50 Sep 10 2018 lost+found
12 -rw- 317600388 16:43:40 Mar 14 2019
```




core.lina.6320.1552607012.gz

1 file(s) total size: 317600388 bytes  
21476089856 bytes total (21255872512 bytes free/98% free)

## FP2100 FXOS/ASA/FTD에서

FP2100 FXOS/ASA/FTD에서 `corefiles` Firepower Threat Defense `local-mgmt cores` ASA 또는 FTD를 사용할지 여부를 지정합니다. FTD에서는 `/ngfw/var/data/cores` (또는 `/var/data/cores`) 및 `/ngfw/var/common/` Expert 모드를 사용합니다. 그러나 FP2100 플랫폼에는 `disk0`이 없습니다. `./coredumpfsys` 디렉터리에 저장할 수 있습니다.

---

 참고: [FP2100](#) | [FP9300](#)/4100 플랫폼과 일치하도록 하기 위해 Cisco 버그 ID CSCvh01912가 제출되었습니다. 이 문제가 해결될 때까지 설명된 위치를 사용하여 `corefiles`.

---

FTD가 Firepower 2100, 1000, ASA Appliance 및 ISA 3000 Appliance에 있는 경우 Firepower 코어 파일의 위치:

이러한 모든 플랫폼에 대해 이 절차를 사용하여 모든 Firepower 프로세스와 관련된 핵심 파일을 찾습니다.

아래 `/ngfw/var/common/`:

1. SSH 또는 콘솔을 통해 어플라이언스의 CLI에 연결합니다.
2. 전문가 모드로 입력합니다.

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

3. 루트 사용자가 됩니다.

```
<#root>
```

```
admin@firepower:~$
```

```
sudo su
```

```
Password:
```

```
root@firepower:/home/admin#
```

4. 다음으로 이동합니다. `/ngfw/var/common/` 핵심 파일이 있는 폴더입니다.

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

## 5. 폴더의 파일을 확인합니다.

```
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
```

FP2100의 FTD: 미만 /ngfw/var/data/cores:

```
> expert
admin@firepower:~$ sudo su
[cut]
root@firepower:/home/admin# ls -l /ngfw/var/data/cores
total 133740
-rw-r--r-- 1 root root 4761622 Jun  4 05:13 core.SFDataCorrelato.28634.1622783636.gz
-rw-r--r-- 1 root root 132014190 Jun  4 05:17 core.lina.11.1378.1622783800.gz
drwx----- 2 root root 16384 Nov  5 2019 lost+found
drwxr-xr-x 3 root root 4096 Nov  5 2019 sysdebug
```

```
> connect fxos
[cut]
firepower# connect local-mgmt
firepower(local-mgmt)# dir cores


1 4761622 Jun 04 05:13:56 2021 core.SFDataCorrelato.28634.1622783636.gz
1 132014190 Jun 04 05:17:25 2021 core.lina.11.1378.1622783800.gz
2 16384 Nov 05 22:35:15 2019 lost+found/
3 4096 Nov 05 22:36:05 2019 sysdebug/
```

```
Usage for workspace://
85963259904 bytes total
15324155904 bytes used
70639104000 bytes free
firepower(local-mgmt)#
```

FP2100의 ASA:

```
firepower-2110(local-mgmt)# dir cores

1 167408075 Jul  4 00:43:25 2018 core.lina.6.2025.1530657764.gz
2      16384 Mar 28 16:17:56 2018 lost+found/
3      4096 Mar 28 16:18:43 2018 sysdebug/
```

 참고: FXOS corefiles 연결에서 동일한 코어 디렉토리에 저장됩니다. local-mgmt.

## FP1000 FXOS/ASA/FTD에서

FP1000 FXOS/ASA/FTD에서 이 프로세스는 FP2100과 유사합니다. 또한 disk0:/coredumpfsys Lina측 아래 디렉토리가 있습니다.

FP1000의 FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
FP1010> ena
```

```
Password:
```

```
FP1010# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
13 -rw- 86493184 19:59:39 Jun 03 2021 core.lina.18707.1622750370.gz
1071057 drwx 4096 23:14:58 Aug 30 2019 sysdebug
14 -rw- 4770749 20:19:24 Jun 03 2021 core.SFDataCorrelato.7098.1622751564.gz
12 -rw- 197689 23:01:08 May 19 2021 core.top.6163.1621465268.gz
16 -rw- 4752067 20:28:03 Jun 03 2021 core.SFDataCorrelato.28195.1622752083.gz
11 drwx 16384 23:13:37 Aug 30 2019 lost+found
15 -rw- 5048839 20:20:32 Jun 03 2021 core.SFDataCorrelato.18952.1622751632.gz
```

```
5 file(s) total size: 101262528 bytes
123418959872 bytes total (110302621696 bytes free/89% free)
```

```
> connect fxos
[cut]
```

```
FP1010# connect local-mgmt
FP1010(local-mgmt)# dir cores
```

```
1 5048839 Jun 03 20:20:32 2021 core.SFDataCorrelato.18952.1622751632.gz
1 4752067 Jun 03 20:28:03 2021 core.SFDataCorrelato.28195.1622752083.gz
1 4770749 Jun 03 20:19:24 2021 core.SFDataCorrelato.7098.1622751564.gz
1 86493184 Jun 03 19:59:39 2021 core.lina.18707.1622750370.gz
1 197689 May 19 23:01:08 2021 core.top.6163.1621465268.gz
2 16384 Aug 30 23:13:37 2019 lost+found/
3 4096 Aug 30 23:14:58 2019 sysdebug/
```

```
Usage for workspace://
159926181888 bytes total
17475063808 bytes used
142451118080 bytes free
```

```
> expert
admin@FP1010:~$ sudo su
Password:
root@FP1010:/home/admin# ls -l /var/data/cores
total 99048
-rw-r--r-- 1 root root 5048839 Jun 3 20:20 core.SFDataCorrelato.18952.1622751632.gz
-rw-r--r-- 1 root root 4752067 Jun 3 20:28 core.SFDataCorrelato.28195.1622752083.gz
```

```
-rw-r--r-- 1 root root 4770749 Jun 3 20:19 core.SFDataCorrelato.7098.1622751564.gz
-rw-r--r-- 1 root root 86493184 Jun 3 19:59 core.lina.18707.1622750370.gz
-rw-r--r-- 1 root root 197689 May 19 23:01 core.top.6163.1621465268.gz
drwx----- 2 root root 16384 Aug 30 2019 lost+found
drwxr-xr-x 3 root root 4096 Aug 30 2019 sysdebug
```

FP1000의 ASA:

```
<#root>
```

```
ciscoasa# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
1071057 drwx 4096 23:14:58 Aug 30 2019 sysdebug
12 -rw- 87580218 04:49:23 Jun 04 2021
```

```
core.lina.27515.1622782155.gz
```

```
11 drwx 16384 23:13:37 Aug 30 2019 lost+found
```

```
1 file(s) total size: 87580218 bytes
16106127360 bytes total (15749222400 bytes free/97% free)
```

```
ciscoasa#
```

```
connect fxos
```

```
[cut]
```

```
FP1010#
```

```
connect local-mgmt
```

```
FP1010(local-mgmt)#
```

```
dir cores
```

```
1 87580218 Jun 04 04:49:23 2021
```

```
core.lina.27515.1622782155.gz
```

```
2 16384 Aug 30 23:13:37 2019 lost+found/
```

```
3 4096 Aug 30 23:14:58 2019 sysdebug/
```

```
Usage for workspace://
159926181888 bytes total
5209071616 bytes used
154717110272 bytes free
```



참고: FXOS corefiles 동일한 코어 디렉토리에 저장된 후 local-mgmt.

---

## 코어 파일 다운로드

Cisco의 copy 아래에 명령 connect local-mgmt 및 Lina/ASA CLI입니다. FTD 전문가 모드의 경우 scp 명령을 실행합니다.

## 기타 확인 사항(Firepower 4100 및 9300 플랫폼 관련)

의 출력을 확인합니다. show pmon state 아래에 명령 local-mgmt FXOS에서 이 예에서는 어떤 프로세스도 crash하지 않을 때 원하는 출력을 보여 줍니다. 이 출력에서는 디바이스 레벨 크래시뿐만 아니라 인터페이스 모듈/DME 크래시 등도 캡처합니다.

```
<#root>
```

```
fp1120-v-1(local-mgmt)#
```

```
show pmon state
```

SERVICE NAME	STATE	RETRY(MAX)	EXITCODE	SIGNAL	CORE
svc_sam_dme	running	0(4)	0	0	no
svc_sam_dcosAG	running	0(4)	0	0	no
svc_sam_portAG	running	0(4)	0	0	no
svc_sam_statsAG	running	0(4)	0	0	no
httpd.sh	running	0(4)	0	0	no
svc_sam_sessionmgrAG	running	0(4)	0	0	no
sam_core_mon	running	0(4)	0	0	no
svc_sam_svcmonAG	running	0(4)	0	0	no
svc_sam_serviceOrchAG	running	0(4)	0	0	no
svc_sam_appAG	running	0(4)	0	0	no
svc_sam_envAG	running	0(4)	0	0	no

관련 FTD/ASA 디렉토리에서 코어 파일을 찾지 못할 경우 코어 파일은 4100/9300의 bootCLI에 있을 수 있습니다.

## 모듈 내의 코어 파일 보기

모듈 콘솔에 연결하려면 다음 명령을 입력합니다.

```
<#root>
```

```
/ssa # connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

support filelist

```
=====
Directory: /
Downloads_Directory
CSP_Downloaded_Files
Archive_Files
Crashinfo_and_Core_Files
Boot_Files
ApplicationLogs
Transient_Core_Files
Type a sub-dir name to list its contents, or [x]

to Exit: Transient_Core_Files
```

```
-----files-----
[No files]
([b] to go back)
Type a sub-dir name to list its contents: b
```

```
=====
Directory: /
Downloads_Directory
CSP_Downloaded_Files
Archive_Files
Crashinfo_and_Core_Files
Boot_Files
ApplicationLogs
Transient_Core_Files
Type a sub-dir name to list its contents, or [x] to Exit:

Crashinfo_and_Core_Files
```

```
-----sub-dirs-----
lost+found
-----files-----
2017-03-20 20:45:06 | 40639151 | core.lina.48857.1490042695.gz
2017-03-20 20:48:47 | 40638054 | core.lina.18113.1490042915.gz
2017-03-20 20:52:28 | 40638186 | core.lina.18112.1490043137.gz
2017-03-20 20:56:10 | 40638466 | core.lina.18123.1490043359.gz
2017-03-20 20:59:53 | 40638345 | core.lina.18262.1490043582.gz
2017-03-20 21:03:35 | 40638120 | core.lina.18476.1490043803.gz
2017-03-20 21:07:22 | 40638335 | core.lina.18529.1490044031.gz ([b] to go back)
Type a sub-dir name to list its contents: b =====
Directory: /
Downloads_Directory
CSP_Downloaded_Files
Archive_Files
Crashinfo_and_Core_Files
Boot_Files
ApplicationLogs
Transient_Core_Files Type a sub-dir name to list its contents, or [x] to Exit: x
Firepower-module1>
```

bootCLI에 코어 파일이 없는 경우 FXOS 레벨에서 로그를 확인할 수 있습니다.

```
connect fxos
1(fxos)# show logging onboard obfl-logs
```

```
2-(fxos)# show logging onboard stack-trace
3-(fxos)# show logging onboard kernel-trace
4-(fxos)# show logging onboard exception-log
5-(fxos)# show logging onboard internal kernel
6-(fxos)# show logging onboard internal platform
7-(fxos)#show logging onboard internal kernel | no-more
8-(fxos)#show logging onboard internal kernel-big | no-more
9-(fxos)#show logging onboard internal platform | no-more
10-(fxos)#show logging onboard internal reset-reason | no-more
```

If logging at fxos level is enabled, you can check the logs on fxos. It contains the syslog buffer and OBFL logs stored in NVRAM

Connect fxos

```
show logging log -----This is a non-persistent syslog buffer
show logging onboard oblf-logs -----Non-volatile storage for history of boot up and reset occurrences.
show logging nvram -----Non-volatile storage for critical logs.Important for historical is
```

On FXOS CLI, at the top-level scope use following command.

```
show fault detail or show fault
```

If you want to view faults for a specific object, scope to that object and then enter the show fault command.

You can check for audit-logs which is a persistent store of user operations.

This moreover stores the sequence of user operations done.

```
firepower# scope security
firepower# /security # show audit-logs
```

때때로 디바이스는 자동으로 충돌하며 충돌 또는 코어 파일을 생성하지 않습니다. 이 경우 로그를 확인할 수 있습니다.

At FTD instance or device level:

```
#####
```

# Navigate to the /ngfw/var/log or /var/log and open the messages log file. Check all the logs generated. You can search for following messages (in /ngfw/var/log or /var/log) to confirm if device rebooted with

```
firepower shutdown[2313]: shutting down for system reboot
Stopping Cisco Firepower 2130 Threat Defense
pm:process [INFO] Begin Process Shutdown
```

# Check for syslogs messages (specific to device up and down )generated when the device rebooted. You can check for syslogs messages generated 15-30 min before and after the device reboot to know if

## 시스템 충돌과 관련된 알려진 버그

시스템 충돌에 대한 자세한 내용은 다음 페이지를 참조하십시오.

- Cisco 버그 ID [CSCvu84127](#) - 코어 또는 충돌 파일을 생성하지 않는 FTD 무음 충돌

- Cisco 버그 ID [CSCwa35845](#) - ASA 5516이 다시 로드되어 코어 파일 생성
- Cisco 버그 ID [CSCvw99444](#) - FTD가 crashinfo/corefile
- Cisco 버그 ID [CSCv86926](#) - FTD crash generating crashfile
- Cisco 버그 ID [CSCvp16482](#) - ASA가 crash하여 코어 파일 생성
- Cisco 버그 ID [CSCvm53545](#) - ASA는 crashinfo 파일



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.