

Fehlerbehebung bei unerwarteten ASA- oder FTD-Neuladevorgängen

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Häufige Prüfungen für alle Plattformen und logischen Geräte](#)
- [Überprüfen des Neustarts oder Absturzes des Geräts \(logisch oder Chassis\)](#)
- [Suchen Sie nach Crashinfo im Fall eines Absturzes der ASA SoftwareLina \(auf FTD\).](#)
- [Wichtige Informationen auf ASA-Plattformen](#)
- [Alle ASA-Plattformen, auf denen ein ASA-Image ausgeführt wird](#)
- [ASA-Plattformen, die die Ausführung eines FTD-Images unterstützen](#)
- [Wichtige Informationen auf FirePOWER Plattformen](#)
- [FP9300/FP4100 FXOS](#)
- [Bei FP9300/FP4100 mit FTD](#)
- [bei FP9300/FP4100 mit ASA](#)
- [FP2100 FXOS/ASA/FTD](#)
- [Bei FP1000 FXOS/ASA/FTD](#)
- [Corefiles herunterladen](#)
- [Weitere Punkte \(spezifisch für FirePOWER 4100- und 9300-Plattformen\)](#)
- [Corefiles im Modul anzeigen](#)
- [Bekannte Fehler im Zusammenhang mit dem Systemabsturz](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung in Szenarien beschrieben, in denen ein FTD- (Firepower Threat Defense) oder ASA-Gerät (Adaptive Security Appliance) ohne offensichtlichen Grund neu geladen wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende Informationen zu FirePOWER- und ASA-Hardwareplattformen
- Logische Geräte auf FirePOWER-Plattformen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA 5500-X mit ASA Software Version 9.x
- ASA 5500-X mit FTD Softwareversion 6.2.3 und höher
- Firepower der Serien 1000, 1100, 2100, 4100 und 9300 mit ASA Software Version 9.x

- Firepower der Serien 1000, 1100, 2100, 4100 und 9300 mit FTD Softwareversion 6.2.3 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument bezieht sich das Gerät auf die ASA oder die Firepower Next-Generation Firewalls (NGFW), die unter der Marke Cisco Secure Firewalls firmieren und auf denen entweder ein ASA- oder FTD-Image als logisches Gerät ausgeführt wird.

Cisco Secure Firewalls umfassen verschiedene Hardware- und Softwareversionen. Die ASA-Produktreihe umfasst Firewalls der Serie 5500-X, die Firepower-Produktreihe umfasst Geräte der Serien FPR 1000, 2100, 4100 und 9300. In diesem Dokument wird der Ansatz erläutert, mit dem Sie den Absturz des Geräts oder der Software auf allen genannten Plattformen identifizieren und feststellen können, ob der Absturz tatsächlich eingetreten ist. Außerdem werden alle zu sammelnden Artefakte aufgelistet, wo sie zu finden sind und wie sie verwendet werden können, um die Ursache des Absturzes zu finden.

Häufige Prüfungen für alle Plattformen und logischen Geräte

Überprüfen des Neustarts oder Absturzes des Geräts (logisch oder Chassis)

Verwenden Sie für ASA den Befehl aus dem Konfigurationsmodus, um die Geräteverfügbarkeit zu überprüfen: `# show version | in Up`

Verwenden Sie auf der Firepower-Hardware die folgenden Befehle, um die Betriebszeit des Geräts und des Gehäuses (FXOS-Ebene) zu überprüfen:

```
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
```

Hinweis: Wenn Sie feststellen, dass das Gerät gerade zum Zeitpunkt der Ausgabe betriebsbereit ist, wird bestätigt, dass das Gerät neu gestartet wurde.

Prüfen und bestätigen Sie, ob es Probleme mit der Stromversorgung gibt, die zu einem plötzlichen Neustart des Geräts führen können.

Wenn sich die Betriebszeit nicht auf den Zeitstempel der Ausfallzeit im Netzwerk (oder Failover oder Einheit verlässt Cluster) bezieht, bedeutet dies, dass das Problem nicht aufgrund des erneuten Ladens des Geräts aufgetreten ist und die Diagnose vollständig in eine andere Richtung navigieren muss.

Suchen Sie nach Crashinfo im Fall eines Absturzes der ASA SoftwareLina (auf FTD).

Ein **Systemabsturz** ist eine Situation, in der das System einen nicht behebbaren Fehler erkannt und sich selbst neu gestartet hat. Wenn eine Firewall abstürzt, wird eine spezielle Textformatdatei erstellt, die als `crashinfo` Datei. Diese Datei enthält Diagnoseinformationen und Protokolle, mit denen die Ursachenanalyse eines Absturzes ermittelt werden kann. Für eine ASA-Lösung `crashinfo` Datei wird als reiner Text gespeichert `Flash:` und enthält die Speicherregisterinhalte mit einer langen Liste weiterer Informationen - Softwareversion, gesammelte Daten usw.

Geben Sie `show crashinfo` in der ASA-CLI im privilegierten `exec`-Modus. Sie können die Ausgabe in jedem Texteditor oder sogar auf der ASA-Konsole selbst betrachten.

```
show flash | in crash
```

Teilen Sie diese Ausgabe mit dem Cisco Technical Assistance Center (TAC) in einer Serviceanfrage, und das Team kann sie mit internen Tools entschlüsseln. Diese Ausgabe enthält nützliche Informationen zu den Prozessen und Threads, die Entwicklern helfen, den Absturz zu überprüfen und mit anderen Ereignissen innerhalb des Geräts zu korrelieren.

Hinweis: Im Allgemeinen gilt Folgendes: `show tech-support` Ausgabe von ASA oder Lina (auf FTD), `show crashinfo` optimal in dieser Ausgabe vorhanden ist. Allerdings ist die Ausgabe oft anders oder unvollständig als beim direkten Ausführen des `show crashinfo` aus. Es wird daher empfohlen, immer die `show crashinfo` direkt auf der ASA oder der Lina CLI.

Zusätzlich zu den allgemeinen Details zu überprüfen, gibt es mehr Informationen und Artefakte zu sammeln, die von den verschiedenen Ebenen von Abstürzen, die auftreten können, abhängen. Auf ASA-Plattformen kann es nur eine Absturzstufe geben. Firepower-Plattformen können jedoch entweder einen Absturz auf Ebene logischer Geräte (FTD oder ASA-Software) oder einen Absturz auf Gehäuseebene (FXOS) haben.

Wenn die Betriebszeit bestätigt, dass das Gerät abgestürzt ist, wird ein `coredump` generiert, was zur weiteren Überprüfung durch das Cisco TAC erforderlich ist. Die Fehlermeldung `coredump` -Datei kann von verschiedenen Typen sein, je nachdem, welche Komponente der Software abgestürzt ist. Die Fehlermeldung `coredump` Dateien werden auch in verschiedenen Verzeichnissen/Teilen der Festplatte gespeichert, je nachdem, welche Komponente abgestürzt ist.

Wichtige Informationen auf ASA-Plattformen

Die ASA-Plattformen haben nur eine Komponente, die entweder ASA oder FTD sein kann.

Alle ASA-Plattformen, auf denen ein ASA-Image ausgeführt wird

Die Fehlermeldung `corefiles` im Zusammenhang mit dem Absturz unter `disk0` des internen Flash-Laufwerks gespeichert. Zur Überprüfung der `corefiles`, geben Sie `dir disk0:/coredumpfsys` command:

```
<#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)
```

Geben Sie `show coredump filesystem` , um alle Dateien auf dem `coredump` -Dateisystem, das auch den Speicherplatz anzeigt. Es wird empfohlen, die `coredump` Dateien zu speichern, da es möglich ist, dass eine nachfolgende `coredump` kann die vorherige `coredump(s)` um in den aktuellen Kern zu passen.

```
<#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
```

Wenn Sie keine `coredump` Datei in `disk0`, besteht eine hohe Wahrscheinlichkeit, dass die `coredump` ist nicht aktiviert, was bedeutet, dass die Überprüfung für diesen Vorfall nicht abgeschlossen werden kann. Um zu aktivieren, `coredump` für zukünftige Vorfälle geben Sie den folgenden Befehl ein:

```
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)

ASA-Plattformen, die die Ausführung eines FTD-Images unterstützen

Die ASA-Plattformen 5506-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X und ASA 5555-X unterstützen die Ausführung eines FTD-Images und machen einer Firewall der nächsten Generation.

Auf all diesen unterstützten ASA-Plattformen, auf denen das FTD-Image ausgeführt wird, corefiles befinden sich unter /var/data/cores Oder /ngfw/var/data/cores über Expertenmodus. Sie werden auch unter dem disk0:/coredumpfsys Verzeichnis von Lina flash.

<#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)

Wichtige Informationen auf FirePOWER Plattformen

Die Firepower-Plattformen sind mit zwei Softwarekomponenten ausgestattet. Das erste ist das FXOS, das als Chassis-Betriebssystem fungiert, und das zweite ist die App-Instanz, die auch als logisches Gerät bezeichnet wird und entweder ASA oder FTD sein kann. Daher ist es wichtig zu identifizieren, welcher Teil abgestürzt ist, um zu bestimmen, an welchem Ort das `corefiles`

Wenn die App-Instanz bei Firepower 1000/2000/4100 und 9300 abstürzt, werden die Absturzinformationen und `corefiles` werden standardmäßig immer generiert. In einigen Fällen kann das Core Dump jedoch deaktiviert werden.

Geben Sie die folgenden Befehle ein, um zu überprüfen, ob das Core Dump auf 4100/9300 aktiviert ist:

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

Aktivieren oder Deaktivieren von FirePOWER-Modul-Core-Dumps:

Aktivieren Sie Core Dumps auf einem FirePOWER-Modul, um bei einem Systemabsturz Hilfestellung zu leisten oder auf Anforderung an das Cisco TAC zu senden.

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

Die Befehlsausgabe zeigt die aktuellen Core Dump-Statusinformationen an und enthält, ob die Core Dump-Komprimierung aktiviert ist.

```
<#root>
```

```
Firepower-module1>
```

```
show coredump detail
```

```
Configured status: ENABLED.
```

```
ASA Coredump: ENABLED.
```

```
Bootup status: ENABLED.
```

```
Compress during crash: DISABLED.
```

Verwenden Sie `config coredump` , um Core Dumps zu aktivieren oder zu deaktivieren und um die Core Dump-Komprimierung während eines Absturzes zu aktivieren oder zu deaktivieren.

- Geben Sie `config coredump enable` , um die Erstellung eines Core Dump während eines Absturzes zu ermöglichen.
- Geben Sie `config coredump disable` , um die Erstellung des Core Dump während eines Absturzes zu deaktivieren.
- Geben Sie `config coredump compress enable`-Befehl, um die Komprimierung von Core Dumps zu aktivieren.

- Geben Sie `config coredump compress disable`-Befehl, um die Core Dump-Komprimierung zu deaktivieren.

In diesem Beispiel wird veranschaulicht, wie der Core Dump aktiviert wird:

```
<#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 s
y
Firepower-module1>
```

Hinweis: Core Dump-Dateien verbrauchen Speicherplatz, und wenn der Speicherplatz knapp wird und die Komprimierung nicht aktiviert ist, wird eine Core Dump-Datei nicht gespeichert, selbst wenn Core Dumps aktiviert sind.

Sowohl Crash- als auch Core-Dateien müssen für eine vollständige Analyse hochgeladen werden, da es möglich ist, dass die Crash-Datei nicht alle Daten enthält.

FP9300/FP4100 FXOS

Bei FP9300/FP4100 wird der FXOS `corefiles` befinden sich unter dem `local-mgmt cores` Verzeichnis.

```
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)#
```

Um die Kerndatei von FXOS auf Ihren lokalen Computer zu kopieren, geben Sie den folgenden Befehl ein:

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

Bei FP9300/FP4100 mit FTD

Bei FP9300/FP4100 mit FTD corefiles befinden sich unter /var/data/cores Oder /ngfw/var/data/cores über Expertenmodus. Sie werden auch unter dem disk0:/coredumpfsys Verzeichnis von Lina flash.

```
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)
```

bei FP9300/FP4100 mit ASA

Bei FP9300/FP4100 mit ASA, corefiles befinden sich unter dem disk0:/coredumpfsys verzeichnis.

```
<#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/FTD

Bei FP2100 FXOS/ASA/FTD corefiles befinden sich unter dem local-mgmt cores -Verzeichnis, ob Sie ASA oder FTD verwenden. Auf FTD werden sie auch gespiegelt unter /ngfw/var/data/cores (Oder /var/data/cores) und /ngfw/var/common/ über Expertenmodus. Beachten Sie jedoch, dass FP2100-Plattformen nicht über die disk0-Schnittstelle verfügen:/coredumpfsys verzeichnis.

Hinweis: Cisco Bug-ID [CSCvh01912](#) wurde übermittelt, um FP2100 mit der FP9300/4100-Plattform konsistent zu machen. Verwenden Sie den beschriebenen Speicherort, um das Problem zu beheben.
corefiles.

Speicherort der Firepower Core-Dateien, wenn sich das FTD in Firepower 2100, 1000, ASA Appliance und ISA 3000 Appliance befindet:

Verwenden Sie für alle diese Plattformen dieses Verfahren, um nach den Kerndateien zu suchen, die sich auf alle FirePOWER-Prozesse beziehen.

Unter `/ngfw/var/common/`:

1. Stellen Sie über SSH oder die Konsole eine Verbindung mit der CLI der Appliance her.

2. Geben Sie dies als Expertenmodus ein:

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

3. Werden Sie Stammbenutzer.

```
<#root>
```

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

```
sudo su
```

```
Password:
```

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

4. Navigieren Sie zum `/ngfw/var/common/` -Ordner, in dem sich die Core-Dateien befinden.

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

5. Überprüfen Sie den Ordner für die Datei.

```
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
```

FTD auf FP2100: Unter `/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)#
```

ASA auf FP2100:

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

```
1 167408075 Jul 04 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/
```

Hinweis: Die FXOS corefiles werden unter demselben Core-Verzeichnis von connect gespeichert local-mgmt.

Bei FP1000 FXOS/ASA/FTD

Bei FP1000 FXOS/ASA/FTD ähnelt dieser Prozess dem FP2100. Darüber hinaus `disk0:/coredumpfsys` unter der Lina-Seite zur Verfügung.

FTD auf FP1000:

```
> 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
```

ASA auf FP1000:

```
<#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
```

Hinweis: FXOS corefiles werden unter demselben Core-Verzeichnis gespeichert, das die Verbindung local-mgmt.

Corefiles herunterladen

Es gibt eine `copy` Kommando unter `connect local-mgmt` und Lina/ASA CLI. Für den FTD-Expertenmodus verwenden Sie `scp` aus.

Weitere Punkte (spezifisch für FirePOWER 4100- und 9300-Plattformen)

Prüfen Sie die Ausgabe des `show pmon state` Kommando unter local-mgmt auf FXOS. Dieses Beispiel zeigt die gewünschte Ausgabe, wenn keiner der Prozesse abstürzte. Diese Ausgabe erfasst nicht nur Abstürze auf Geräteebene, sondern auch Schnittstellenmodul-/DME-Abstürze usw.

```
<#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

Wenn Sie keine Core-Dateien in den zugehörigen FTD/ASA-Verzeichnissen finden, können die Core-Dateien in der bootCLI auf 4100/9300 vorhanden sein.

Corefiles im Modul anzeigen

Geben Sie den folgenden Befehl ein, um eine Verbindung zur Modulkonsole herzustellen:

```
<#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>
```

Wenn es keine Core-Dateien bei bootCLI gibt, können Sie auf FXOS-Ebene nach Protokollen suchen:

```
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 obfl-logs -----Non-volatile storage for history of boot up and reset occurrences.
show logging nvram -----Non-volatile storage for critical logs.Important for historical iss
```

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 com

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
```

Manchmal stürzt das Gerät im Hintergrund ab und erzeugt keine Absturz- oder Core-Dateien. In diesem Fall können Sie nach den Protokollen suchen:

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

Bekannte Fehler im Zusammenhang mit dem Systemabsturz

Weitere Informationen zum Systemabsturz finden Sie auf den folgenden Seiten:

- Cisco Bug-ID [CSCvu84127](#) - FTD-Absturz ohne Core- oder Absturzdatei
- Cisco Bug-ID [CSCwa35845](#) - ASA 5516 lädt neu generierende Core-Dateien
- Cisco Bug-ID [CSCvw9944](#) - FTD abgestürzt mit crashinfo/corefile
- Cisco Bug-ID [CSCvv86926](#) - FTD-Absturz generiert crashfile
- Cisco Bug-ID [CSCvp16482](#) - ASA ist beim Generieren einer Core-Datei abgestürzt
- Cisco Bug-ID [CSCvm53545](#) - ASA kann Traceback und Neuladen, ohne crashinfo Datei

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.