Risoluzione dei problemi di ricaricamenti imprevisti di ASA o FTD

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al ricaricamento di un dispositivo Firepower Threat Defense (FTD) o Adaptive Security Appliance (ASA) senza una ragione ovvia.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comprendere le basi delle piattaforme hardware Firepower e ASA
- Informazioni sulle periferiche logiche sulle piattaforme Firepower

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA 5500-X con software ASA versione 9.x
- ASA 5500-X con software FTD versione 6.2.3 e successive
- Firepower serie 1000, 1100, 2100, 4100 e 9300 con software ASA versione 9. x
- Firepower serie 1000, 1100, 2100, 4100 e 9300 con software FTD versione 6.2.3 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento, il dispositivo si riferisce ad ASA o Firepower Next-Generation Firewall (NGFW), rinominati Cisco Secure Firewall, che eseguono un'immagine ASA o FTD su di esso come dispositivo logico.

Cisco Secure Firewall include diverse versioni hardware e software. La famiglia ASA include i firewall serie 5500-X e la famiglia Firepower include i dispositivi serie 1000, 2100, 4100 e 9300. In questo documento viene descritto l'approccio con cui iniziare per identificare il livello di arresto anomalo del dispositivo o del software su tutte le piattaforme indicate e se l'arresto anomalo è stato reale o meno. Vengono inoltre elencati tutti gli elementi da raccogliere, dove trovarli e come utilizzarli per trovare la causa principale dell'arresto anomalo.

Elementi comuni da verificare su tutte le piattaforme e i dispositivi logici

Confermare il riavvio o l'arresto anomalo del dispositivo (logico o chassis)

Per l'appliance ASA, usare il comando dalla modalità di configurazione per verificare il tempo di attività del dispositivo: # show version | in Up

Sull'hardware Firepower, utilizzare questi comandi per controllare il tempo di attività del dispositivo e dello chassis (livello FXOS):

```
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
```

> **Nota**: se si osserva che il dispositivo è attivo appena dal momento del rilascio, ciò conferma che il dispositivo è stato riavviato.

Verificare e confermare se vi sono problemi relativi all'alimentazione che possono causare un riavvio improvviso del dispositivo.

Se il tempo di attività non è correlato al timestamp del tempo di inattività della rete (o del failover o dell'uscita dell'unità dal cluster), il problema non si è verificato a causa del ricaricamento del dispositivo e la diagnosi deve essere eseguita in una direzione completamente diversa.

Verifica la presenza di Crashinfo in caso di arresto anomalo del software ASA Lina (su FTD)

Un **arresto anomalo del sistema** è una situazione in cui il sistema ha rilevato un errore irreversibile e si è riavviato da solo. Quando un firewall si blocca, crea uno speciale file in formato testo noto come crashinfo file. Questo file fornisce informazioni di diagnostica e log che aiutano a determinare la root cause analysis di un arresto anomalo del sistema. Per un'ASA, crashinfo il file è testo normale archiviato in Flash: e contiene il contenuto del registro di memoria con un lungo elenco di altre informazioni, quali la versione del software, i dati raccolti e così via.

Immettere il show crashinfo nella CLI dell'appliance ASA in modalità di esecuzione privilegiata. L'output può essere visualizzato in un editor di testo qualsiasi o sulla console ASA stessa.

```
show flash | in crash
```

Condividi questo output con il Cisco Technical Assistance Center (TAC) in una richiesta di servizio e possono decodificarlo con strumenti interni. Questo output fornisce informazioni utili sui processi e i thread, che consentono agli sviluppatori di esaminare e correlare l'arresto anomalo ad altri eventi all'interno del dispositivo.

> **Nota**: in genere, quando si raccoglie show tech-support output dell'ASA o di Lina (su FTD), show crashinfo è idealmente presente in tale output. Tuttavia, molte volte l'output è diverso o incompleto rispetto all'esecuzione diretta del show crashinfo Pertanto, si consiglia di immettere sempre il show crashinfo direttamente sull'appliance ASA o sulla CLI di Lina.

Oltre ai dettagli comuni da controllare, ci sono altre informazioni e artefatti da raccogliere che dipendono dai vari livelli di arresti anomali che possono verificarsi. Sulle piattaforme ASA, il crash può essere solo di un livello. Tuttavia, le piattaforme Firepower possono avere un crash a livello di dispositivo logico (FTD o software ASA) o a livello di chassis (FXOS).

Quando l'uptime conferma che il dispositivo si è bloccato, viene visualizzata una coredump file necessario per un ulteriore esame da parte di Cisco TAC. OSPF (Open Shortest Path First) coredump I tipi di file possono essere diversi a seconda del componente del software in cui si è verificato il crash. OSPF (Open Shortest Path First) coredump i file vengono inoltre salvati in diverse directory/parti del disco, a seconda del componente che si è arrestato in modo anomalo.

Elementi da verificare sulle piattaforme ASA

Le piattaforme ASA hanno un solo componente che può essere ASA o FTD.

Tutte le piattaforme ASA che eseguono un'immagine ASA

OSPF (Open Shortest Path First) corefiles relativi all'arresto anomalo sono memorizzati sul disco 0 dell'unità flash interna. Per verificare il corefiles, immettere il dir disk0:/coredumpfsys comando:

<#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)
```

Immettere il show coredump filesystem per visualizzare tutti i file sul coredump file system, che mostra anche lo spazio su disco. Si consiglia di archiviare coredump file quando è opportuno, in quanto è possibile che una successiva coredump è possibile rimuovere il precedente coredump(s) per adattarsi al core corrente.

<#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
```

Se non viene visualizzato un coredump nel disco 0, è molto probabile che il coredump non è abilitato, il che significa che non è possibile completare la revisione per questa occorrenza. Al fine di coredump per occorrenze future, immettere questo comando:

```
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)
```

Piattaforme ASA che supportano l'esecuzione dell'immagine FTD

Le piattaforme ASA 5506-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X e ASA 5555-X supportano l'esecuzione dell'immagine FTD e lo rendono un firewall di nuova generazione.

Su tutte le piattaforme ASA supportate che eseguono l'immagine FTD, corefiles si trovano sotto /var/data/cores o /ngfw/var/data/cores tramite modalità esperto. Viene inoltre eseguito il mirroring sotto disk0:/coredumpfsys directory di 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)
```

Informazioni da verificare sulle piattaforme Firepower

Le piattaforme Firepower sono dotate di due componenti software. Il primo è il FXOS, che è il sistema operativo dello chassis, e il secondo è l'istanza dell'applicazione, nota anche come dispositivo logico, che può essere ASA o FTD. Pertanto, è importante identificare quale parte si è arrestata in modo anomalo per determinare in quale posizione scaricare corefiles

Se l'istanza dell'app si blocca su Firepower 1000/2000/4100 e 9300, le informazioni sull'arresto anomalo e corefiles vengono sempre generati per default. In alcuni casi, tuttavia, è possibile disattivare la memoria di base.

Per controllare se il core dump è abilitato sugli switch 4100/9300, immettere questi comandi:

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

Abilitare o disabilitare i dump del core del modulo Firepower:

Abilitare i dump di base su un modulo Firepower per facilitare la risoluzione dei problemi in caso di arresto anomalo del sistema o per inviarli a Cisco TAC, se richiesto.

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

Il risultato del comando mostra le informazioni correnti sullo stato del dump del core e indica se la compressione dei dump del core è abilitata.

<#root>

```
Firepower-module1>
```

show coredump detail

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

Utilizzare il config coredump per abilitare o disabilitare i core dump e per abilitare o disabilitare la compressione dei core dump durante un arresto anomalo del sistema.

- Immettere il config coredump enable per abilitare la creazione di un dump del core durante un crash.
- Immettere il config coredump disable per disabilitare la creazione di core dump durante un arresto anomalo del sistema.
- Immettere il config coredump compress enable per abilitare la compressione dei dump della memoria.
- Immettere il config coredump compress disable per disabilitare la compressione della memoria di massa.

Nell'esempio viene mostrato come abilitare il dump del core:

<#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>
```

> **Nota**: i file di dump del core occupano spazio su disco e, se lo spazio è insufficiente e la compressione non è abilitata, un file di dump del core non viene salvato anche se sono abilitati i dump del core.

Per un'analisi completa è necessario caricare sia i file di arresto anomalo del sistema che i file di base, poiché è possibile che il file di arresto anomalo non contenga tutti i dati.

FP9300/FP4100 FXOS

Su FP9300/FP4100, FXOS corefiles si trovano sotto local-mgmt cores directory.

```
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)#
```

Per copiare il file di base da FXOS al computer locale, immettere questo comando:

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

FP9300/FP4100 con FTD

FP9300/FP4100 con FTD, corefiles si trovano sotto /var/data/cores o /ngfw/var/data/cores tramite modalità esperto.

Viene inoltre eseguito il mirroring sotto disk0:/coredumpfsys directory di 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)
```

FP9300/FP4100 con ASA

Sui modelli FP9300/FP4100 con ASA, corefiles si trovano sotto disk0:/coredumpfsys directory.

<#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

FP2100 FXOS/ASA/FTD corefiles si trovano sotto local-mgmt cores se si utilizza ASA o FTD. In FTD, vengono anche specchiati in /ngfw/var/data/cores (o /var/data/cores)e /ngfw/var/common/ tramite modalità esperto. Tuttavia, si noti che le piattaforme FP2100 non dispongono del disco 0:/coredumpfsys directory.

> **Nota**: l'ID bug Cisco CSCvh01912 è stato inviato per rendere il sistema FP2100 coerente con la piattaforma FP9300/4100. Fino a quando non viene risolto, utilizzare il percorso descritto per trovare corefiles.

Posizione dei file di base di Firepower quando il FTD si trova in Firepower 2100, 1000, Appliance ASA e Appliance ISA 3000:

Per tutte queste piattaforme, utilizzare questa procedura per individuare i file di base relativi a tutti i processi di Firepower.

Inferiore /ngfw/var/common/:

1. Connettersi alla CLI dell'accessorio tramite SSH o console.

2. Inserire la modalità esperto:

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

3. Diventare un utente root.

<#root>

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

sudo su

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

4. Passare alla /ngfw/var/common/ , in cui si trovano i file di base.

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

5. Controllare la cartella del file.

```
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 su FP2100: sotto /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 su 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/
```

Nota: FXOS corefiles sono archiviati nella stessa directory core da connect local-mgmt.

FP1000 FXOS/ASA/FTD

Su FP1000 FXOS/ASA/FTD, questo processo è simile a FP2100. Inoltre, la disk0:/coredumpfsys è disponibile sul lato Lina.

FTD su 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 su FP100:

<#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
```

Nota: FXOS corefiles sono archiviati nella stessa directory core dalla connessione local-mgmt.

Scarica Corefiles

Esiste un copy comando in connect local-mgmt e Lina/ASA CLI. Per la modalità FTD expert, utilizzare il scp

Altri elementi da verificare (specifici delle piattaforme Firepower 4100 e 9300)

Controllare l'output del show pmon state comando in local-mgmt su FXOS. In questo esempio viene mostrato l'output desiderato quando nessuno dei processi si è arrestato in modo anomalo. Questo output non cattura solo gli arresti anomali a livello di dispositivo, ma anche quelli del modulo di interfaccia/DME e così via.

<#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
```

Se non si trovano file core nelle directory FTD/ASA correlate, i file core possono essere presenti su bootCLI su 4100/9300.

Visualizza i corefile all'interno del modulo

Immettere questo comando per connettersi alla console del modulo:

<#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>
```

Se non ci sono file di base in bootCLI, è possibile controllare i log a livello FXOS:

```
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 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
```

A volte il dispositivo si blocca in modo invisibile all'utente e non genera arresti anomali o file di base. In

questo caso, è possibile controllare i registri:

```
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 wit

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

# Check for syslogs messsages (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 t
```

Bug noti relativi all'arresto anomalo del sistema

Fare riferimento a queste pagine per ulteriori informazioni sull'arresto anomalo del sistema:

- ID bug Cisco CSCvu84127 - Arresto anomalo FTD senza generare un file di core o di crash
- ID bug Cisco CSCwa35845 - ASA 5516 ricaricato generando i file core
- ID bug Cisco CSCvw9444 - arresto anomalo di FTD crashinfo/corefile
- Cisco ID bug CSCv86926 - Arresto anomalo del FTD, generazione crashfile
- ID bug Cisco CSCvp16482 - Arresto anomalo dell'ASA durante la generazione di un file di base
- Cisco ID bug CSCvm53545 - L'ASA può tracciare e ricaricare senza generare un crashinfo file

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).