

識別FTD中高CPU的Linux進程和核心

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[疑難排解](#)

[確定佔用高CPU的Linux進程](#)

[思科安全防火牆系統核心上的CPU使用率高](#)

[相關資訊](#)

簡介

本檔案介紹思科安全防火牆威脅防禦(FTD)上的CPU使用率高，其中「高」表示90%或以上的CPU使用率。

必要條件

需求

- 思科安全防火牆管理中心(FMC)。
- 思科安全防火牆威脅防禦(FTD)。

採用元件

- 思科安全防火牆管理中心運行版本7.4.2。
- 思科安全防火牆威脅防禦運行版本7.4.2。

背景資訊

Cisco安全防火牆是Lina和Snort的整合映像。進程會危及思科安全防火牆系統的後端。思科安全防火牆上的進程和執行緒具有親合性，這意味著能夠將一個進程或執行緒繫結到特定CPU核心或一組核心。某些進程（例如Lina或Snort）與特定核心具有獨佔的親合性，這意味著其他進程或執行緒不能在這些核心上運行。

疑難排解

確定佔用高CPU的Linux進程

要確定Cisco安全防火牆上佔用高CPU的進程，請參閱以下輸出：

top命令輸出可幫助我們識別佔用大部分CPU的進程。

```
top - 17:27:37 up 62 days, 22:52, 2 users, load average: 0.41, 0.55, 0.48
Tasks: 158 total, 1 running, 157 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.9 us, 1.1 sy, 0.7 ni, 93.4 id, 3.9 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7981.8 total, 821.0 free, 3184.3 used, 3976.5 buff/cache
MiB Swap: 5378.2 total, 4361.2 free, 1017.0 used. 4563.9 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3394	root	25	5	425680	4860	4652	S	7.6	0.1	6494:36	loggerd
3685	root	0	-20	2958720	1.4g	130268	S	6.0	18.0	5062:29	lina
4494	root	1	-19	1339224	509956	44688	S	1.7	6.2	1659:12	snort3
3979	root	20	0	2270592	141480	16840	S	0.7	1.7	637:29.39	SFDataCorrelator

按1並檢查每個核心的CPU使用率。

```
top - 17:30:36 up 62 days, 22:55, 2 users, load average: 0.33, 0.47, 0.45
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie
%Cpu0 : 3.0 us, 0.0 sy, 0.0 ni, 97.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu1 : 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu2 : 0.0 us, 0.3 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu3 : 1.3 us, 5.3 sy, 2.7 ni, 90.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7981.8 total, 831.5 free, 3173.6 used, 3976.7 buff/cache
MiB Swap: 5378.2 total, 4361.2 free, 1017.0 used. 4574.7 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3394	root	25	5	425680	4860	4652	S	7.6	0.1	6494:36	loggerd
3685	root	0	-20	2958720	1.4g	13026	S	6.0	18.0	5062:29	lina
4494	root	1	-19	1339224	509956	44688	S	1.7	6.2	1659:12	snort3
3979	root	20	0	2270592	141480	16840	S	0.7	1.7	637:29.39	SFDataCorrelator

按c檢查進程的詳細資訊。

```
top - 17:31:53 up 62 days, 22:56, 2 users, load average: 0.34, 0.45, 0.45
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie
%Cpu0 : 3.7 us, 1.0 sy, 0.0 ni, 95.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu1 : 0.0 us, 0.3 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu2 : 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu3 : 2.0 us, 3.7 sy, 2.7 ni, 91.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7981.8 total, 831.4 free, 3173.7 used, 3976.7 buff/cache
MiB Swap: 5378.2 total, 4361.2 free, 1017.0 used. 4574.5 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3394	root	25	5	425680	4860	4652	S	7.3	0.1	6494:55	/ngfw/usr/local/sf/bin/loggerd
3685	root	0	-20	2958720	1.4g	130268	S	6.0	18.0	5062:45	lina -p 3562 -t -l
4494	root	1	-19	1339224	509956	44688	S	2.3	6.2	1659:17	/ngfw/var/sf/detection_engines/ad5
3418	root	20	0	1640540	16824	13900	S	0.7	0.2	274:48.05	/ngfw/usr/local/sf/bin/adi
3979	root	20	0	2270592	141480	16840	S	0.7	1.7	637:31.13	/ngfw/usr/local/sf/bin/SFDataCorre

```
3380 root 20 0 3860 2852 2336 S 0.3 0.0 6:27.14 /bin/bash /ngfw/usr/local/sf/bin/p
```

考慮使用top命令驗證monetdb是罪魁禍首的流程(monetdb)消耗高CPU的示例。

您可以在專家模式ngfw/var/log/monetdb/merovingian.log下跟蹤merovingian.log。

```
root@FirePower:/# cd /ngfw/var/log/#catmerovingian.log
```

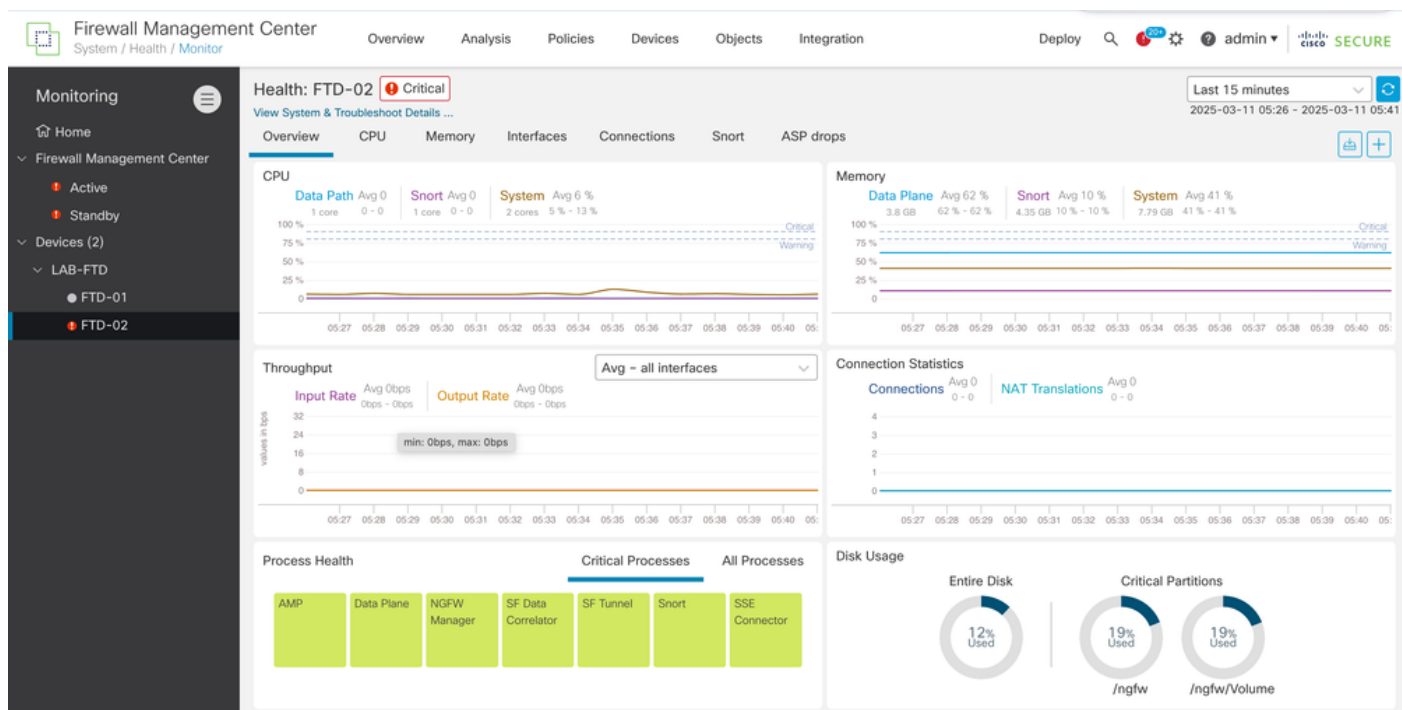
```
2025-03-06 23:24:11 ERR eventdb[26531]: #client12: createExceptionInternal:
!ERROR: SQLException:sql.drop_table:42000!DROP TABLE: unable to drop table connectionevent_1720808160_0
2025-03-06 23:24:11 ERR eventdb[26531]: #client12: createExceptionInternal:
!ERROR: SQLException:sql.drop_table:42000!DROP TABLE: unable to drop table
connectionevent_1720971900_0 (there are database objects which depend on it)
```

思科安全防火牆系統核心上的CPU使用率高

以下是Cisco安全防火牆系統核心上高CPU情況下的故障排除步驟。

1. 在FMC運行狀況監控中確認CPU系統使用率高。

- 檢查FMC上的通知列以檢查CPU使用率是否過高。
- 導覽至System > Health > Monitor，然後觀察受影響的核心。



2. 在FTD CLI上驗證受影響的CPU核心。

- 檢查CPU親和力並確認受影響的核心是系統核心。

```
> pmtool show affinity
```

```
Received status (0):
```

```
Affinity Status
```

```
System CPU Affinity: 3,9 (desired 3,9 )
```

```
..
```

```
<#root>
```

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

```
sudo mpstat -P 3,9 1
```

```
Linux 4.18.45-yocto-standard (firepower)      03/03/25      _x86_64_      (64 CPU)
```

```
1:06:15      CPU
```

```
%usr  %nice  %sys
```

```
%iowait  %irq  %soft  %steal  %guest  %gnice
```

```
%idle
```

```
1:06:15      3
```

```
4
```

```
.00  54.00  24.00
```

```
0.00  0.00  0.00  0.00  0.00  0.00
```

```
14.00
```

```
1:06:15      9
```

```
0.00  74.00  25.00
```

```
0.00  0.00  0.00  0.00  0.00  0.00
```

```
0.00
```

```
1:06:15      CPU
```

```
%usr  %nice  %sys
```

```
%iowait  %irq  %soft  %steal  %guest  %gnice  %idle
```

```
1:06:16      3
```

```
6
```

```
.00  44.00  34.00
```

```
0.00  0.00  0.00  0.00  0.00  0.00
```

```
4
```

```
.00
```

```

1:06:16      9
2.00  74.00  22.00
    0.00    0.00  0.00  0.00  0.00  0.00
0.00

1:06:16      CPU
%usr  %nice  %sys
    %iowait  %irq  %soft  %steal  %guest  %gnice  %idle
1:06:16      3
6
.00  34.00  24.00
    0.00    0.00  0.00  0.00  0.00  0.00
34.00

1:06:16      9
0.00  74.00  24.00
    0.00    0.00  0.00  0.00  0.00  0.00
0.00

...

Average:      9   3.71  67.43   22.14   0.00    0.00   0.00   0.00   0.00   0.00   9.71

```

- Runmpstatatorsarto監視系統核心上的CPU利用率。在本示例中，1表示監控間隔1/秒。

CPU使用率越高，因為%idle等於100 — 其他%列的總數，因此它越低。

<#root>

```

admin@firepower:~$
sudo

```

```

sar -P 3,9 1

```

```

Linux 4.18.45-yocto-standard (firepower)      03/03/24      _x86_64_      (64 CPU)

1:06:17      CPU
%user      %nice  %system
    %iowait  %steal
%idle

```

1:06:18 3

5

.00 54.00 28.00

0.00 0.00

14.00

1:06:18 9

1.00 80.00 19.00

0.00 0.00

0.00

1:06:18 CPU

%user %nice %system

%iowait %steal

%idle

1:06:19 3

5

.00 41.00 22.00

0.00 0.00

24.00

1:06:19 9

2.00 84.00 12.00

0.00 0.00

0.00

1:06:19 CPU

%user %nice %system

%iowait %steal

%idle

1:06:20 3

1.00 67.00 15.00

0.00 0.00

4

.00

```

1:06:20          9
5
.00      68.00      24.00
      0.00      0.00
0.00

```

```

1:06:20          CPU
%user    %nice    %system
      %iowait    %steal
%idle

```

```

1:09:21          3
6.00      26.00      27.00
      0.00      0.00
41.00

```

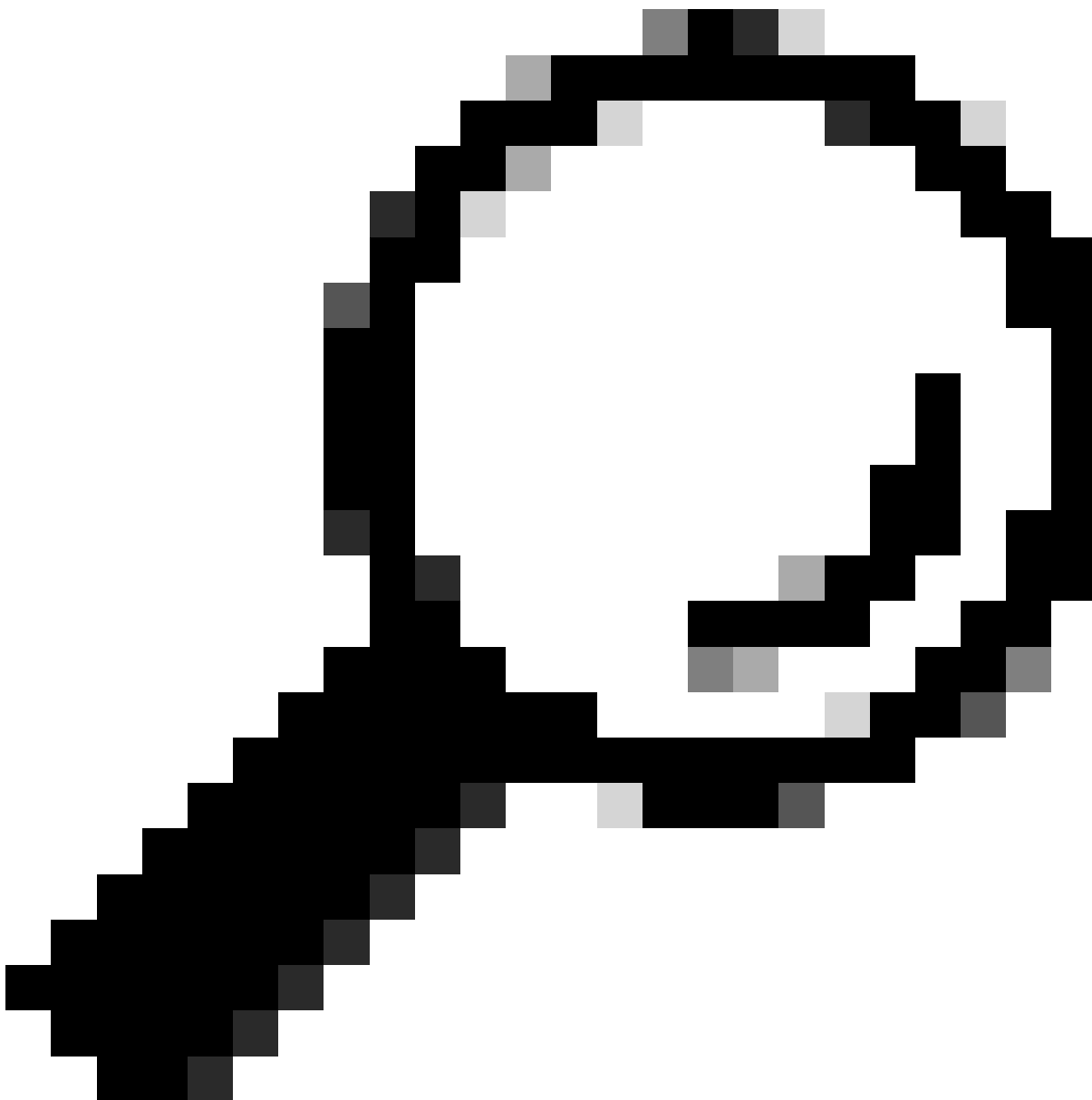
```

1:09:21          9
0.00      86.00      14.00
      0.00      0.00
0.00

```

列標題概述如下：

- %user — 使用者空間中的CPU使用率（應用程式碼），使用預設nice值。
- %nice — 使用者空間（應用程式碼）中的CPU使用率（正值nice）。
- %system — 核心空間中的CPU使用率。%idle - 100%減去其餘欄位



提示：運行此命令可查詢在特定核心上運行的執行緒清單。

```
pidstat -h -t -p ALL 1 | awk '($10=="%CPU") || ($10==XX || $10==YY)& $9+0 > 10.00)
```

在專家模式下運行top命令可查詢在特定核心上運行的進程清單。

3.檢查進程是否為多執行緒。

<#root>

[admin@firepower](#)

:

~\$

```
sudo pidstat -h -t -p $(pidof snort3) 1
```

Linux 4.18.45-yocto-standard (firepower)				03/03/25		_x86_64_		(64 CPU)		
# Time	UID	TGID	TID	%usr	%system	%guest	%wait	%CPU	CPU	Command
4:20:05	0	4162	-	279.08	17.17	0.00	0.99	285.15	3	snort3 <--
4:20:05	0	-	4162	3.96	0.99	0.00	0.99	4.95	3	__
snort3										
4:20:05	0	-	4165	0.00	0.00	0.00	0.00	0.00	7	__
snort3										
4:20:05	0	-	4167	0.00	0.00	0.00	0.00	0.00	9	__
snort3										
4:20:05	0	-	4168	0.00	0.00	0.00	0.00	0.00	9	__
snort3										
4:20:05	0	-	4169	0.00	0.00	0.00	0.00	0.00	9	__snort3
4:20:05	0	-	4172	0.00	0.00	0.00	0.00	0.00	9	__snort3
4:20:05	0	-	4175	0.00	0.00	0.00	0.00	0.00	9	__snort3
4:20:05	0	-	4177	0.00	0.00	0.00	0.00	0.00	3	__snort3

<#root>

admin@firepower

:

~\$

sudo

pidstat -h -t -p \$(pidof rsyslog) 1

Linux 4.18.45-yocto-standard (firepower)				03/03/25		_x86_64_		(64 CPU)		
# Time	UID	TGID	TID	%usr	%system	%guest	%wait	%CPU	CPU	Command
4:22:47	0	1	-	0.00	0.00	0.00	0.00	0.00	32	init
4:22:47	0	-	1	0.00	0.00	0.00	0.00	0.00	32	__init <---- single

4.檢查是否有任何進程執行緒在系統核心上運行。

<#root>

admin@firepower:~\$

```
sudo pidstat -h -t -p $(pidof EventHandler) 1
```

Password:

Linux 4.18.45-yocto-standard (firepower) 03/03/25 _x86_64_ (64 CPU)

#	Time	UID	TGID	TID	%usr	%system	%guest	%wait	%CPU	CPU	Command
04:46:01		0	327455	-	61.00	23.00	0.00	0.00	83.00	3	

EventHandler

<--- All threads run on system cores

04:46:01	0	-	327455	0.00	0.00	0.00	0.00	0.00	3	__EventH
04:46:01	0	-	327456	30.00	0.00	0.00	60.00	40.00	3	__EventH
04:46:01	0	-	327457	29.00	9.00	0.00	64.00	33.00	9	__EventH
04:46:01	0	-	327458	0.00	0.00	0.00	0.00	0.00	3	__EventH
04:46:01	0	-	327459	0.00	0.00	0.00	0.00	0.00	3	__zmqio
04:46:01	0	-	327465	0.00	0.00	0.00	0.00	0.00	9	__zmqio
04:46:01	0	-	327466	0.00	0.00	0.00	1.00	0.00	9	__EventH
04:46:01	0	-	327468	3.00	2.00	0.00	3.00	5.00	9	__EventH
04:46:01	0	-	327470	0.00	0.00	0.00	0.00	0.00	9	__EventH
04:46:01	0	-	327475	0.00	0.00	0.00	0.00	0.00	3	__EventH
04:46:01	0	-	327476	0.00	0.00	0.00	0.00	0.00	9	__EventH
04:46:01	0	-	327477	0.00	0.00	0.00	0.00	0.00	3	__EventH
04:46:01	0	-	327478	0.00	0.00	0.00	0.00	0.00	9	__zmqio
04:46:01	0	-	327479	0.00	0.00	0.00	0.00	0.00	9	__zmqio

5.檢查任何執行緒都貢獻於或導致系統核心上的CPU使用率高。

<#root>

[admin@firepower:~\\$](#)

```
sudo pidstat -h -t -p $(pidof EventHandler) 1
```

Linux 4.18.45-yocto-standard (firepower) 03/03/25 _x86_64_ (64 CPU)

#	Time	UID	TGID	TID	%usr	%system	%guest	%wait	%CPU	CPU	Command
05:13:30		0	327455	-	111.77	19.80	0.00	0.00	136.57	3	EventHa

<---- Process CPU usage = Σ (threads %CPU).

05:13:30	0	-	327455	0.00	0.00	0.00	0.00	0.00	3	__Even
05:13:30	0	-	327456	33.64	0.00	0.00	65.17	37.54	9	__Event

<---- Thread on system cores with highest CPU usage

05:13:30	0	-	327457	74.24	15.83	0.00	7.92	94.18	3	__Event
----------	---	---	--------	-------	-------	------	------	-------	---	---------

<---- Thread on system cores with highest CPU usage

05:13:30	0	-	327458	0.00	0.00	0.00	0.00	0.00	3	__Even
05:13:30	0	-	327459	0.00	0.00	0.00	0.00	0.00	9	__zmqi
05:13:30	0	-	327465	0.00	0.00	0.00	0.00	0.00	9	__zmqi
05:13:30	0	-	327466	0.00	0.99	0.00	0.00	0.99	3	__Even
05:13:30	0	-	327468	1.98	2.97	0.00	5.94	4.85	9	__Even
05:13:30	0	-	327470	0.00	0.00	0.00	0.99	0.00	3	__Even
05:13:30	0	-	327475	0.00	0.00	0.00	0.00	0.00	9	__Even
05:13:30	0	-	327476	0.00	0.00	0.00	0.00	0.00	9	__Even
05:13:30	0	-	327477	0.00	0.00	0.00	0.00	0.00	9	__Even
05:13:30	0	-	327478	0.00	0.00	0.00	0.00	0.00	3	__zmqi
05:13:30	0	-	327479	0.00	0.00	0.00	0.00	0.00	9	__zmqi

- EventHandler是在系統核心上運行的多執行緒CPU。
- 執行緒TID=327456和TID=327457的CPU使用率最高。
- 進程CPU使用率等於所有執行緒的CPU使用率之和。

相關資訊

[思科安全防火牆管理中心管理指南7.6](#)
[思科安全防火牆管理中心裝置配置指南7.6](#)

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）。