疑難排解SWA中的異常程式狀態

目錄

簡介

必要條件

- 需求
- 採用元件

監視進程狀態

- 從GUI檢視程式狀態
- CLI命令
  - 狀態
  - 速率(proxystat)
  - shd_logs
  - process_status

在SWA中重新啟動進程

- 一般程式

簡介

本文檔介紹進程狀態以及如何使用此狀態對安全Web裝置(SWA)和效能問題進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬SWA。
- 許可證已啟用或已安裝。
- 安全殼層(SSH)使用者端。
- 安裝精靈已完成。
- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

監視進程狀態

您可以從圖形使用者介面(GUI)或命令列介面(CLI)監視進程狀態。

從GUI檢視程式狀態

要在GUI中檢視流程統計資訊，請導航到Reporting，然後選擇System Capacity。您可以選取「時間範圍」來檢視所需時間戳記的資源配置。

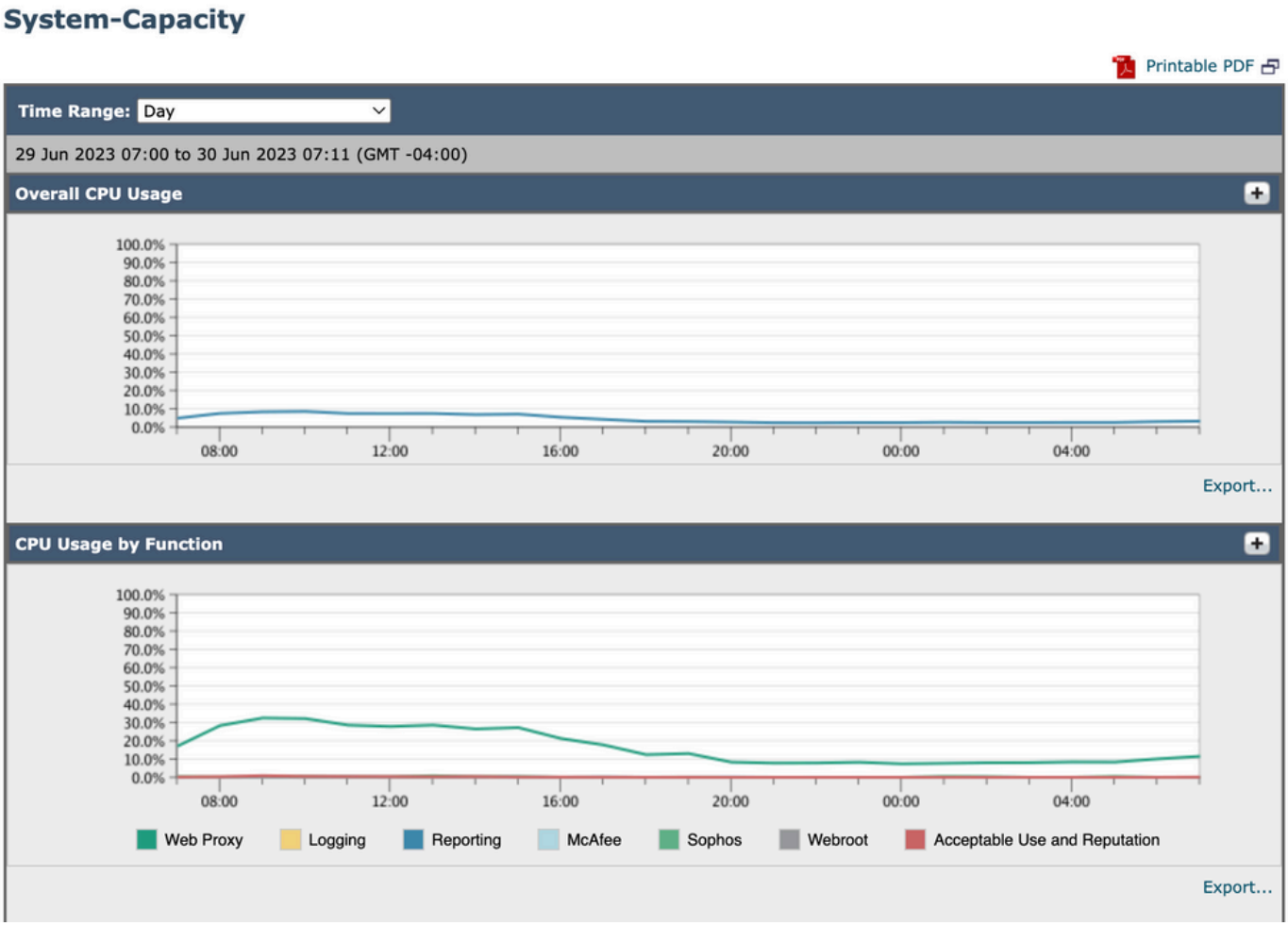
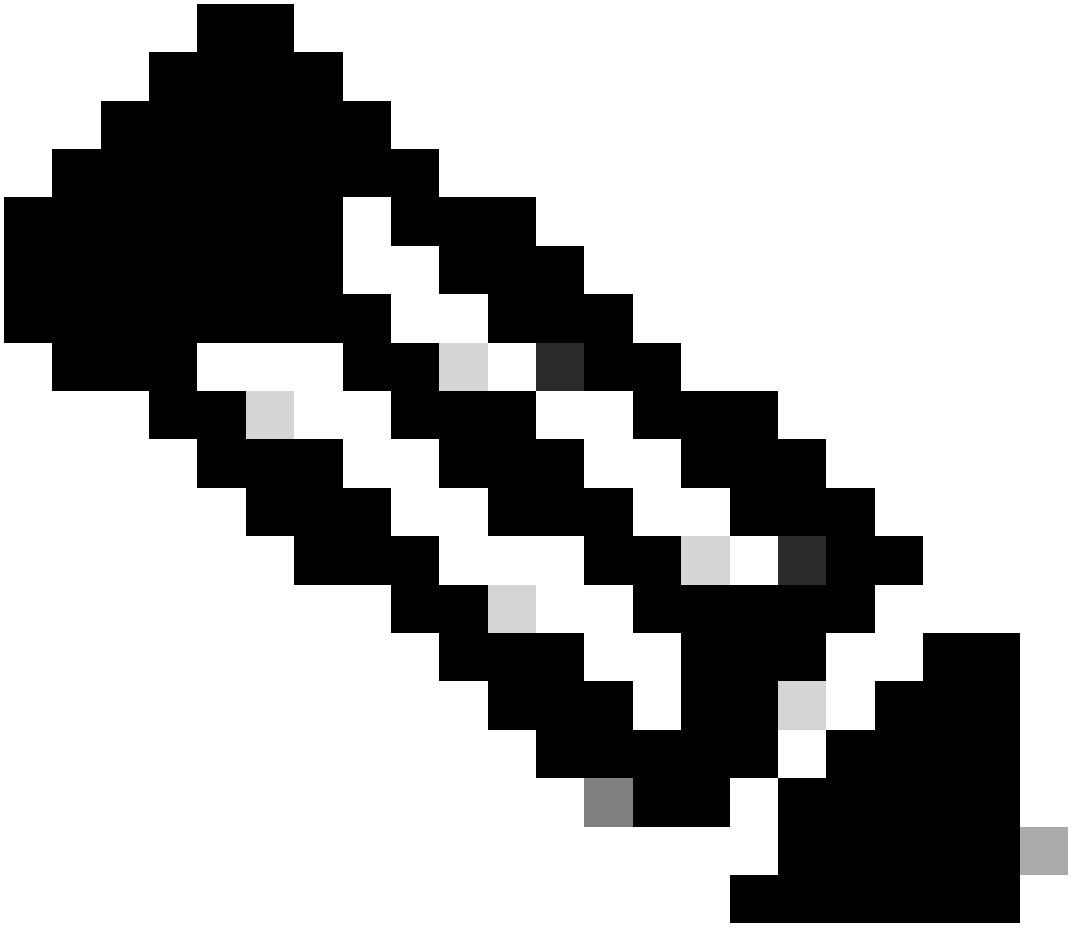


Image-System-Capacity

總體CPU使用率：顯示總CPU使用率

按功能列出的CPU使用率：顯示每個子進程、CPU分配。

代理緩衝記憶體：顯示代理進程的記憶體分配。



注意：「代理緩衝記憶體」不是SWA的記憶體使用總量。

CLI命令

有多個CLI命令可顯示主CPU負載或子進程狀態：

狀態

從status或status detail的輸出中，您可以檢視SWA的整體CPU使用情況，以下命令顯示了當前CPU負載。

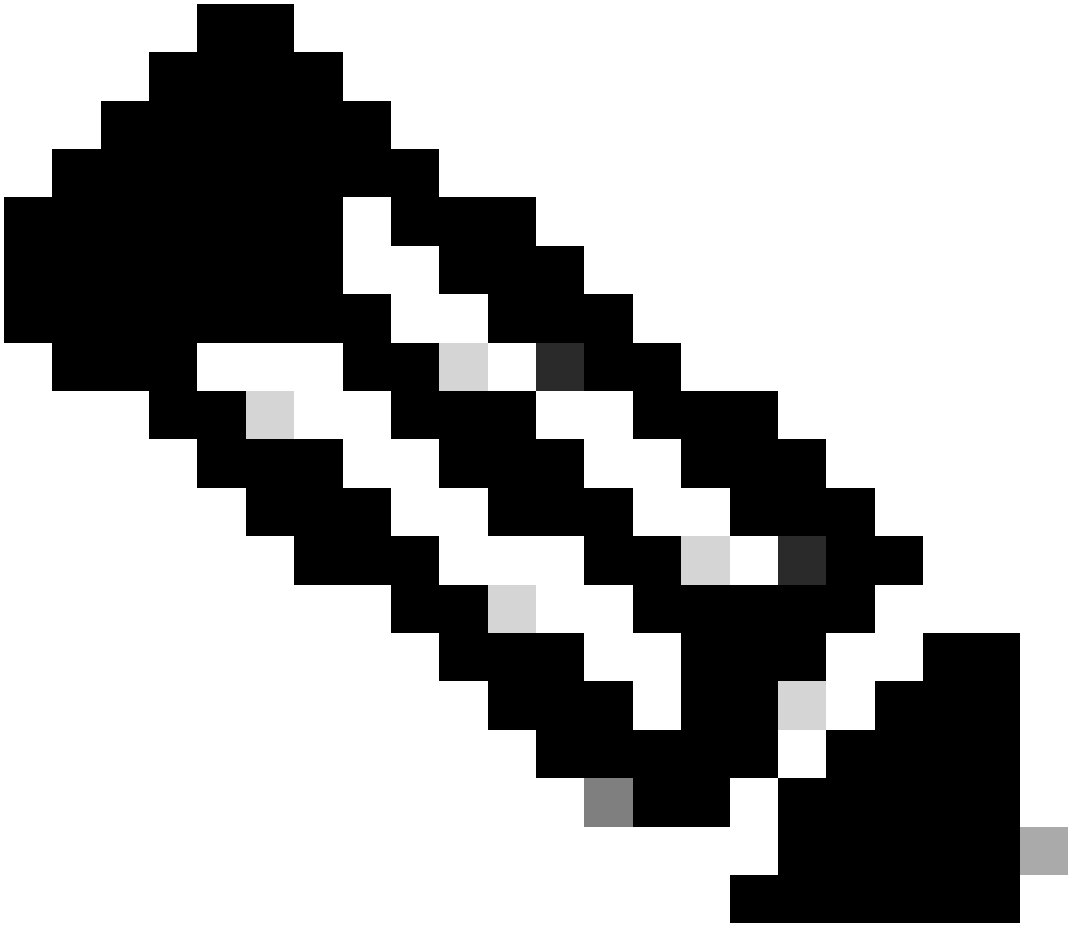
```
SWA_CLI)> status

Enter "status detail" for more information.

Status as of:                  Sat Jun 24 06:29:42 2023 EDT
Up since:                      Fri May 05 22:40:40 2023 EDT (49d 7h 49m 2s)
```

```
System Resource Utilization:
  CPU                                    3.0%
  RAM                                    9.9%
  Reporting/Logging Disk                14.4%
Transactions per Second:
  Average in last minute                  101
Bandwidth (Mbps):
  Average in last minute                4.850
Response Time (ms):
  Average in last minute                  469
Connections:
  Total connections                     12340


SWA_CLI> status detail

Status as of:                  Sat Jun 24 06:29:50 2023 EDT
Up since:                      Fri May 05 22:40:40 2023 EDT (49d 7h 49m 10s)
System Resource Utilization:
  CPU                                    3.5%
  RAM                                    9.8%
  Reporting/Logging Disk                14.4%
...
```

速率(proxystat)

rate CLI命令，顯示代理進程負載，該負載是SWA中的主進程的子進程。此命令每15秒自動刷新一次。

```
SWA_CLI>  rate

Press Ctrl-C to stop.
  %proxy  reqs                          client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
  8.00   116      0    237    928       3801      3794    0.2     6     0
  7.00   110      0    169    932       4293      4287    0.1     2     0
```



註：「proxystat」是另一個輸出與「rate」命令相同的CLI命令

---

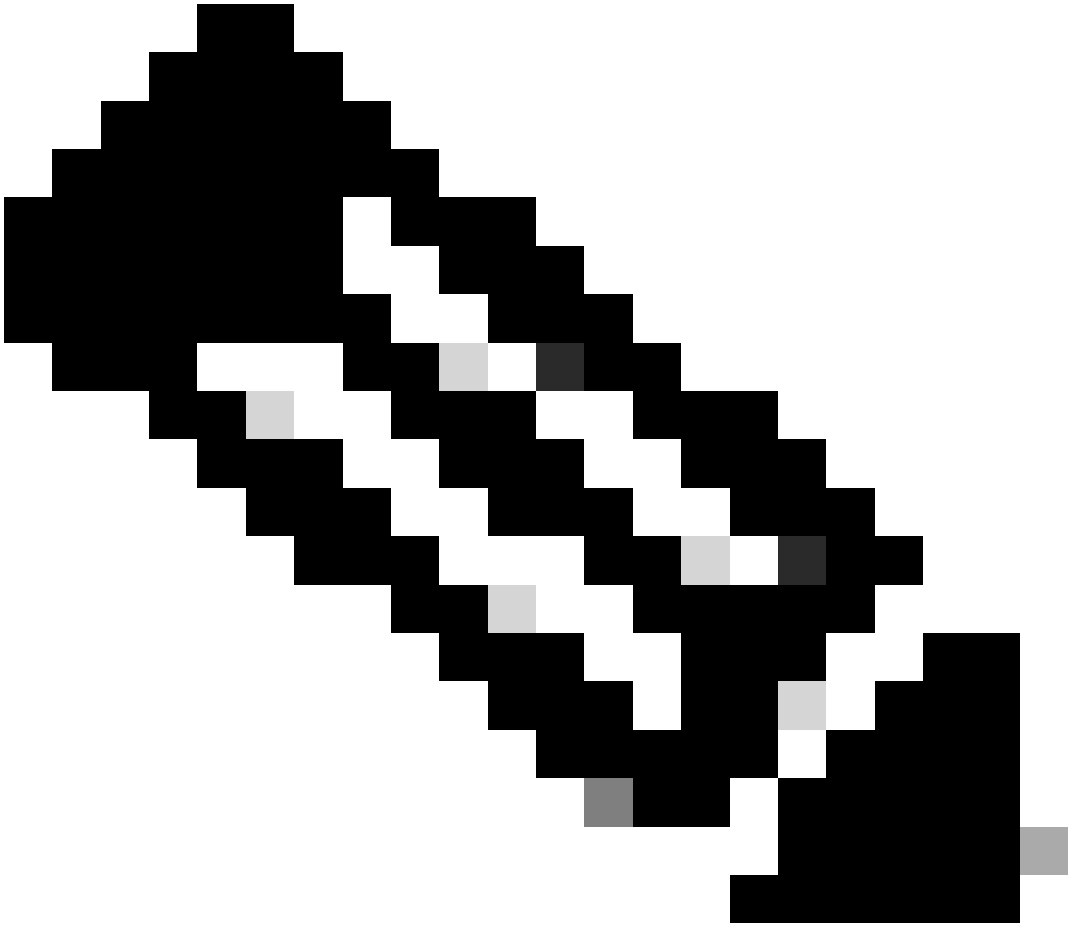
shd_logs

您可以從SHD_Logs檢視主要程式狀態，例如Proxy程式狀態、報告程式狀態等。有關SHD日誌的更多資訊，請訪問此連結：

https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance/220446-troubleshoot-secure-web-appliance-perfor.html

以下是shd_logs輸出的示例：

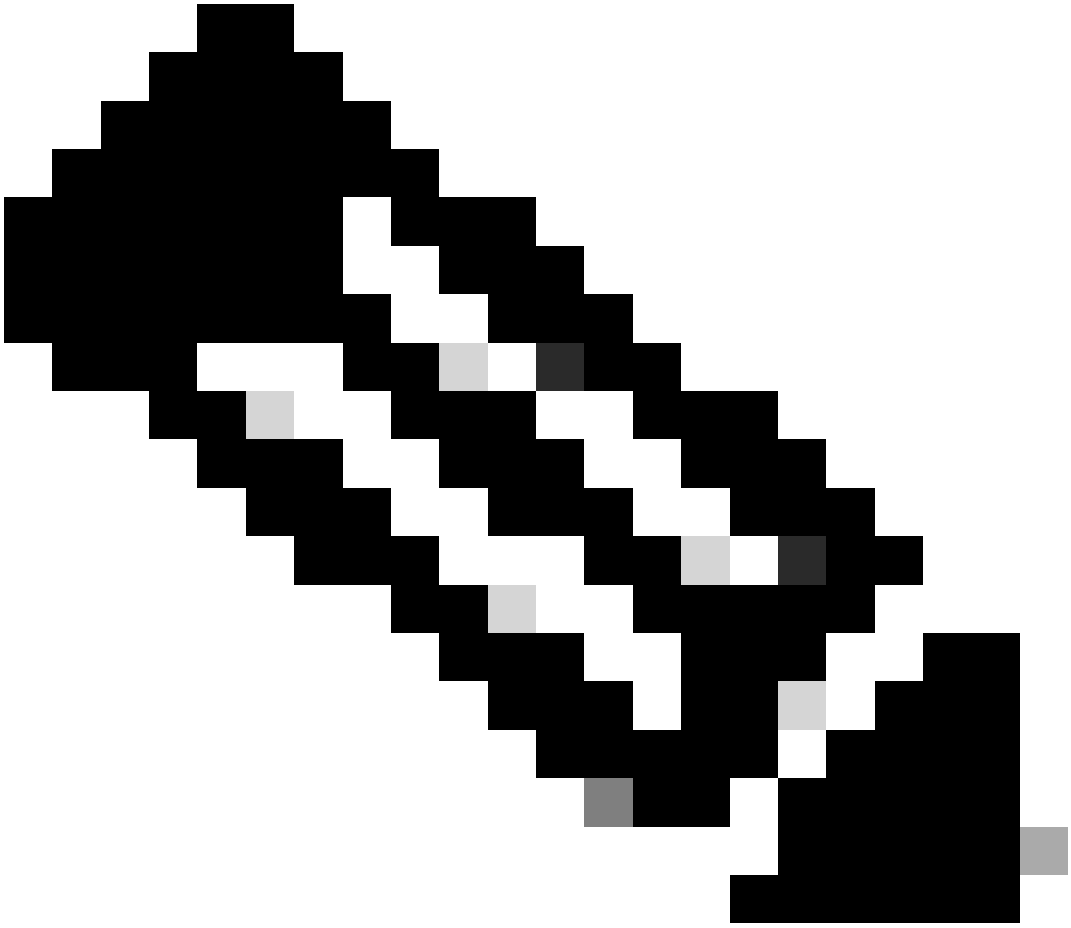
```
Sat Jun 24 06:30:29 2023 Info: Status: CPULd 2.9 DskUtil 14.4 RAMUtil 9.8 Reqs 112 Band 22081 Latency 4
```



注意：可以透過grep或tail CLI命令訪問shd_logs。

process_status

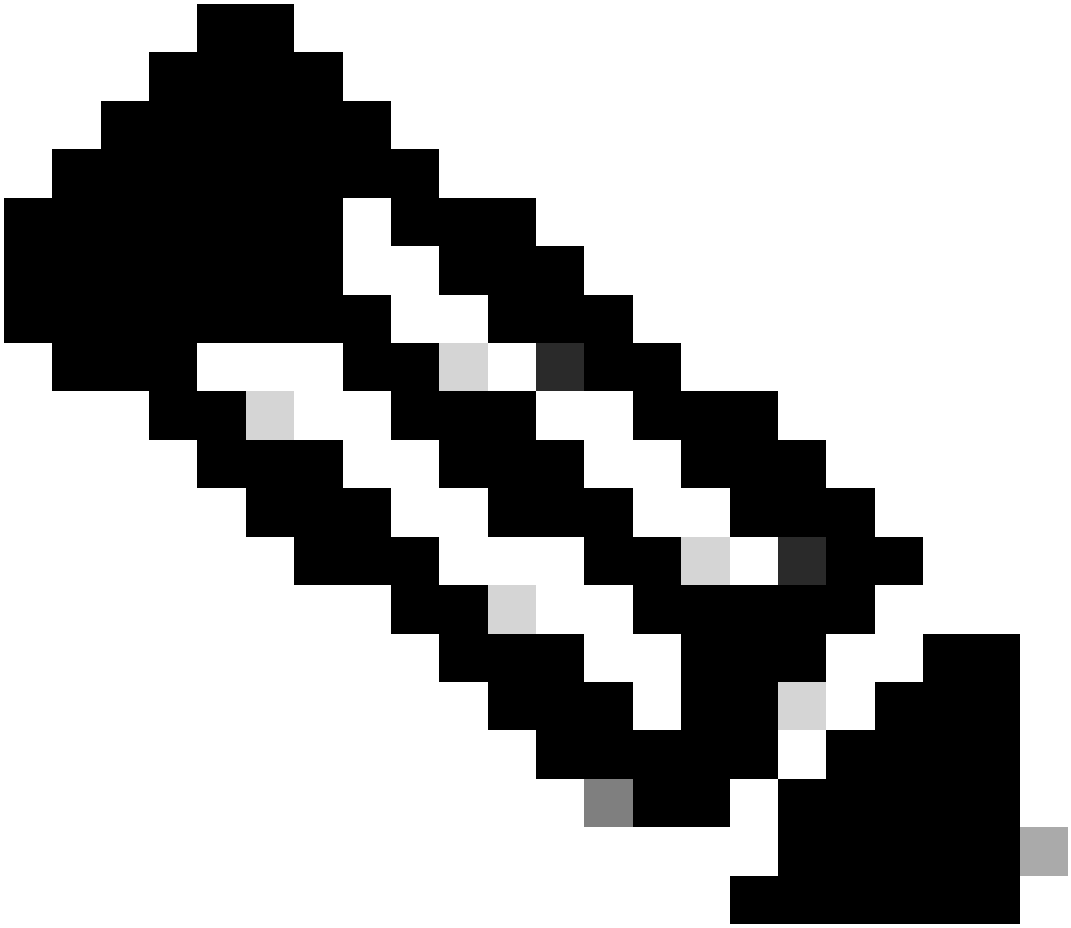
若要檢視「處理狀態」，在14.5版及更新版本中，SWA有新的命令：process_status，可取得SWA的處理詳細資訊。



注意：此命令僅在管理模式下可用。

```
SWA_CLI> process_status

USER     PID   %CPU %MEM     VSZ     RSS TT  STAT STARTED          TIME COMMAND
root      11 4716.6  0.0       0     768  -  RNL   5May23 3258259:51.69 idle
root   53776   13.0  4.7 6711996 3142700  -  S    14:11       220:18.17 prox
admin  15664    8.0  0.2  123404  104632  0  S+   06:23         0:01.49 cli
admin  28302    8.0  0.2  123404  104300  0  S+   06:23         0:00.00 cli
root      12    4.0  0.0       0    1856  -  WL    5May23    7443:13.37 intr
root   54259    4.0  4.7 6671804 3167844  -  S    14:11       132:20.14 prox
root   91401    4.0  0.2  154524  127156  -  S     5May23    1322:35.88 counterd
root   54226    3.0  4.5 6616892 2997176  -  S    14:11        99:19.79 prox
root    2967    2.0  0.1  100292   80288  -  S     5May23     486:49.36 interface_controlle
root   81330    2.0  0.2  154524  127240  -  S     5May23    1322:28.73 counterd
root      16    1.0  0.0       0      16  -  DL    5May23    9180:31.03 ipmi0: kcs
root   79941    1.0  0.2  156572  103984  -  S     5May23    1844:37.60 counterd
root   80739    1.0  0.1  148380   94416  -  S     5May23    1026:01.89 counterd
root   92676    1.0  0.2  237948  124040  -  S     5May23    2785:37.16 wbnpd
root       0    0.0  0.0       0    1808  -  DLs   5May23      96:10.66 kernel
root       1    0.0  0.0    5428     304  -  SLs   5May23       0:09.44 init
```

```
root       2    0.0  0.0       0      16  -  DL    5May23       0:00.00 crypto
root       3    0.0  0.0       0      16  -  DL    5May23       0:00.00 crypto returns
root       4    0.0  0.0       0     160  -  DL    5May23      62:51.56 cam
root       5    0.0  0.0       0      16  -  DL    5May23       0:16.47 mrsas_ocr0
root       6    0.0  0.0       0      16  -  DL    5May23       0:00.52 soaiod1
root       7    0.0  0.0       0      16  -  DL    5May23       0:00.52 soaiod2
root       8    0.0  0.0       0      16  -  DL    5May23       0:00.52 soaiod3
root       9    0.0  0.0       0      16  -  DL    5May23       0:00.52 soaiod4
```



注意：進程的CPU使用率；這是過去（即時）時間內最多一分鐘的衰減平均值。由於計算此值的時間基數不同（因為進程可能非常年輕），因此所有%CPU欄位的總和可能會超過100%。

%MEM：此進程使用的實際記憶體百分比

VSZ：虛擬大小，以KB為單位（別名vsize）

RSS：進程的實際記憶體（駐留集）大小（以1024位元組為單位）。

TT：控制終端路徑名稱的縮寫（如果有）。

STAT

stat由一系列字元提供，例如「RNL」。第一個字元代表程式的執行狀態：

D：在磁碟（或其他短期、不可中斷）等待中標籤進程。

I：標籤處於空閒狀態（睡眠時間超過約20秒）的進程。

L：標籤等待獲取鎖定的進程。

R ：標籤可運行的進程。

S：標籤睡眠時間小於約20秒的進程。

T：標籤已停止的進程。

W：標籤空閒中斷執行緒。

Z：標籤一個死進程（一個「殭屍」）。

這些字元之後的其他字元（如果有的話）表示其他狀態資訊：

+：進程位於其控制終端的前台進程組中。

<：進程提高了CPU排程優先順序。

C ：進程處於辣椒(4)功能模式。

E：進程正在嘗試退出。J標籤處於監牢中的進程(2)。

L：該程式有鎖在核心中的頁面（例如，用於原始I/O）。

N：進程降低了CPU排程優先順序。

s：進程是會話領導。

V：進程的父進程在vfork(2)期間暫停，等待進程執行或退出。

W：進程被換出。

X ：正在跟蹤或調試進程。

時間：累積CPU時間，使用者+系統

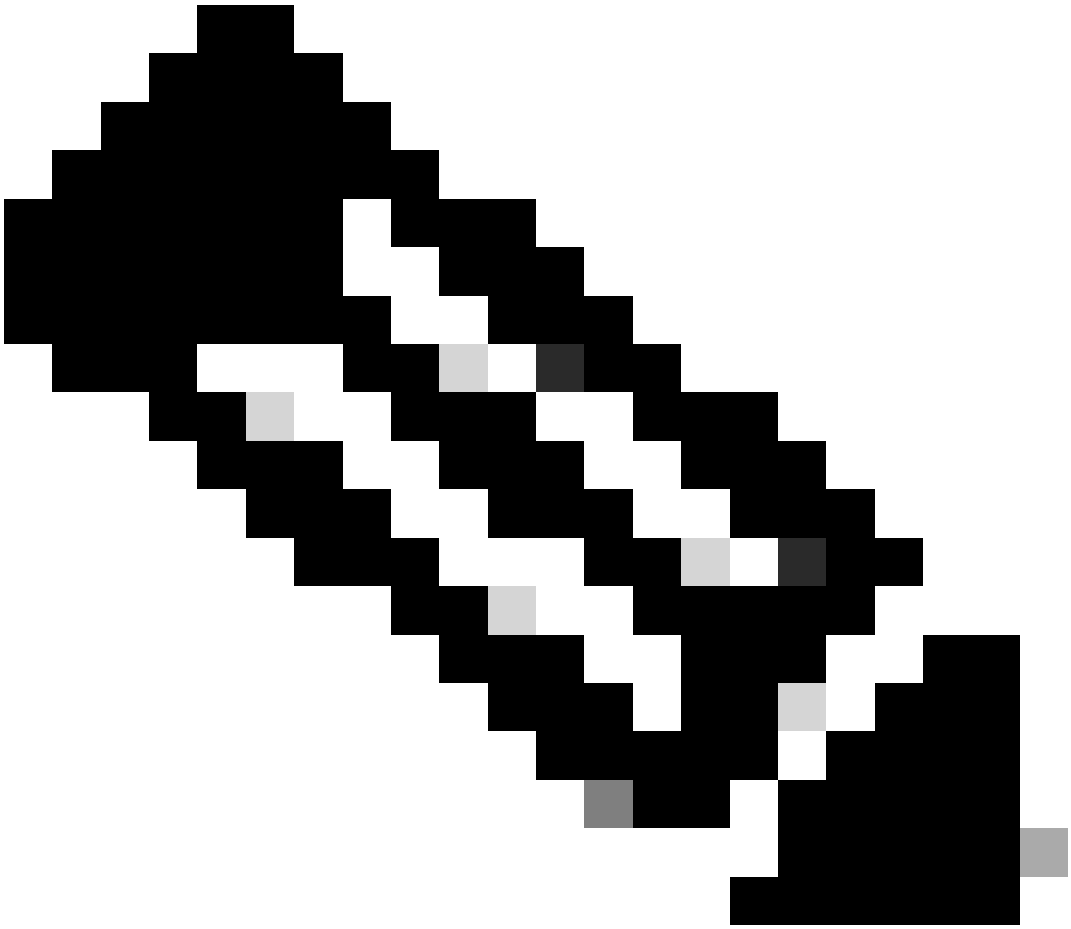
在SWA中重新啟動進程

一般程式

您可以從CLI重新啟動SWA服務和進程，步驟如下：

步驟1.登入CLI

步驟 2.型別診斷

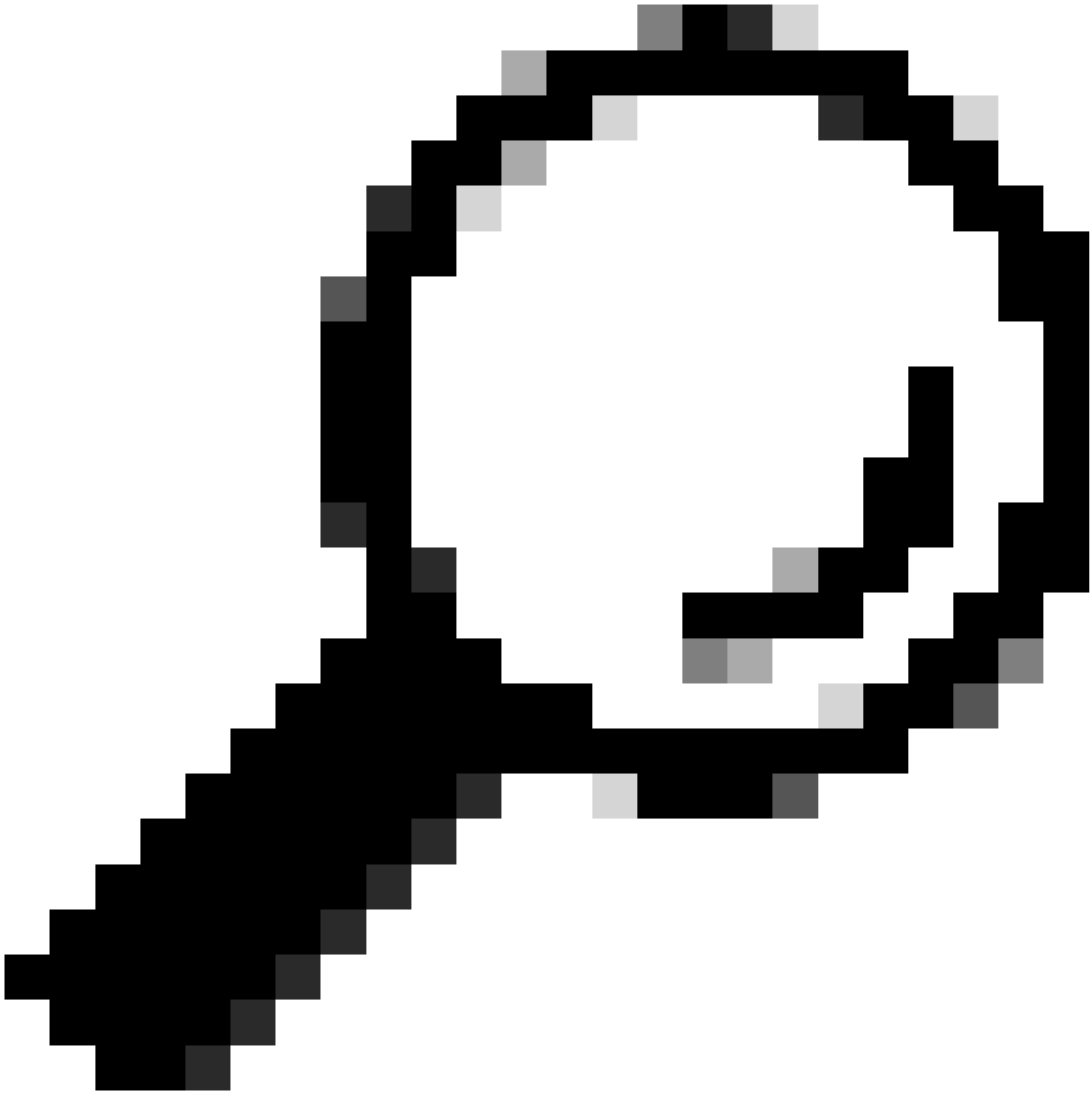


注意：diagnostic是CLI隱藏命令，因此您無法使用TAB鍵自動填充命令。

步驟 3.選擇服務

步驟 4.選擇要重新啟動的服務/進程。

步驟 5.選擇「重新啟動」



秘訣：您可以從STATUS區段檢視處理作業的狀態。

在本示例中，已重新啟動了負責GUI的WEBUI進程：

```
SWA_CLI> diagnostic

Choose the operation you want to perform:
- NET - Network Diagnostic Utility.
- PROXY - Proxy Debugging Utility.
- REPORTING - Reporting Utilities.
- SERVICES - Service Utilities.
[]> SERVICES

Choose one of the following services:
- AMP - Secure Endpoint
- AVC - AVC
```

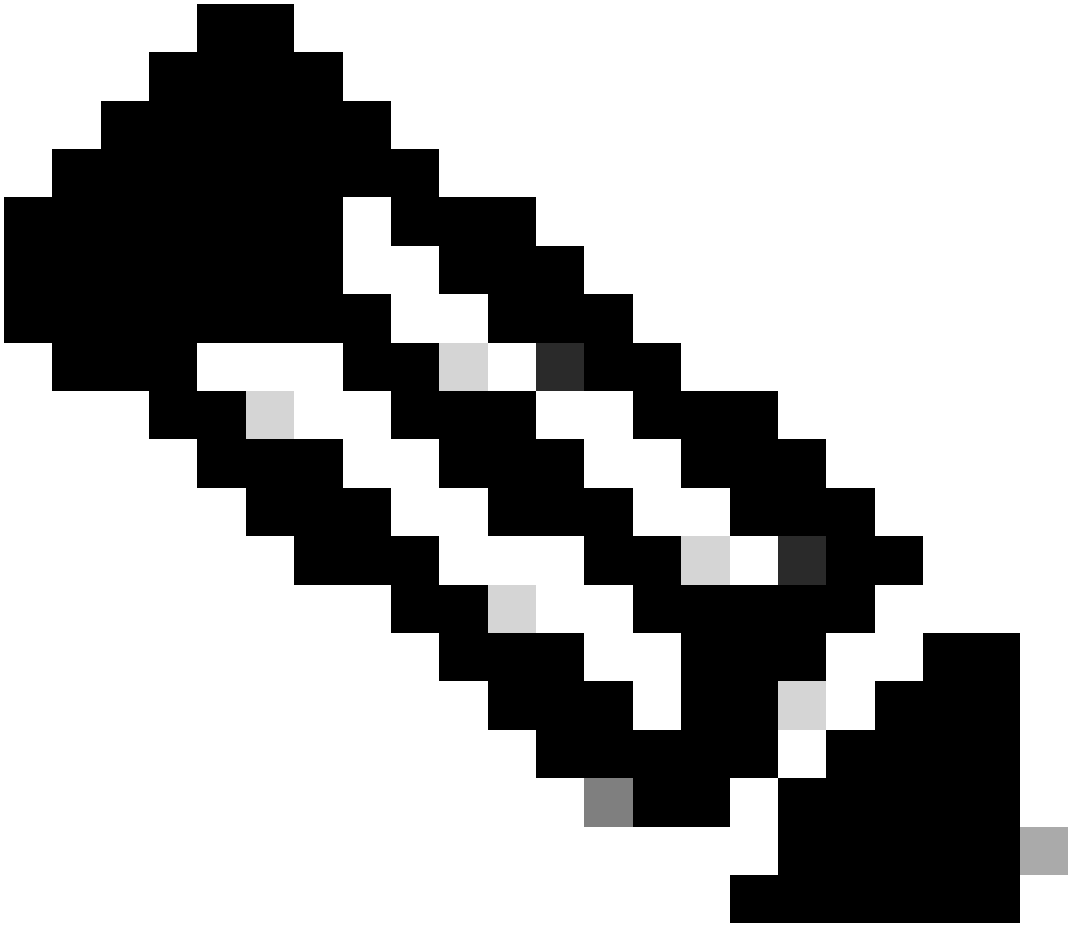
```
- ADC - ADC
- DCA - DCA
- WBRS - WBRS
- EXTFEED - ExtFeed
- L4TM - L4TM
- ANTIVIRUS - Anti-Virus xiServices
- AUTHENTICATION - Authentication Services
- MANAGEMENT - Appliance Management Services
- REPORTING - Reporting Associated services
- MISCSERVICES - Miscellaneous Service
- OCSP - OSCP
- UPDATER - UPDATER
- SICAP - SICAP
- SNMP - SNMP
- SNTP - SNTP
- VMSERVICE - VM Services
- WEBUI - Web GUI
- SMART_LICENSE - Smart Licensing Agent
- WCCP - WCCP
[]> WEBUI

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> RESTART

gui is restarting.
```

重新啟動代理進程

要重新啟動代理進程（代理進程的主要進程），可以使用CLI，步驟如下：

步驟1.登入CLI

步驟 2.型別診斷



注意：diagnostic是CLI隱藏命令，因此您無法使用TAB鍵自動填充命令。

步驟 3.選擇PROXY

步驟 4.鍵入KICK，（它是一個隱藏的命令）。

步驟 5.選擇Y作為「yes」。

```
SWA_CLI>diagnostic

Choose the operation you want to perform:
- NET - Network Diagnostic Utility.
- PROXY - Proxy Debugging Utility.
- REPORTING - Reporting Utilities.
- SERVICES - Service Utilities.
[]> PROXY

Choose the operation you want to perform:
- SNAP - Take a snapshot of the proxy
```

```
- OFFLINE - Take the proxy offline (via WCCP)
- RESUME - Resume proxy traffic (via WCCP)
- CACHE - Clear proxy cache
- MALLOCSTATS - Detailed malloc stats in the next entry of the track stat log
- PROXYSCANNERMAP - Show mapping between proxy and corresponding scanners
[]> KICK

Kick the proxy?
Are you sure you want to proceed? [N]> Y
```

相關資訊

- Cisco Secure Web Appliance的AsyncOS 15.0使用手冊- LD（有限部署）-故障排除[Cisco Secure Web Appliance] -思科
- 使用安全Web裝置最佳實踐-思科
- ps(1)（freebsd組織）

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）。