对SWA中的异常进程状态进行故障排除

目录

简介

本文档介绍进程状态以及如何使用此状态对安全网络设备(SWA)和性能问题进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟SWA。
- 许可证已激活或已安装。
- 安全外壳(SSH)客户端。
- 安装向导已完成。
- 对SWA的管理权限。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

监控进程状态

您可以通过图形用户界面(GUI)或命令行界面(CLI)监控进程状态。

通过GUI查看进程状态

要在GUI中查看进程统计信息，请导航到Reporting并选择System Capacity。您可以选择时间范围(Time Range)以查看所需时间戳的资源分配。

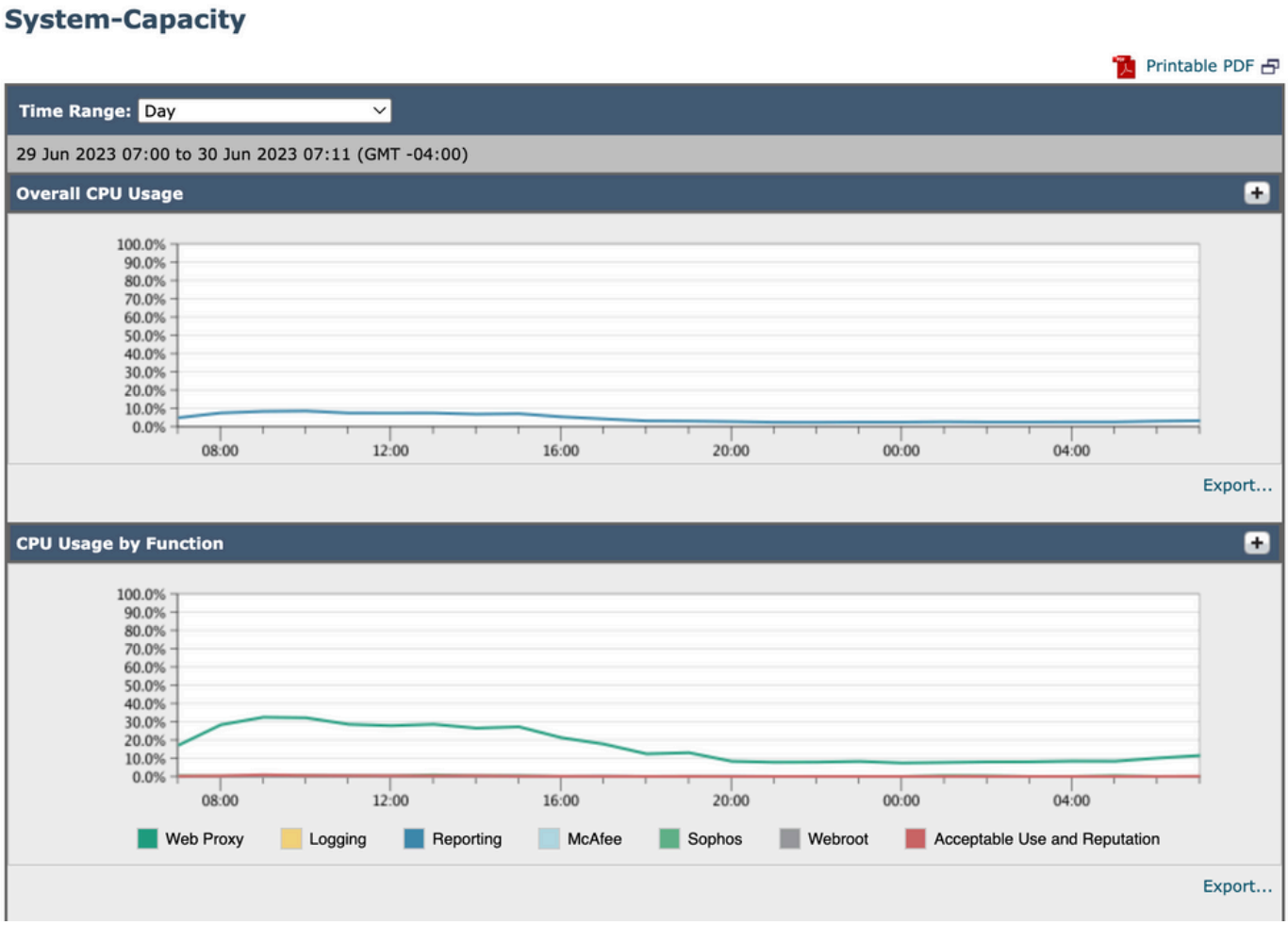
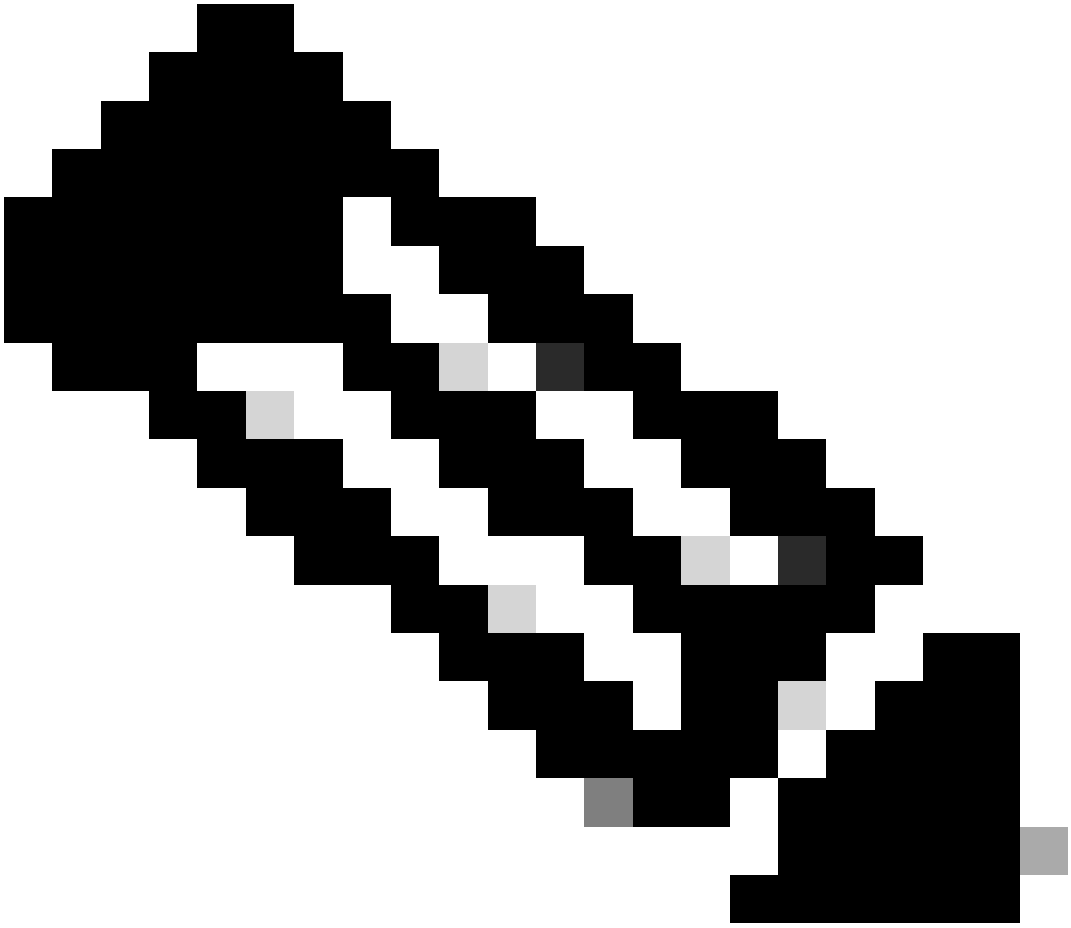


Image-System-Capacity

总体CPU使用情况：显示总CPU使用情况

按功能划分的CPU使用情况：显示每个子进程、CPU分配。

Proxy Buffer Memory：显示代理进程的内存分配。



注意：代理缓冲区内存不是SWA的总内存使用率。

CLI命令

有多个CLI命令可显示主CPU负载或子进程状态：

状态

从status或status detail的输出中，您可以查看SWA的整体CPU使用情况，这些命令显示当前的CPU负载。

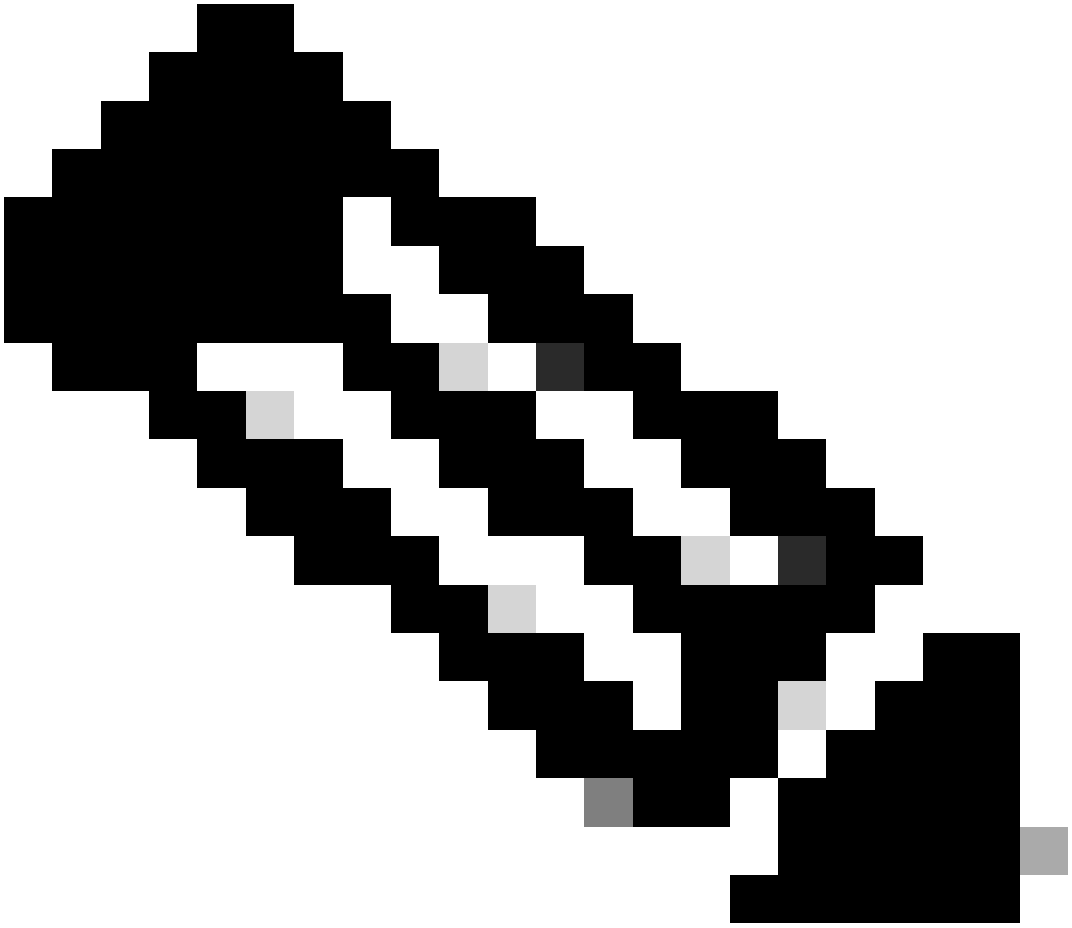
```
SWA_CLI)> status

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命令显示代理进程负载，该负载是一个子进程，是SWA中的主要进程。此命令每15秒自动刷新一次。

```
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
```



注意：“proxystat”是另一个输出与“rate”命令相同的CLI命令

---

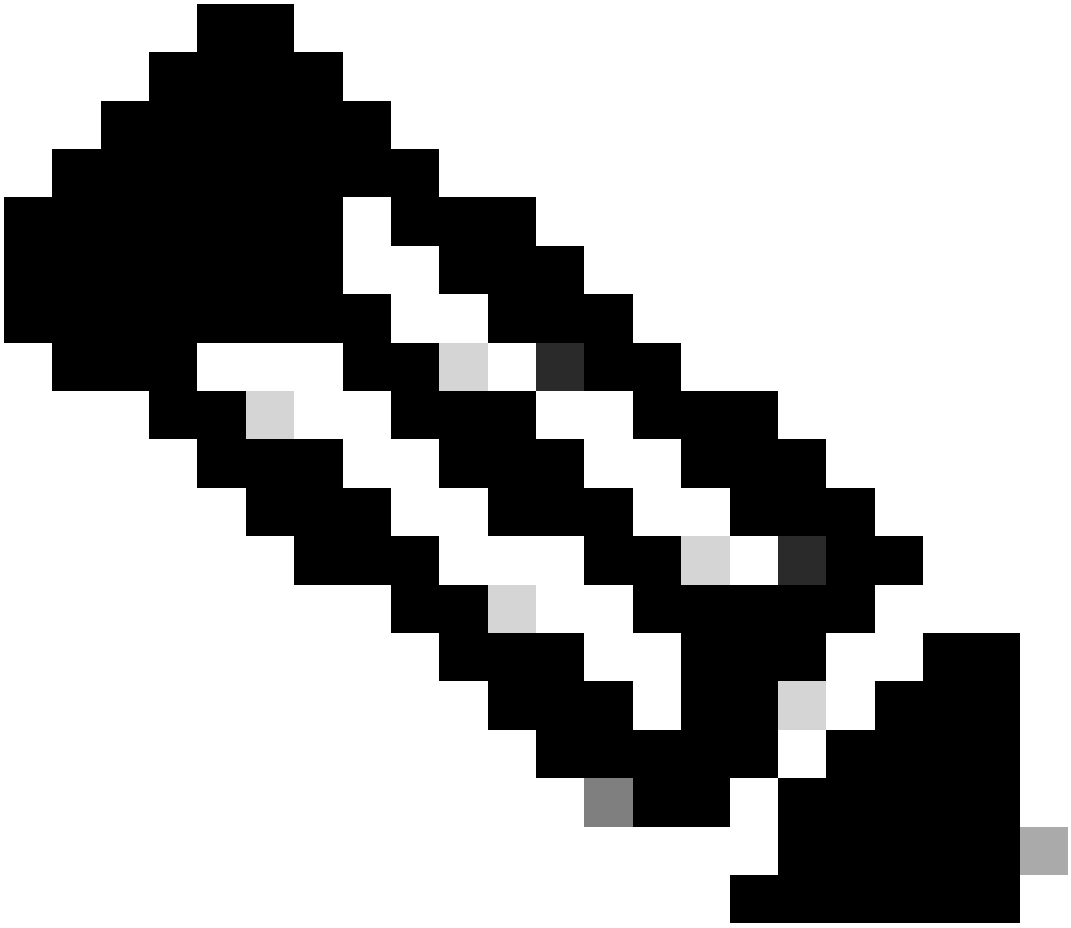
shd_logs

您可以从SHD_Logs查看主进程状态，如代理进程状态、报告进程状态等。有关SHD日志的更多信息，请访问以下链接：

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输出的示例：

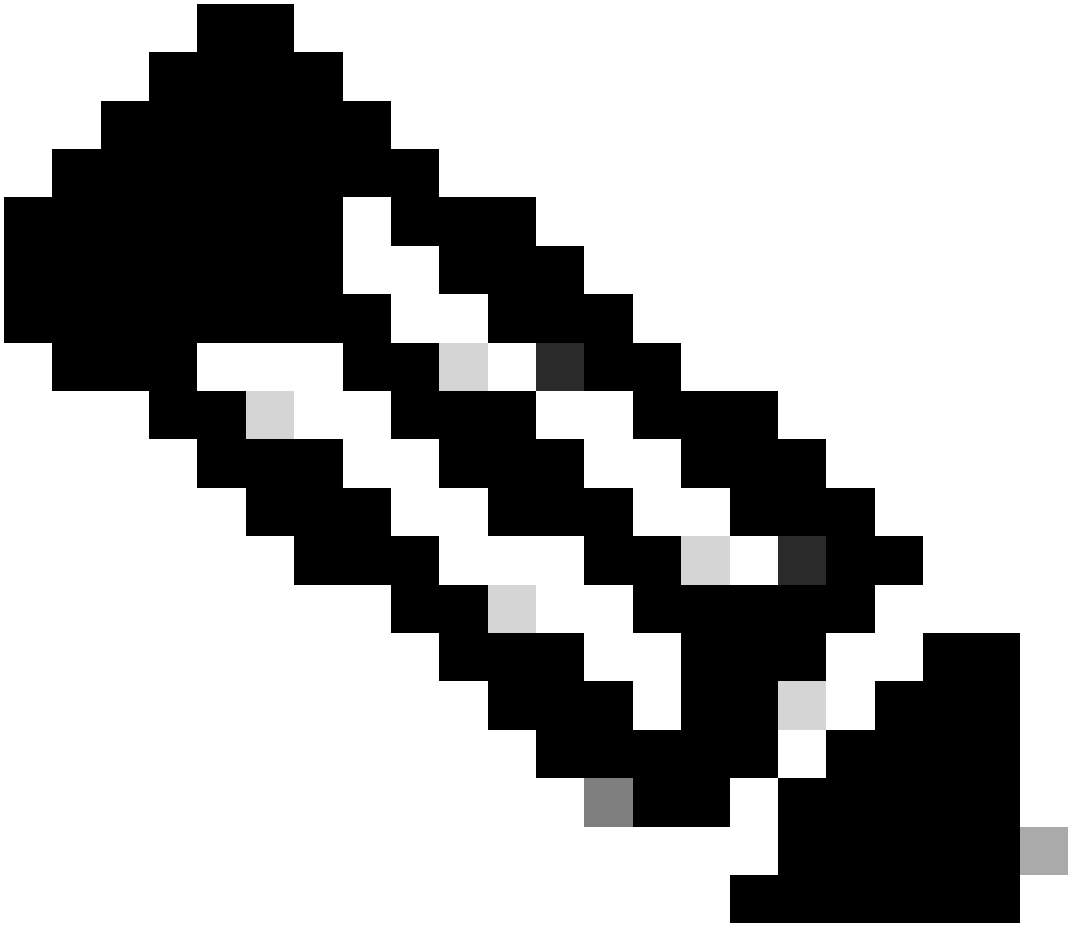
```
Sat Jun 24 06:30:29 2023 Info: Status: CPULd 2.9 DskUtil 14.4 RAMUtil 9.8 Reqs 112 Band 22081 Latency 4
```



注意：您可以通过grep或tail CLI命令访问shd_logs。

process_status

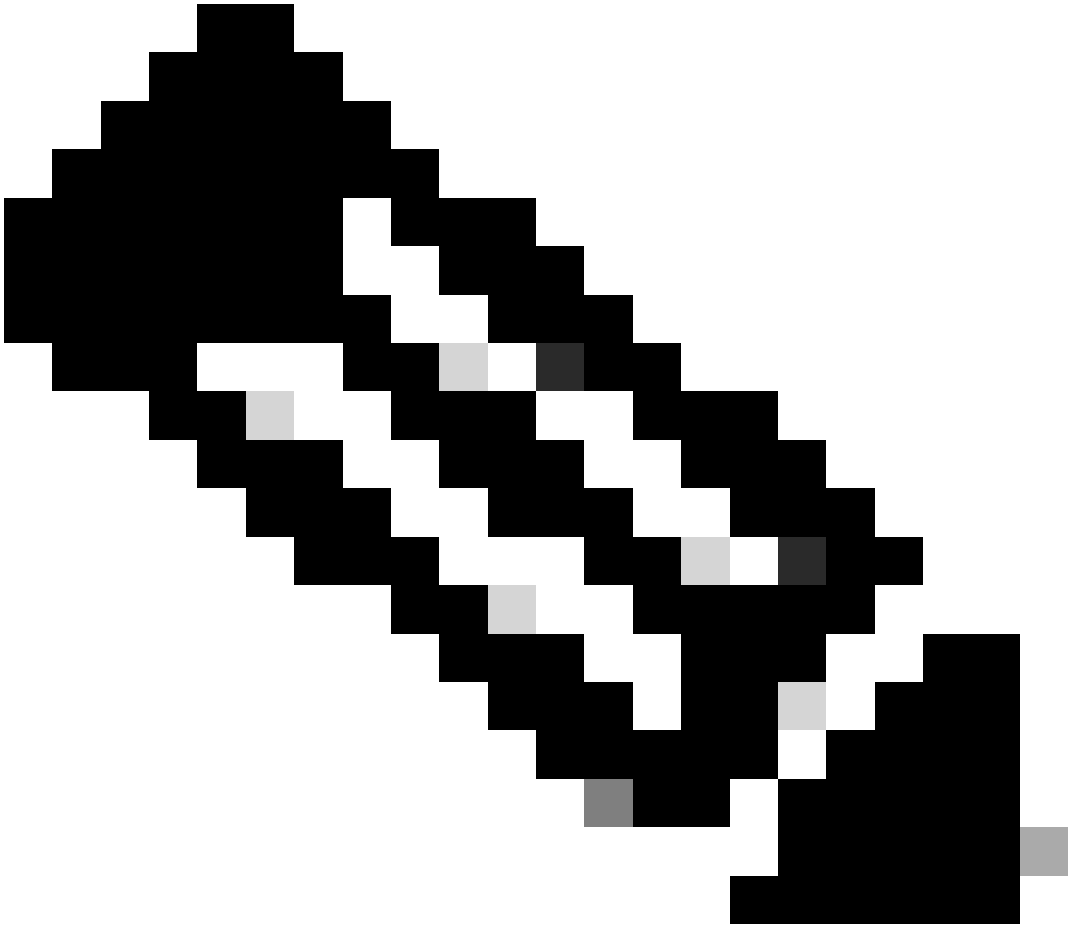
要查看流程状态，在版本14.5及更高版本中，SWA有一个新命令：process_status，用于获取SWA的流程详细信息。



注意：此命令仅在管理模式下可用。

```
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：进程的CPU使用率；这是过去（实时）时间内最多一分钟的衰减平均值。由于计算此值的时间基数不同（因为进程可能非常年轻），因此所有%CPU字段的总和可能超过100%。

%MEM：此进程使用的实际内存的百分比

VSZ：虚拟大小（千字节）（别名vsize）

RSS：进程的实际内存（常驻集）大小（以1024字节为单位）。

TT：控制终端的路径名称的缩写（如果有）。

STAT

stat由一系列字符组成，例如“RNL”。第一个字符指示进程的运行状态：

D ：在磁盘（或其他短期的、不可中断的）等待中标记进程。

I：标记空闲的进程（休眠时间大于约20秒）。

L：标记等待获取锁的进程。

R：标记可运行的进程。

S：标记休眠时间小于约20秒的进程。

T：标记已停止的进程。

W：标记空闲的中断线程。

Z：标记死进程（“僵尸”）。

后面添加的字符（如果有）表示其他状态信息：

+：进程位于其控制终端的前台进程组中。

<：进程已提高CPU调度优先级。

C：该过程处于辣椒(4)功能模式。

E：进程正在尝试退出。J标记处于监狱中的进程(2)。

L：该进程具有锁定在核心中的页面（例如，用于原始I/O）。

N：进程已降低CPU调度优先级。

s：进程是会话领导。

V：进程的父进程在vfork(2)期间暂停，等待进程执行或退出。

W：进程已换出。

X ：正在跟踪或调试进程。

时间：累计CPU时间，用户+系统

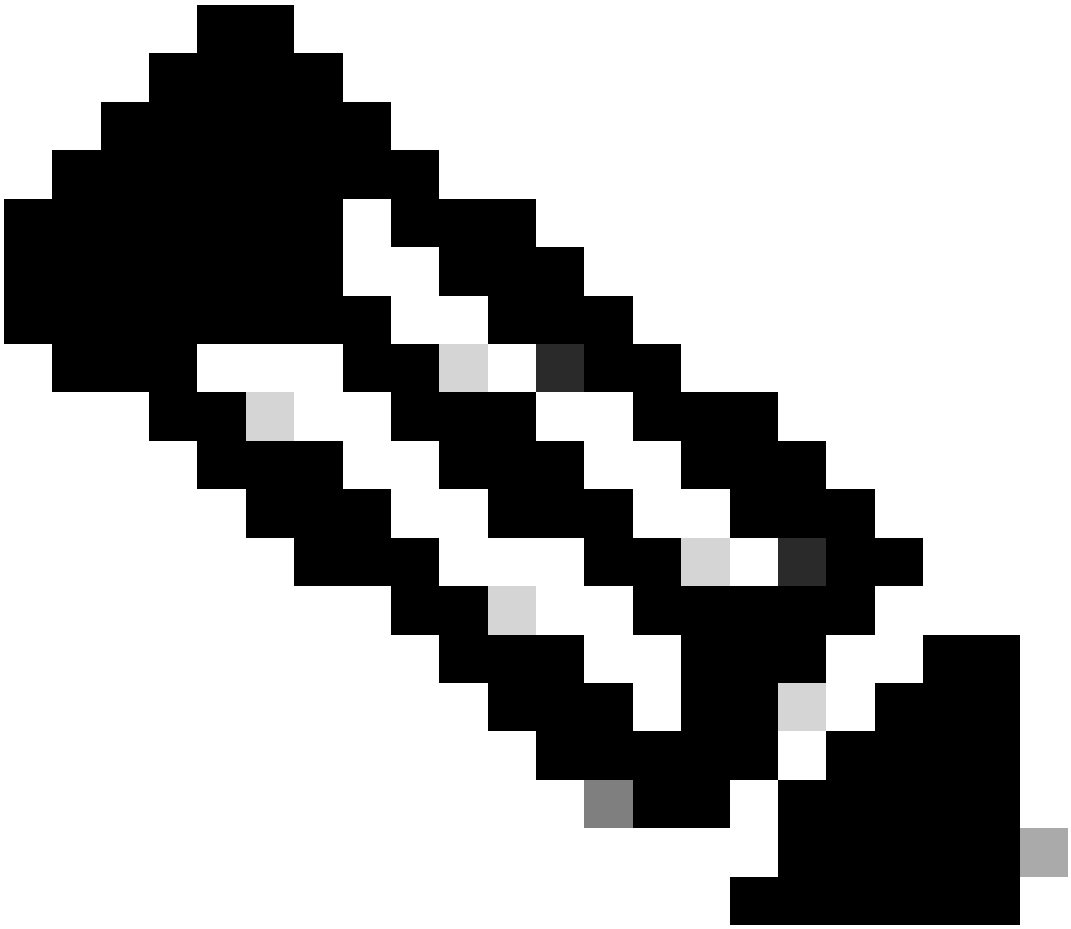
在SWA中重新启动进程

一般流程

您可以从CLI重新启动SWA服务和进程，步骤如下：

步骤1.登录CLI

第二步：类型诊断

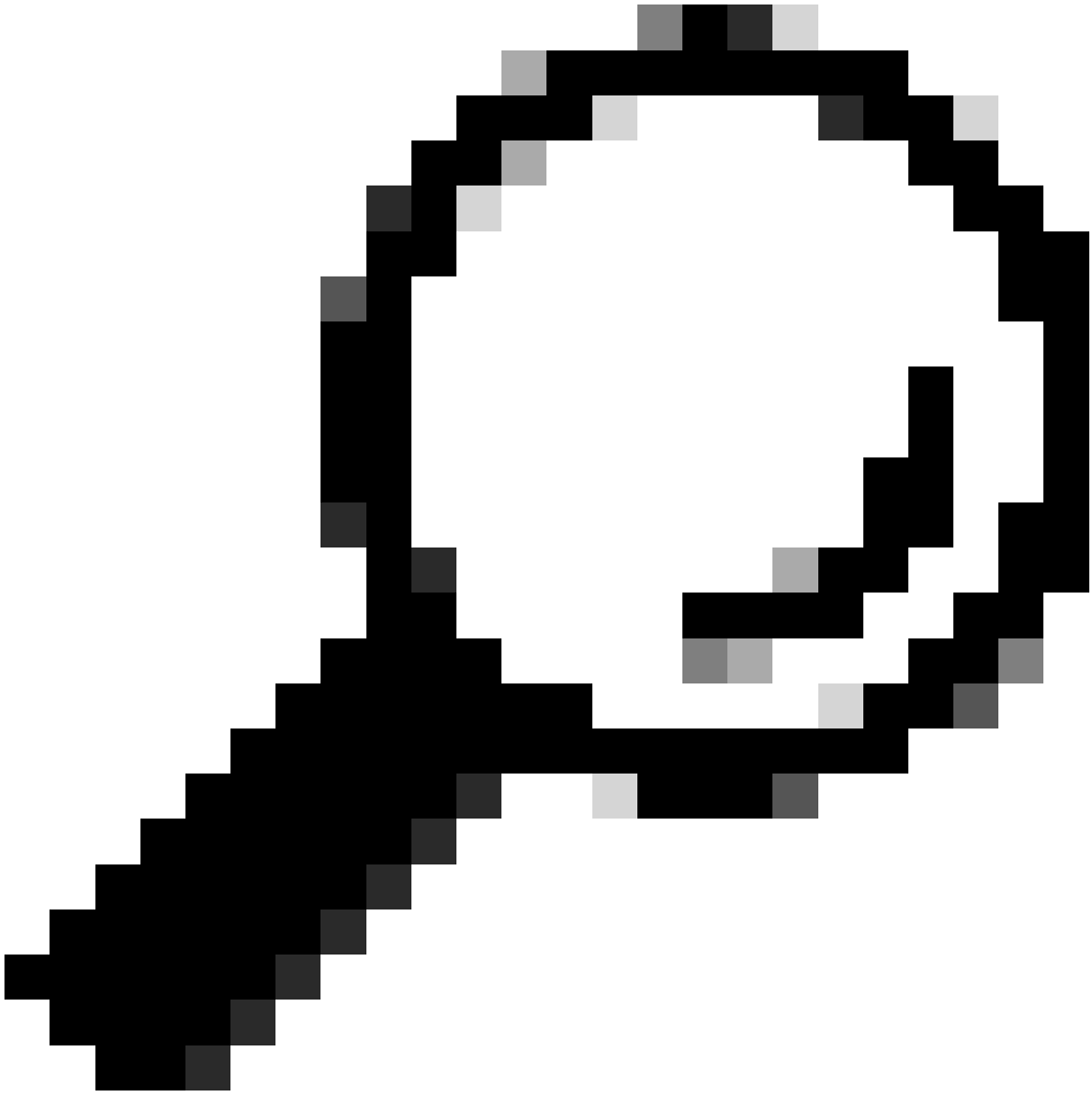


注意：diagnostic是CLI隐藏的命令，因此您无法使用TAB自动填充命令。

第三步：选择服务

第四步：选择要重新启动的服务/进程。

第五步：选择重新启动



提示：您可以从STATUS部分查看进程的状态。

在本示例中，已重新启动了负责GUI的WEBUI进程：

```
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
```

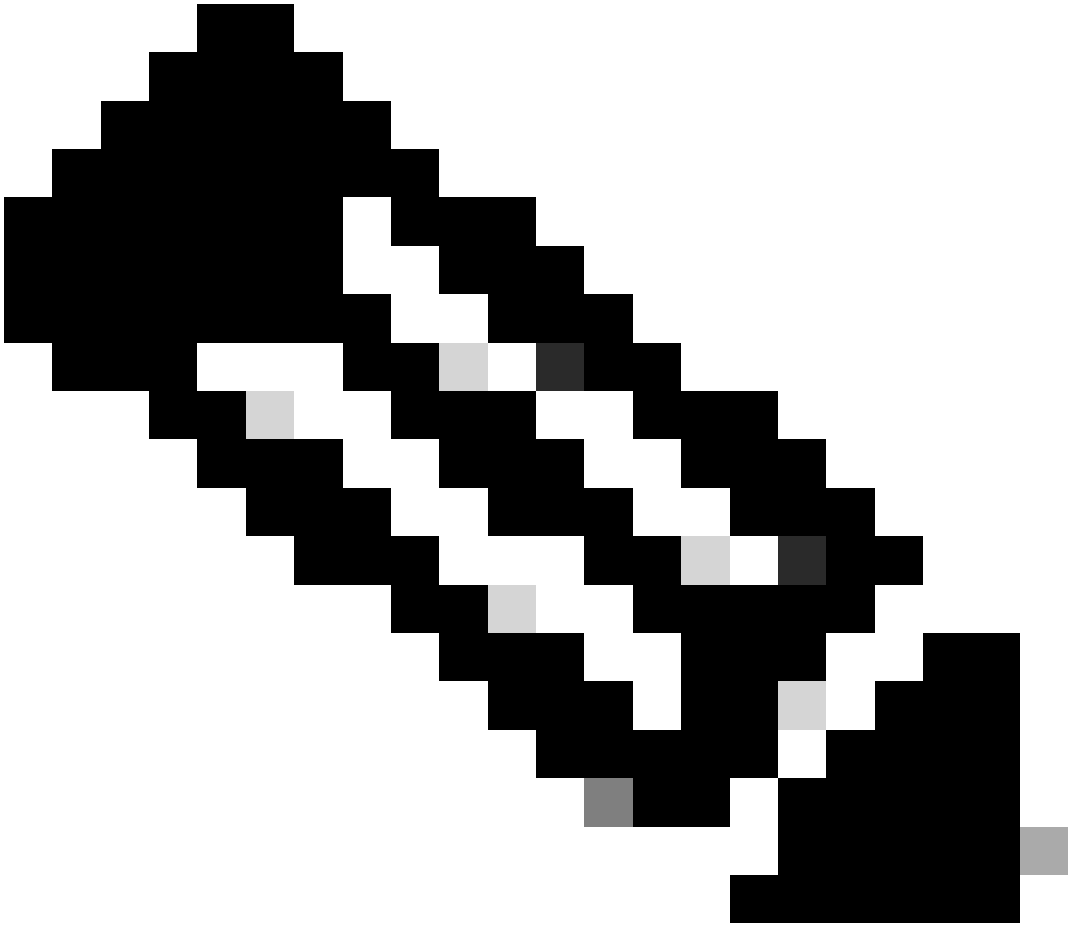
```
- ADC - ADC
- DCA - DCA
- WBRS - WBRS
- EXTFEED - ExtFeed
- L4TM - L4TM
- ANTIVIRUS - Anti-Virus xiServices
- AUTHENTICATION - Authentication Services
- MANAGEMENT - Appliance Management Services
- REPORTING - Reporting Associated services
- MISCSERVICES - Miscellaneous Service
- OCSP - OSCP
- UPDATER - 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.
```

重新启动代理进程

要重新启动代理进程（代理的主要进程），您可以使用CLI，步骤如下：

步骤1.登录CLI

第二步：类型诊断



注意：diagnostic是CLI隐藏的命令，因此您无法使用TAB自动填充命令。

第三步：选择代理

第四步：键入KICK，（它是一个隐藏命令）。

第五步：选择Y表示是。

```
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
```

相关信息

- 思科安全网络设备AsyncOS 15.0用户指南- LD（有限部署）-故障排除[思科安全网络设备] -思科
- 使用安全Web设备最佳实践-思科
- ps(1) (freebsd org)

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。