SWAでの異常なプロセス状態のトラブルシューティング

内容

はじめに

このドキュメントでは、プロセスステータスと、これを使用してSecure Web Appliance(SWA)のパフォーマンス問題をトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 物理または仮想SWAがインストールされている。
- ライセンスの有効化またはインストール
- セキュアシェル(SSH)クライアント。
- セットアップウィザードが完了しました。

- SWAへの管理アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

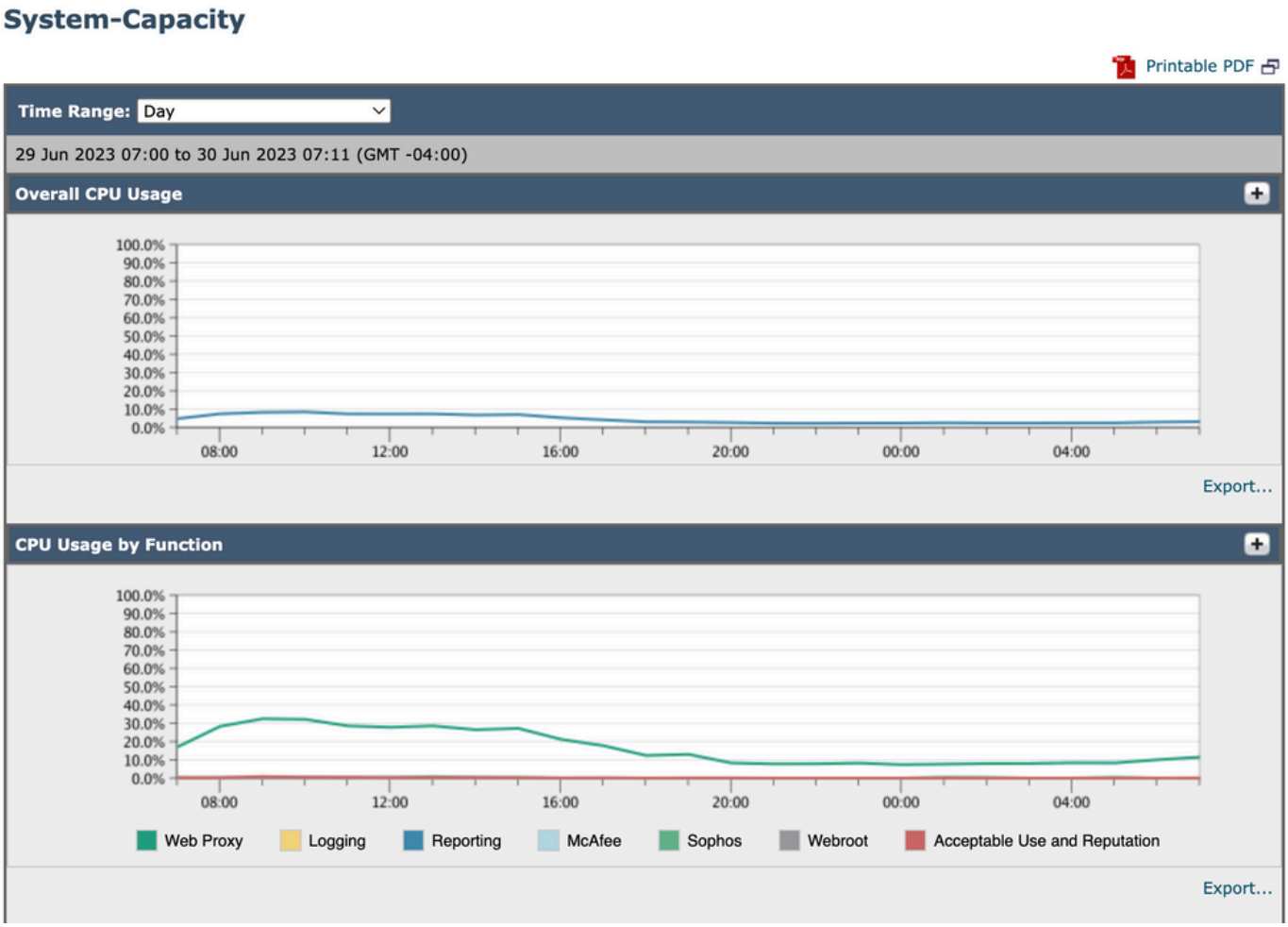
キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

プロセスステータスの監視

プロセス・ステータスは、GUI（グラフィカル・ユーザー・インタフェース）またはCLI（コマンド・ライン・インタフェース）から監視できます。

GUIからのプロセスステータスの表示

GUIでプロセスの統計情報を表示するには、Reportingに移動してSystem Capacityを選択します。[Time Range]を選択すると、目的のタイムスタンプのリソース割り当てを表示できます。

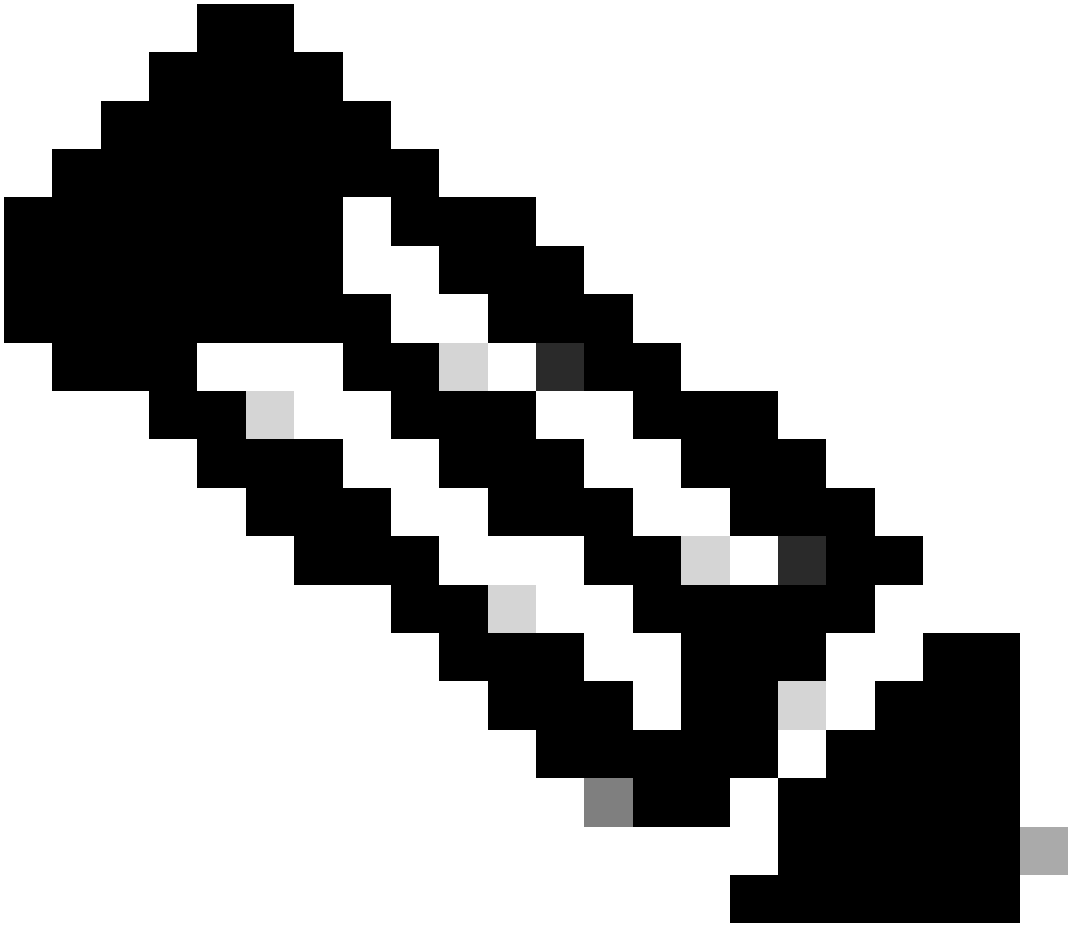


イメージシステムキャパシティ

Overall CPU Usage:合計CPU使用率の表示

機能別のCPU使用率：各サブプロセス、CPU割り当てを表示します。

プロキシバッファメモリ：プロキシプロセスのメモリ割り当てを表示します。



注：プロキシバッファメモリは、SWAの合計メモリ使用量ではありません。

CLI コマンド

メインCPU負荷またはサブプロセスのステータスを表示する複数のCLIコマンドがあります。

ステータス

statusまたはstatus detailの出力から、SWAの全体的なCPU使用率を確認できます。これらのコマンドは、現在のCPU負荷を示します。

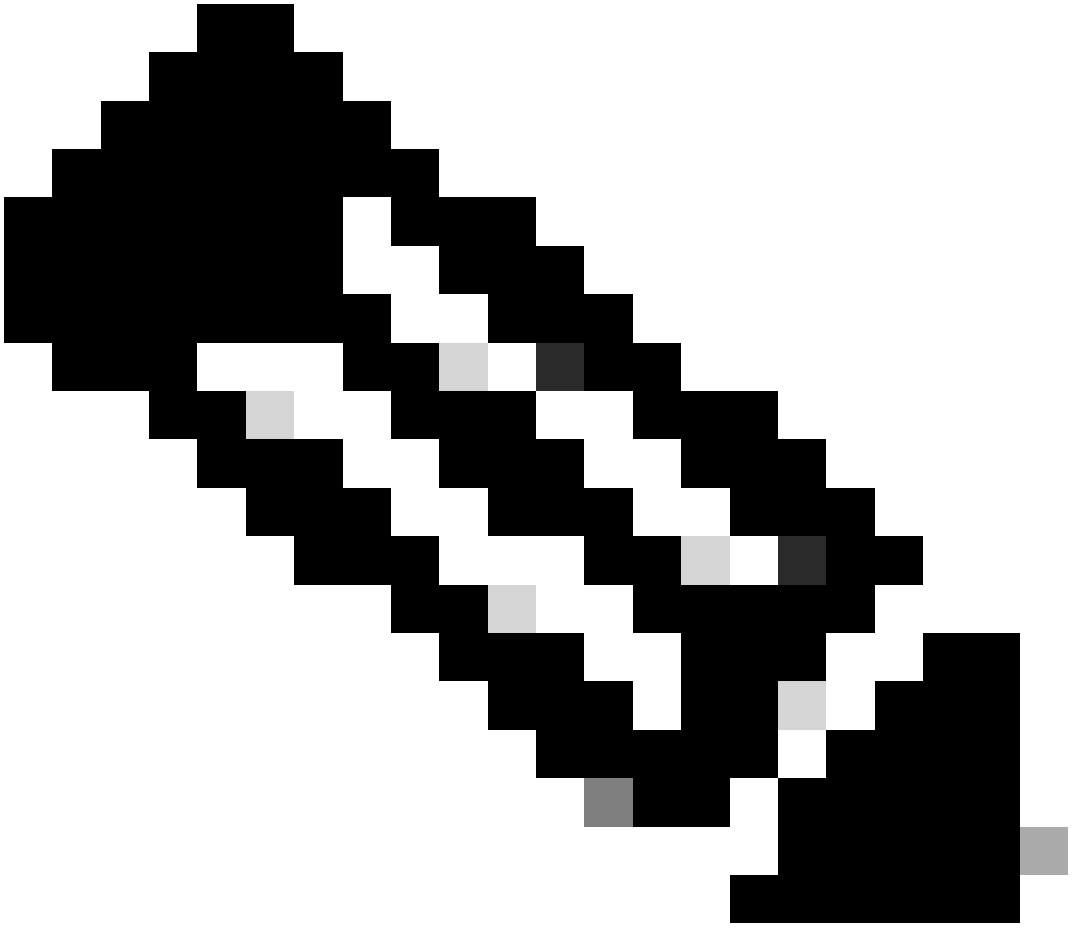
```
SWA_CLI)> status

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%
...
```

レート（プロキシスタット）

rate CLIコマンドを使用すると、プロキシプロセスの負荷が表示されます。これは、SWAのメインプロセスであるサブプロセスです。このコマンドは、15秒ごとに自動的に更新されます。

```
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:「proxystat」は、「rate」コマンドと同じ出力を持つ別のCLIコマンドです

---

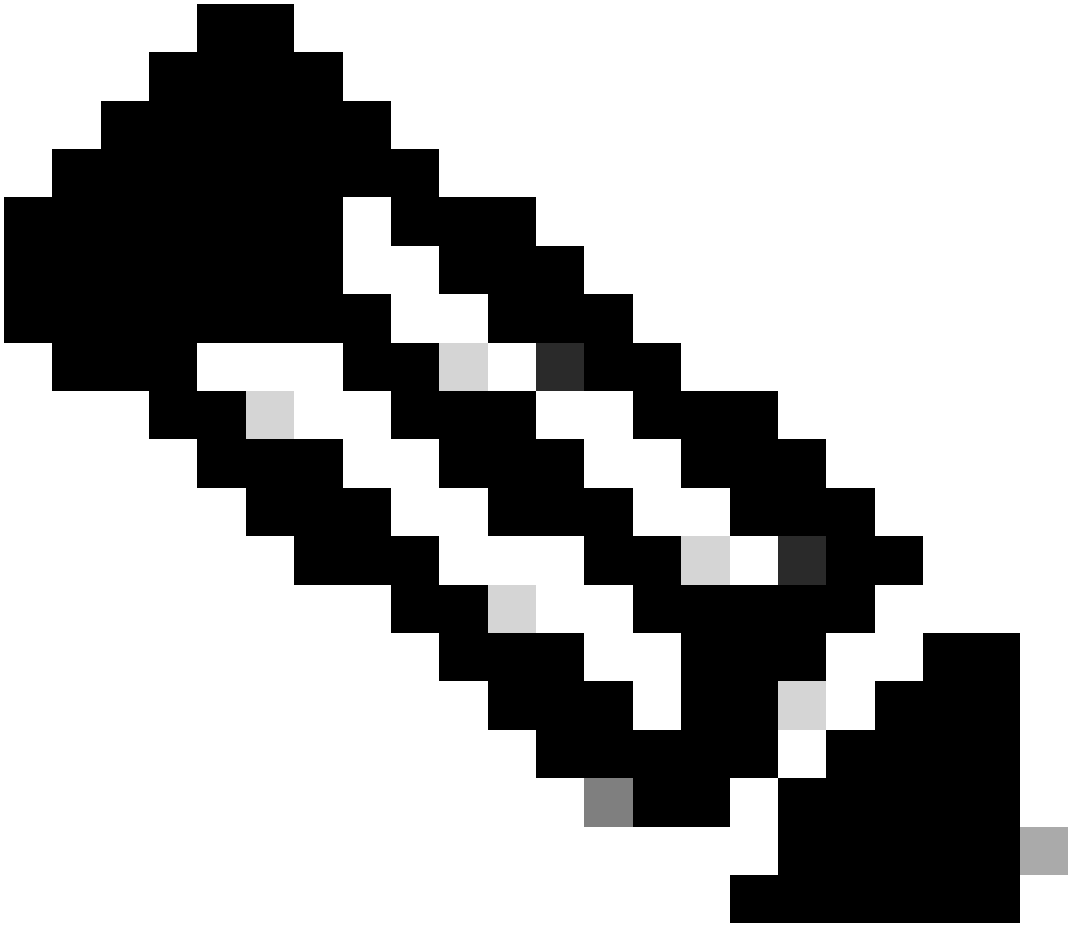
shd_logs

プロキシプロセスのステータスやレポートプロセスのステータスなどのメインプロセスのステータスは、SHD_Logsから表示できます。SHDログの詳細については、次のリンクを参照してください。

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

shd_logsの出力例を次に示します。

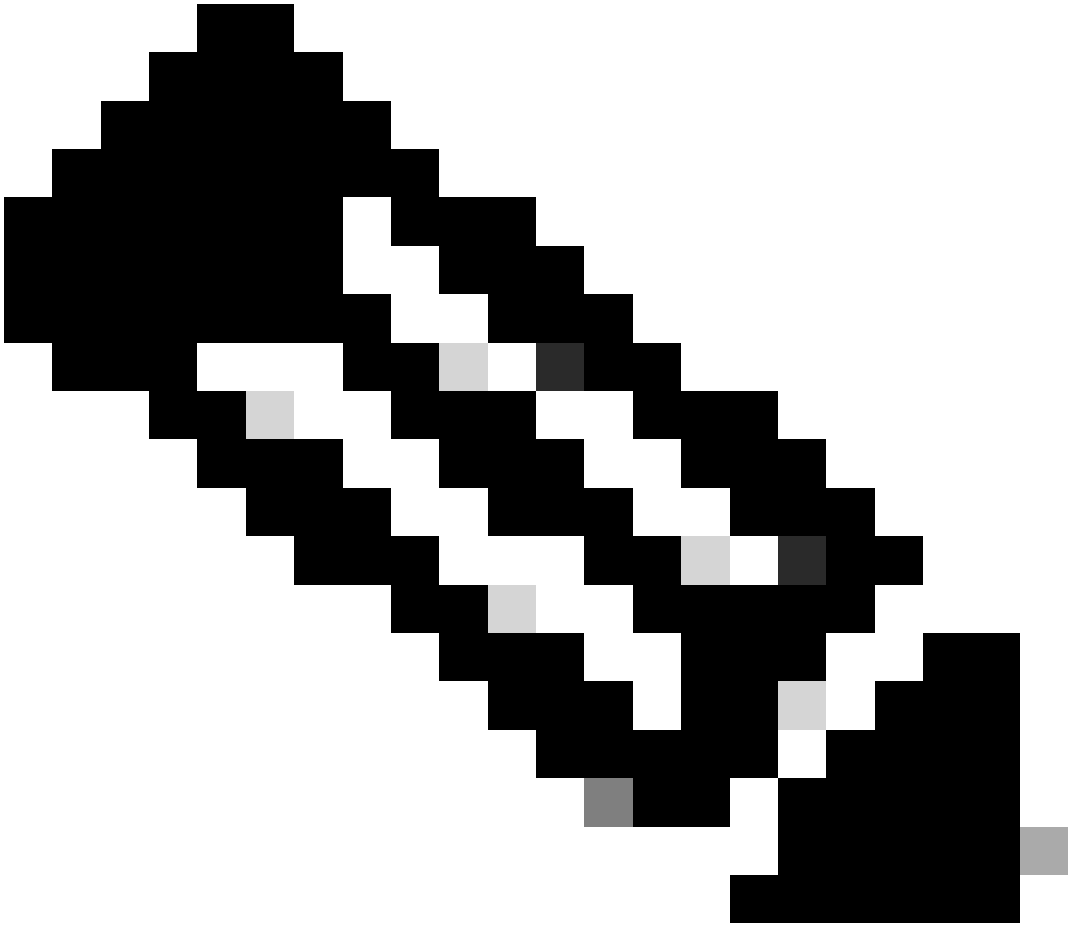
```
Sat Jun 24 06:30:29 2023 Info: Status: CPULd 2.9 DskUtil 14.4 RAMUtil 9.8 Reqs 112 Band 22081 Latency 4
```



注：shd_logsには、grepまたはtail CLIコマンドからアクセスできます。

プロセス_ステータス

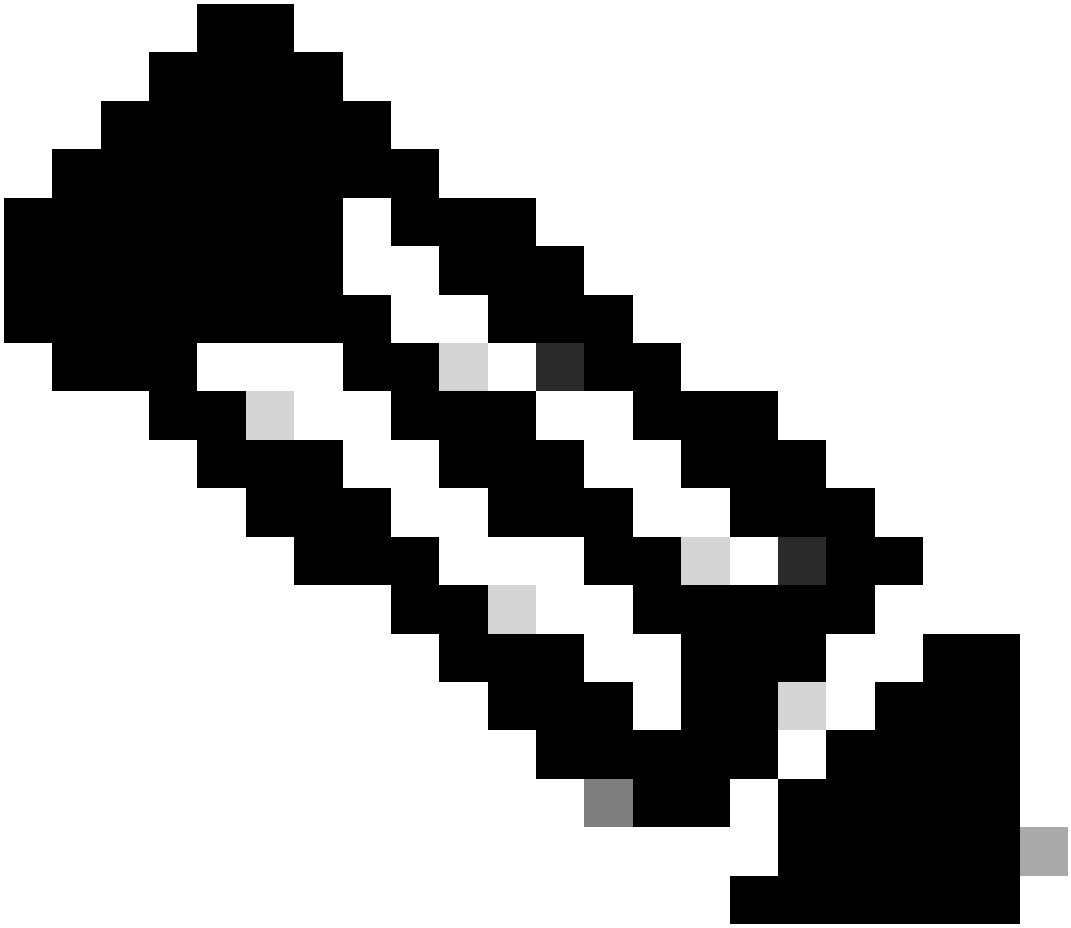
プロセスステータスを表示するために、バージョン14.5以降では、SWAに新しいコマンドprocess_statusがあります。このコマンドは、SWAのプロセスの詳細を取得します。



注：このコマンドは管理モードでのみ使用できます。

```
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：プロセスのCPU使用率。これは直前（リアルタイム）の1分間までの減衰平均です。これが計算される時間ベースは変化するため（プロセスが非常に若くなる可能性があるため）、すべての%CPUフィールドの合計が100%を超える可能性があります。

%MEM:このプロセスが使用する実メモリの割合

VSZ:仮想サイズ（Kバイト）（別名vsize）

RSS:プロセスの実メモリ（常駐セット）サイズ（1024バイト単位）。

TT:制御端末のパス名の省略形（存在する場合）。

STAT

統計情報は、「RNL」などの一連の文字によって示されます。最初の文字は、プロセスの実行状態を示します。

D:ディスク（またはその他の短期的な割り込み不可）待機のプロセスをマークします。

I:アイドル状態（約20秒より長くスリープ状態にある）のプロセスをマークします。

L:ロックの獲得を待機しているプロセスをマークします。

R:実行可能なプロセスをマークします。

S:約20秒未満スリープ状態のプロセスをマークします。

T:停止したプロセスをマークします。

W:アイドル状態の割り込みスレッドをマークします。

Z:デッドプロセス（「ゾンビ」）をマークします。

これらの後に追加の文字がある場合は、追加の状態情報を示します。

+:プロセスは、その制御端末のフォアグラウンドプロセスグループにあります。

<:プロセスによってCPUスケジューリングの優先度が上がっています。

C:プロセスはcapsicum(4)機能モードです。

E:プロセスを終了しようとしています。Jはjail(2)に含まれるプロセスをマークします。

L :プロセスのコアにロックされたページがある（raw I/Oなど）。

N：プロセスのCPUスケジューリングの優先度が低下している

s:プロセスはセッションリーダーです。

V：vfork(2)の間、プロセスの親プロセスは一時停止され、プロセスの実行または終了を待機します。

W:プロセスが交換されます。

X：プロセスはトレースまたはデバッグされています。

TIME:累積CPU時間、ユーザ+システム

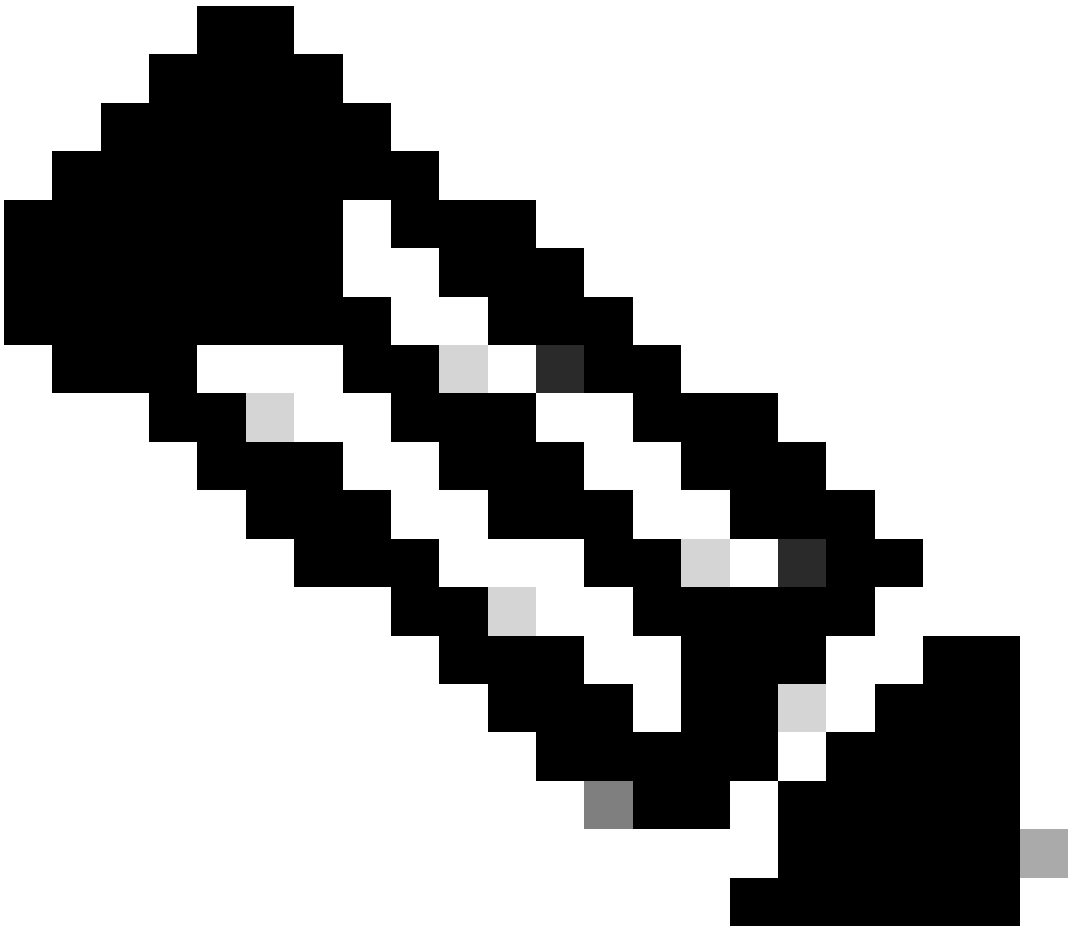
SWAでのプロセスの再起動

一般的なプロセス

CLIからSWAサービスとプロセスを再起動できます。次に手順を示します。

ステップ1:CLIにログインします。

ステップ 2：型診断

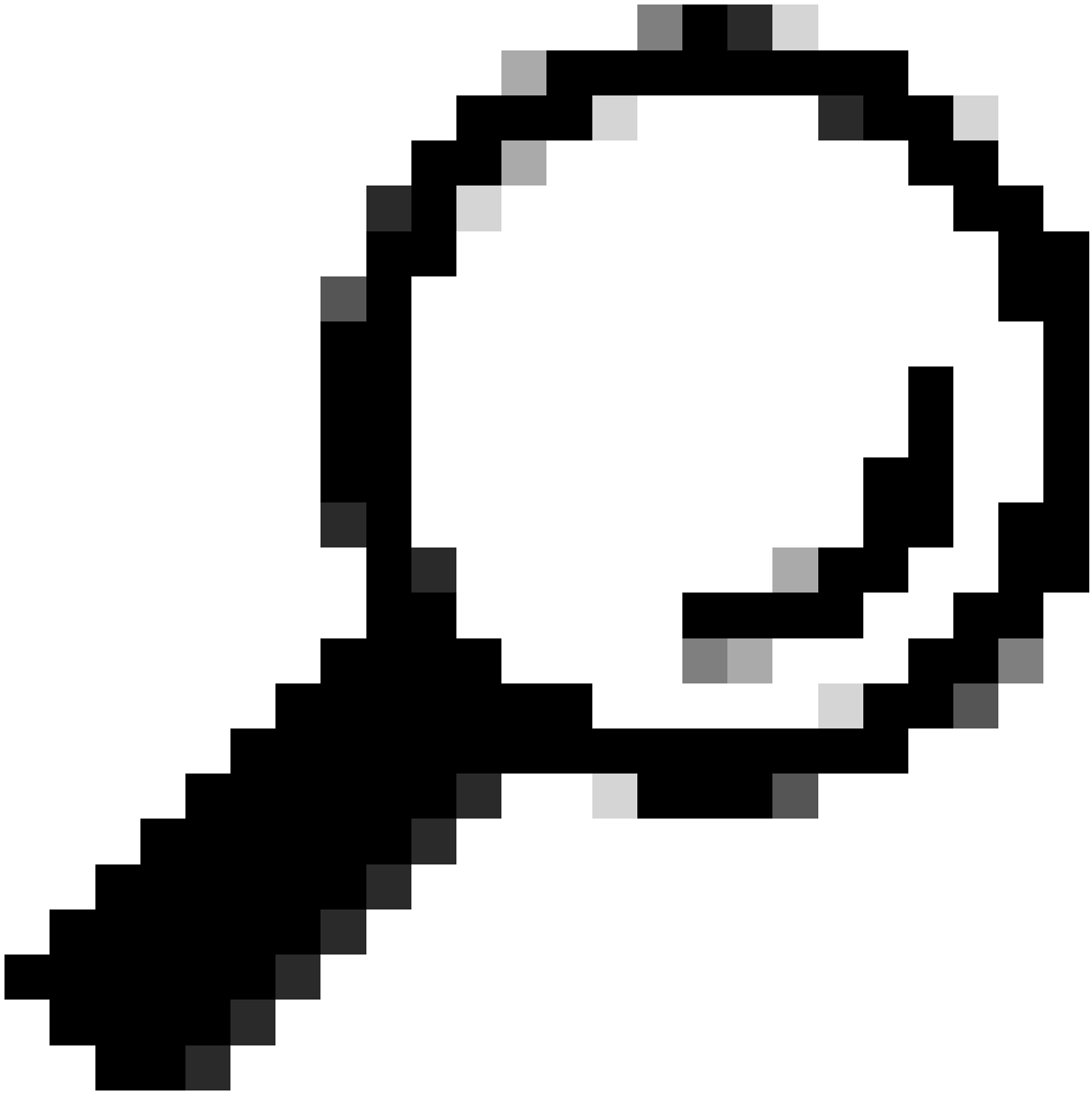


> 注：diagnosticはCLIの隠しコマンドであるため、このコマンドにTABを自動入力することはできません。

ステップ 3：サービスの選択

ステップ 4：再起動するサービス/プロセスを選択します。

ステップ 5：再起動を選択します



ヒント：プロセスのステータスは「ステータス」セクションで確認できます。

この例では、GUIに対して応答のあるWEBUIプロセスが再起動されています。

```
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
```

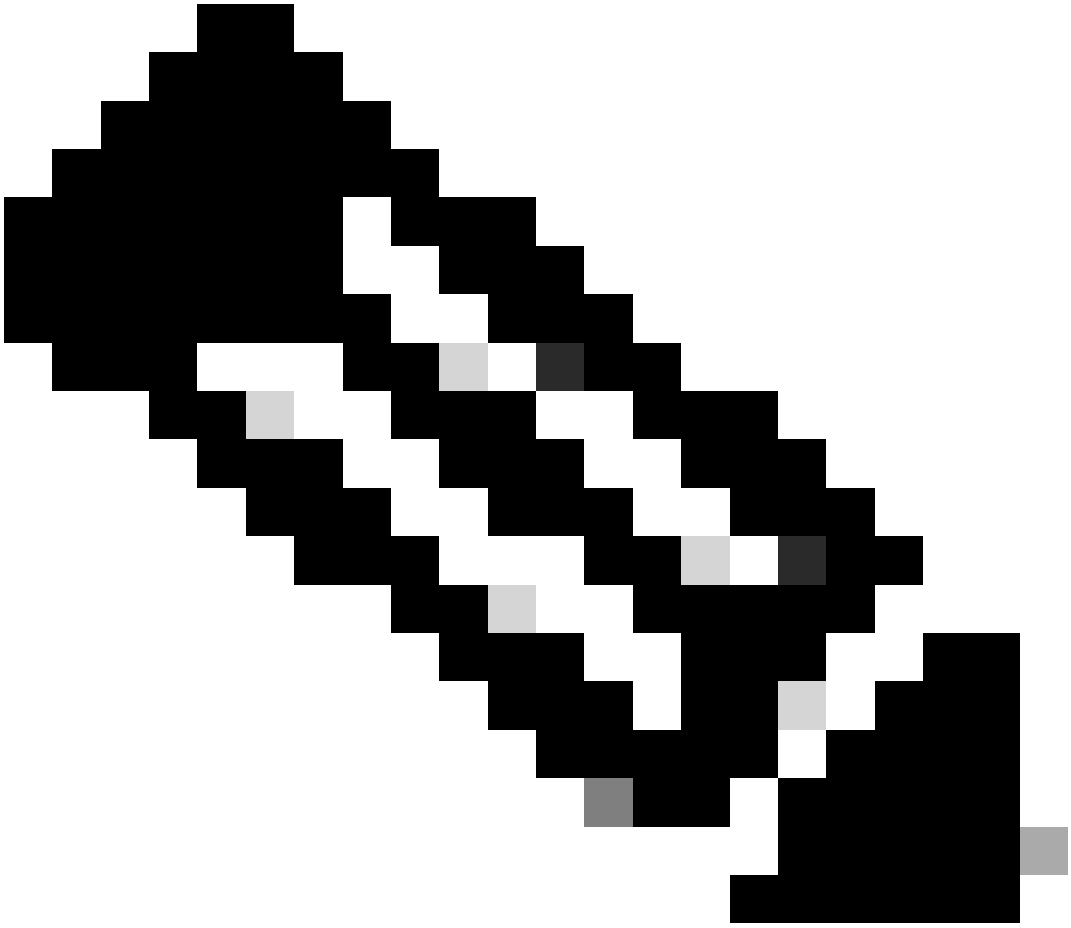
```
- ADC - ADC
- DCA - DCA
- WBRS - WBRS
- EXTFEED - ExtFeed
- L4TM - L4TM
- ANTIVIRUS - Anti-Virus xiServices
- AUTHENTICATION - Authentication Services
- MANAGEMENT - Appliance Management Services
- REPORTING - Reporting Associated services
- MISCSERVICES - Miscellaneous Service
- OCSP - OSCP
- UPDATER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

プロキシプロセスの再起動

プロキシのメインプロセスであるプロキシプロセスを再起動するには、次の手順でCLIを使用できます。

ステップ1:CLIにログインします。

ステップ 2：型診断



注：diagnosticはCLIの隠しコマンドであるため、このコマンドにTABを自動入力することはできません。

ステップ 3：プロキシの選択

ステップ 4：KICKと入力します（これは隠しコマンドです）。

ステップ 5：yesの場合はYを選択します。

```
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
```

関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – LD (限定導入) – トラブルシューティング[Cisco Secure Web Appliance] – シスコ
- セキュアなWebアプライアンスのベストプラクティスの使用：シスコ
- ps(1) (freebsd org)

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。