Fehlerbehebung bei ungewöhnlichen Prozesszuständen in SWA

Inhalt

Einleitung

Dieses Dokument beschreibt den Prozessstatus und dessen Verwendung zur Fehlerbehebung bei Problemen mit der Secure Web Appliance (SWA).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Installierte physische oder virtuelle SWA.
- Lizenz aktiviert oder installiert.
- Secure Shell (SSH)-Client.
- Der Setup-Assistent ist abgeschlossen.

- Administratorzugriff auf die SWA.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Prozessstatus überwachen

Sie können den Prozessstatus über die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) überwachen.

Prozessstatus über GUI anzeigen

Um Prozessstatistiken in der GUI anzuzeigen, navigieren Sie zu Reporting, und wählen Sie System Capacity (Systemkapazität). Sie können "Zeitbereich" auswählen, um die Ressourcenzuordnung für den gewünschten Zeitstempel anzuzeigen.

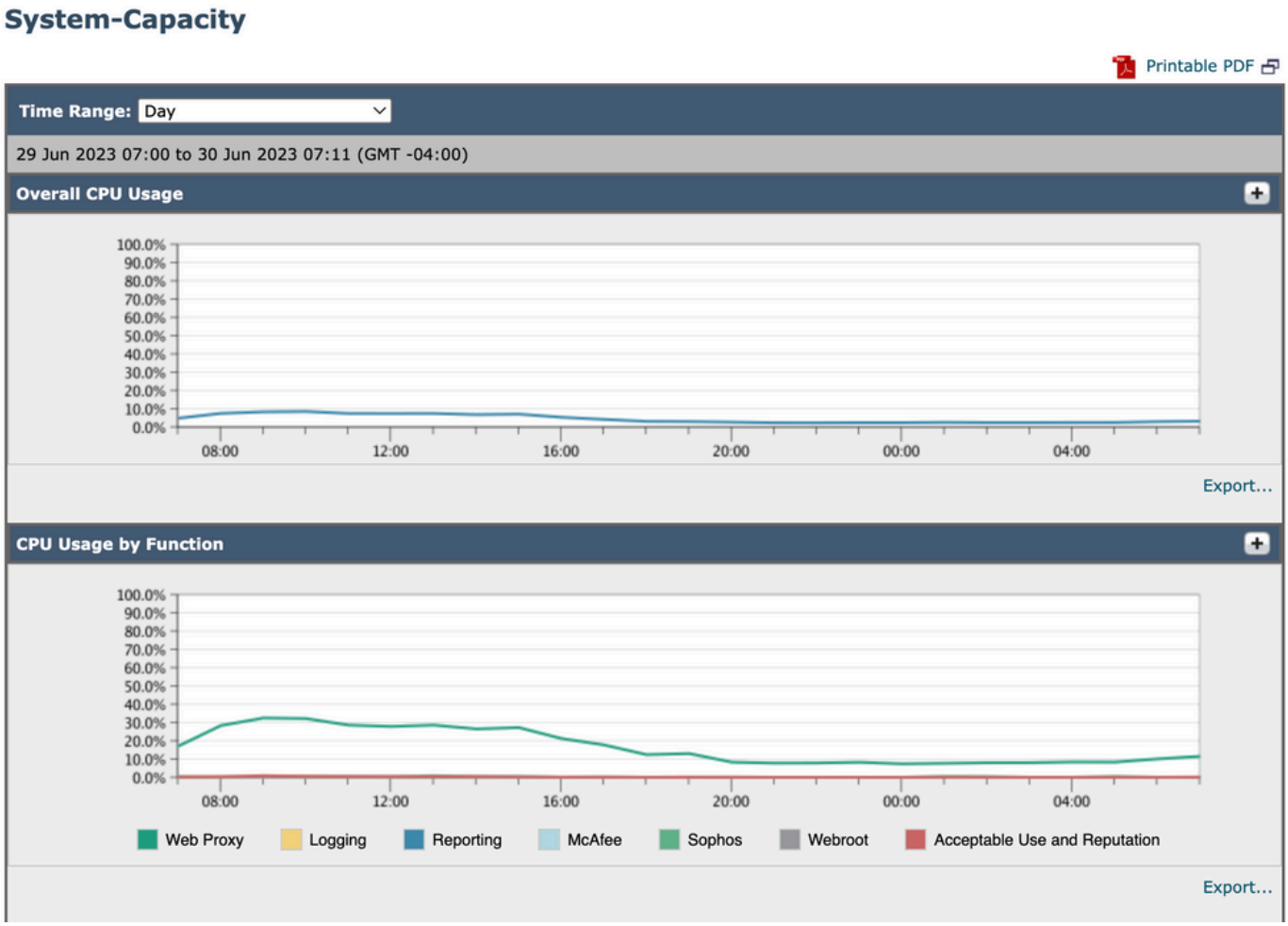
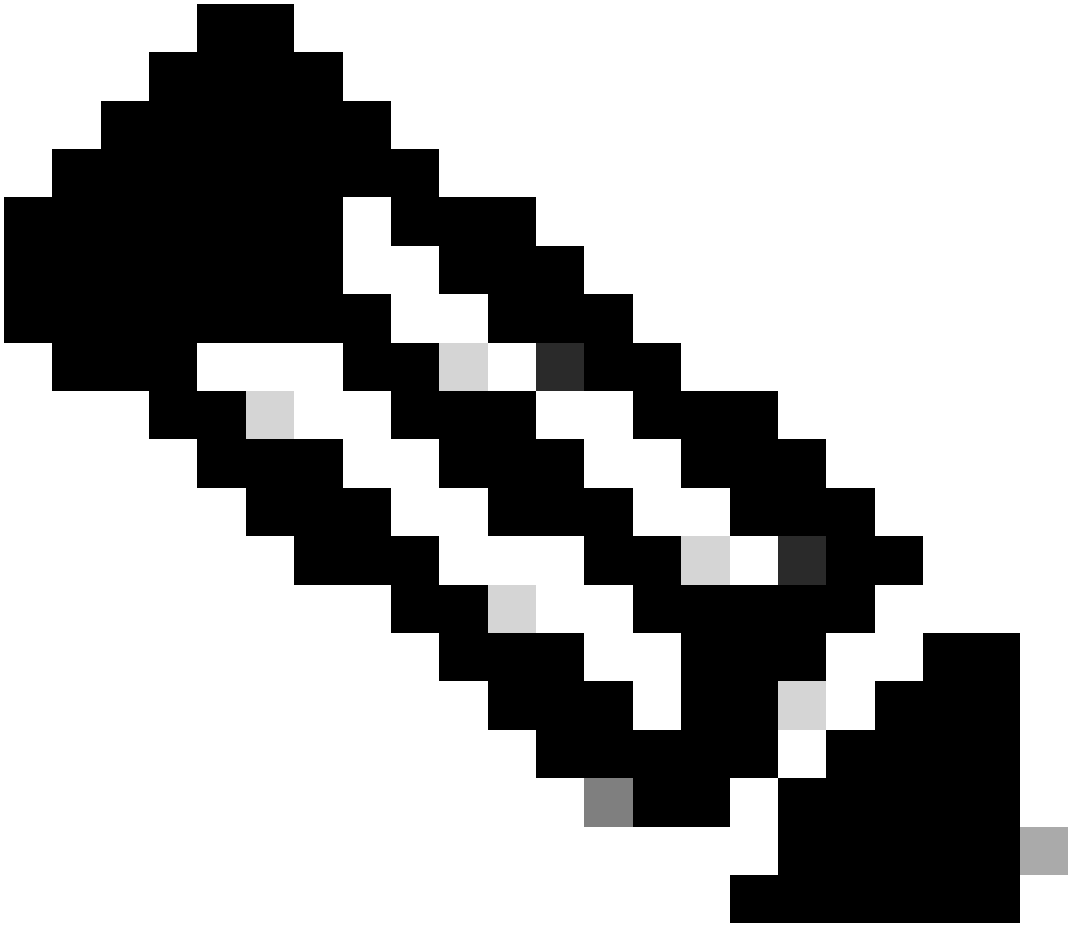


Image-System-Kapazität

CPU-Gesamtauslastung: Zeigt die CPU-Gesamtauslastung an

CPU-Nutzung nach Funktion: Zeigt jeden Unterprozess und die CPU-Zuweisung an.

Proxy-Pufferspeicher: Zeigt die Speicherzuordnung für den Proxyprozess an.



Hinweis: Der Proxy-Pufferspeicher entspricht nicht der Gesamtspeicherauslastung von SWA.

CLI-Befehle

Es gibt mehrere CLI-Befehle, die den Status der Haupt-CPU-Last oder des Unterprozesses anzeigen:

status

Aus der Ausgabe von Status- oder Statusdetails können Sie die Gesamt-CPU-Auslastung von SWA anzeigen. Diese Befehle zeigen die aktuelle CPU-Auslastung an.

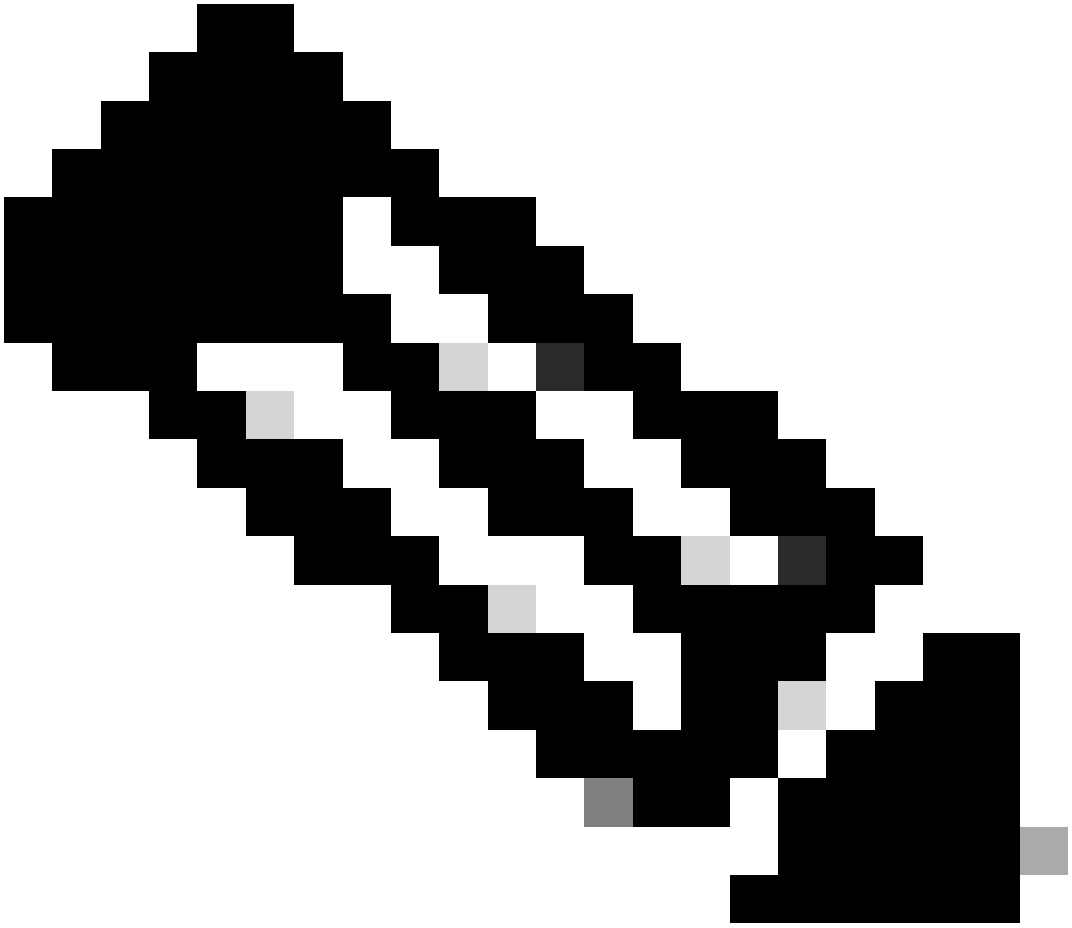
```
SWA_CLI)> status

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%
...
```

Rate (Proxystat)

rate CLI-Befehl, zeigt die Proxy-Prozesslast an. Hierbei handelt es sich um einen untergeordneten Prozess, der den Hauptprozess in SWA darstellt. Dieser Befehl wird automatisch alle 15 Sekunden aktualisiert.

```
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
```



Hinweis: "proxystat" ist ein weiterer CLI-Befehl, der dieselbe Ausgabe wie der Befehl "rate" hat.

---

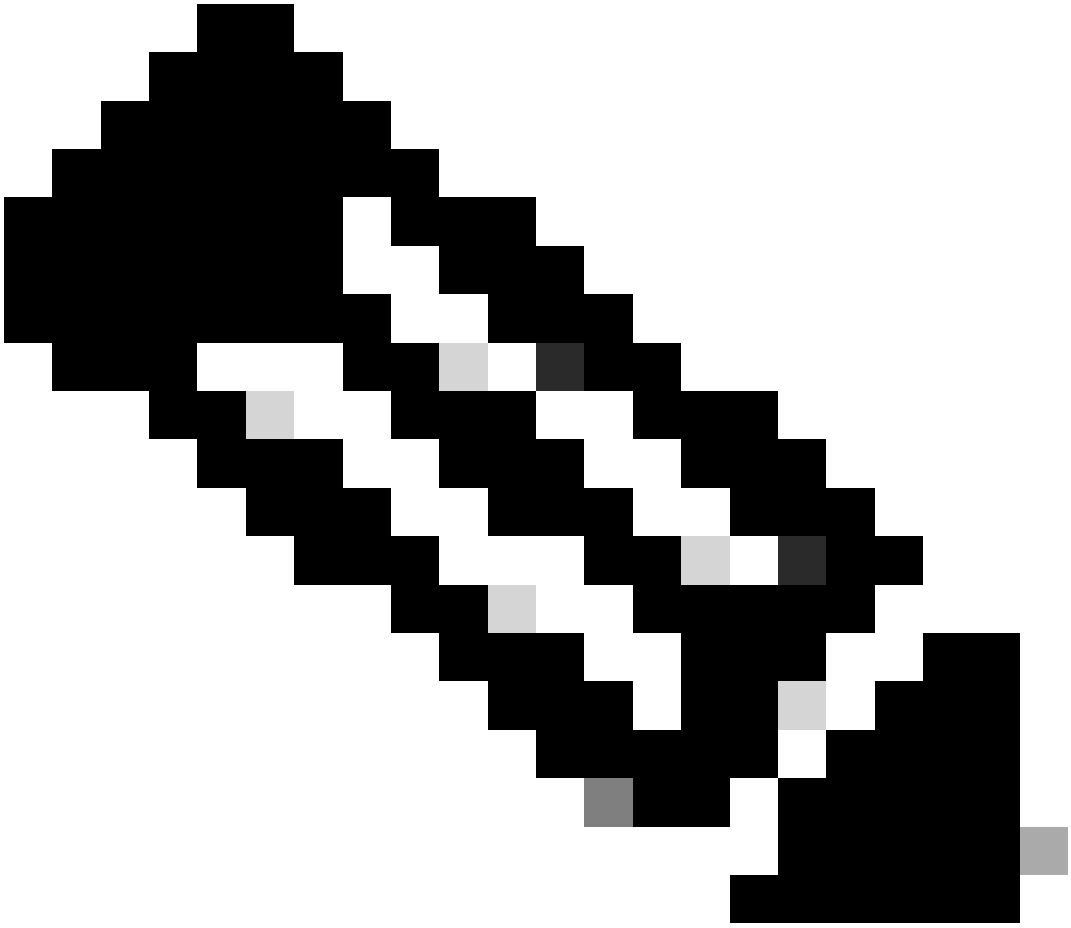
shd_logs

Sie können den Status des Hauptprozesses wie den Proxyprozessstatus, den Status des Berichtsprozesses usw. in SHD_Logs anzeigen. Weitere Informationen zu SHD-Protokollen finden Sie unter diesem Link:

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

Hier ist ein Beispiel für die Ausgabe von shd_logs:

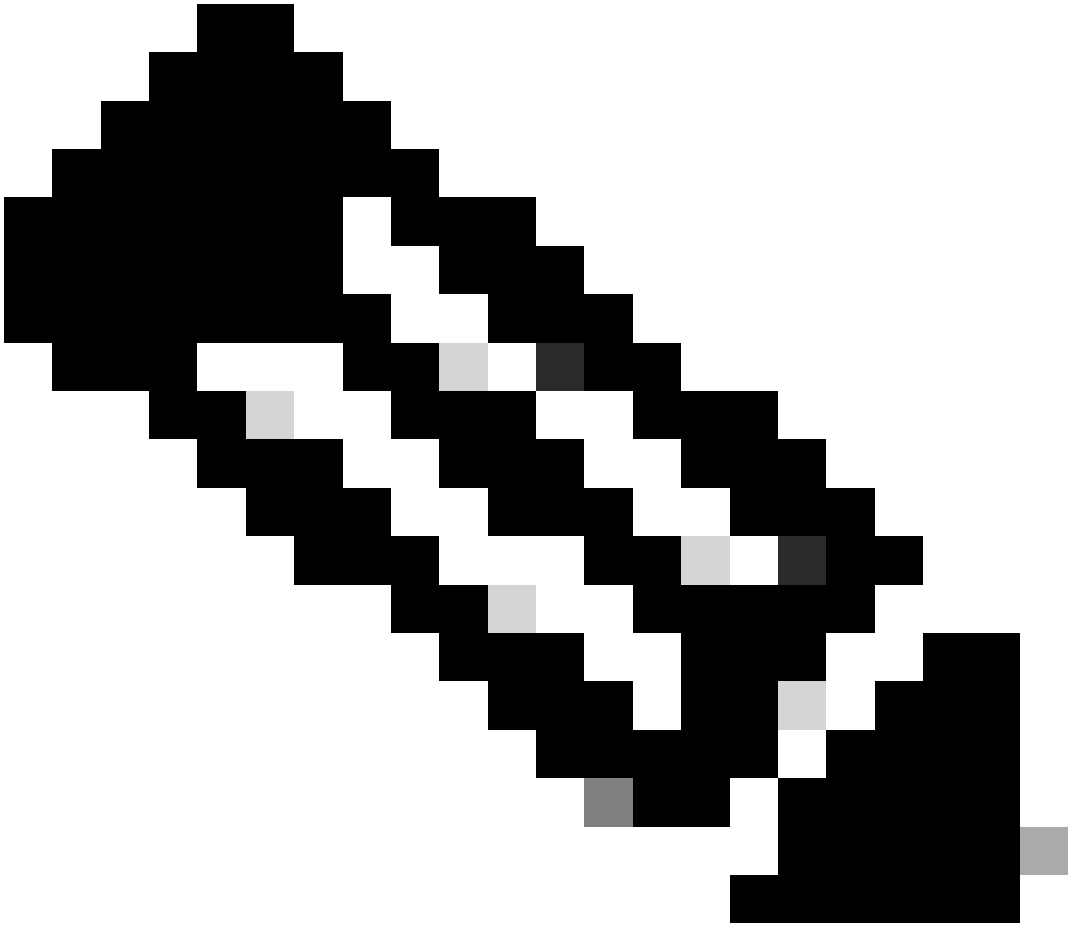
```
Sat Jun 24 06:30:29 2023 Info: Status: CPULd 2.9 DskUtil 14.4 RAMUtil 9.8 Reqs 112 Band 22081 Latency 4
```



Hinweis: Sie können shd_logs über den CLI-Befehl grep oder tail aufrufen.

Status des Prozesses

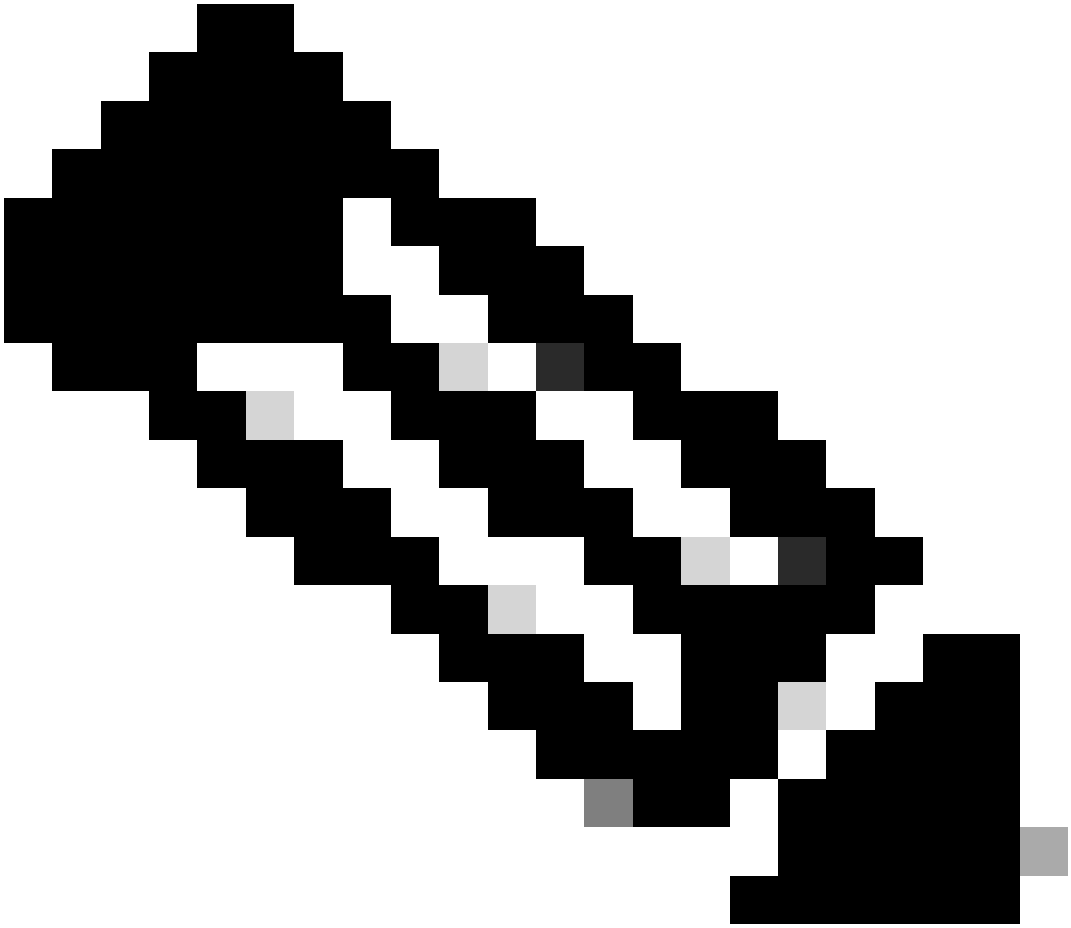
Zum Anzeigen des Prozessstatus in Version 14.5 und höher verfügt SWA über den neuen Befehl process_status, mit dem die Prozessdetails von SWA abgerufen werden.



Hinweis: Dieser Befehl ist nur im Admin-Modus verfügbar.

```
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
```



Hinweis: Die CPU-Auslastung des Prozesses. Dies ist ein abnehmender Durchschnitt über eine Minute der vorherigen (Echtzeit). Da die Zeitbasis, über die diese berechnet wird, variiert (da Prozesse sehr jung sein können), kann die Summe aller %CPU-Felder 100% überschreiten.

%MEM : Der von diesem Prozess verwendete Prozentsatz des realen Speichers

VSZ: Virtuelle Größe in KB (Alias vsize)

RSS : Die reale Speichergröße (Resident Set) des Prozesses (in 1024 Byte Einheiten).

TT : Eine Abkürzung für den Pfadnamen des steuernden Terminals, falls vorhanden.

STAT

Der Zustand ist durch eine Folge von Zeichen gegeben, z.B. "RNL". Das erste Zeichen gibt den Ausführungsstatus des Prozesses an:

D : Markiert einen Prozess auf der Festplatte (oder auf andere kurzfristige, nicht unterbrechbare Weise) warten.

I : Markiert einen Prozess, der ungenutzt ist (länger als etwa 20 Sekunden schlafend).

L : Markiert einen Prozess, der darauf wartet, eine Sperre zu erhalten.

R : Markiert einen ausführbaren Prozess.

S : Markiert einen Prozess, der weniger als etwa 20 Sekunden im Ruhezustand ist.

T: Markiert einen angehaltenen Prozess.

W : Markiert einen inaktiven Interrupt-Thread.

Z : Markiert einen toten Prozess (ein "Zombie").

Zusätzliche Zeichen nach diesen, sofern vorhanden, geben zusätzliche Statusinformationen an:

+ : Der Prozess befindet sich in der Vordergrundprozessgruppe seines Control-Terminals.

< : Der Prozess hat die CPU-Planungspriorität erhöht.

C : Der Prozess befindet sich im Capsicum(4)-Funktionsmodus.

E : Der Vorgang wird beendet. J Markiert einen Prozess, der sich im Gefängnis befindet(2).

L : Der Prozess hat Seiten, die im Kern gesperrt sind (z. B. für unformatierte E/A).

N : Der Prozess hat die CPU-Planungspriorität reduziert.

s : Der Prozess ist ein Sitzungsleiter.

V : Das übergeordnete Element des Prozesses wird während eines vfork(2)-Vorgangs angehalten und wartet darauf, dass der Prozess ausgeführt oder beendet wird.

W : Der Prozess ist ausgetauscht.

X : Der Prozess wird verfolgt oder gedebuggt.

ZEIT: Gesamte CPU-Zeit, Benutzer + System

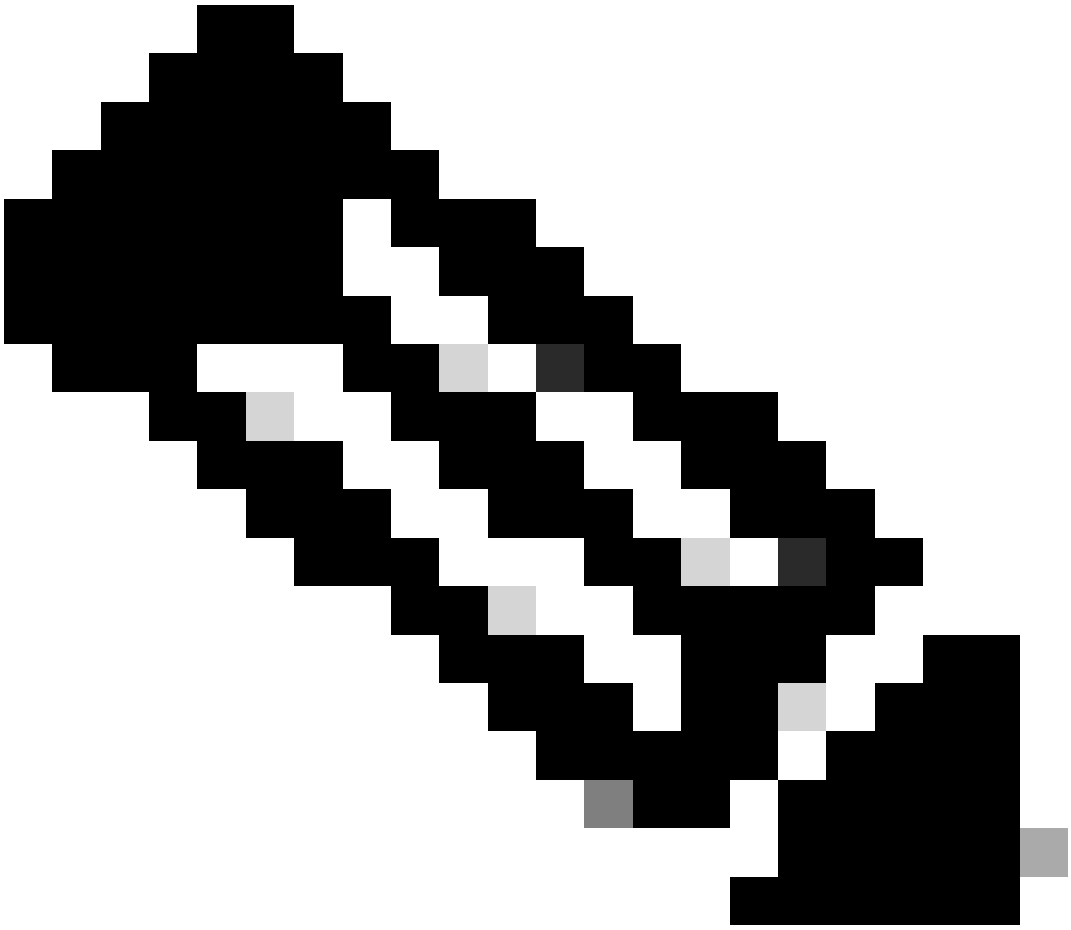
Neustartprozess in SWA

Allgemeiner Prozess

Sie können die SWA-Services neu starten und den Prozess über die CLI starten. Dies sind die Schritte:

Schritt 1: Anmeldung bei CLI

Schritt 2: Typdiagnose

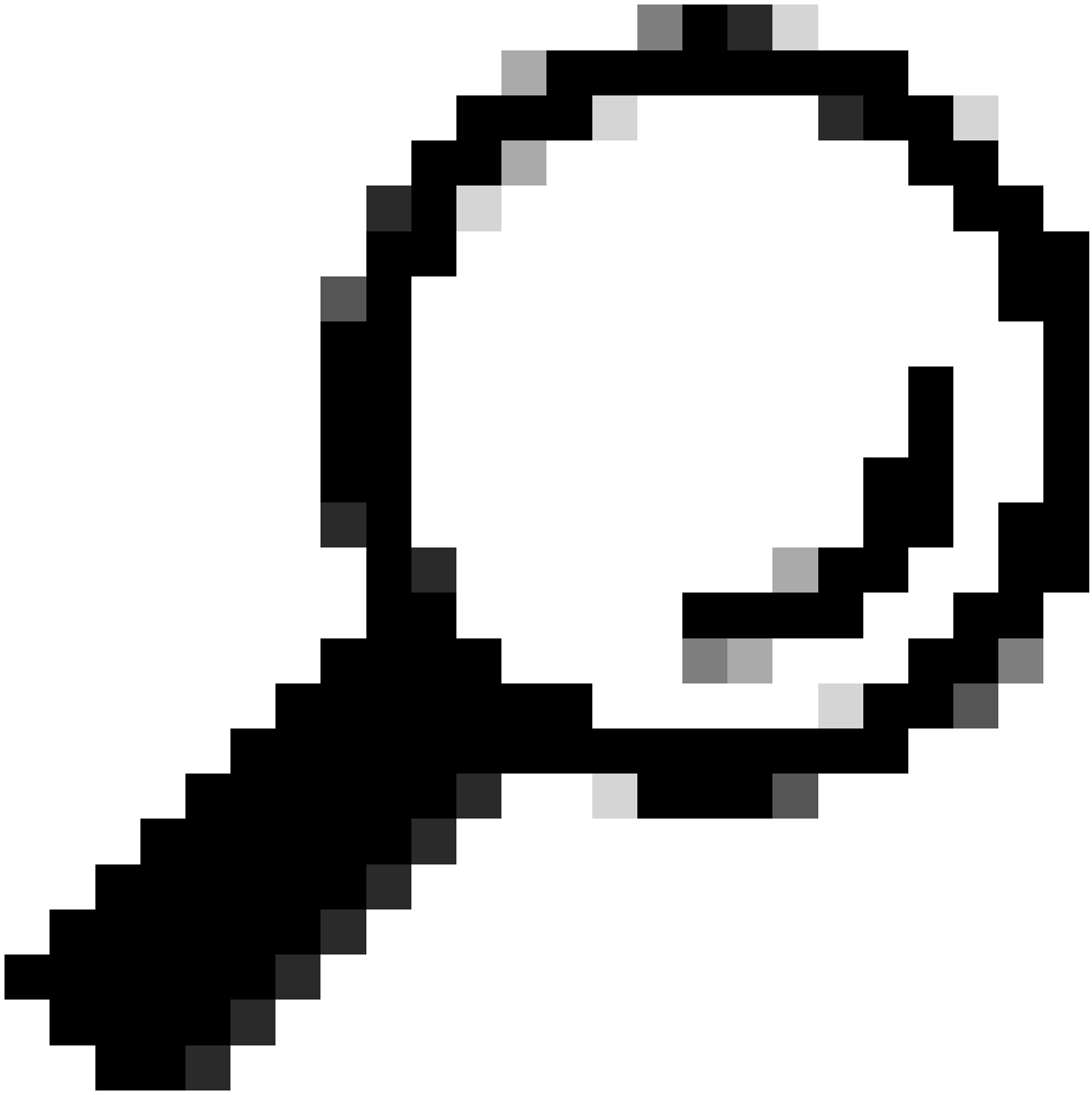


> Hinweis: Die Diagnose ist ein ausgeblendeter CLI-Befehl, daher können Sie den Befehl nicht automatisch mit TAB ausfüllen.

Schritt 3: Services auswählen

Schritt 4: Wählen Sie den Dienst/Prozess aus, den Sie neu starten möchten.

Schritt 5: Neustart auswählen



Tipp: Sie können den Status des Prozesses im Abschnitt STATUS anzeigen.

In diesem Beispiel wurde der WEBUI-Prozess, der für die GUI zuständig ist, neu gestartet:

```
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
```

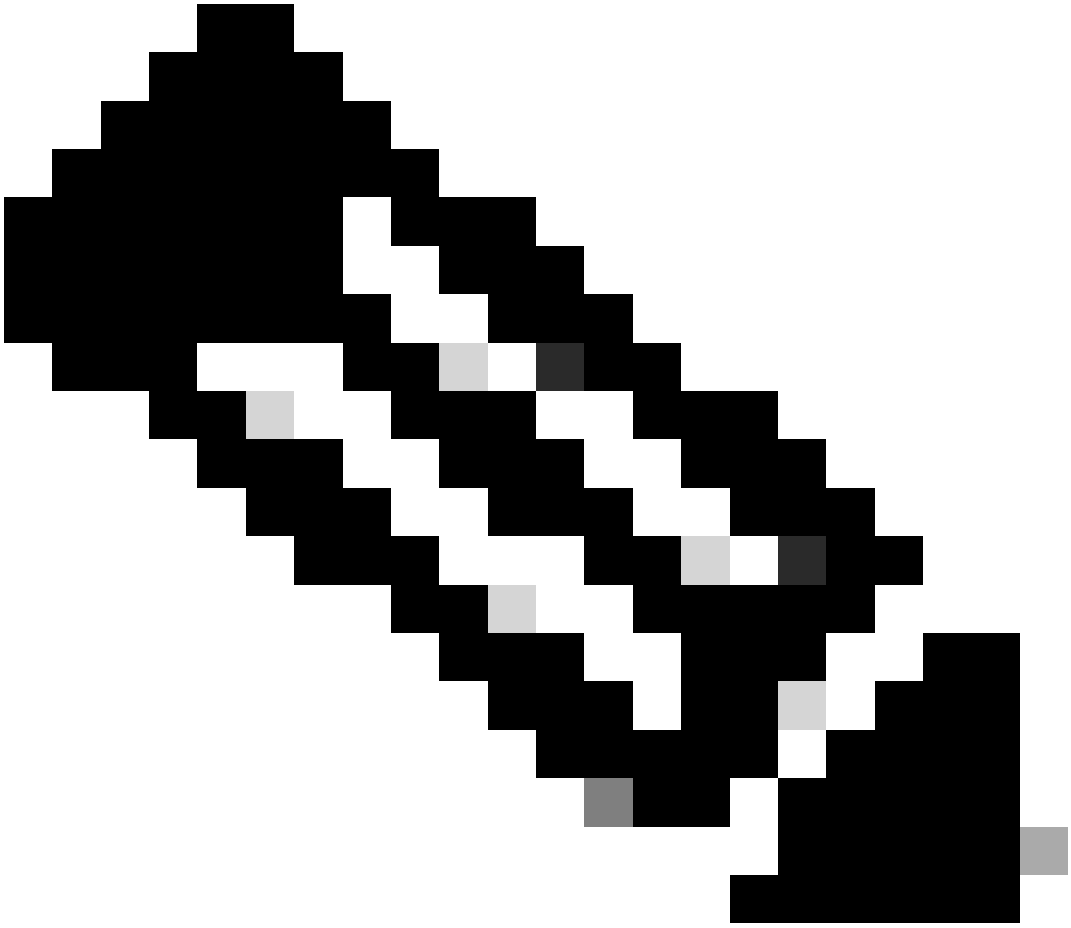
```
Choose one of the following services:
- AMP - Secure Endpoint
- AVC - AVC
- ADC - ADC
- DCA - DCA
- WBRS - WBRS
- EXTFEED - ExtFeed
- L4TM - L4TM
- ANTIVIRUS - Anti-Virus xiServices
- AUTHENTICATION - Authentication Services
- MANAGEMENT - Appliance Management Services
- REPORTING - Reporting Associated 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.
```

Proxy-Prozess neu starten

Um den Proxy-Prozess neu zu starten, der der Hauptprozess für den Proxy ist, können Sie CLI verwenden. Gehen Sie wie folgt vor:

Schritt 1: Anmeldung bei CLI

Schritt 2: Typdiagnose



Hinweis: Die Diagnose ist ein ausgeblendeter CLI-Befehl, daher können Sie den Befehl nicht automatisch mit TAB ausfüllen.

Schritt 3: PROXY auswählen

Schritt 4: Geben Sie KICK ein (dies ist ein ausgeblendeter Befehl).

Schritt 5: Wählen Sie Y für Ja aus.

```
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
```

Zugehörige Informationen

- Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - LD (begrenzte Bereitstellung) - Fehlerbehebung [Cisco Secure Web Appliance] - Cisco
- Best Practices für sichere Web-Appliances - Cisco
- ps(1) (freebsd org)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.