

Risoluzione dei problemi relativi agli stati di processo insoliti in SWA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Controlla stato processo](#)

[Visualizzazione dello stato del processo dalla GUI](#)

[Comandi CLI](#)

[stato](#)

[rate \(proxystat\)](#)

[log_shd](#)

[stato_processo](#)

[Riavvia processo in SWA](#)

[Processo generale](#)

Introduzione

In questo documento viene descritto lo stato del processo e viene spiegato come utilizzarlo per risolvere i problemi relativi a Secure Web Appliance (SWA) e prestazioni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Client Secure Shell (SSH).
- Installazione guidata completata.

- Accesso amministrativo all'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

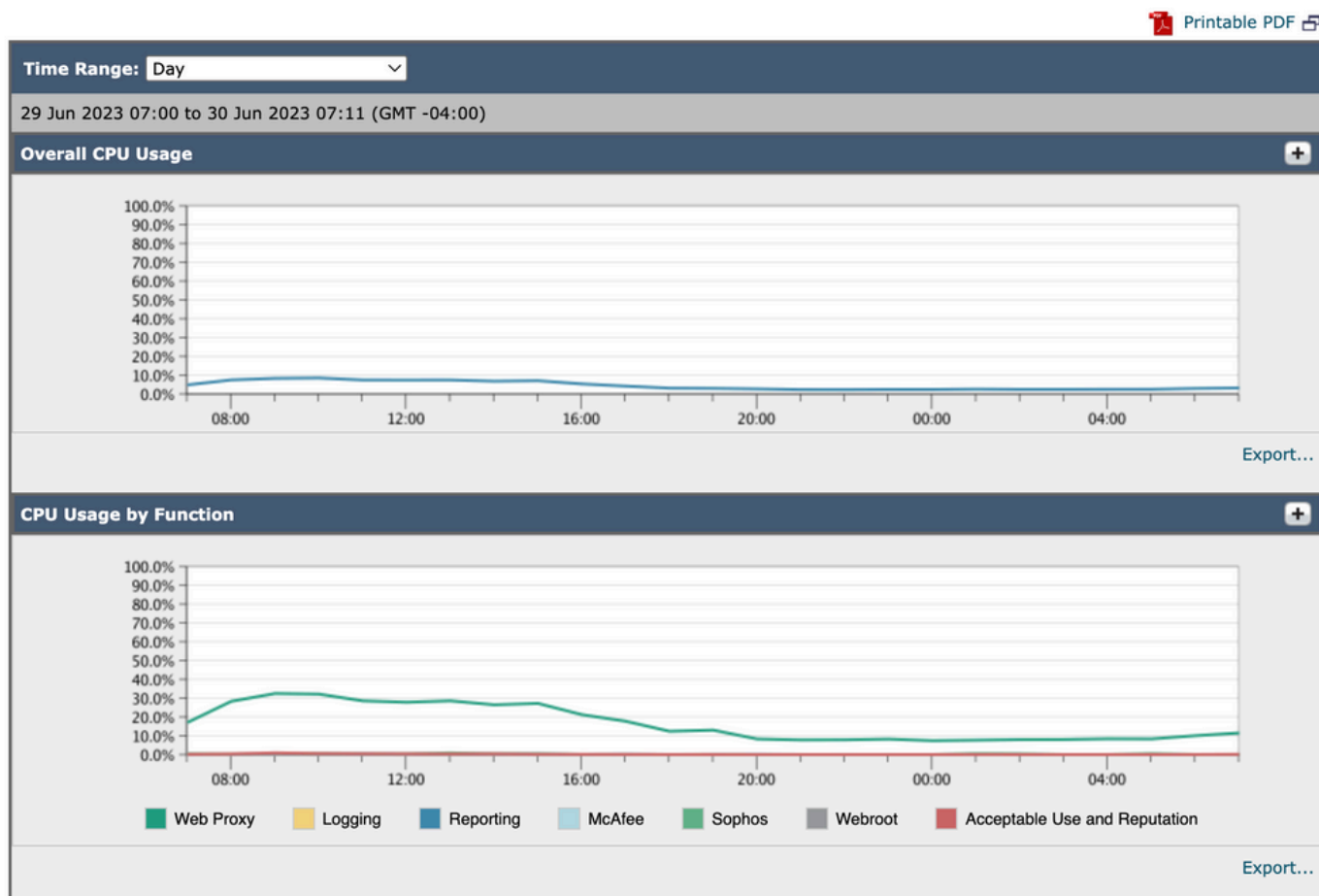
Controlla stato processo

È possibile monitorare lo stato del processo dall'interfaccia grafica dell'utente (GUI) o dall'interfaccia della riga di comando (CLI).

Visualizzazione dello stato del processo dalla GUI

Per visualizzare le statistiche di processo nella GUI, passare a Reporting e scegliere Capacità sistema. È possibile selezionare Intervallo di tempo per visualizzare l'allocazione delle risorse per l'indicatore di data e ora desiderato.

System-Capacity



Capacità-Immagine-Sistema

Utilizzo CPU complessivo: visualizza l'utilizzo totale della CPU

Utilizzo CPU per funzione: visualizza ogni sottoprocesso, allocazione CPU.

Memoria buffer proxy: visualizza l'allocazione di memoria per il processo proxy.

Nota: la memoria buffer proxy non è l'utilizzo totale di memoria di SWA.

Comandi CLI

Sono disponibili più comandi CLI che mostrano il carico della CPU principale o lo stato dei sottoprocessi:

stato

Dall'output dello stato o dei dettagli sullo stato, è possibile visualizzare l'utilizzo complessivo della CPU dell'interfaccia SWA. Questi comandi mostrano il carico corrente della CPU.

```
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, mostra il caricamento del processo proxy, un sottoprocesso che è il processo principale in SWA. Questo comando viene aggiornato automaticamente ogni 15 secondi.

```
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



Nota: "proxystat" è un altro comando CLI che ha lo stesso output del comando "rate"

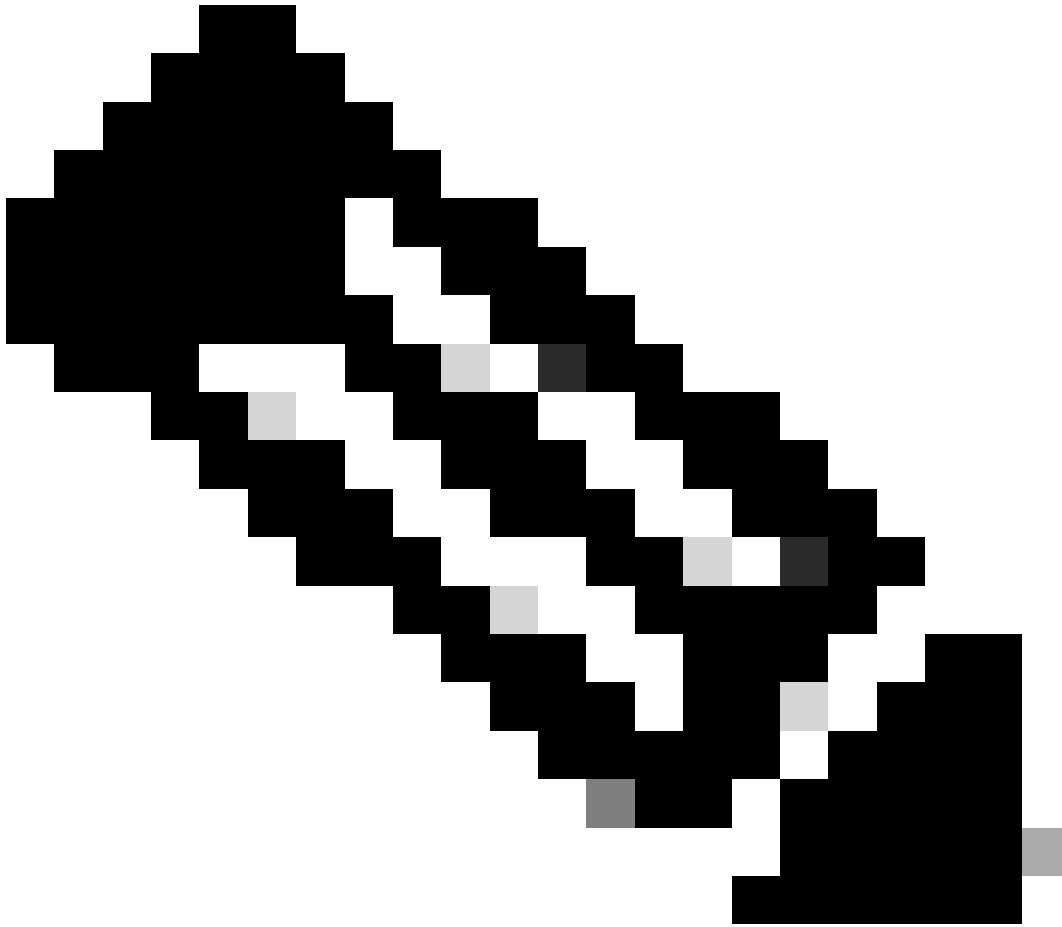
log_shd

Da SHD_Logs è possibile visualizzare lo stato del processo principale, ad esempio lo stato del processo proxy, lo stato del processo di reporting e così via. Per ulteriori informazioni sui registri SHD, visitare questo collegamento:

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

Di seguito è riportato un esempio di output di 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



Nota: è possibile accedere a shd_logs dal comando grep o tail CLI.

stato_processo

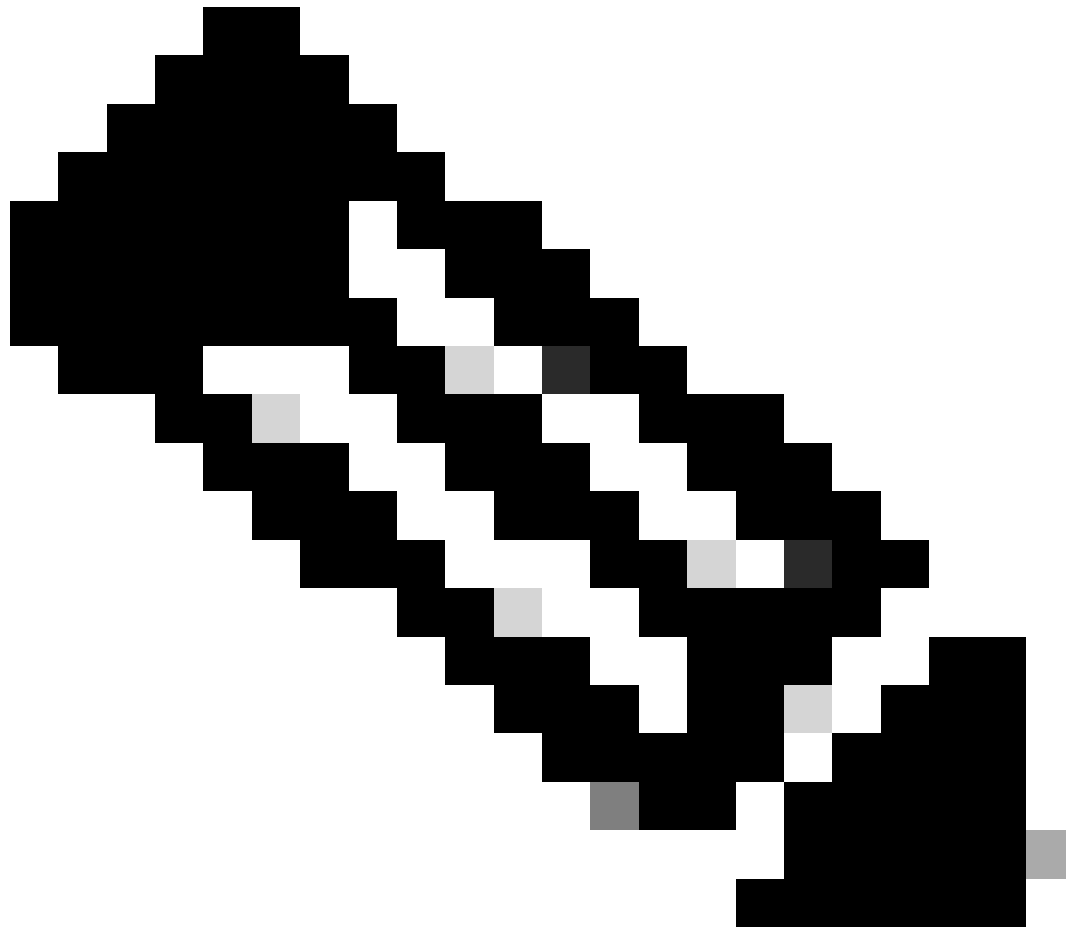
Per visualizzare lo stato del processo, nelle versioni 14.5 e successive, SWA ha un nuovo comando: `process_status` che ottiene i dettagli del processo SWA.

Nota: questo comando è disponibile solo in modalità admin.

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_controll
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



Nota: l'utilizzo della CPU del processo. Si tratta di una media decrescente rispetto a un minuto di tempo (reale) precedente. Poiché la base di tempo su cui viene calcolato questo valore varia (poiché i processi potrebbero essere molto giovani), è possibile che la somma di tutti i campi %CPU superi il 100%.

%MEM: percentuale di memoria reale utilizzata dal processo

VSZ: dimensioni virtuali in Kbyte (alias vsize)

RSS : dimensione della memoria reale (set residente) del processo (in unità da 1024 byte).

TT: abbreviazione dell'eventuale nome del percorso del terminale di controllo.

STAT

Lo stato viene dato da una sequenza di caratteri, ad esempio "RNL". Il primo carattere indica lo stato di esecuzione del processo:

D : Contrassegna un processo in attesa (o in un altro breve periodo, non interrompibile).

I: contrassegna un processo inattivo (in sospensione per più di 20 secondi circa).

L: contrassegna un processo in attesa di acquisire un blocco.

R: contrassegna un processo eseguibile.

S: contrassegna un processo che rimane inattivo per meno di 20 secondi.

T: contrassegna un processo interrotto.

W: contrassegna un thread di interrupt inattivo.

Z : Contrassegna un processo inattivo (uno "zombie").

Eventuali caratteri aggiuntivi dopo questi indicano ulteriori informazioni sullo stato:

+: il processo si trova nel gruppo di processi in primo piano del terminale di controllo.

<: il processo ha aumentato la priorità di pianificazione della CPU.

C: il processo è in modalità capsicum(4).

E: il processo sta tentando di uscire. J Segna un processo che è in prigione(2).

L: il processo ha pagine bloccate nel core (ad esempio, per I/O raw).

N: il processo ha ridotto la priorità di pianificazione della CPU.

s: il processo è un coordinatore della sessione.

V: l'elemento padre del processo viene sospeso durante un vfork(2), in attesa dell'esecuzione o dell'uscita del processo.

W: Il processo viene scambiato.

X: traccia o debug del processo.

TIME: tempo CPU cumulativo, utente + sistema

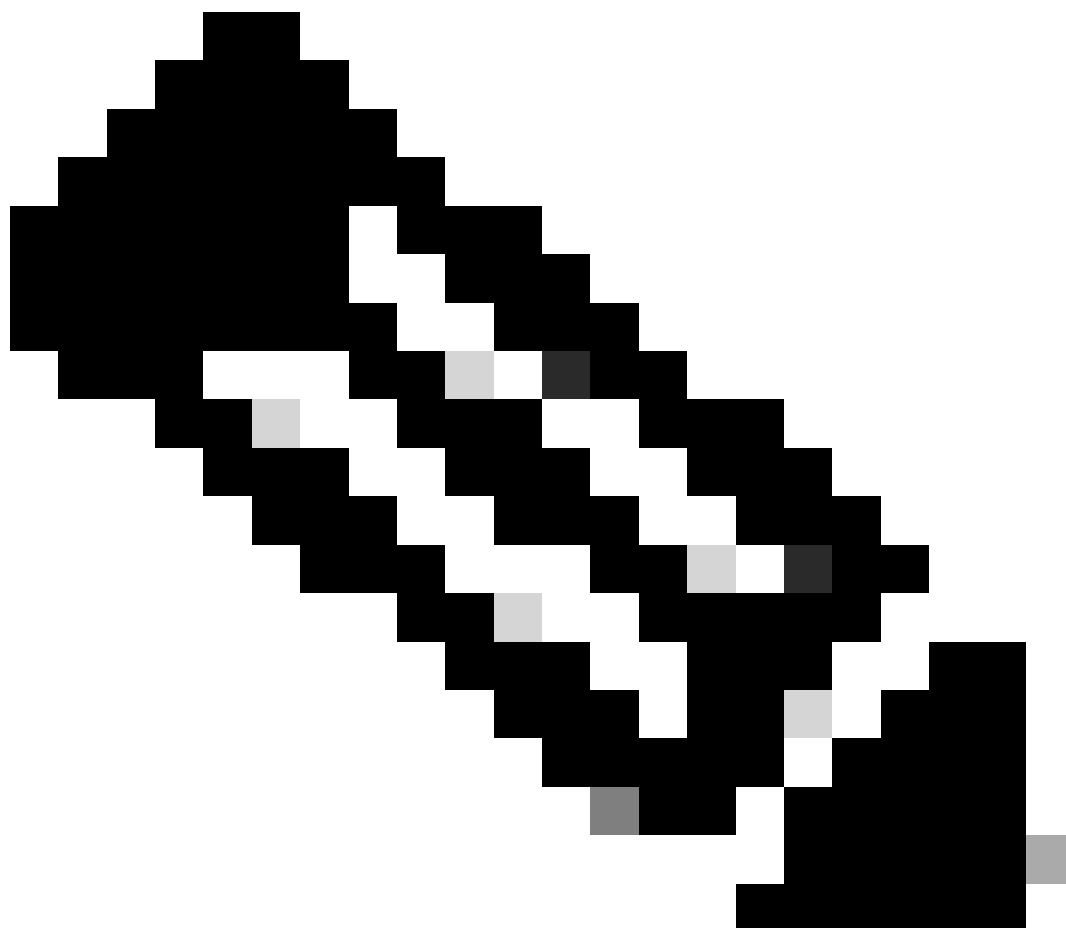
Riavvia processo in SWA

Processo generale

È possibile riavviare i servizi e l'elaborazione SWA dalla CLI. Di seguito sono riportati i passaggi:

Passaggio 1. accedere alla CLI

Passaggio 2. Diagnostica tipo

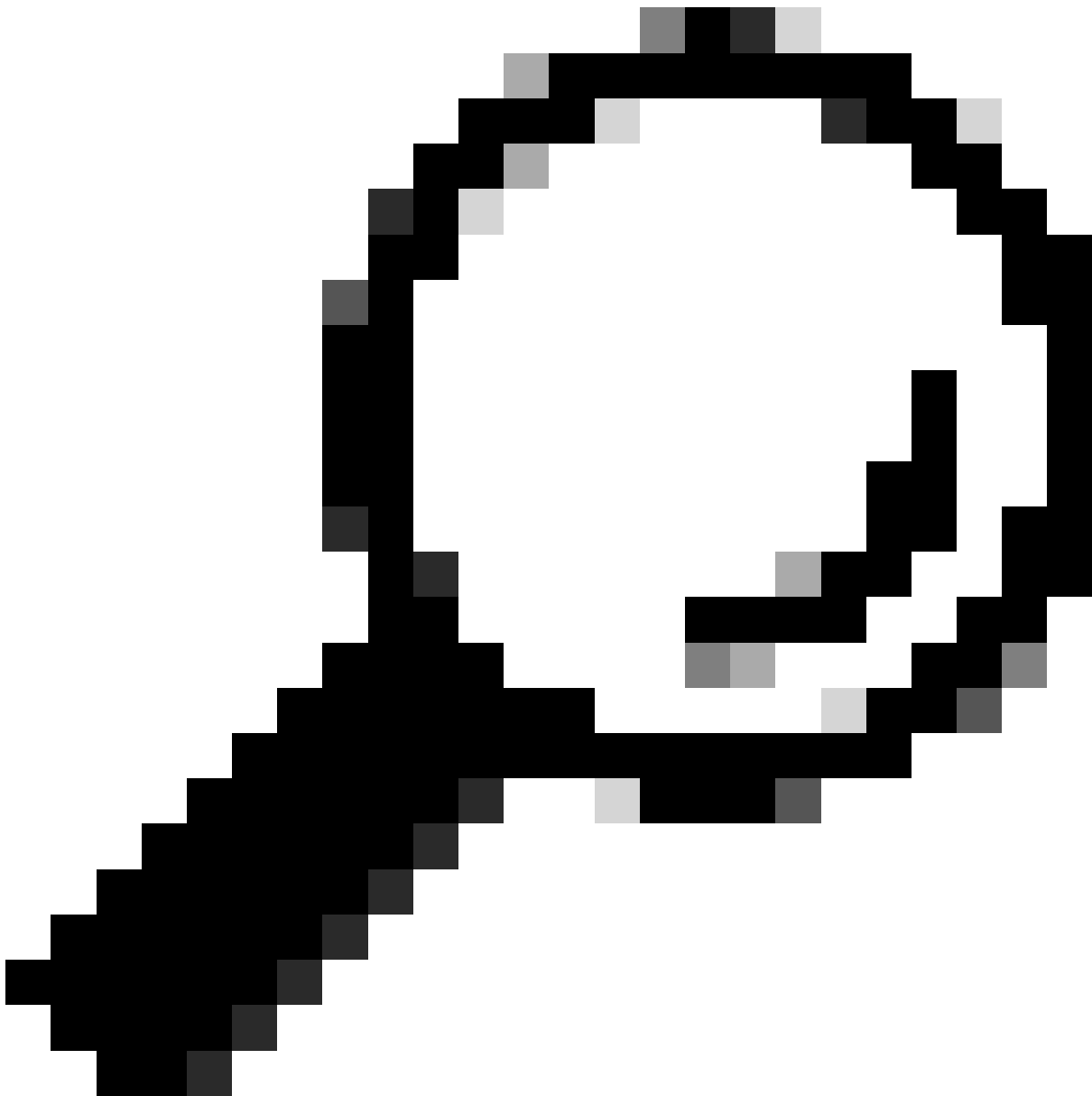


Nota: il comando `diagnostic is CLI hidden` non può essere riempito automaticamente con TAB.

Passaggio 3. Scegli servizi

Passaggio 4. Scegliere il servizio/processo che si desidera riavviare.

Passaggio 5. Scegliere Riavvia



Suggerimento: è possibile visualizzare lo stato del processo dalla sezione STATUS.

Nell'esempio, il processo WEBUI responsabile della GUI è stato riavviato:

```
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
- OSCP - OSCP
- UPDATER - UPDATER
- SICAP - SICAP
- SNMP - SNMP
- SNTF - SNTF
- 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.

Riavvia processo proxy

Per riavviare il processo proxy, che è il processo principale per il proxy, è possibile utilizzare CLI, procedere come segue:

Passaggio 1. accedere alla CLI

Passaggio 2. Diagnostica tipo

Nota: il comando diagnostic is CLI hidden non può essere riempito automaticamente con TAB.

Passaggio 3. Scegli PROXY

Passaggio 4. Digitare KICK, (si tratta di un comando nascosto).

Passaggio 5. Selezionate Y per 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

Informazioni correlate

- [Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance - LD \(installazione limitata\) - Risoluzione dei problemi \[Cisco Secure Web Appliance\] - Cisco](#)
- [Uso delle best practice di Secure Web Appliance - Cisco](#)
- [ps\(1\) \(freebsd.org\)](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).