

Solución de problemas de estados de proceso inusuales en SWA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Supervisar el estado del proceso](#)

[Ver el estado del proceso desde la GUI](#)

[Comandos CLI](#)

[estado](#)

[rate \(proxystat\)](#)

[shd_logs](#)

[process_status](#)

[Reiniciar proceso en SWA](#)

[Proceso general](#)

Introducción

En este documento se describe el estado del proceso y cómo utilizarlo para solucionar problemas de rendimiento del dispositivo web seguro (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SWA físico o virtual instalado.
- Licencia activada o instalada.
- Cliente Secure Shell (SSH).
- El asistente de configuración ha finalizado.

- Acceso administrativo al SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Supervisar el estado del proceso

Puede supervisar el estado del proceso desde la interfaz gráfica de usuario (GUI) o desde la interfaz de línea de comandos (CLI).

Ver el estado del proceso desde la GUI

Para ver las estadísticas de proceso en la GUI, navegue hasta Informes y elija Capacidad del sistema. Puede seleccionar Rango de tiempo para ver la asignación de recursos para la marca de tiempo deseada.

System-Capacity

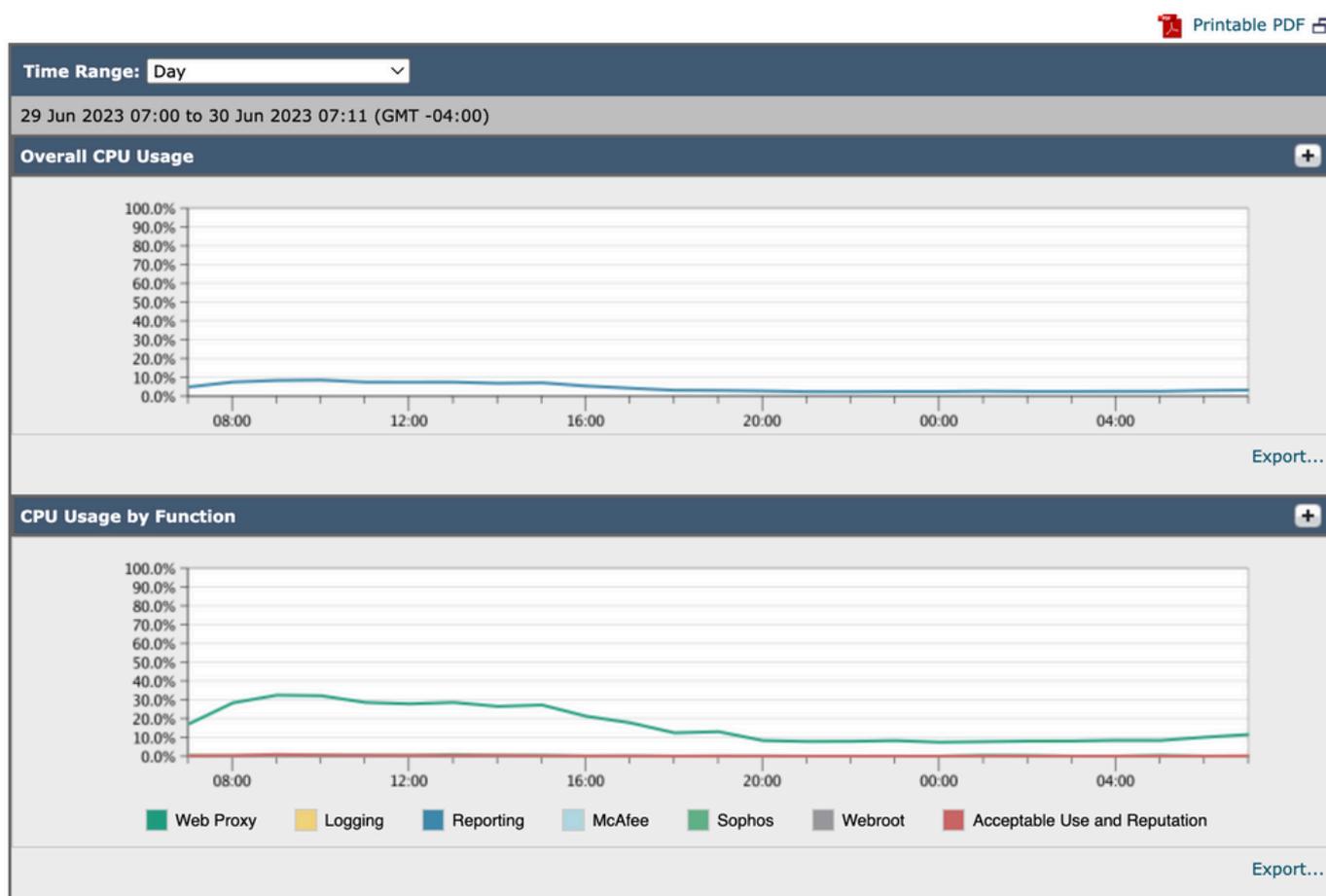
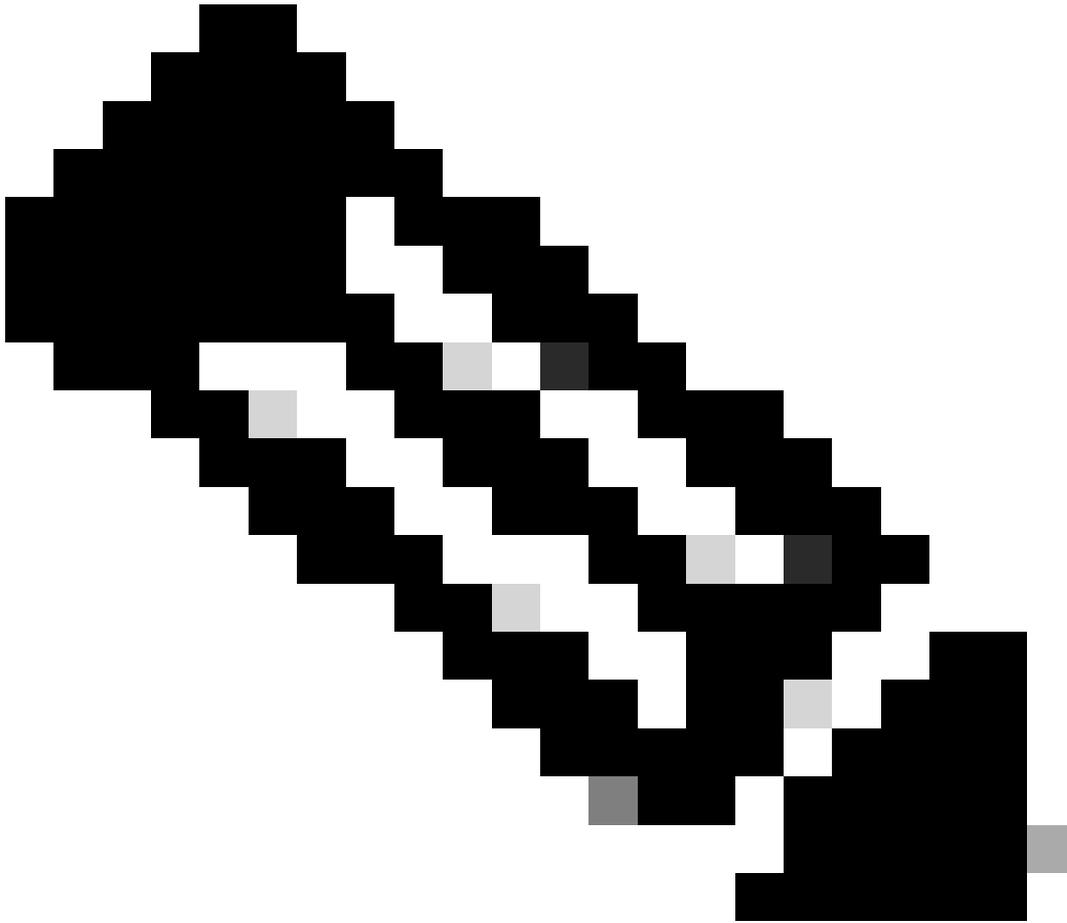


Image-System-Capacity

Uso general de CPU: muestra el uso total de CPU

Uso de CPU por función: muestra cada subprocesso, asignación de CPU.

Memoria de búfer de proxy: muestra la asignación de memoria para el proceso de proxy.



Nota: La memoria del búfer del proxy no es el uso total de memoria de SWA.

Comandos CLI

Existen varios comandos CLI que muestran el estado de la carga principal de la CPU o del subproceso:

estado

Desde la salida de status o status detail, puede ver el uso general de la CPU de SWA, estos comandos muestran la carga actual de la 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, muestra la carga del proceso proxy, que es un subproceso que es el proceso principal en SWA. Este comando se actualiza automáticamente cada 15 segundos.

```
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" es otro comando CLI que tiene el mismo resultado que el comando "rate"

shd_logs

Puede ver el estado del proceso principal, como el estado del proceso Proxy, el estado del proceso de generación de informes, etc., desde SHD_Logs. Para obtener más información sobre los registros SHD, visite este enlace:

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

A continuación se muestra un ejemplo de resultado de 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: puede acceder a shd_logs desde los comandos grep o tail de la CLI.

process_status

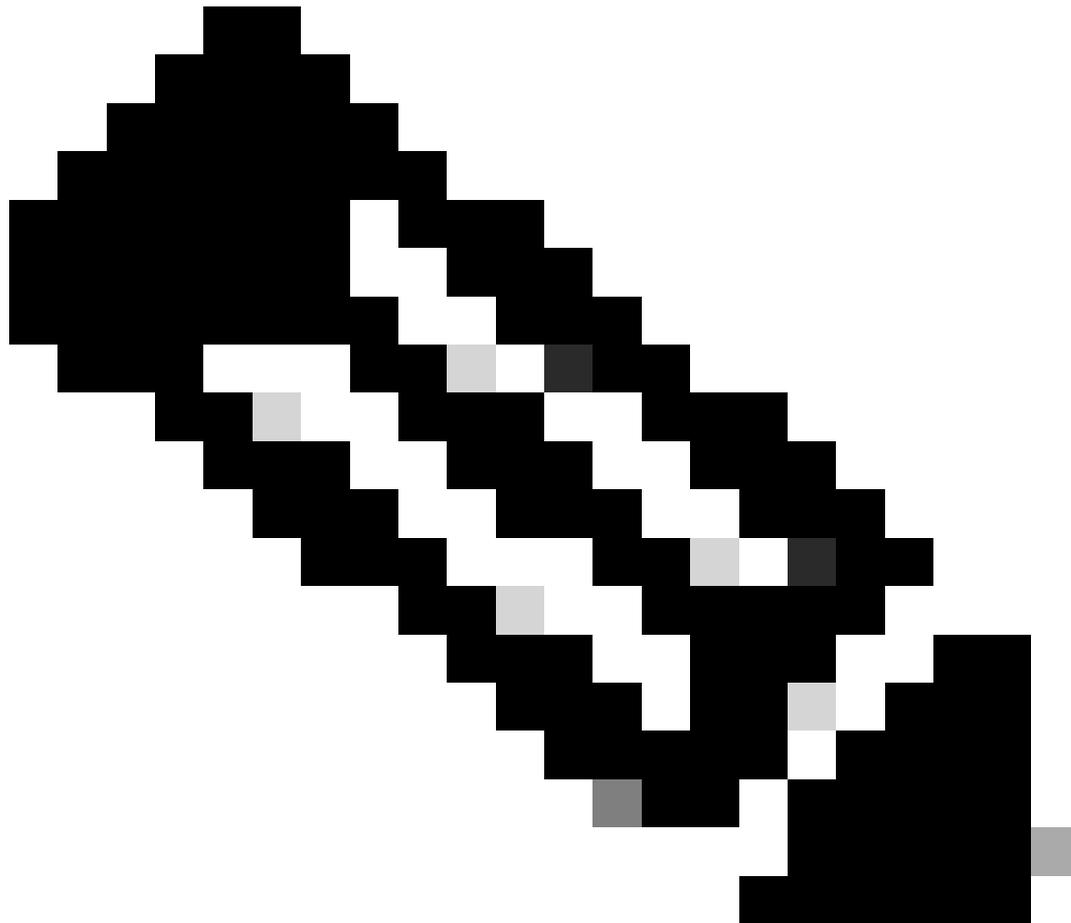
Para ver el estado del proceso, en las versiones 14.5 y posteriores, SWA tiene un nuevo comando: process_status que obtiene los detalles del proceso de SWA.

Nota: Este comando sólo está disponible en el modo de administración.

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: La utilización de la CPU del proceso; se trata de un promedio en descomposición de hasta un minuto de tiempo anterior (real). Dado que la base de tiempo sobre la que se calcula varía (ya que los procesos pueden ser muy jóvenes), es posible que la suma de todos los campos %CPU supere el 100%.

%MEM: Porcentaje de memoria real que utiliza este proceso

VSZ: Tamaño virtual en Kbytes (alias vsize)

RSS: tamaño de la memoria real (conjunto residente) del proceso (en unidades de 1024 bytes).

TT: Abreviatura del nombre de la trayectoria del terminal de control, si existe.

STAT

La estadística viene dada por una secuencia de caracteres, por ejemplo, "RNL". El primer carácter indica el estado de ejecución del proceso:

D : Marca un proceso en disco (u otro corto plazo, ininterrumpible) espera.

I: Marca un proceso que está inactivo (durmiendo más de 20 segundos).

L : Marca un proceso que está esperando para adquirir un bloqueo.

R : Marca un proceso ejecutable.

S : Marca un proceso que está inactivo durante menos de 20 segundos.

T : Marca un proceso detenido.

W : Marca un subprocesso de interrupción inactivo.

Z: Marca un proceso muerto (un "zombi").

Los caracteres adicionales posteriores a éstos, si los hubiera, indican información de estado adicional:

+ : El proceso está en el grupo de procesos en primer plano de su terminal de control.

<: El proceso ha aumentado la prioridad de programación de la CPU.

C: El proceso está en modo de capacidad capsicum(4).

E: El proceso está intentando salir. J Marca un proceso que está en la cárcel(2).

L: El proceso tiene páginas bloqueadas en el núcleo (por ejemplo, para E/S sin procesar).

N: El proceso ha reducido la prioridad de programación de la CPU.

s: El proceso es un líder de sesión.

V: El padre del proceso se suspende durante un vfork(2), esperando a que el proceso se ejecute o salga.

W: El proceso se intercambia.

X: Se está realizando un seguimiento del proceso o se está depurando.

TIME: Tiempo de CPU acumulado, usuario + sistema

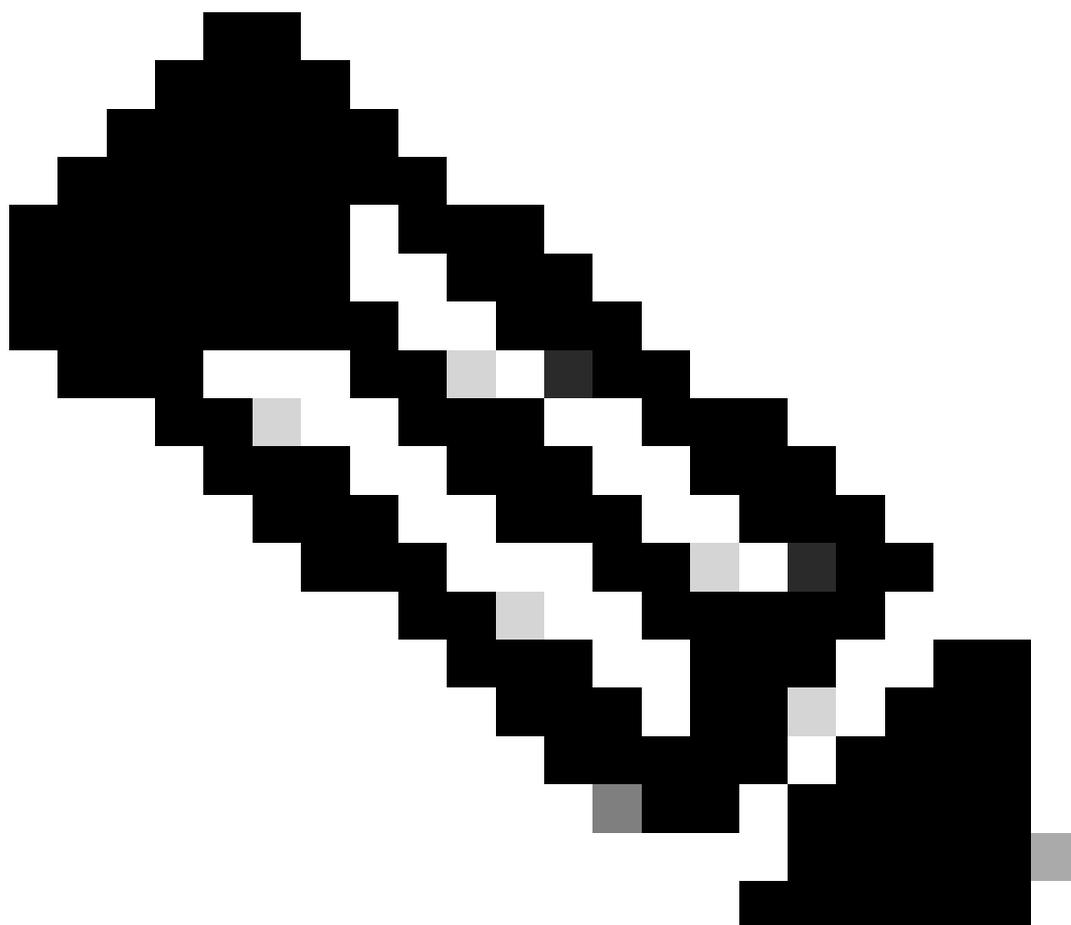
Reiniciar proceso en SWA

Proceso general

Puede reiniciar los servicios SWA y el proceso desde CLI. A continuación se indican los pasos:

Paso 1. inicie sesión en CLI

Paso 2. Diagnóstico de tipo

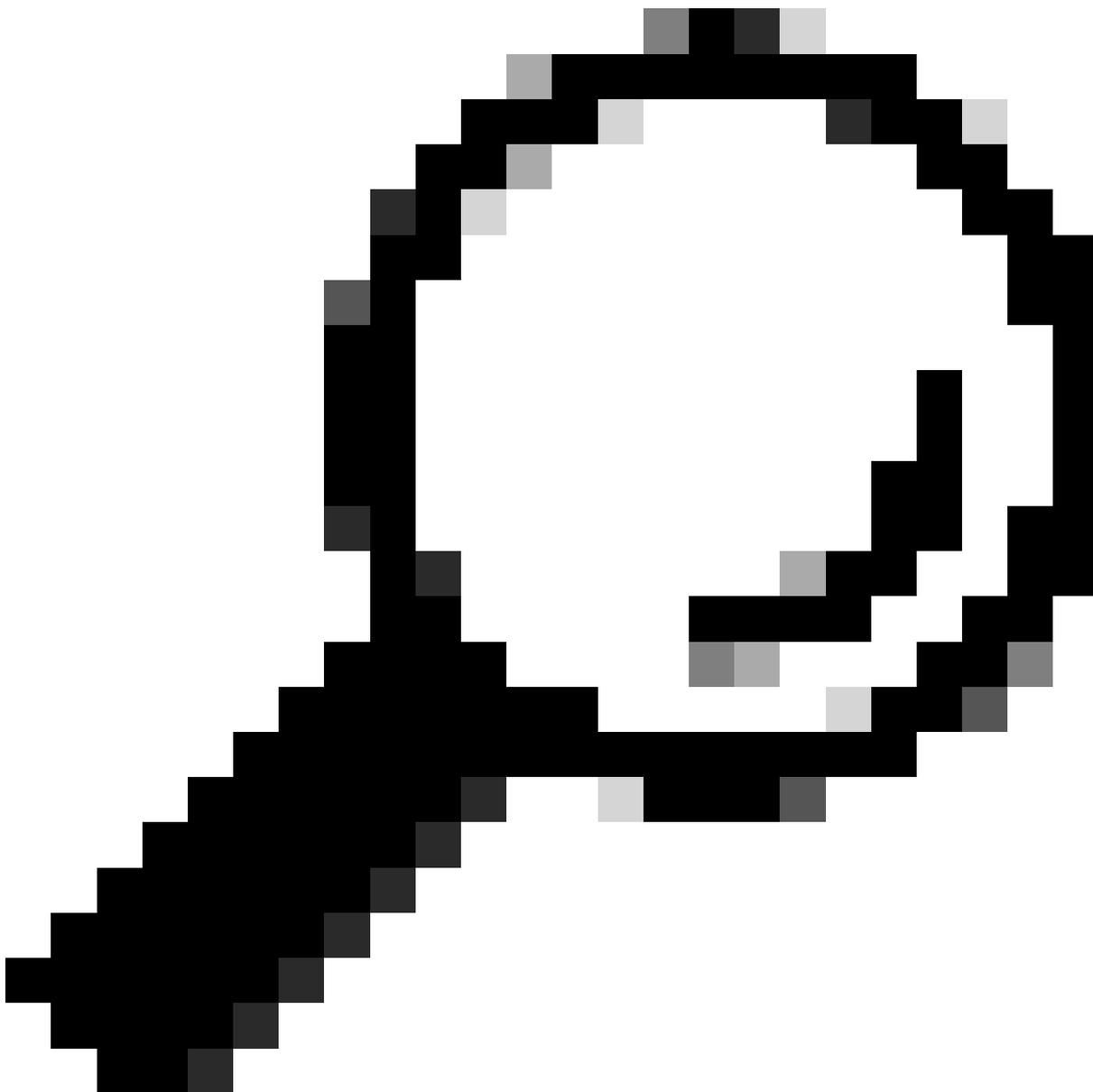


Nota: diagnostic es el comando oculto de CLI, por lo que no puede rellenar automáticamente el comando con TAB.

Paso 3. Seleccione Servicios

Paso 4. Elija el servicio/ proceso que desea reiniciar.

Paso 5. Seleccione Reiniciar



Sugerencia: Puede ver el estado del proceso desde la sección STATUS (Estado).

En este ejemplo, se ha reiniciado el proceso WEBUI responsable de la GUI:

```
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
 - 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.

Reiniciar proceso de proxy

Para reiniciar el proceso de proxy, que es el proceso principal para el proxy, puede utilizar CLI. A continuación se indican los pasos:

Paso 1. inicie sesión en CLI

Paso 2. Diagnóstico de tipo



Nota: diagnostic es el comando oculto de CLI, por lo que no puede rellenar automáticamente el comando con TAB.

Paso 3. Elegir PROXY

Paso 4. Escriba KICK, (es un comando oculto).

Paso 5. Elija Y para 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

Información Relacionada

- [Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - LD \(implementación limitada\) - Resolución de problemas \[Cisco Secure Web Appliance\] - Cisco](#)
- [Uso de las prácticas recomendadas de los dispositivos web seguros: Cisco](#)
- [ps\(1\) \(freebsd.org\)](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).