

SWA의 비정상적인 프로세스 상태 트러블슈팅

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [프로세스 상태 모니터링](#)
 - [GUI에서 프로세스 상태 보기](#)
 - [CLI 명령](#)
 - [상태](#)
 - [속도\(proxystat\)](#)
 - [shd_logs](#)
 - [프로세스 상태](#)
 - [SWA에서 프로세스 다시 시작](#)
 - [일반 프로세스](#)
-

소개

이 문서에서는 프로세스 상태 및 이를 사용하여 SWA(Secure Web Appliance), 성능 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.
- 라이센스가 활성화되었거나 설치되었습니다.
- SSH(Secure Shell) 클라이언트.
- 설치 마법사가 완료되었습니다.

- SWA에 대한 관리 액세스.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

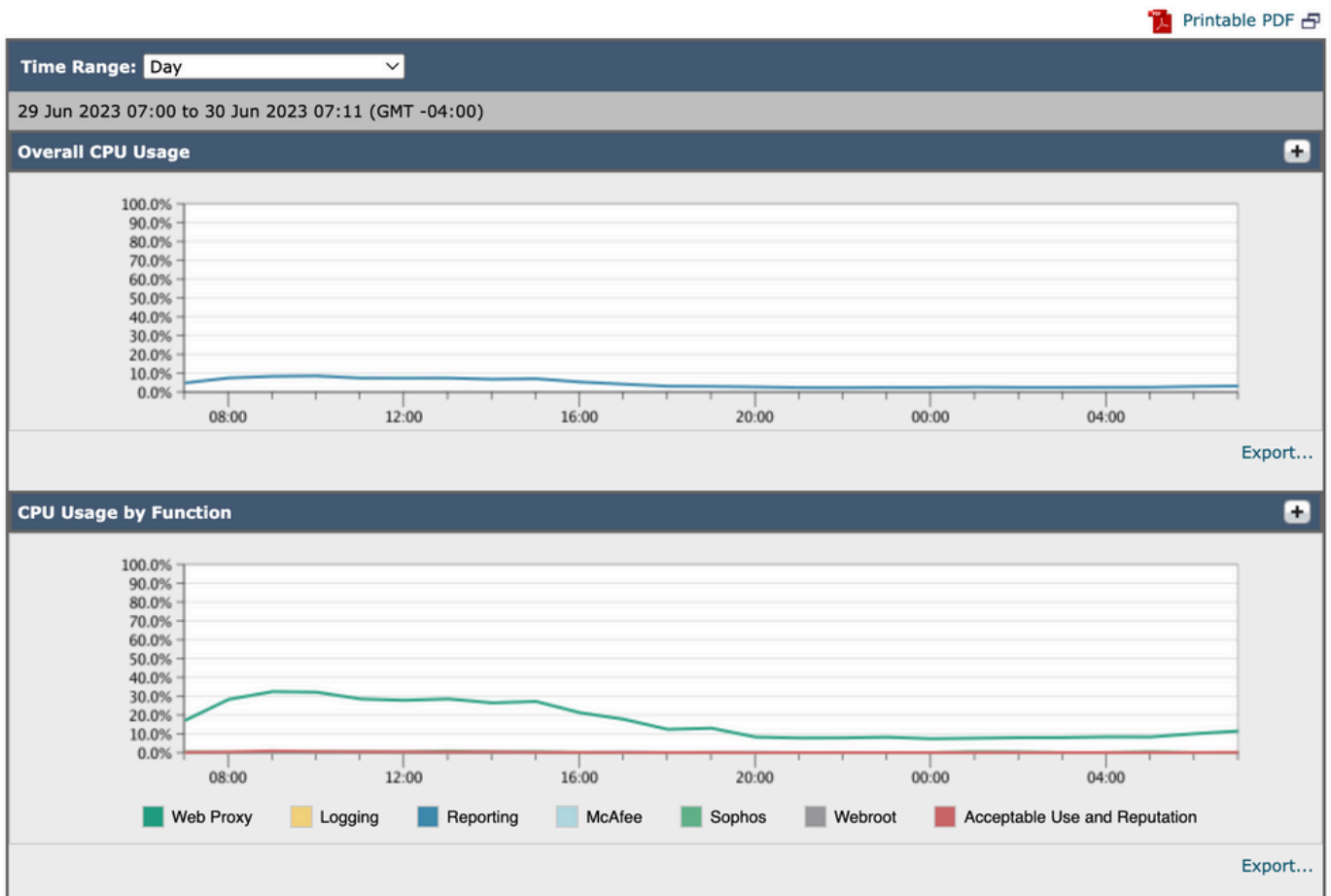
프로세스 상태 모니터링

GUI 또는 CLI에서 프로세스 상태를 모니터링할 수 있습니다.

GUI에서 프로세스 상태 보기

GUI에서 프로세스 통계를 보려면 Reporting(보고)으로 이동하고 System Capacity(시스템 용량)를 선택합니다. 원하는 타임스탬프에 대한 리소스 할당을 보려면 Time Range(시간 범위)를 선택할 수 있습니다.

System-Capacity



이미지 시스템 용량

전체 CPU 사용량: 총 CPU 사용량을 표시합니다.

기능별 CPU 사용량: 각 하위 프로세스, CPU 할당을 표시합니다.

프록시 버퍼 메모리: 프록시 프로세스에 대한 메모리 할당을 표시합니다.

참고: 프록시 버퍼 메모리는 SWA의 총 메모리 사용량이 아닙니다.

CLI 명령

기본 CPU 로드 또는 하위 프로세스 상태를 표시하는 여러 CLI 명령이 있습니다.

상태

상태 또는 상태 세부 정보의 출력에서 SWA의 전체 CPU 사용량을 볼 수 있으며, 이러한 명령은 현재 CPU 로드를 표시합니다.

```
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%
...

```

속도(proxystat)

rate CLI 명령은 SWA의 기본 프로세스인 하위 프로세스인 프록시 프로세스 로드를 표시합니다. 이 명령은 15초마다 자동으로 새로 고쳐집니다.

```
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

참고: "proxystat"는 "rate" 명령과 출력이 동일한 또 다른 CLI 명령입니다

shd_logs

SHD_Logs에서 Proxy process status(프록시 프로세스 상태), Reporting Process status(보고 프로세스 상태) 등의 기본 프로세스 상태를 볼 수 있습니다. SHD 로그에 대한 자세한 내용은 다음 링크를 참조하십시오.

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

다음은 shd_logs 출력의 샘플입니다.

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

참고: grep 또는 tail CLI 명령에서 shd_logs에 액세스할 수 있습니다.

프로세스 상태

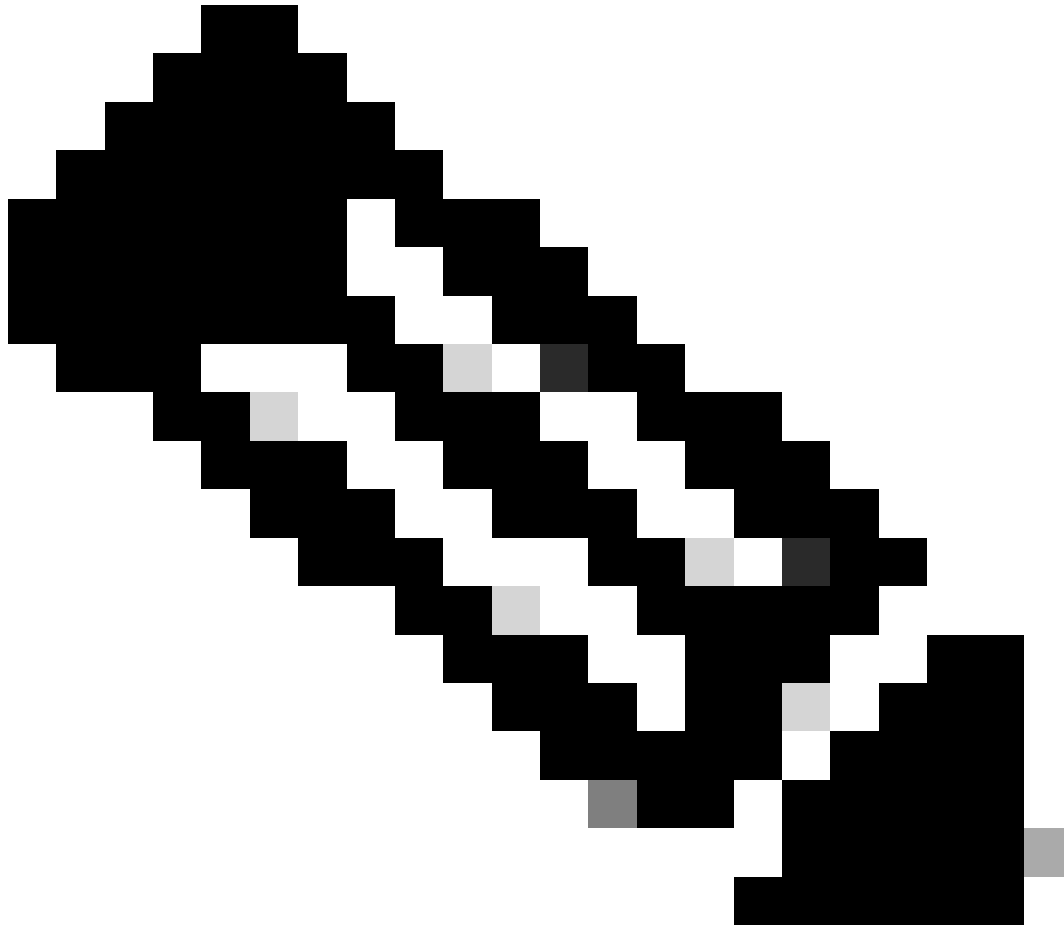
Process Status(프로세스 상태)를 보기 위해 버전 14.5 이상에서 SWA에는 새로운 명령 process_status가 있습니다. 이 명령은 SWA의 프로세스 세부사항을 가져옵니다.

참고: 이 명령은 관리자 모드에서만 사용할 수 있습니다.

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



참고: 프로세스의 CPU 사용률. 이전(실시간) 시간의 최대 1분에 걸쳐 감소하는 평균입니다. 계산되는 시간 기준이 다양하기 때문에(프로세스가 매우 젊을 수 있으므로) 모든 %CPU 필드의 합계가 100%를 초과할 수 있습니다.

%MEM: 이 프로세스에서 사용하는 실제 메모리의 비율

VSZ: 가상 크기(KB)(별칭 vsize)

RSS : 프로세스의 실제 메모리(상주 집합) 크기(1024바이트 단위).

TT : 제어 단말기의 경로 이름에 대한 약어(있는 경우).

통계

상태는 문자 시퀀스로 제공됩니다(예: "RNL"). 첫 번째 문자는 프로세스의 실행 상태를 나타냅니다.

D : 디스크(또는 다른 단기, 파일 불가능) 대기 프로세스를 표시합니다.

I: 유휴 상태(약 20초 이상 휴지 상태)인 프로세스를 표시합니다.

L: 잠금을 얻기 위해 대기 중인 프로세스를 표시합니다.

R : 실행 가능한 프로세스를 표시합니다.

S: 약 20초 미만 휴지 상태인 프로세스를 표시합니다.

T: 중지된 프로세스를 표시합니다.

W: 유휴 인터럽트 스레드를 표시합니다.

Z: 데드 프로세스("좀비")를 표시합니다.

뒤에 추가 문자가 있으면 추가 상태 정보를 나타냅니다.

+ : 프로세스가 해당 제어 터미널의 포그라운드 프로세스 그룹에 있습니다.

<: 프로세스에서 CPU 예약 우선 순위를 높였습니다.

C: 프로세스가 capsicum(4) 기능 모드입니다.

E: 프로세스를 종료하려고 합니다. J는 감옥(2)에 있는 프로세스를 표시합니다.

L: 프로세스에 페이지가 코어에서 잠겨 있습니다(예: 원시 I/O).

N: 프로세스에서 CPU 스케줄링 우선 순위를 줄였습니다.

s: 프로세스는 세션 리더입니다.

V: 프로세스의 상위가 vfork(2) 중에 중단되어 프로세스가 실행되거나 종료되기를 기다립니다.

W: 프로세스가 교체됩니다.

X: 프로세스를 추적하거나 디버깅하는 중입니다.

TIME: 누적 CPU 시간, 사용자 + 시스템

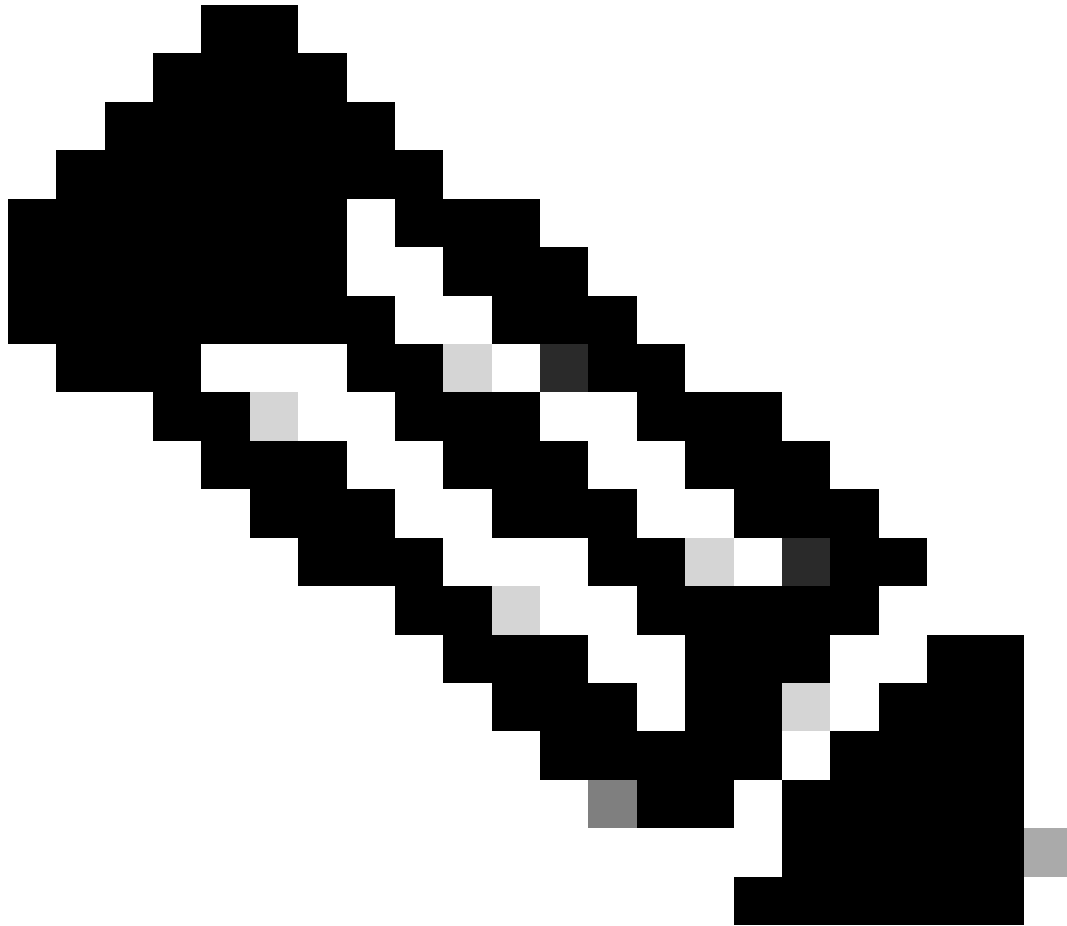
SWA에서 프로세스 다시 시작

일반 프로세스

CLI에서 SWA 서비스 및 프로세스를 다시 시작할 수 있습니다. 단계는 다음과 같습니다.

1단계. CLI에 로그인

2단계. 유형 진단

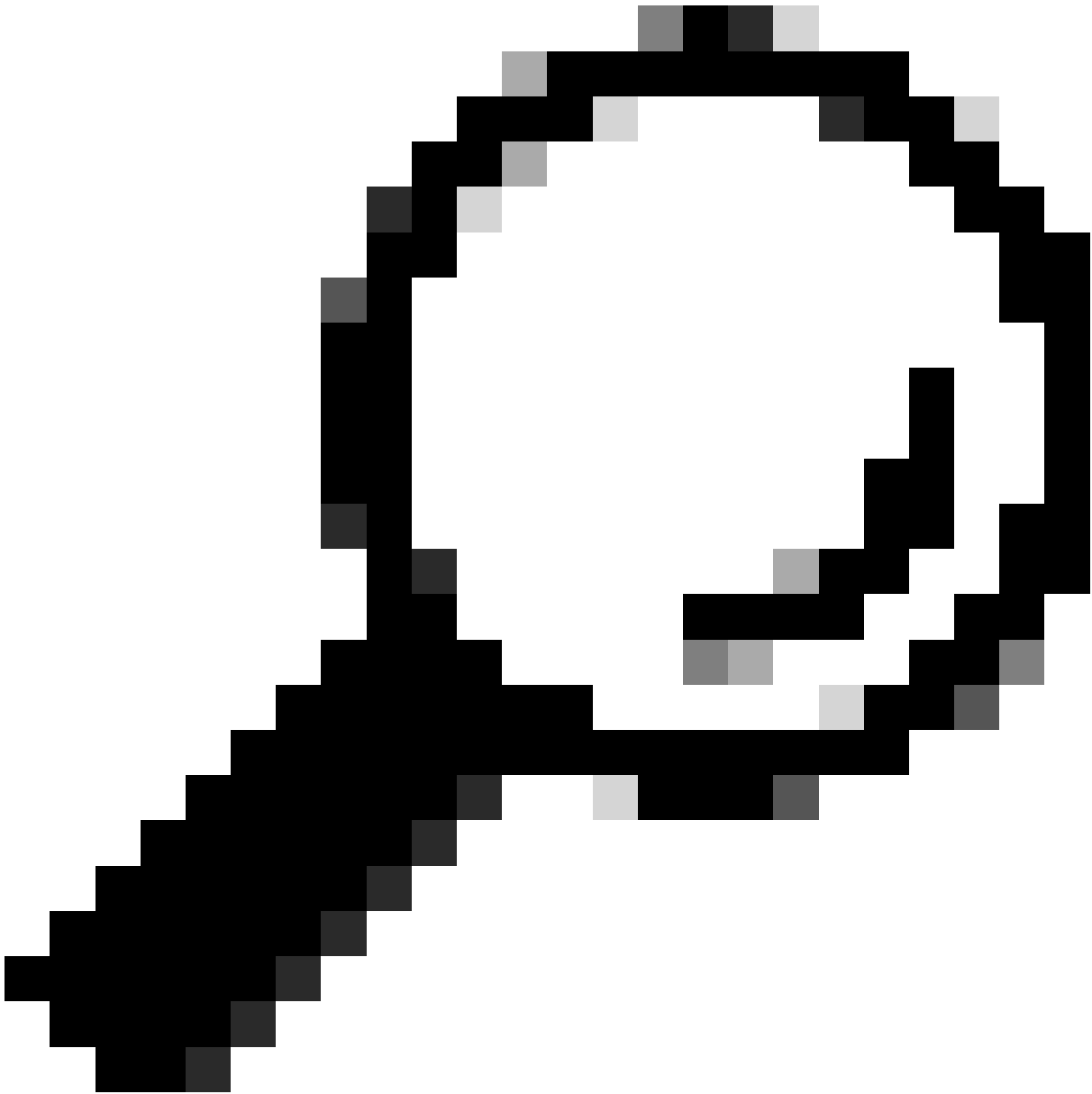


참고: 진단은 CLI 숨겨진 명령이므로 TAB으로 명령을 자동 채울 수 없습니다.

3단계. 서비스 선택

4단계. 다시 시작할 서비스/프로세스를 선택합니다.

5단계. Restart(재시작)를 선택합니다



팁: STATUS 섹션에서 프로세스의 상태를 볼 수 있습니다.

이 예에서는 GUI를 담당하는 WEBUI 프로세스가 다시 시작되었습니다.

```
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.

프록시 프로세스 다시 시작

프록시의 기본 프로세스인 프록시 프로세스를 다시 시작하려면 CLI를 사용할 수 있습니다. 다음 단계는 다음과 같습니다.

1단계. CLI에 로그인

2단계. 유형 진단

참고: 진단은 CLI 숨겨진 명령이므로 TAB으로 명령을 자동 채울 수 없습니다.

3단계. 프록시 선택

4단계. KICK, (숨겨진 명령)을 입력합니다.

5단계. 예로 Y를 선택합니다.

```
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

관련 정보

- [AsyncOS 15.0 for Cisco Secure Web Appliance - LD 사용 설명서\(제한적 배포\) - 문제 해결 \[Cisco Secure Web Appliance\] - Cisco](#)
- [Use Secure Web Appliance 모범 사례 - Cisco](#)
- [ps\(1\)\(freebsd 조직\)](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.