

Solucionar problemas de estados de processo incomuns em SWA

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Monitorar Status do Processo](#)

[Visualizar o status do processo a partir da GUI](#)

[Comandos CLI](#)

[status](#)

[taxa \(proxystat\)](#)

[shd_logs](#)

[process_status](#)

[Reiniciar processo no SWA](#)

[Processo geral](#)

Introdução

Este documento descreve o Status do processo e como usá-lo para solucionar problemas de desempenho do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- Cliente Secure Shell (SSH).
- O assistente de instalação foi concluído.

- Acesso administrativo ao SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

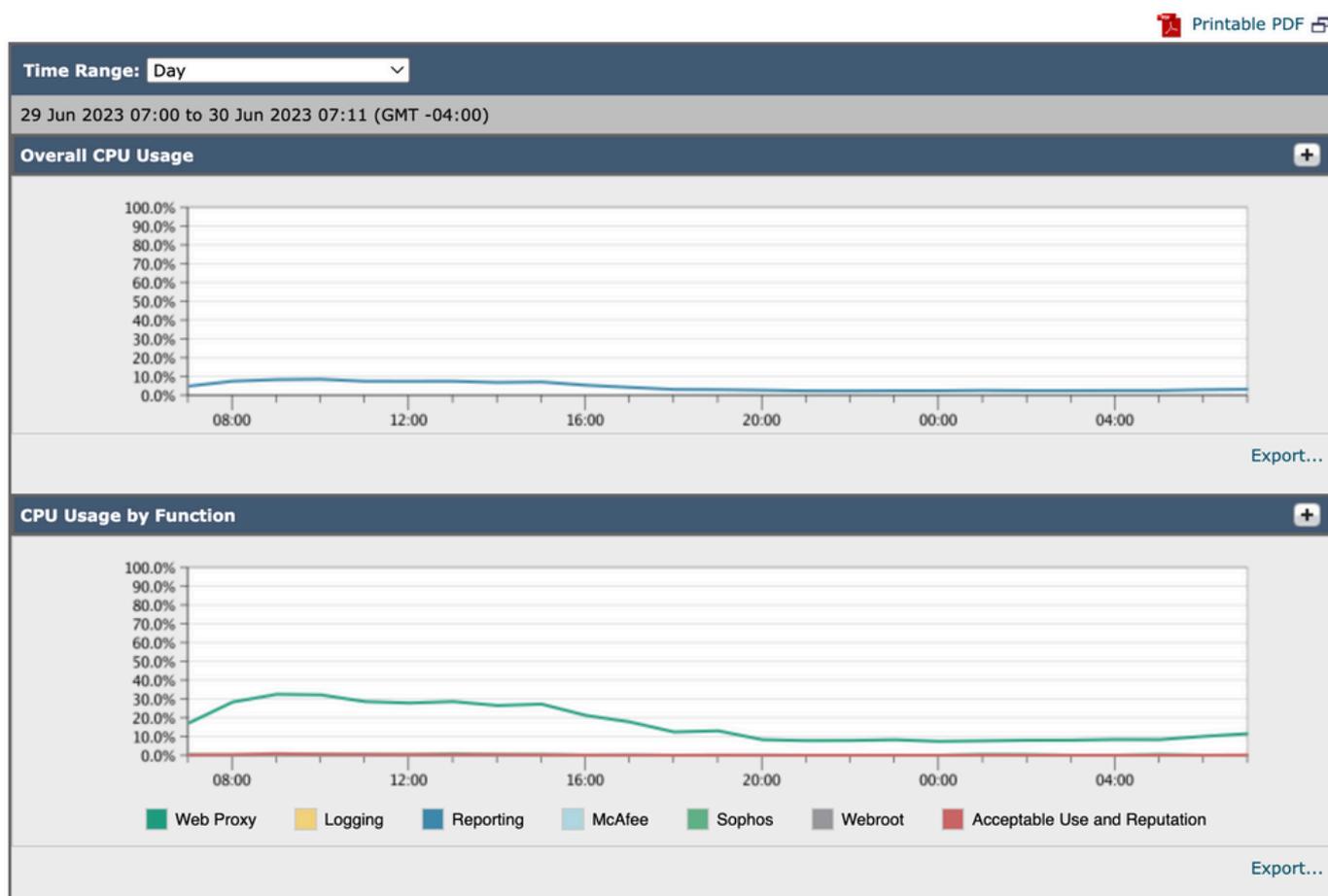
Monitorar Status do Processo

Você pode monitorar o Status do processo na Interface gráfica do usuário (GUI) ou na Interface de linha de comando (CLI).

Visualizar o status do processo a partir da GUI

Para exibir estatísticas do processo na GUI, navegue para Relatórios e escolha Capacidade do sistema. Você pode selecionar Intervalo de tempo para exibir a alocação de recursos para o carimbo de data/hora desejado.

System-Capacity



Capacidade do sistema de imagem

Uso Geral da CPU: Mostra o Uso Total da CPU

Uso da CPU por Função: Mostra cada subprocesso, alocação da CPU.

Memória de buffer do proxy: mostra a alocação de memória para o processo do proxy.

Observação: a memória de buffer do proxy não é o uso total de memória do SWA.

Comandos CLI

Há vários comandos CLI que mostram o status principal de carga ou subprocesso da CPU:

status

Na saída de status ou status detail, você pode ver o uso geral da CPU do SWA, esses comandos mostram a carga atual da 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%
...

```

taxa (proxystat)

rate CLI, mostra o carregamento do processo proxy, que é um subprocesso que é o processo principal no SWA. Esse comando é atualizado automaticamente a 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

Observação: "proxystat" é outro comando CLI que tem a mesma saída do comando "rate"

shd_logs

Você pode exibir o status principal do processo, como o status do processo de proxy, o status do processo de relatório etc., em SHD_Logs. Para obter mais informações sobre logs SHD, visite este link:

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

Aqui está um exemplo da saída 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



Observação: você pode acessar shd_logs do comando CLI grep ou tail.

process_status

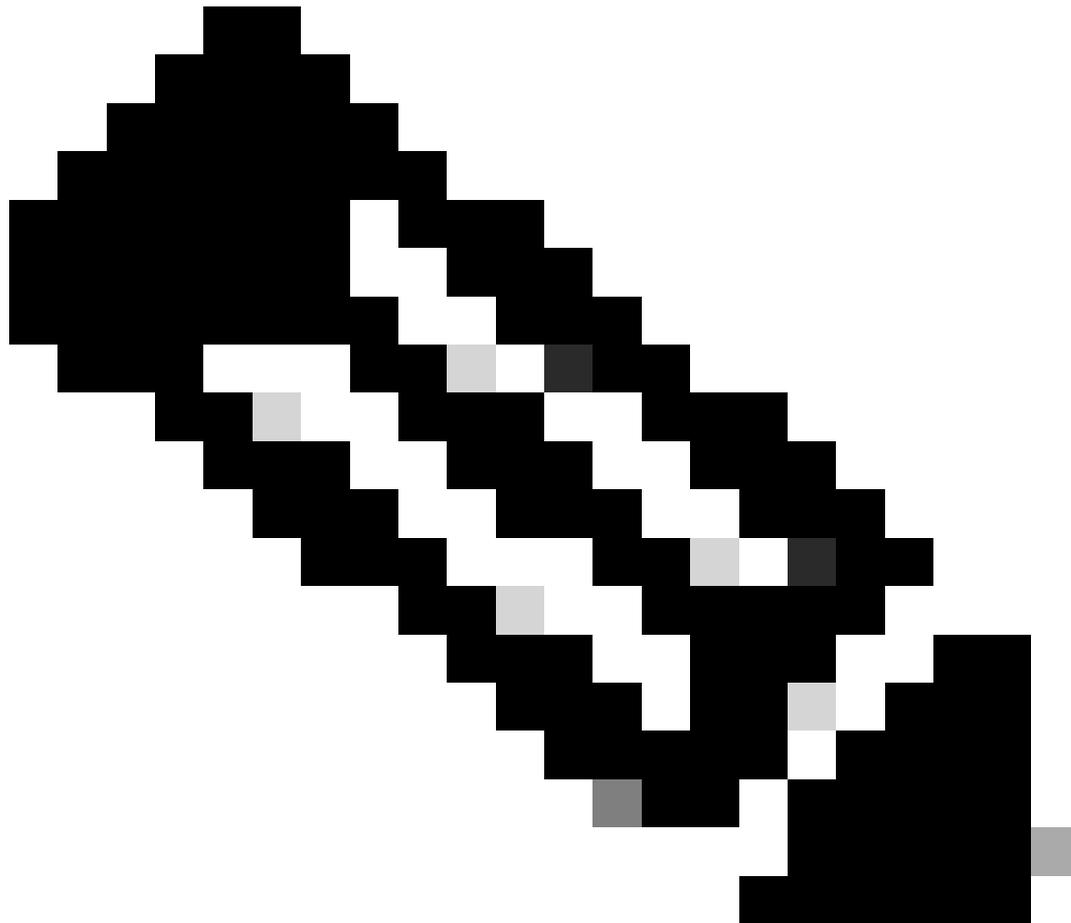
Para visualizar o Status do processo, nas versões 14.5 e superiores, o SWA tem um novo comando: `process_status`, que obtém os detalhes do processo do SWA.

Observação: esse comando está disponível somente no modo de administrador.

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



Observação: a utilização da CPU do processo; essa é uma média decrescente de até um minuto do tempo anterior (real). Como a base de tempo sobre a qual isso é computado varia (já que os processos podem ser muito jovens), é possível que a soma de todos os %campos da CPU exceda 100%.

%MEM : A porcentagem de memória real usada por este processo

VSZ: tamanho virtual em Kbytes (alias vsize)

RSS : O tamanho da memória real (conjunto residente) do processo (em unidades de 1024 bytes).

TT : Uma abreviação para o nome do caminho do terminal de controle, se houver.

STAT

A estatística é dada por uma sequência de caracteres, por exemplo, "RNL". O primeiro caractere indica o estado de execução do processo:

D : Marca um processo em disco (ou outro curto prazo, ininterrupto).

I : Marca um processo que está ocioso (dormindo por mais de 20 segundos).

L : Marca um processo que está aguardando para adquirir um bloqueio.

R : Marca um processo executável.

S : Marca um processo que está em espera por menos de 20 segundos.

T : Marca um processo parado.

W : Marca um thread de interrupção ocioso.

Z : Marca um processo morto (um "zumbi").

Caracteres adicionais após estes, se houver, indicam informações adicionais de estado:

+ : O processo está no grupo de processo de primeiro plano de seu terminal de controle.

< : O processo aumentou a prioridade de agendamento da CPU.

C : O processo está no modo de capacidade Capsicum(4).

E : O processo está tentando sair. J Marca um processo que está na cadeia(2).

L: O processo tem páginas bloqueadas no núcleo (por exemplo, para E/S bruta).

N : O processo reduziu a prioridade de programação da CPU.

s : O processo é um líder de sessão.

V : O pai do processo é suspenso durante um vfork(2), aguardando o processo ser executado ou encerrado.

W : O processo é trocado.

X : O processo está sendo rastreado ou depurado.

TIME: Tempo de CPU acumulado, usuário + sistema

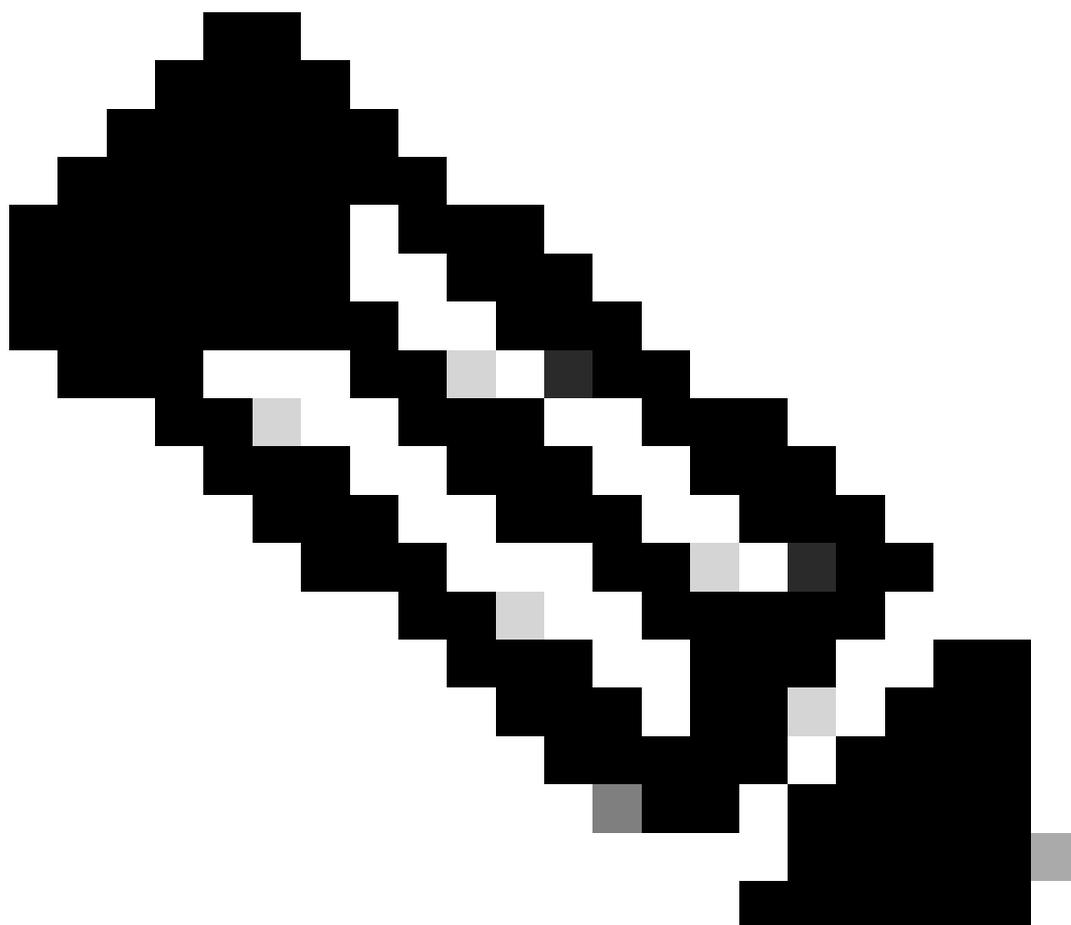
Reiniciar processo no SWA

Processo geral

Você pode reiniciar os serviços e o processo do SWA a partir do CLI. Estas são as etapas:

Etapa 1. iniciar sessão na CLI

Etapa 2. Diagnóstico de tipo

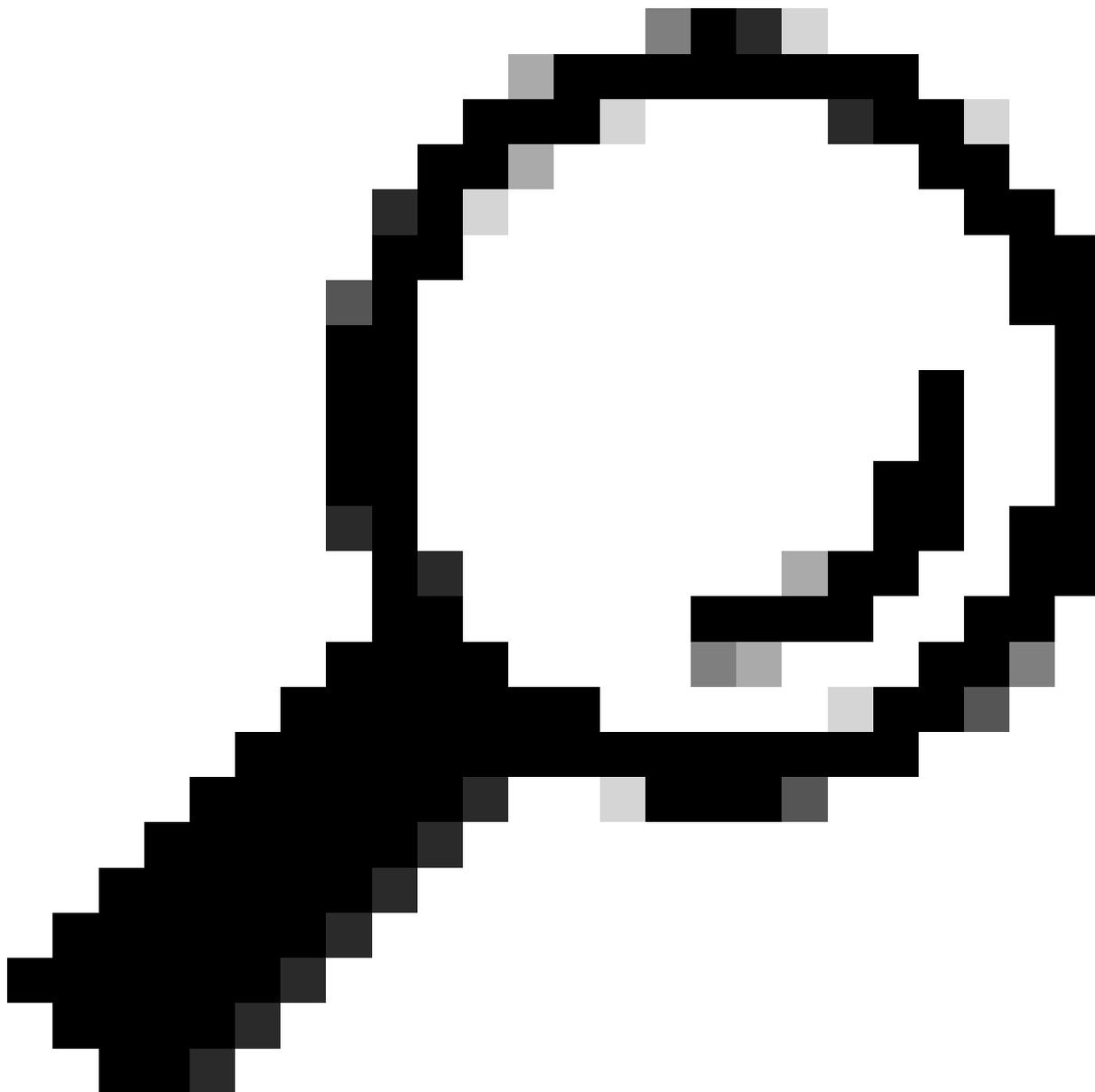


Observação: o diagnóstico é um comando oculto da CLI, portanto, você não pode preencher automaticamente o comando com TAB.

Etapa 3. Escolher serviços

Etapa 4. Escolha o Serviço/Processo que deseja reiniciar.

Etapa 5. Escolha Reiniciar



Dica: você pode exibir o status do processo na seção STATUS.

Neste exemplo, o processo WEBUI responsável pela GUI foi reiniciado:

```
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
 - SNTIP - SNTIP
 - 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

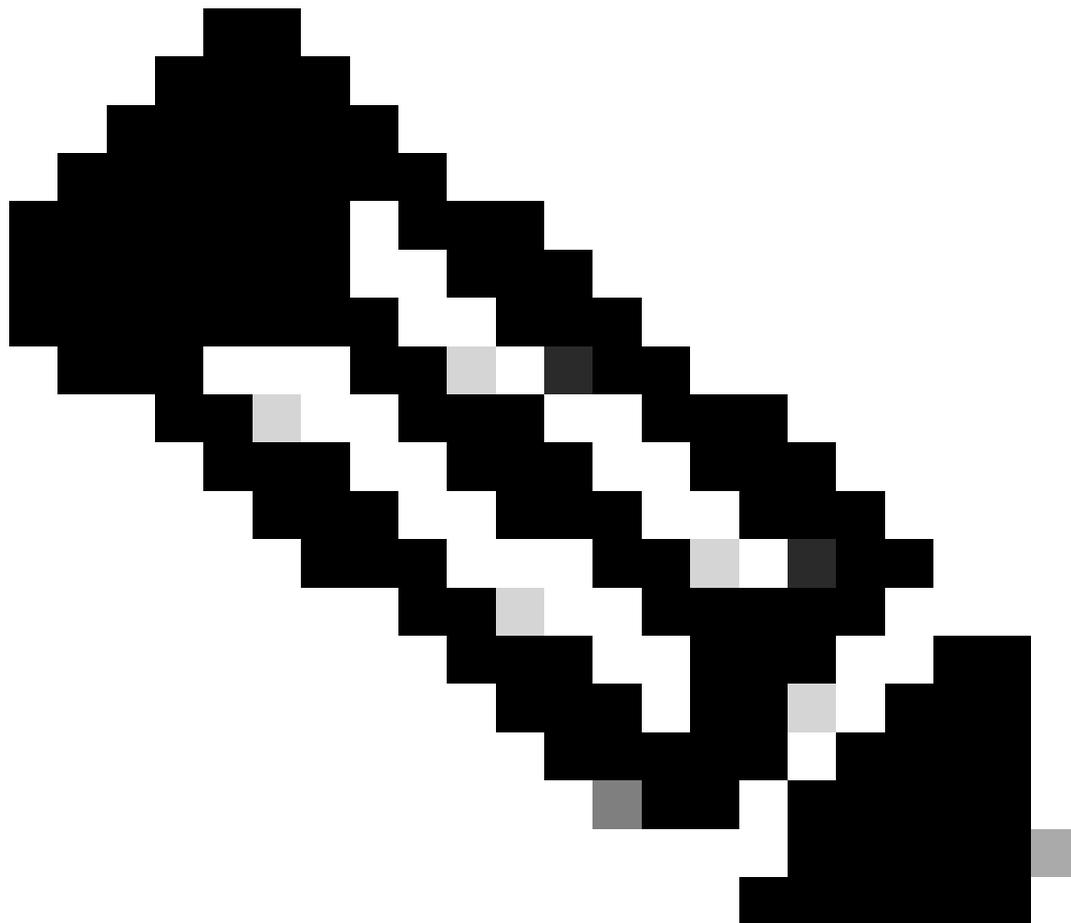
gui is restarting.

Reiniciar processo de proxy

Para reiniciar o processo Proxy, que é o processo principal do proxy, você pode usar a CLI. Estas são as etapas:

Etapa 1. iniciar sessão na CLI

Etapa 2. Diagnóstico de tipo



Observação: o diagnóstico é um comando oculto da CLI, portanto, você não pode preencher automaticamente o comando com TAB.

Etapa 3. Escolher PROXY

Etapa 4. Digite KICK, (é um comando oculto).

Etapa 5. Escolha Y para sim.

```
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

Informações Relacionadas

- [Manual do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - LD \(Implantação limitada\) - Solução de problemas \[Cisco Secure Web Appliance\] - Cisco](#)
- [Use as práticas recomendadas de dispositivos da Web seguros - Cisco](#)
- [ps\(1\) \(freebsd.org\)](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.