Dépannage des états de processus inhabituels dans SWA

Table des matières

Introduction

Ce document décrit l'état du processus et comment l'utiliser pour dépanner un problème de performances de l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SWA physique ou virtuel installé.
- Licence activée ou installée.
- Client Secure Shell (SSH).
- L'Assistant de configuration est terminé.
- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

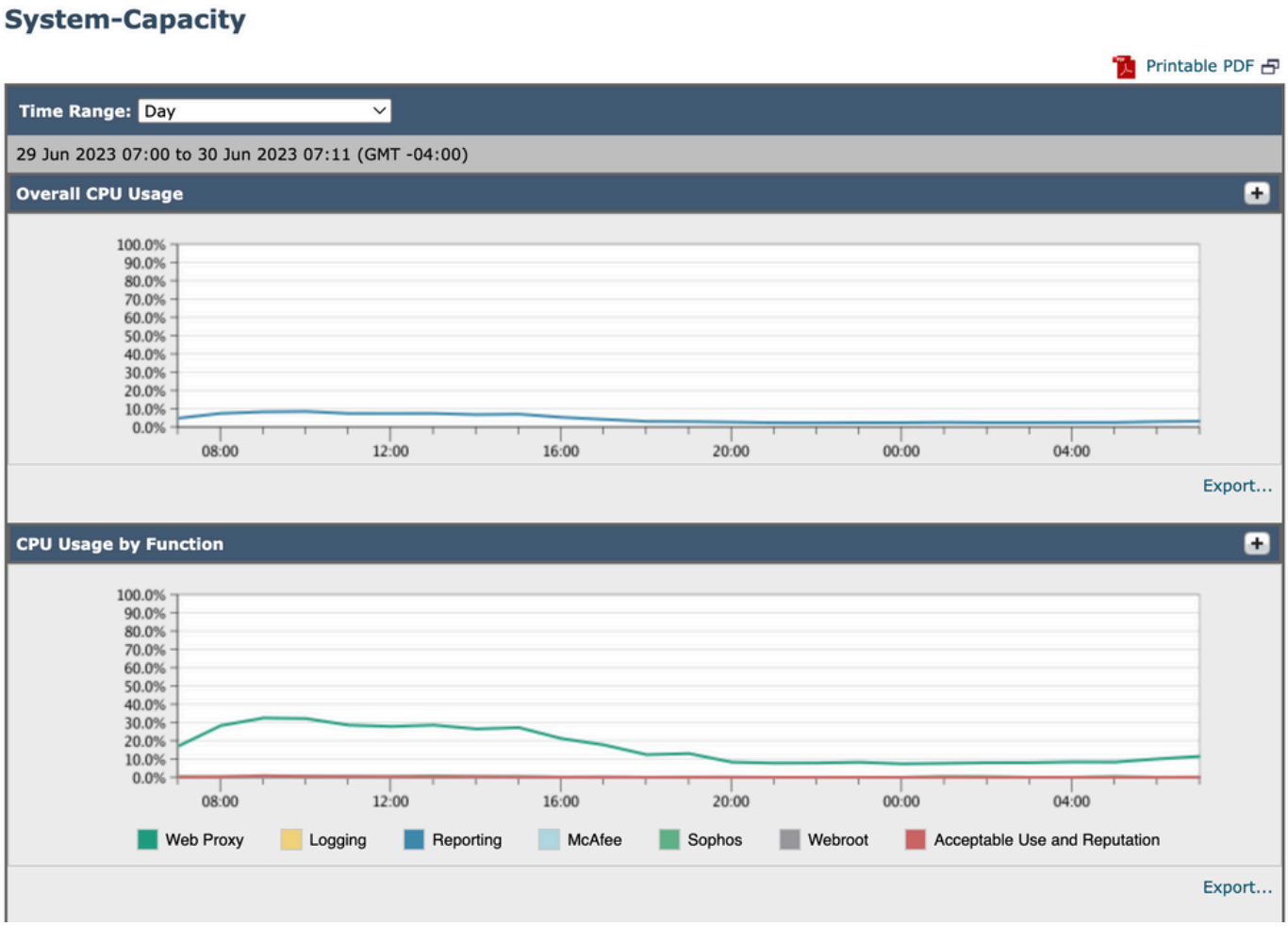
est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Surveiller l'état du processus

Vous pouvez surveiller l'état du processus à partir de l'interface graphique utilisateur (GUI) ou de l'interface de ligne de commande (CLI).

Afficher l'état du processus depuis la GUI

Pour afficher les statistiques de processus dans l'interface utilisateur graphique, accédez à Reporting et sélectionnez System Capacity. Vous pouvez sélectionner Intervalle de temps pour afficher l'allocation de ressources pour l'horodatage souhaité.

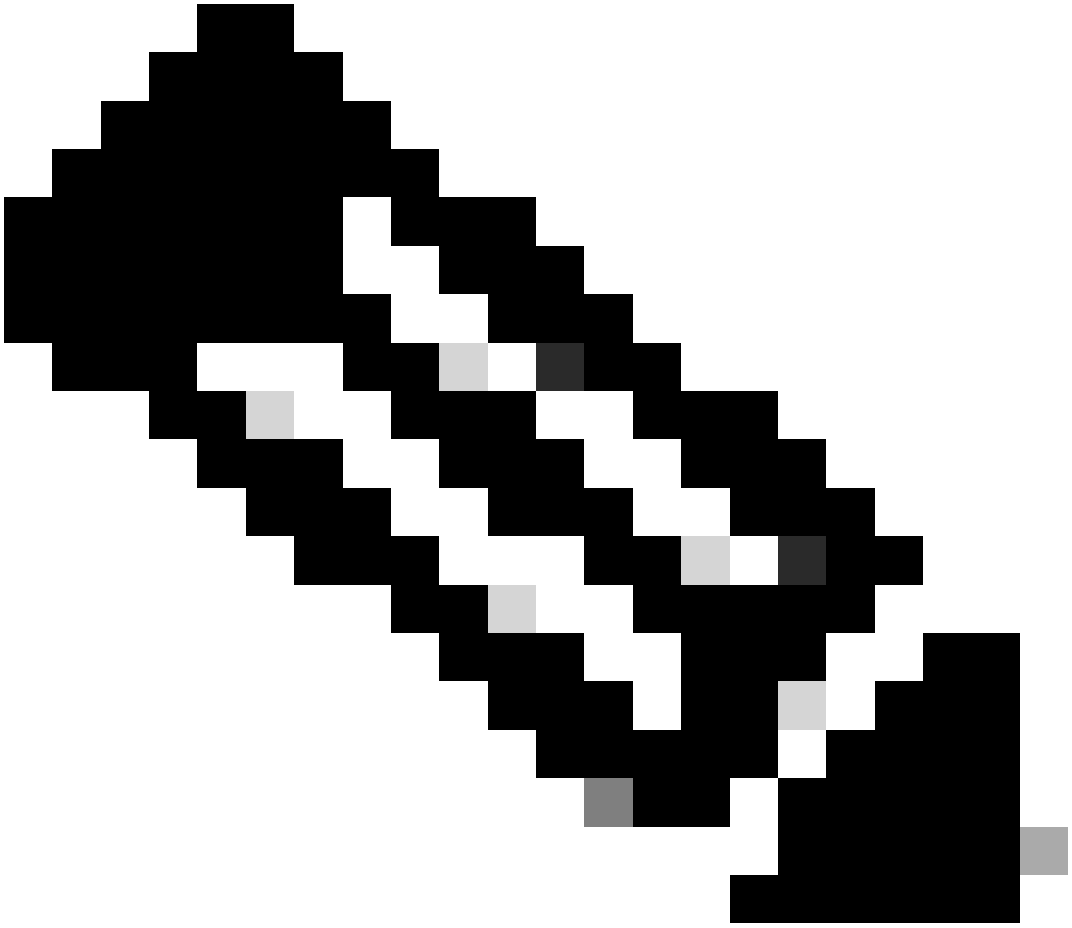


Capacité du système d'images

Utilisation totale du processeur : affiche l'utilisation totale du processeur

Utilisation de l'UC par fonction : affiche chaque sous-processus, allocation de l'UC.

Proxy Buffer Memory : affiche l'allocation de mémoire pour le processus proxy.



Remarque : la mémoire tampon du proxy n'est pas l'utilisation totale de la mémoire de SWA.

Commandes CLI

Il existe plusieurs commandes CLI qui indiquent la charge principale du processeur ou l'état du sous-processus :

status (état)

À partir de la sortie de status ou status detail, vous pouvez afficher l'utilisation CPU globale de SWA, ces commandes indiquent la charge CPU actuelle.

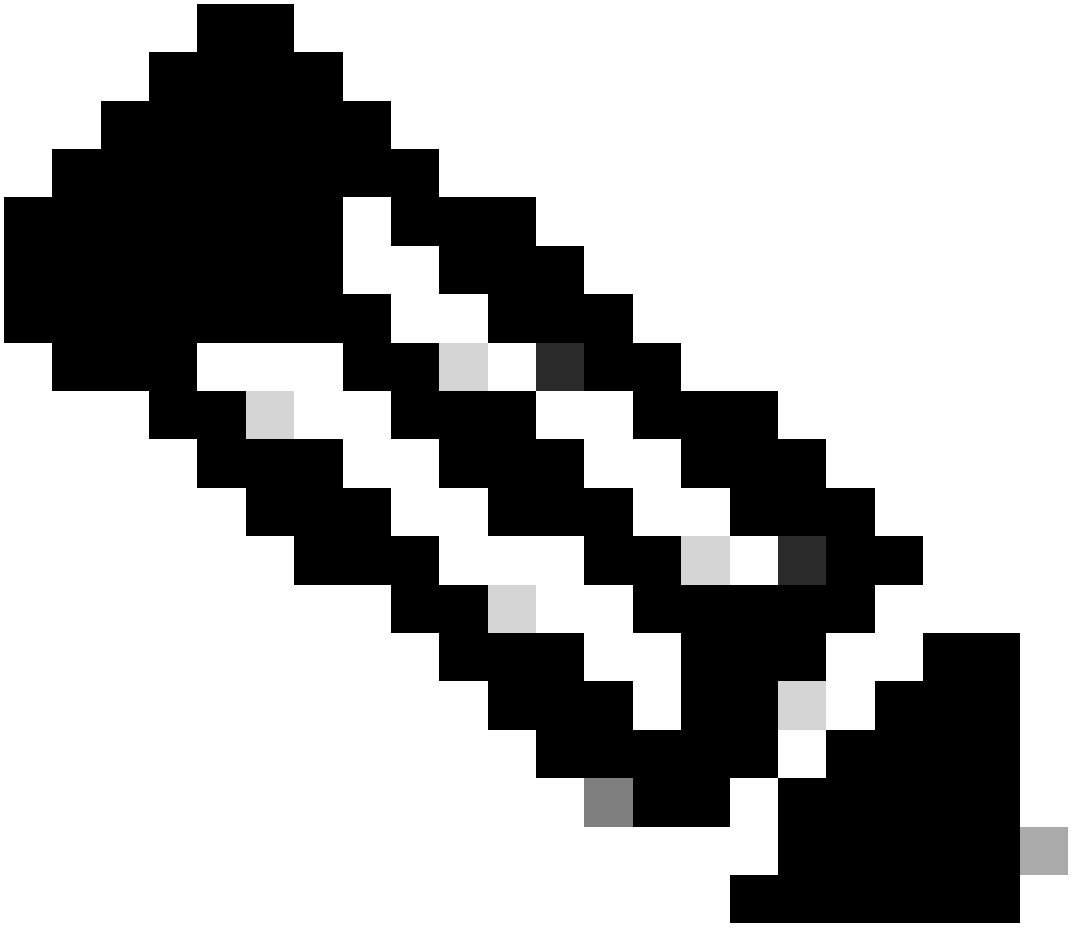
```
SWA_CLI)> status

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, affiche la charge du processus proxy, qui est un sous-processus qui est le processus principal dans SWA. Cette commande actualise automatiquement toutes les 15 secondes.

```
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
```



Remarque : "proxystat" est une autre commande CLI qui a le même résultat que la commande "rate"

---

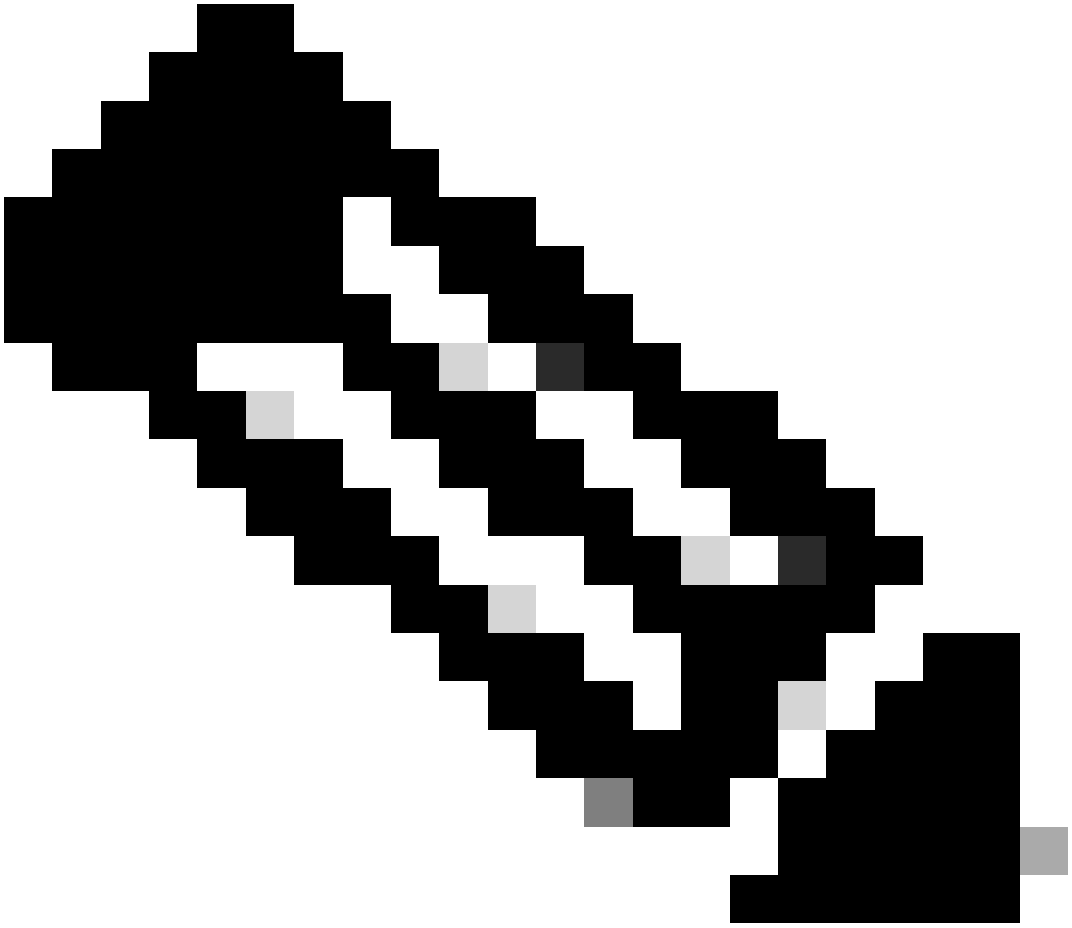
journaux_shd

Vous pouvez afficher l'état du processus principal, tel que l'état du processus proxy, l'état du processus de création de rapports, etc., à partir de SHD_Logs. Pour plus d'informations sur les journaux SHD, veuillez consulter ce lien :

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

Voici un exemple de résultat de shd_logs :

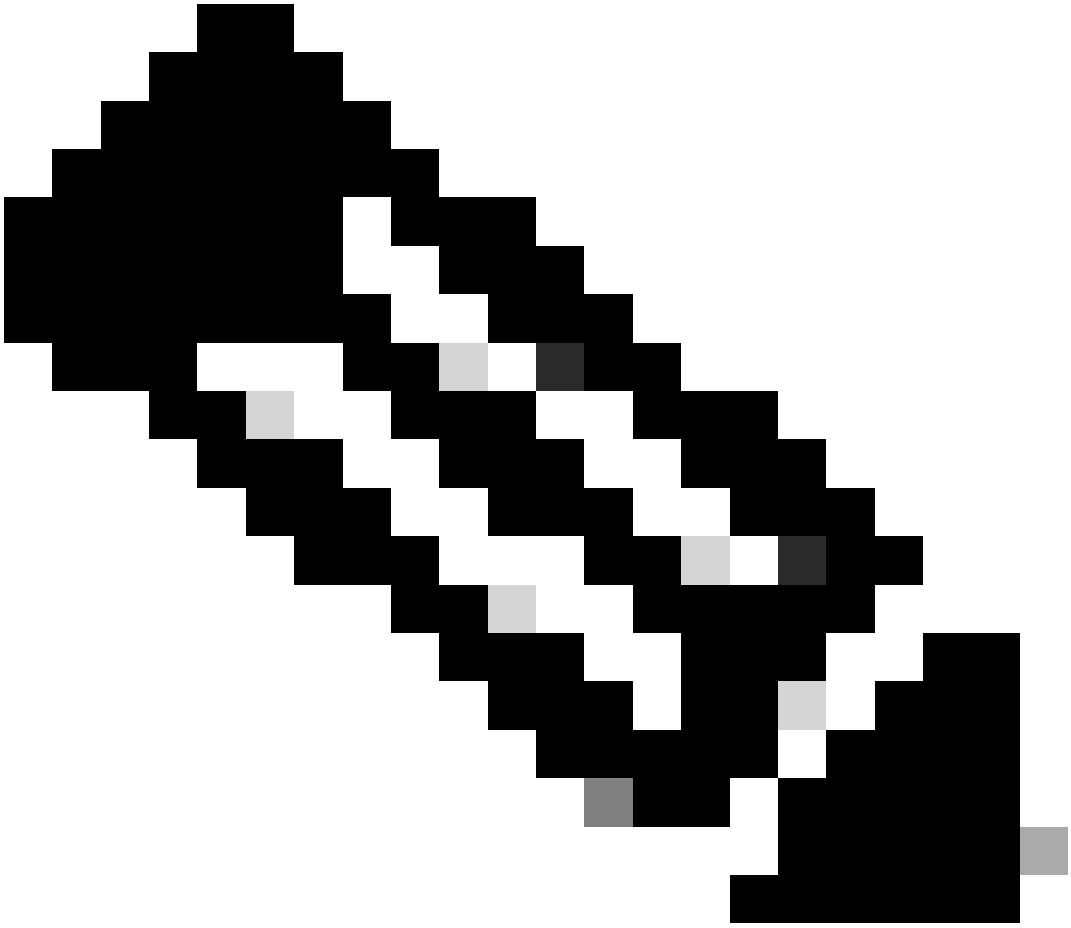
```
Sat Jun 24 06:30:29 2023 Info: Status: CPULd 2.9 DskUtil 14.4 RAMUtil 9.8 Reqs 112 Band 22081 Latency 4
```



Remarque : vous pouvez accéder à shd_logs à partir de la commande CLI grep ou tail.

statut_processus

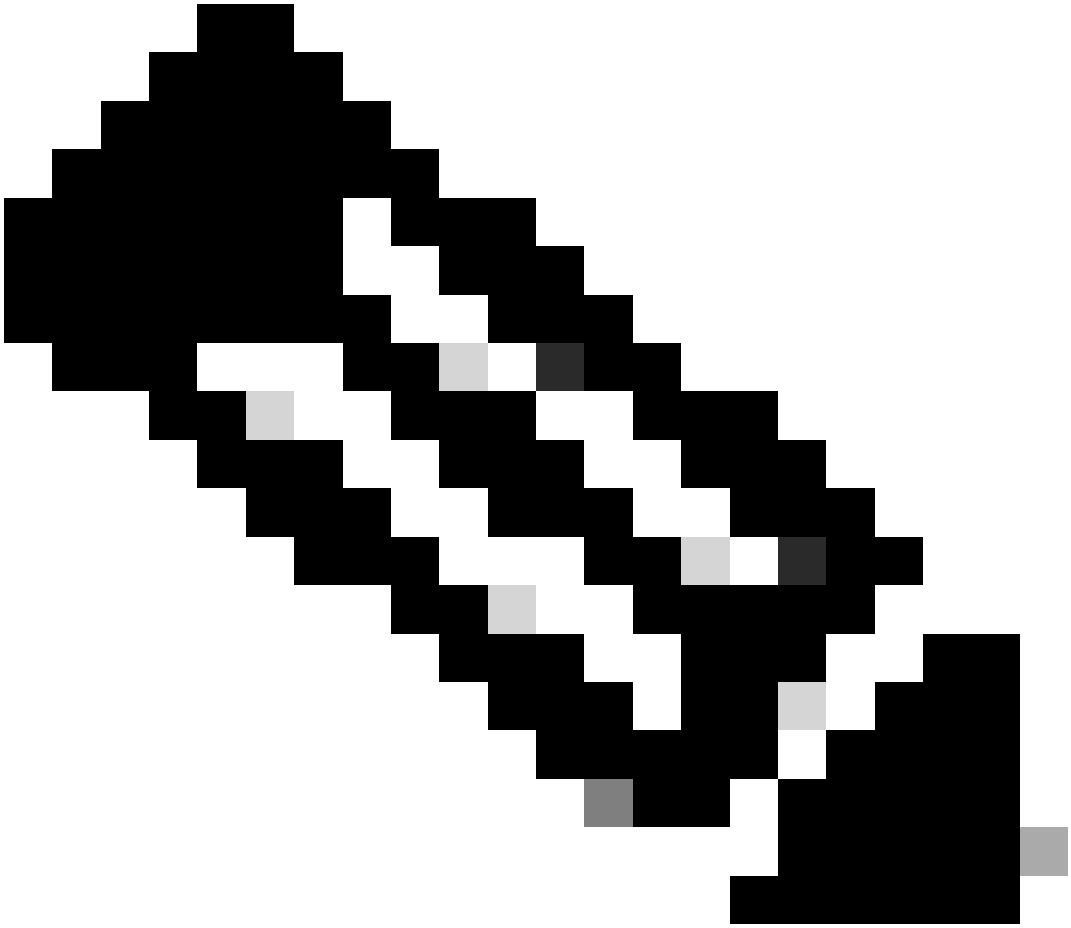
Pour afficher l'état du processus, dans les versions 14.5 et ultérieures, SWA a une nouvelle commande : process_status qui obtient les détails du processus de SWA.



Remarque : cette commande n'est disponible qu'en mode 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_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
```



Remarque : utilisation du processeur du processus ; il s'agit d'une moyenne décroissante sur une minute de temps précédent (réel). Étant donné que la base de temps sur laquelle ce calcul est effectué varie (puisque les processus peuvent être très jeunes), il est possible que la somme de tous les champs %CPU dépasse 100 %.

%MEM : pourcentage de mémoire réelle utilisé par ce processus

VSZ : taille virtuelle en kilo-octets (alias vsize)

RSS : Taille réelle de la mémoire (ensemble résident) du processus (en unités de 1024 octets).

TT : abréviation du nom de chemin du terminal de contrôle, le cas échéant.

ÉTAT

L'état est donné par une séquence de caractères, par exemple, "RNL". Le premier caractère indique l'état d'exécution du processus :

D : Marque un processus en attente sur disque (ou à court terme, ininterrompue).

I : Marque un processus inactif (en veille pendant plus de 20 secondes environ).

L : marque un processus en attente d'acquisition d'un verrou.

R : marque un processus exécutable.

S : marque un processus qui est en veille pendant moins d'environ 20 secondes.

T : marque un processus arrêté.

W : marque un thread d'interruption inactif.

Z : Marque un processus mort (un "zombie").

Les caractères supplémentaires suivants, le cas échéant, indiquent des informations d'état supplémentaires :

+ : Le processus se trouve dans le groupe de processus de premier plan de son terminal de contrôle.

< : le processus a augmenté la priorité de planification du processeur.

C : Le processus est en mode capsicum(4).

E : Le processus tente de se fermer. J Marque un processus qui est en prison(2).

L : le processus a des pages verrouillées dans le coeur (par exemple, pour les E/S brutes).

N : le processus a une priorité de planification CPU réduite.

s : Le processus est un amorce de session.

V : Le parent du processus est suspendu pendant un vfork(2), en attendant que le processus s'exécute ou s'arrête.

W : Le processus est échangé.

X : Le processus est suivi ou débogué.

TEMPS : temps CPU cumulé, utilisateur + système

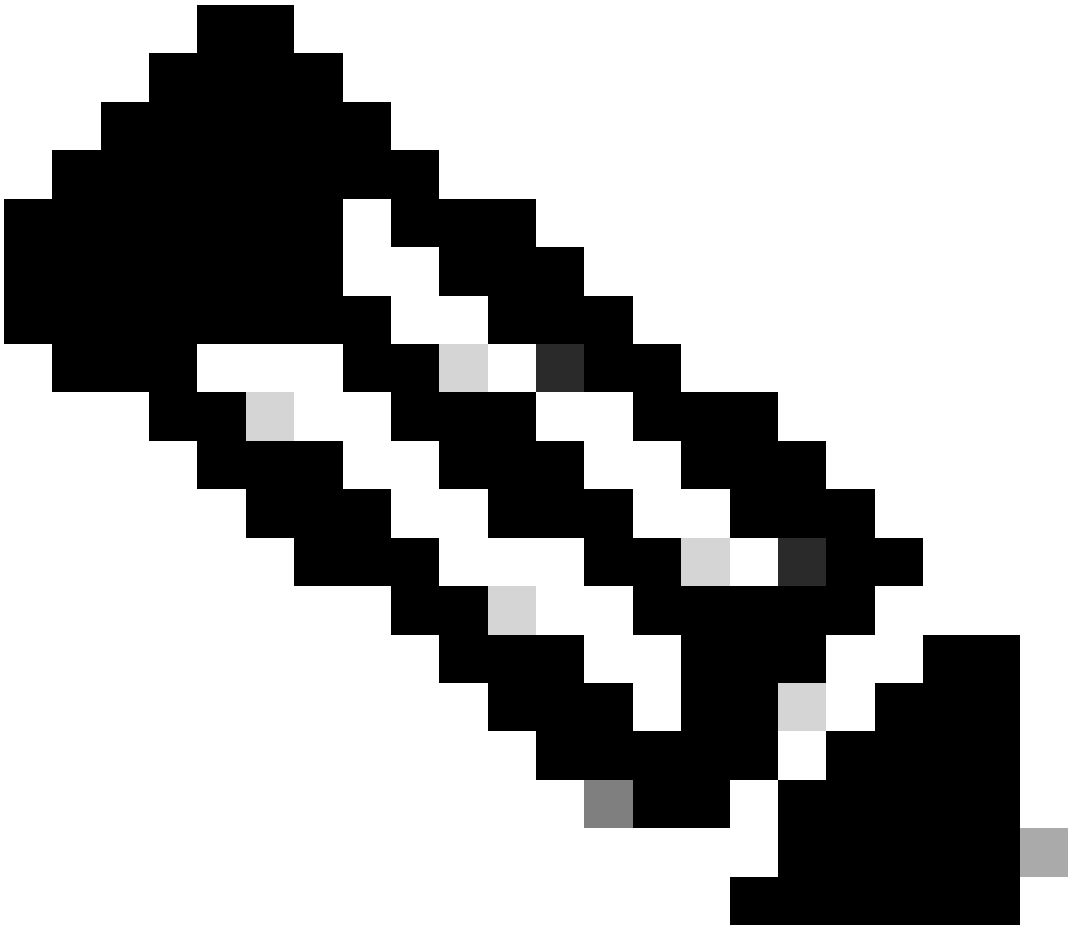
Redémarrer le processus dans SWA

Processus général

Vous pouvez redémarrer les services et le processus SWA à partir de l'interface de ligne de commande. Voici les étapes à suivre :

Étape 1 : connexion à l’interface de ligne de commande

Étape 2. Type de diagnostic

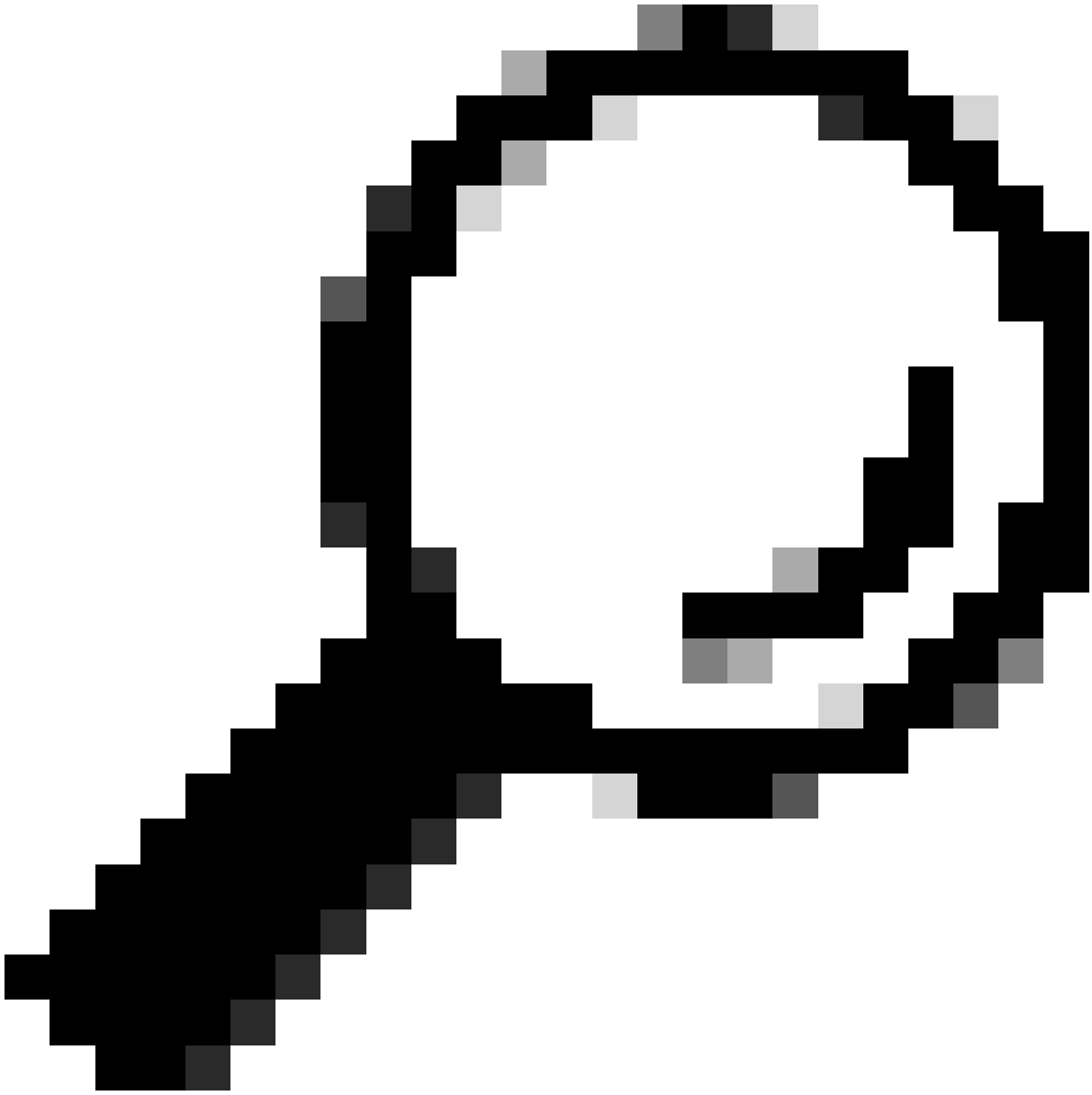


> Remarque : diagnostic est une commande masquée de l'interface de ligne de commande. Vous ne pouvez donc pas remplir automatiquement la commande avec la touche TAB.

Étape 3. Choisir des services

Étape 4. Sélectionnez le service/processus que vous souhaitez redémarrer.

Étape 5. Sélectionnez Redémarrer



Conseil : vous pouvez afficher l'état du processus à partir de la section STATUS.

Dans cet exemple, le processus WEBUI responsable de l'interface utilisateur graphique a été redémarré :

```
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
```

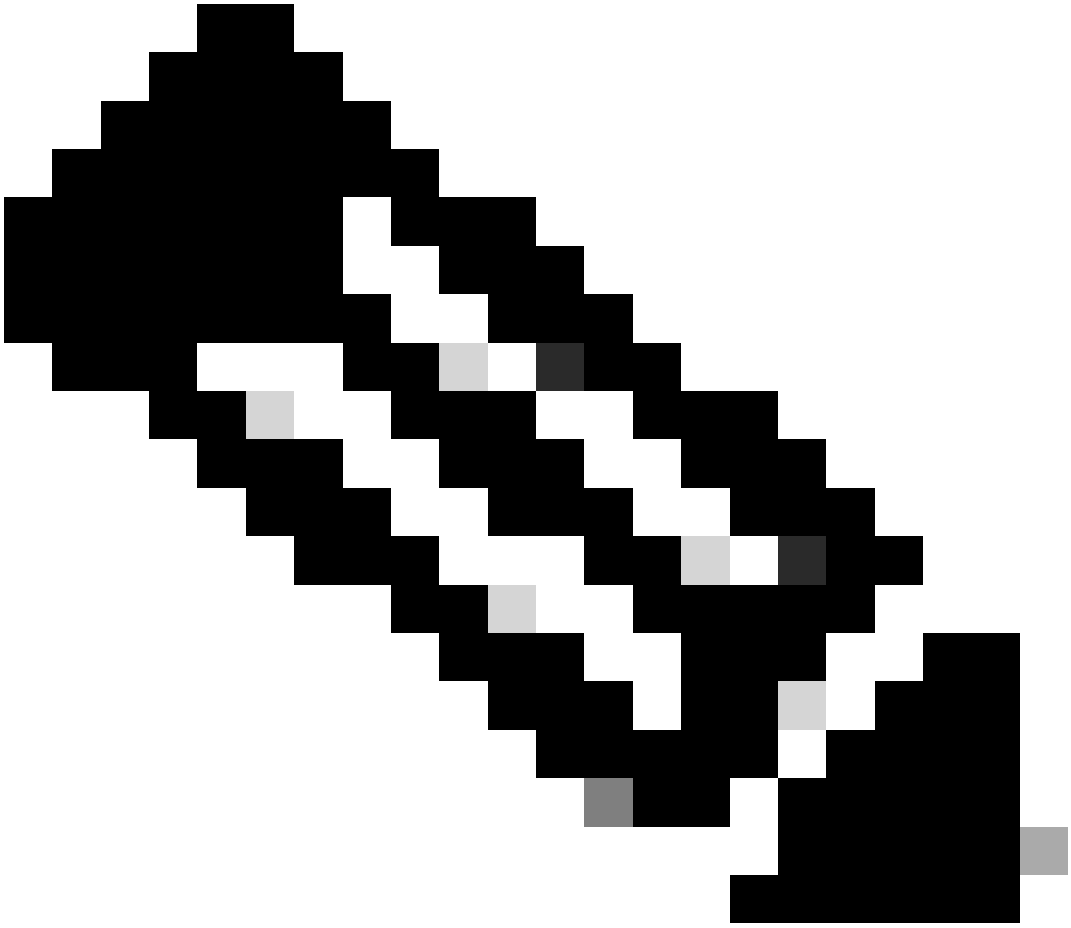
```
Choose one of the following services:
- AMP - Secure Endpoint
- AVC - AVC
- ADC - ADC
- DCA - DCA
- WBRS - WBRS
- EXTFEED - ExtFeed
- L4TM - L4TM
- ANTIVIRUS - Anti-Virus xiServices
- AUTHENTICATION - Authentication Services
- MANAGEMENT - Appliance Management Services
- REPORTING - Reporting Associated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

Redémarrer le processus proxy

Pour redémarrer le processus Proxy, qui est le processus principal du proxy, vous pouvez utiliser l'interface de ligne de commande. Voici les étapes à suivre :

Étape 1 : connexion à l’interface de ligne de commande

Étape 2. Type de diagnostic



Remarque : diagnostic est une commande masquée de l'interface de ligne de commande. Vous ne pouvez donc pas remplir automatiquement la commande avec la touche TAB.

Étape 3. Choisir un proxy

Étape 4. Tapez KICK, (il s'agit d'une commande masquée).

Étape 5. Sélectionnez Y pour 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
```

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooting [Cisco Secure Web Appliance] - Cisco
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco
- ps(1) (freebsd org)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.