Dépannage de la latence des appareils Web sécurisés

Table des matières

Introduction

Ce document décrit les étapes de dépannage permettant de résoudre les problèmes de latence élevée, de disque élevé et de CPU élevé dans Cisco Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration Cisco SWA
- Méthodes de déploiement de proxy (explicites et transparentes)
- Commandes de l'interface de ligne de commande (CLI) 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.

Informations générales

Lorsque vous contactez l'assistance technique Cisco, vous êtes invité à fournir des détails sur l'activité réseau sortante et entrante SWA, qui peut être surveillée en exécutant une capture de paquets pour collecter le trafic à des fins de débogage ou de vérification.

Causes fréquentes de la latence élevée dans SWA

En général, il existe trois catégories principales pour la latence élevée dans SWA :

1. Dimensionnement inadéquat des MFS ou ressources surchargées
2. Configurations complexes
3. Problèmes de latence liés au réseau

L'une des causes les plus courantes de latence élevée dans SWA est le dimensionnement inadéquat de la solution. Un dimensionnement approprié est essentiel pour garantir que le système SWA dispose de ressources suffisantes pour gérer les charges de travail actuelles et prévues. Si le système est sous-dimensionné, il peut avoir du mal à traiter les demandes efficacement, ce qui entraîne des retards dans les opérations et une baisse des performances. Des facteurs tels que le nombre d'utilisateurs, le volume de décryptage et les demandes d'analyse spécifiques doivent être soigneusement évalués au cours du déploiement afin d'éviter des contraintes de ressources. L'incapacité à aligner la capacité SWA sur les besoins de l'entreprise peut entraîner une latence persistante et une dégradation de l'expérience utilisateur.

Des configurations complexes peuvent dégrader les performances et provoquer une latence sur le SWA, en particulier en cas de charge élevée, car chaque demande doit être traitée dans de nombreuses conditions.

La latence liée au réseau peut provenir du SWA lui-même, de services tiers tels qu'Active Directory, DLP, DNS ou de retards réseau entre le client, le SWA et les serveurs en amont.

L'analyse des requêtes envoyées à l'agent SWA, y compris l'identification des principaux utilisateurs et des URL les plus consultées, peut aider à détecter les comportements potentiellement incorrects et à identifier les causes profondes de la latence. Ces informations sont précieuses pour diagnostiquer les problèmes de performances, gérer la consommation de bande passante et garantir une utilisation appropriée du système.

Outils de dépannage de latence SWA

État du système

Pour vérifier la consommation actuelle des ressources dans SWA, procédez comme suit :

Étape 1 : accès à l’interface graphique utilisateur de SWA

Étape 2. Accédez à Reporting > System Information > System Status.

Étape 3. Vérifiez ces indicateurs critiques pour évaluer les performances du système :

- Utilisation du processeur (%) : Indique la charge actuelle du processeur
- Utilisation de la mémoire vive (%) : Reflète l'utilisation de la mémoire
- Utilisation des rapports/consignations (%) : Affiche le pourcentage d'espace disque utilisé pour la création de rapports et la journalisation
- Temps de disponibilité du système : Affiche la durée totale d'exécution du système sans redémarrage

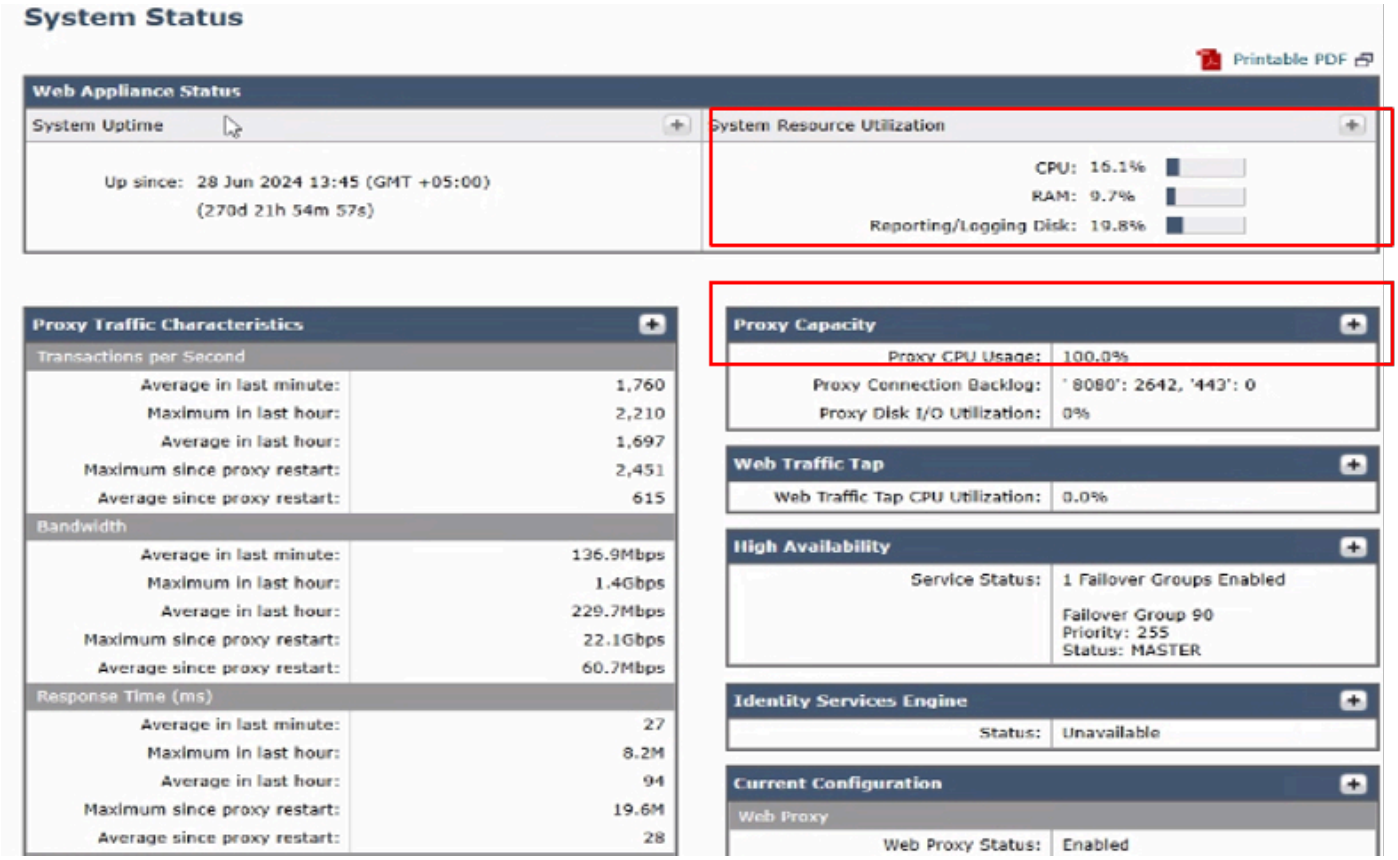


Image - État du système

Cette page présente l'état actuel de l'utilisation de la mémoire vive, du processeur et du disque. Pour afficher l'utilisation des ressources dans le temps, à partir de l'interface utilisateur graphique de SWA, naviguez jusqu'à Reporting et choisissez System Capacity.

Capacité du système

La page System Capacity du SWA fournit une vue complète de l'utilisation des ressources et des mesures de performances sur une période donnée. Cette page propose des graphiques détaillés qui permettent de surveiller et d'analyser le comportement du système, de garantir des performances optimales et d'identifier les goulots d'étranglement potentiels.

Les graphiques et mesures disponibles dans la page Capacité du système sont les suivants :

1. Utilisation globale du processeur : Affiche l'utilisation totale du processeur, ce qui donne une vue d'ensemble générale des performances du système.
2. Utilisation de l'UC par fonction : ventile l'utilisation de l'UC en fonction de fonctions spécifiques, notamment :

- Proxy Web
- Journalisation
- Rapports
- McAfee
- Sophos
- Webroot
- Utilisation et réputation acceptables

3. Temps de réponse/Latence (millisecondes) : effectue le suivi des temps de réponse pour identifier tout retard dans le traitement des demandes.

4. Transactions par seconde : Affiche le nombre de transactions traitées par le SWA par seconde.

5. Connexions sortantes Surveille le nombre de connexions sortantes en cours d'établissement.

6. Bande passante sortante (octets) : Mesure la quantité de bande passante sortante utilisée.

7. Mémoire tampon du proxy (%) : Affiche le pourcentage de mémoire utilisé par le processus proxy.

Vérifiez les mesures pour détecter tout signe d'utilisation élevée des ressources dans ce tableau de bord.

Capacité du système d'images

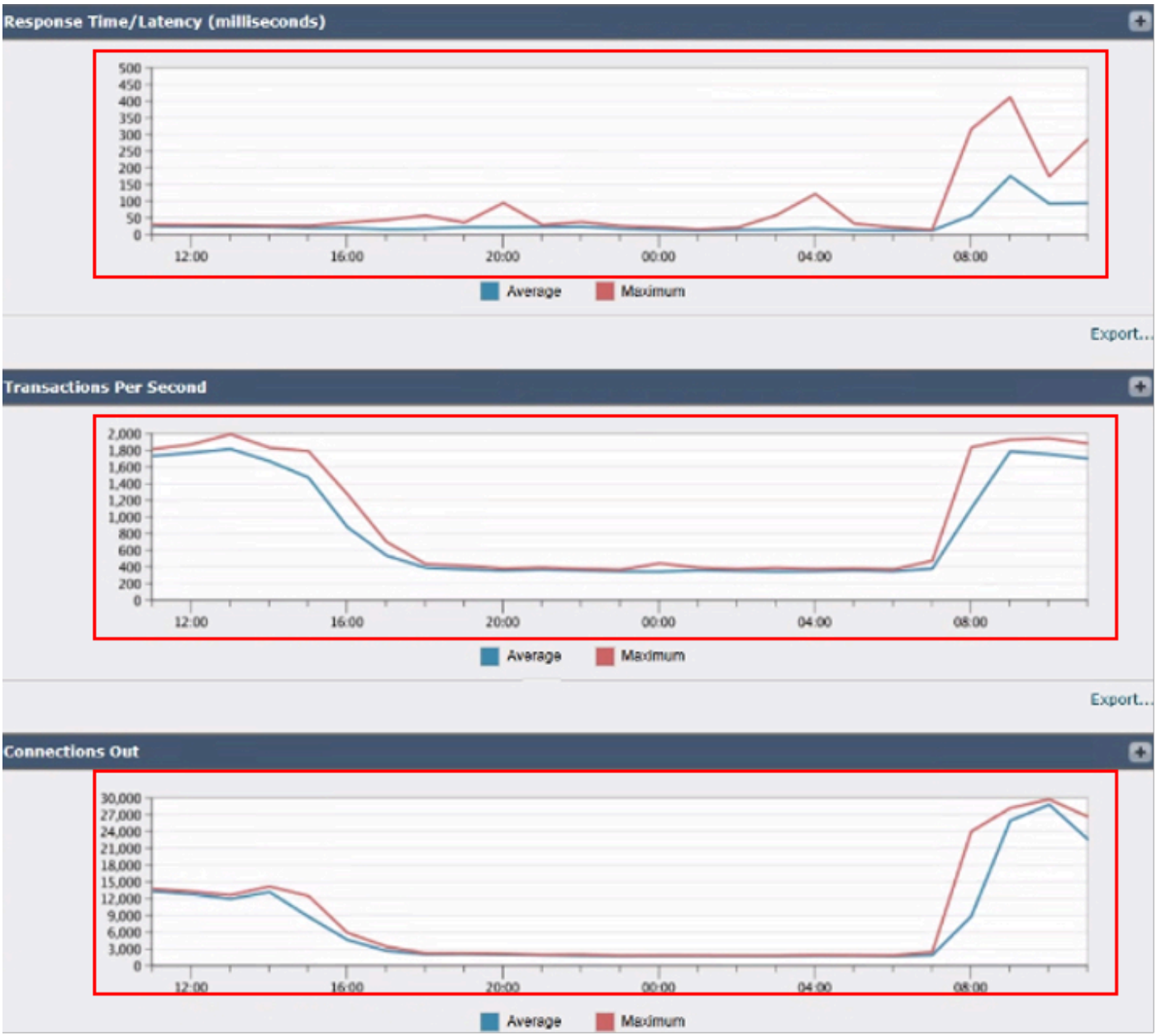


Image - Transactions SWA par seconde et connexions sortantes

Image - Utilisation de la mémoire SWA

Analyser les principales destinations

Pour analyser les principales destinations, accédez à l'interface utilisateur graphique de SWA, accédez à Reporting et sélectionnez Websites. Passez en revue la liste des principaux sites Web HTTP/HTTPS et identifiez les domaines à trafic élevé ou fréquemment consultés.

En fonction de vos conclusions, envisagez de contourner ou d'exempter les URL génériques, telles que Microsoft Updates, Adobe, Office365 et les plates-formes de réunion en ligne. Cette approche permet de réduire le trafic sur le SWA, ce qui réduit la latence et la charge de traitement du proxy.

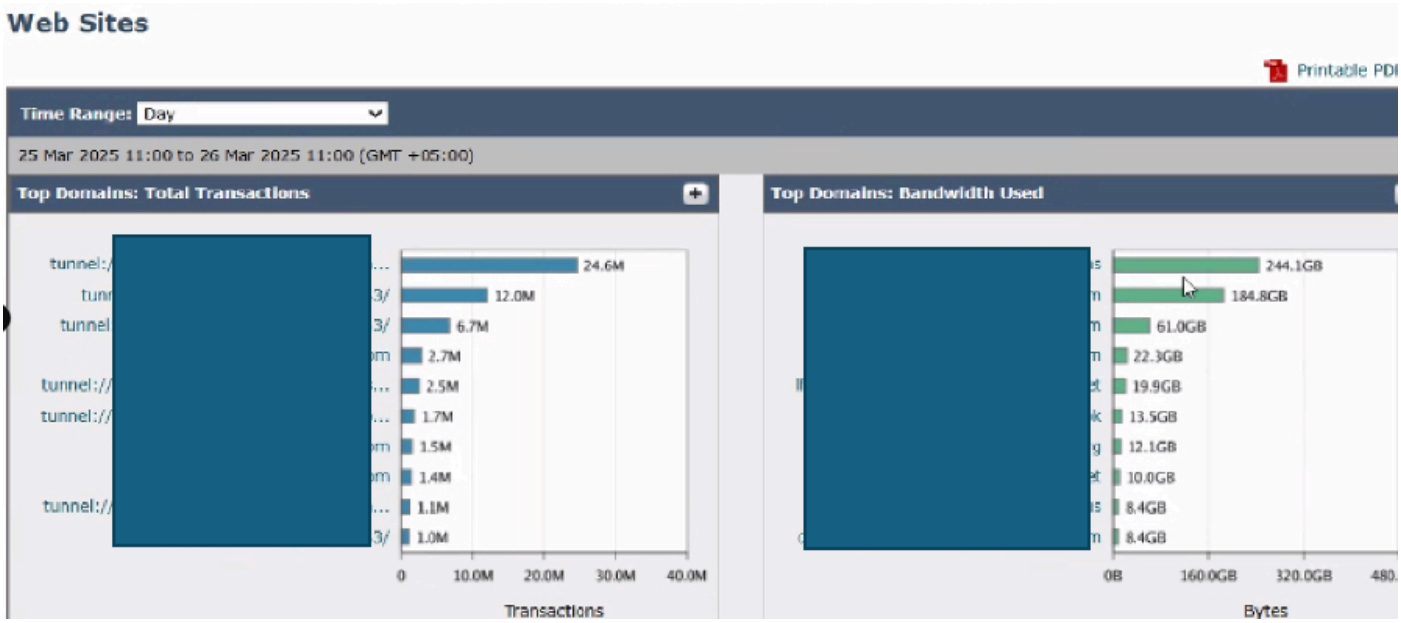


Image- Tableau de bord des principaux sites Web SWA

Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted]	0B	23514:57	0	24.6M	24.6M
	0B	1909:50	0	12.0M	12.0M
	0B	26710:03	0	6.7M	6.7M
	3.0MB	4941:17	2,798	2.7M	2.7M
	0B	10029:17	0	2.5M	2.5M
	0B	2579:58	0	1.7M	1.7M
	4.2GB	5981:18	1.5M	0	1.5M
	184.8GB	2125:54	1.4M	1,806	1.4M
	0B	2062:27	0	1.1M	1.1M
	0B	1354:09	0	1.0M	1.0M
Totals (all available data):	741.1GB	111839:46	6.7M	64.8M	71.5M

Image - Tableau de bord des principaux domaines SWA

Analyser les principaux utilisateurs

Pour identifier les sources potentielles de trafic excessif, accédez à l'interface utilisateur graphique SWA à partir de Reporting et sélectionnez Users.

Consultez la liste pour déterminer les utilisateurs qui génèrent le plus grand nombre de transactions vers l'agent SWA. En outre, recherchez les machines utilisateur qui génèrent le plus grand nombre de transactions vers le SWA et qui consomment la bande passante maximale.

Cette analyse peut aider à identifier les utilisateurs ou les périphériques responsables de charges de trafic importantes, permettant ainsi des actions ciblées pour réduire la pression globale du système.

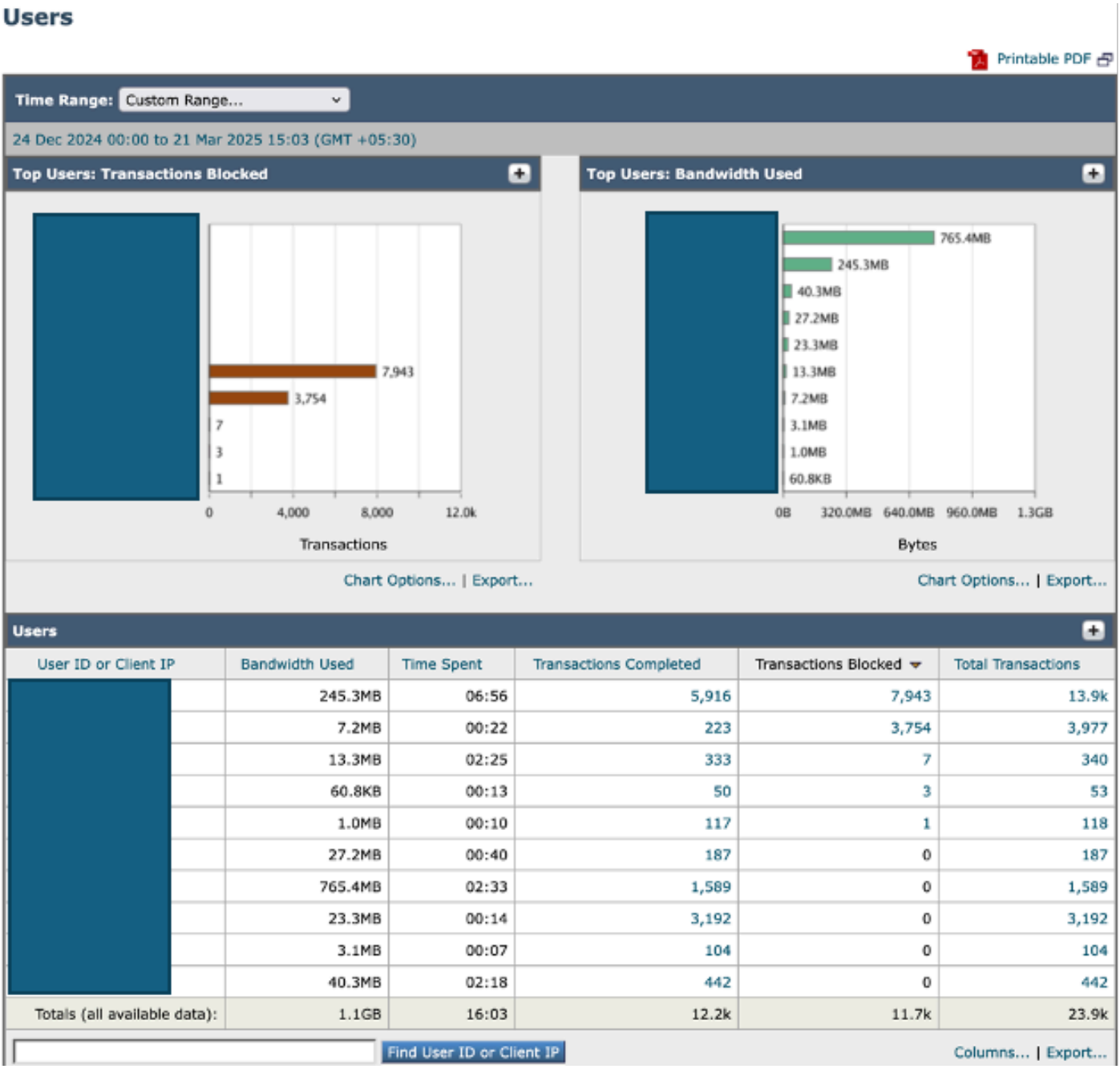


Tableau de bord des principaux utilisateurs Image-SWA

Journaux SHD

En examinant le fichier SHD_log, vous pouvez analyser certaines mesures de performances telles que le nombre de sessions des utilisateurs vers SWA (CliConn), le nombre de sessions de SWA vers Internet (SrvConn), la moyenne des demandes par seconde (Reqs), etc.

Pour plus d'informations sur le journal SHD, référez-vous au lien Dépannage des performances de l'appareil Web sécurisé avec les journaux SHD,

Voici quelques paramètres clés à examiner dans les journaux SHD :

- Connexions client : Nombre de connexions client actives

- Connexions serveur : Nombre de connexions serveur actives
- ProxLd : Charge moyenne du processus proxy
- CPULD : Charge moyenne globale du processeur
- RAMUTIL : utilisation de la RAM
- Latence : temps moyen de service en une minute
- DiskUtil : utilisation du disque et performances d'E/S

Comme dans cet exemple, le fait d'avoir environ 1 600 requêtes par seconde entraîne une charge de processus proxy élevée.

```
Wed Mar 26 11:09:30 2025 Info: Status: CPULd 16.3 DskUtil 19.9 RAMUtil 9.3 Reqs 1661 Band 152966 Latenc
Wed Mar 26 11:10:31 2025 Info: Status: CPULd 13.6 DskUtil 19.9 RAMUtil 9.5 Reqs 1699 Band 107048 Latenc
Wed Mar 26 11:11:31 2025 Info: Status: CPULd 15.0 DskUtil 19.9 RAMUtil 9.5 Reqs 1669 Band 178803 Latenc
Wed Mar 26 11:12:31 2025 Info: Status: CPULd 17.6 DskUtil 19.9 RAMUtil 9.2 Reqs 1785 Band 143721 Latenc
```

Utilisation des journaux d'accès pour résoudre les problèmes de latence

Lorsque des problèmes de latence surviennent lorsque le trafic est transmis par proxy via un SWA, les journaux d'accès peuvent servir d'outil précieux pour identifier la cause racine probable. Pour améliorer les efforts de dépannage, vous pouvez modifier les paramètres existants du journal d'accès ou créer un nouveau journal d'accès. En incluant les paramètres de performance dans le champ personnalisé, vous pouvez obtenir des informations plus détaillées sur les facteurs contribuant à la latence, ce qui permet une analyse et une résolution plus efficaces.

Pour plus d'informations sur les paramètres de performance et les étapes de configuration, référez-vous au lien : Configurer le paramètre de performance dans les journaux d'accès

Voici le guide détaillé pour collecter les journaux dans le SWA : Accéder aux journaux de l'appliance Web sécurisée

Les sources de latence peuvent être analysées en examinant les paramètres clés qui aident à déterminer si des retards se produisent entre le client et le SWA, à l'intérieur des processus internes du SWA ou entre le SWA et le serveur Web. Les indicateurs importants à prendre en compte incluent les services réseau tels que la résolution DNS, le temps d’authentification et les temps de réponse du serveur ou du client. En outre, les retards provoqués par des moteurs d'analyse tels qu'AMP, Sophos et AVC doivent être évalués afin d'identifier leur impact sur la latence globale.

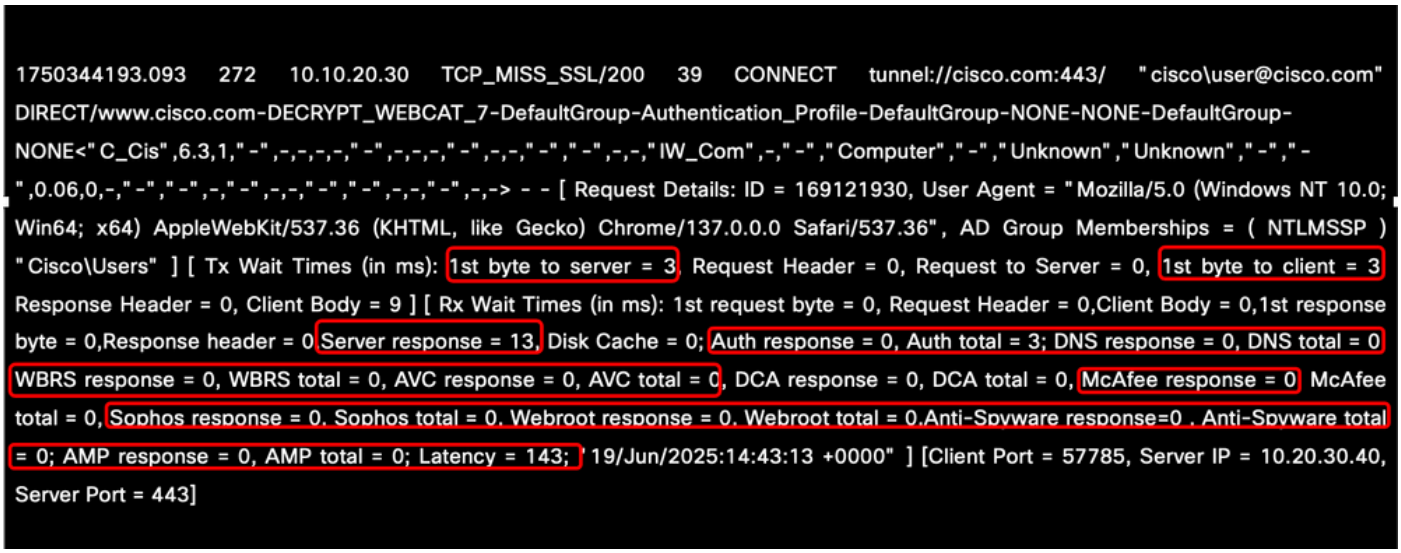


Image - Paramètres de performance dans AccessLog

Temps d'authentification élevé

Si le temps de réponse de l'authentification est élevé, ces informations sont nécessaires pour que le TAC puisse dépanner la latence de l'authentification de manière plus efficace et plus rapide :

- Configuration SWA actuelle
- Journaux d'authentification en mode débogage ou trace
- Captures de paquets depuis
    - Ordinateur client.
    - SWA (avec filtre pour capturer le trafic client et le trafic SWA vers tous les répertoires actifs configurés dans les paramètres de domaine.)
- Assurez-vous que les journaux d'accès comportent les champs personnalisés %m et %g pour identifier le mécanisme et les groupes d'authentification
- Fichier HAR du client lors de la reproduction du problème
- Le résultat de la commande testauthconfig de l'interface de ligne de commande

Cet exemple montre le temps de latence élevé lié à l'authentification :

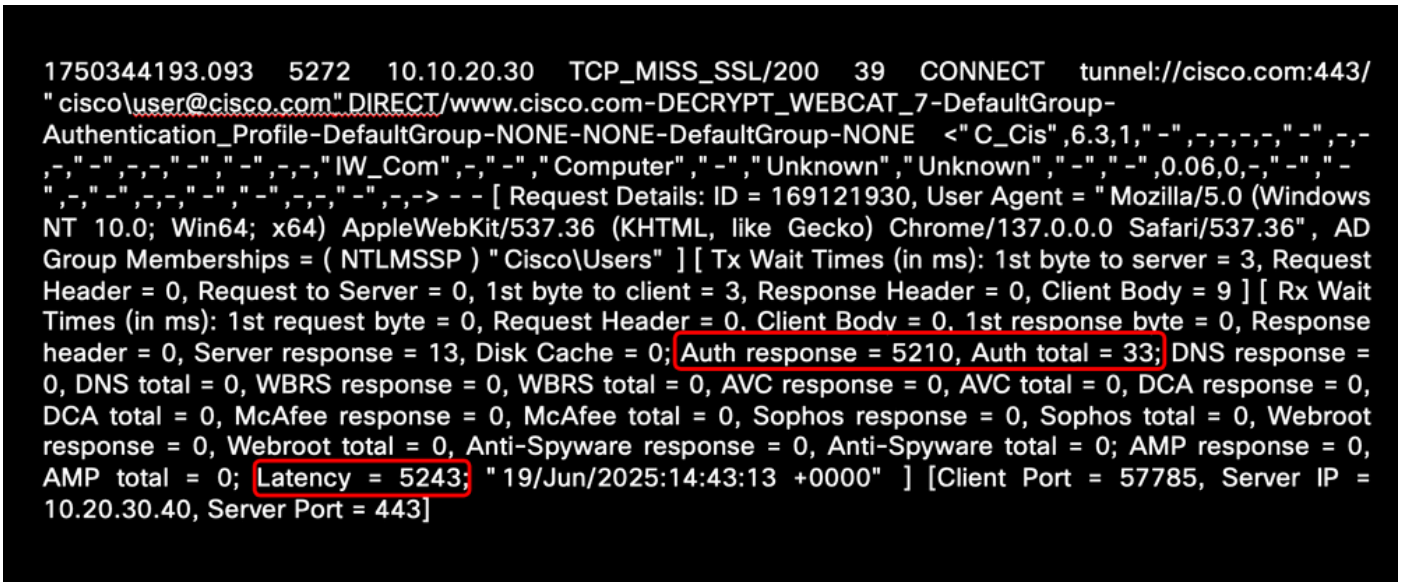


Image - Exemple de latence d'authentification élevée

Temps DNS élevé

Si le temps de réponse DNS est élevé, ces informations sont requises pour que le TAC puisse résoudre les problèmes de latence DNS :

- Configuration SWA actuelle
- Journaux système en mode trace
- Adresse IP des serveurs DNS
- Captures de paquets depuis
    - Ordinateur client
    - SWA (Filtrage avec l'adresse IP des serveurs DNS)
- Assurez-vous que les journaux d'accès contiennent %:<d et %:>d dans le champ personnalisé
- Fichier HAR du client lors de la reproduction du problème

Pour en savoir plus sur la configuration et le dépannage DNS, référez-vous au lien Dépannage du service DNS de l'appliance Web sécurisé

Cet exemple montre le temps de latence élevé lié à la résolution de noms DNS :

```
1750344193.093    4472    10.10.20.30    TCP_MISS_SSL/200    39    CONNECT    tunnel://cisco.com:443/
" cisco\user@cisco.com" DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-
Authentication_Profile-DefaultGroup-NONE-NONE-DefaultGroup-NONE    <" C_Cis" ,6.3,1," -" ,-,-,-,-," -" ,-,-
,-," -" ,-,-," -" ," -" ,-,-," IW_Com" ,-," -" ," Computer" ," -" ," Unknown" ," Unknown" ," -" ," -" ,0.06,0,-," -" ," -
" ,-," -" ,-,-," -" ," -" ,-,-," -" ,-,-> - - [ Request Details: ID = 169121930, User Agent = " Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36" , AD
Group Memberships = ( NTLMSSP ) " Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request
Header = 0, Request to Server = 0, 1st byte to client = 3, Response Header = 0, Client Body = 9 ] [ Rx Wait
Times (in ms): 1st request byte = 0, Request Header = 0, Client Body = 0, 1st response byte = 0, Response
header = 0, Server response = 13, Disk Cache = 0; Auth response = 0, Auth total = 3; DNS response = 4320,
DNS total = 65, WBRS response = 0, WBRS total = 0, AVC response = 0, AVC total = 0, DCA response = 0,
DCA total = 0, McAfee response = 0, McAfee total = 0, Sophos response = 0, Sophos total = 0, Webroot
response = 0, Webroot total = 0, Anti-Spyware response = 0, Anti-Spyware total = 0; AMP response = 0,
AMP total = 0; Latency = 4353; " 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP =
10.20.30.40, Server Port = 443]
```

Image - Exemple de latence haute résolution DNS

Temps de moteur d'analyse élevé

Si le temps de réponse est élevé pour les moteurs Web Reputation Score (WBRS), Application and Visibility Control (AVC) et Malware Scanning, ces informations sont requises pour que le TAC puisse dépanner le moteur d'analyse en cas de temps de réponse élevé :

- Configuration SWA actuelle.
- Selon le moteur qui a un temps de réponse élevé, changez le niveau de journalisation en debug.

Cet exemple montre le temps de latence élevé associé au moteur Sophos :

```
1750344193.093    4500    10.10.20.30    TCP_MISS_SSL/200    39    CONNECT    tunnel://cisco.com:443/
" cisco\user@cisco.com"DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-Authentication_Profile-
DefaultGroup-NONE-NONE-DefaultGroup-NONE    <" C_Cis" ,6.3,1," -" ,-,-,-,-," -" ,-,-,-," -" ,-,-,-," -" ,-,-
," IW_Com" ,-," -" ," Computer" ," -" ," Unknown" ," Unknown" ," -" ," -" ,0.06,0,-," -" ," -" ,-,-," -" ,-,-> - - [ Request Details: ID = 169121930, User Agent = " Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36" , AD Group Memberships = (
NTLMSSP ) " Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request Header = 0, Request to
Server = 0, 1st byte to client = 3, Response Header = 0, Client Body = 9 ] [ Rx Wait Times (in ms): 1st request
byte = 0, Request Header = 0, Client Body = 0, 1st response byte = 0, Response header = 0, Server response =
13, Disk Cache = 0; Auth response = 0, Auth total = 0; DNS response = 0, DNS total = 0, WBRS response = 0,
WBRS total = 0, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0,
McAfee total = 0, Sophos response = 4376, Sophos total = 145, Webroot response = 0, Webroot total = 0,
Anti-Spyware response = 0, Anti-Spyware total = 0; AMP response = 0, AMP total = 0; Latency = 4409;
" 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP = 10.20.30.40, Server Port = 443]
```

Image - Latence élevée du moteur d'analyse des programmes malveillants

Si les moteurs d'analyse affichent une réponse élevée, pour une récupération immédiate, vous pouvez redémarrer le service d'analyse à partir de l'interface de ligne de commande en procédant comme suit :

Étape 1. Tapez diagnostic et appuyez sur Entrée (il s’agit d’une commande masquée et vous devez taper la commande exacte.)

Étape 2. Sélectionnez SERVICES.

Étape 3. Pour redémarrer le service WBRS, choisissez WBRS sinon passez à l'étape 6.

Étape 4. Choisissez RESTART.

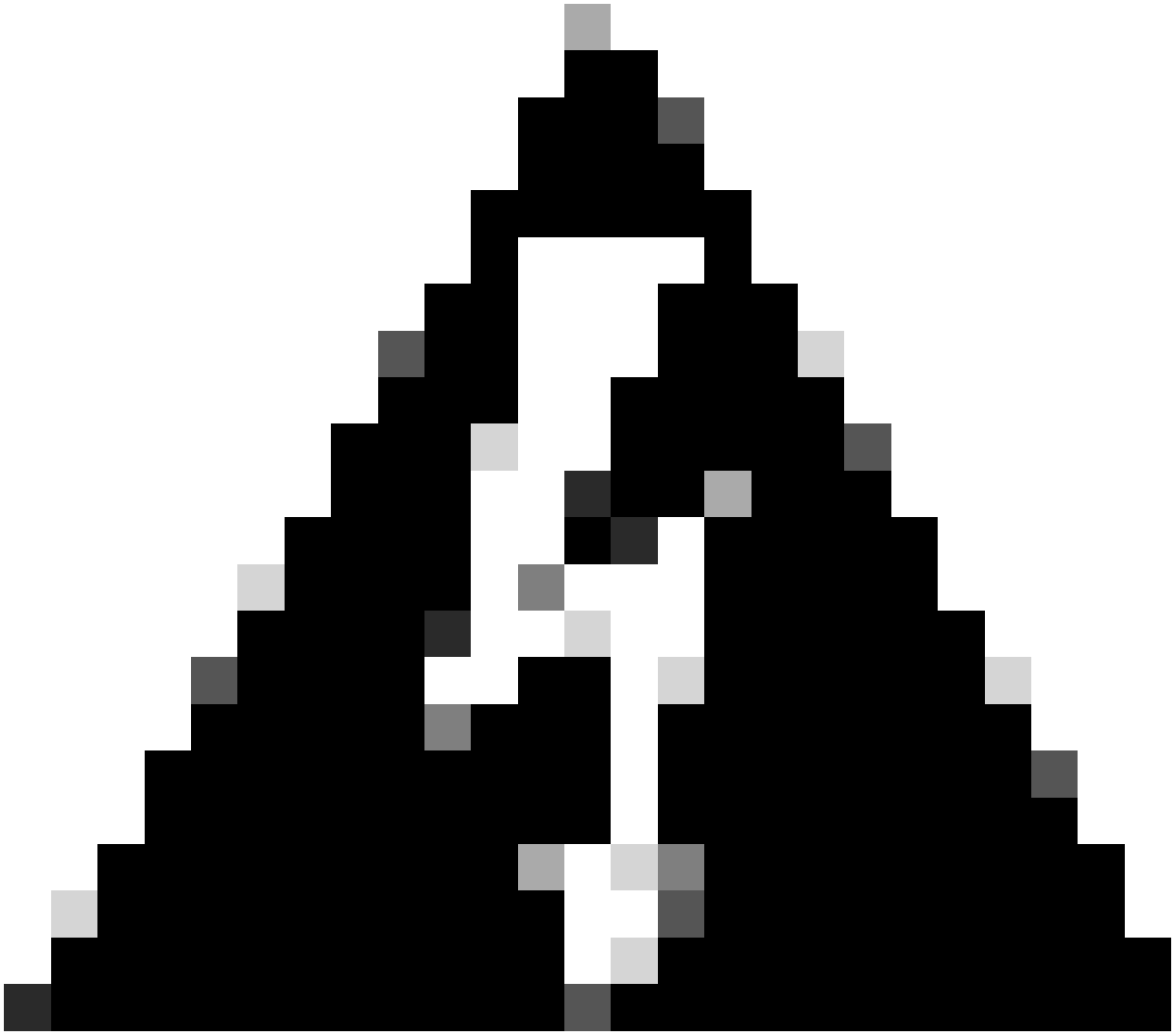
Étape 5. Continuez à appuyer sur Entrée pour quitter l'assistant.

Étape 6. Si vous envisagez de redémarrer un moteur d'analyse de programme malveillant, sélectionnez ANTIVIRUS.

Étape 7. Sélectionnez vos scanners.

Étape 8. Sélectionnez RESTART.

Étape 9. Continuez à appuyer sur Entrée pour quitter l'assistant.



Avertissement : Le redémarrage des services internes entraîne une interruption du service. Nous vous recommandons d'effectuer cette opération en dehors des heures de production ou par précaution.

Meilleure pratique lors de la connexion de la capture de paquets

Lors de la capture de paquets, collectez et partagez ces informations avec le TAC Cisco.

- Adresse IP du client.
- URL à laquelle vous tentez d'accéder.
- Adresse IP résolue pour cette URL à partir du PC client et du SWA.
- Expérience utilisateur (par exemple, la page n'a pas été chargée ou a été partiellement chargée, et s'il y a des messages d'erreur, veuillez prendre une capture d'écran).
- Horodatage de l'essai.
- Fermez tous les autres navigateurs et applications sur l'ordinateur client. Accédez au site Web, capturez les journaux dans le Bloc-notes pour une seule tentative réussie/échouée et

partagez-les avec l'assistance Cisco.

Pour des informations détaillées sur la façon d'effectuer la capture de paquets dans SWA, référez-vous au lien Configurer la capture de paquets sur l'appareil de sécurité de contenu

Complexité de configuration

La complexité de la configuration est une autre cause courante de latence élevée et de performances médiocres. Cela se produit lorsque le SWA est configuré avec un nombre excessif de conditions, de profils et de politiques. Une telle complexité peut augmenter considérablement les temps de réponse et imposer une charge importante au processus proxy. Ce problème a tendance à devenir plus prononcé pendant les heures de pointe, lorsque le trafic est à son maximum.

Voici quelques conseils pour optimiser la configuration :

1. Limiter le déchiffrement HTTPS : Ne décryptez que le trafic essentiel à vos stratégies de sécurité. Dans la mesure du possible, réduisez la charge de traitement tout en préservant la sécurité.
2. Hiérarchiser les politiques pour plus d'efficacité : Placez les stratégies les plus fréquemment utilisées en haut de la liste des stratégies. Cela garantit un traitement plus rapide en traitant en premier le trafic le plus exigeant.
3. Rationalisation de la conception des politiques : Simplifier les politiques en réduisant leur nombre autant que possible. Cela réduit les traitements inutiles et améliore les performances globales du système.
4. Optimiser l'analyse antivirus et anti-programme malveillant : vérifiez les configurations d'analyse pour les processus antivirus et anti-programme malveillant. Ils peuvent être gourmands en ressources processeur, de sorte qu'un réglage précis peut considérablement réduire la consommation de ressources sans compromettre la sécurité.
5. Utiliser des expressions régulières légères : Évitez les expressions régulières complexes ou gourmandes en ressources. Assurez-vous que les caractères tels que les points (.) et les étoiles (*) sont correctement échappés pour réduire la charge de traitement et éviter les inefficacités.

Pour plus d'informations sur les meilleures pratiques SWA, consultez Utiliser les meilleures pratiques des appliances Web sécurisées

Commandes CLI

Version

Utilisez la commande version pour vérifier l'allocation matérielle (pour Virtual SWA) et l'état RAID (pour Physical SWA). Vérifiez la configuration matérielle : Assurez-vous que le nombre de coeurs de processeur, la mémoire et les disques durs sont alloués comme prévu. Dans les modèles virtuels, l'état RAID indique Inconnu. Si l'état RAID est Dégradé ou En panne dans l'appareil physique, contactez le TAC Cisco pour vérifier l'état du disque à partir du back-end.

Voici un exemple d'allocation de plus de CPU au SWA qui peut conduire à un mauvais comportement :

```
SWA Lab> version
Current Version
===============
Product: Cisco S100V Secure Web Appliance
Model: S100V
BIOS: 6.00
CPUs: 3 expected, 4 allocated
Memory: 8192 MB expected, 8192 MB allocated
Hard disk: 200 GB, or 250 GB expected; 200 GB allocated
RAID: NA
RAID Status: Optimal
```

afficher les alertes

Utilisez la commande displayalerts pour vérifier les messages d'alerte liés au réseau SWA qui peuvent indiquer la cause première.

Dans cet exemple, le serveur DNS à l'adresse IP 10.10.10.10 ne répondait pas et le message « The File Reputation service is not reachable » peut indiquer un problème de connectivité réseau.

```
SWA LAB> displayalerts
Date and Time Stamp           Description
--------------------------------------------------------------------------------
26 Mar 2025 11:20:07 +0500 The File Reputation service is not reachable.
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 10:16:18 +0500 Warning: Communication with the File Reputation service has been established
```

statut_processus

Utilisez la commande process_status pour afficher l'utilisation du processus et de la mémoire des services internes SWA.

Si le processus Prox, qui est le processus principal traitant le proxy de trafic, dépasse constamment 100 % d'utilisation pendant plusieurs minutes, il indique une charge élevée soutenue sur le processus. Cependant, de courts pics occasionnels dans l'utilisation du CPU sur le Prox ou d'autres processus sont normaux et attendus.

<#root>

```
SWA LAB> process_status
USER     PID
```

%CPU

%MEM

VSZ RSS TT STAT STARTED TIME

COMMAND

root 11 2805.4 0.0 0 512 - RNL 28Jun24 11863204:12.63 idle
root 71189

102.0

19.5

6670700 6478032 - R 23Feb25 18076:32.80

prox

root 91880 99.0 0.6 369564 214832 - R 28Jun24 58854:51.78 counterd
root 91267 76.0 0.9 379804 292324 - R 28Jun24 59371:01.26 counterd
root 12 25.9 0.0 0 1600 - WL 28Jun24 30899:57.88 intr
root 46955 25.0 0.2 91260 59336 - S 23Jan25 7547:02.96 wbnpd
root 95056 23.0 11.2 5369332 3710348 - I 28Jun24 31719:23.99 java
root 93190 12.0 1.4 3118384 456088 - S 01:15 29:57.05 beakerd
root 64579 11.0 0.2 101336 71204 - S 6Aug24 12074:55.55 coeuslogd

détail d'état

La commande status detail fournit un résumé en temps réel de l'utilisation des ressources système, des métriques de trafic réseau et des statistiques de connexion, reflétant l'état et les performances globales du SWA. Il reproduit la vue État du système de l'interface utilisateur graphique pour une surveillance et un dépannage rapides.

<#root>

SWA LAB> Status detail

Status as of: Wed Mar 26 11:51:27 2025 PKT

Up since: Fri Jun 28 13:45:43 2024 PKT (270d 22h 5m 43s)

System Resource Utilization:

CPU 16.0%

RAM 10.3%

Reporting/Logging Disk 19.8%

```
Transactions per Second:
  Average in last minute                 1745
  Maximum in last hour                   2210
  Average in last hour                   1708
  Maximum since proxy restart            2451
  Average since proxy restart             615
Bandwidth (Mbps):
  Average in last minute              149.699
  Maximum in last hour               1356.387
  Average in last hour                229.634
  Maximum since proxy restart       22075.244
  Average since proxy restart          60.689
Response Time (ms):
  Average in last minute                   99
  Maximum in last hour                8194128
  Average in last hour                     87
  Maximum since proxy restart         19608632
  Average since proxy restart               28
Cache Hit Rate:
  Average in last minute                    3
  Maximum in last hour                      6
  Average in last hour                      2
  Maximum since proxy restart               89
  Average since proxy restart               2
Connections:
  Idle client connections                3481
  Idle server connections                 754


Total client connections               21866


  Total server connections              19049


SSLJobs:
  In queue Avg in last minute               0
  Average in last minute                12050
  SSLInfo Average in last min               0
Network Events:
  Average in last minute                 16.0
  Maximum in last minute                  171
  Network events in last min           151918
```

Ipcheck

La commande ipcheck affiche des informations système détaillées pour l'appliance Web sécurisée, y compris les spécifications matérielles, l'utilisation du disque, les interfaces réseau, les clés logicielles installées et les détails de version, fournissant un instantané complet de l'état actuel de l'appliance.

<#root>

```
SWA LAB > ipcheck
  Ipcheck Rev           1
  Date                  Fri Mar 21 16:34:56 2025
```

```
Model                 S100V
Platform              vmware (VMware Virtual Platform)
Secure Web Appliance Version  Version: 15.2.1-011
Build Date            2024-10-03
Install Date          2025-02-13 17:49:24
Burn-in Date          Unknown
BIOS Version          6.00
RAID Version          NA
RAID Status           Unknown
RAID Type             NA
RAID Chunk            Unknown
BMC Version           NA
Disk 0                200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
Disk Total            200GB

Root                  4GB 64%


Nextroot              4GB 65%


Var                   400MB 38%


Log                   130GB 24%


DB                    2GB 0%


Swap                  8GB
Proxy Cache           50GB
RAM Total             8192M
```

taux

La commande rate imprime les débits de connexion et le nombre de requêtes par seconde toutes les 10 secondes .

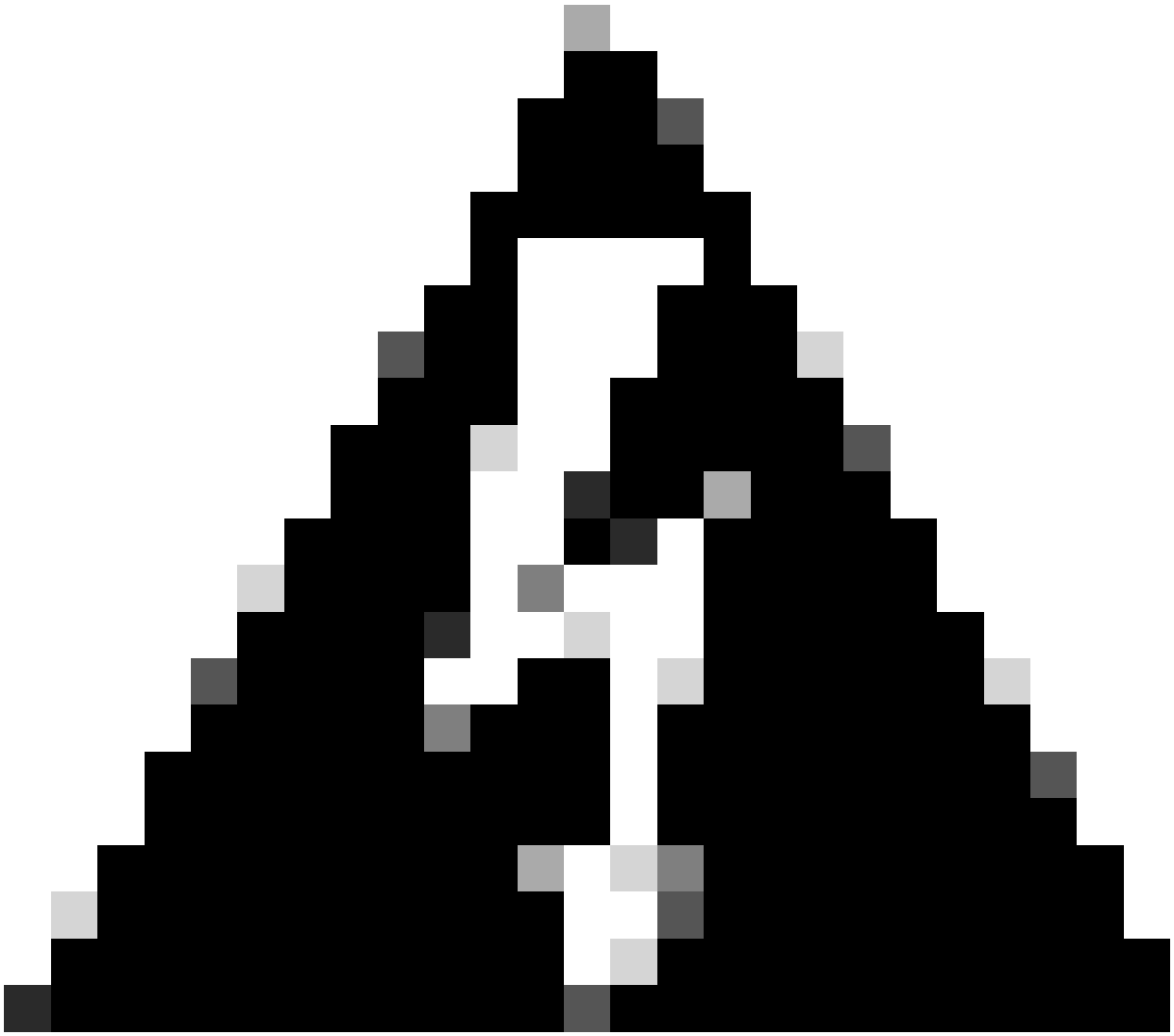
<#root>

```
SWA LAB> 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

100.00  1800     17  16352   1626    178551    178551    0.0  2366   0

100.00  1813     18  16453   1659    226301    224952    0.6  3008   0
```

```
99.00  1799      10  16338   1645    206234    206234    0.0  3430   1
```

Collecte des journaux pour une latence élevée

Cela dépend de la section dans laquelle vous voyez un temps de réponse élevé des journaux d'accès ou une charge de processus élevée des journaux SHD. Pour un dépannage plus approfondi, il est préférable de changer l'abonnement de journal correspondant en Debug.



Avertissement : La définition du niveau de journalisation sur debug ou trace peut entraîner une utilisation accrue des ressources et entraîner une rotation ou un remplacement rapide des fichiers journaux.

Champ Journal d'accès	Champ Journal SHD	Abonnement au journal correspondant

Réponse d'authentification , Total d'authentification	—	authlogs
Réponse DNS, total DNS	—	journaux_système
Réponse WBRS, total WBRS	Wbrs_WucLd	Contactez le centre d'assistance technique Cisco TAC
Réponse AVC, total AVC	—	avc_logs
Réponse McAfee, total McAfee	McafeeLd	journaux_mcafee
Réponse Sophos, total Sophos	SophosLd	journaux_sophos
Réponse de Webroot, total de Webroot	WebrootLtd	webrootlogs
Réponse AMP, total AMP	AMPLD	amp_logs

Informations connexes

Dépannage des performances de l'appliance Web sécurisée avec les journaux SHD

Accéder aux journaux de l'appliance Web sécurisée

Configurer la capture de paquets sur l'appliance de sécurité du contenu

Utilisation des meilleures pratiques de sécurisation des appliances Web

Configurer le paramètre de performance dans les journaux d'accès

Dépannage des états de processus inhabituels dans SWA

Déterminer le taux de déchiffrement dans SWA

Dépannage du service DNS de l'appliance Web sécurisée

Accéder aux journaux de l'appliance Web sécurisée

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.