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

Table des matières

Introduction

Ce document décrit les journaux du démon d'intégrité du système (shd_logs) et comment dépanner le problème de performances de l'appliance Web sécurisée (SWA) avec ce journal.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil Web sécurisé physique ou virtuel (SWA) 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.

Qu'est-ce que SHD LOGS

Les journaux SHD contiennent la plupart des statistiques de processus liées aux performances dans SWA chaque minute.

Voici un exemple de ligne de journal SHD :

```
Mon Jun 9 23:46:14 2022 Info: Status: CPULd 66.4 DskUtil 5.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 Cache
SrvConn 0 MemBuf 0 SwpPgOut 0 ProxLd 0 Wbrs_WucLd 0.0 LogLd 0.0 RptLd 0.0 WebrootLd 0.0 SophosLd 0.0 Mc
```

Les journaux SHD sont acceptables à partir de l'interface de ligne de commande (CLI) et du protocole FTP (File Transfer Protocol). Il n'existe aucune option permettant d'afficher le journal à partir de l'interface utilisateur graphique (GUI).

Accéder aux journaux SHD

À partir de la CLI :

1. Tapez grep ou tail dans CLI.
2. Recherchez "shd_logs Type: SHD Logs Retrieval: FTP Poll dans la liste et tapez le numéro associé.
3. Dans Entrez l'expression régulière à grep. Vous pouvez taper des expressions régulières pour effectuer une recherche dans les journaux, par exemple, vous pouvez taper date et heure.
4. Voulez-vous que cette recherche ne respecte pas la casse ? [Y]> Vous pouvez conserver cette valeur par défaut, sauf si vous devez rechercher des valeurs sensibles à la casse, ce qui n'est pas nécessaire dans SHD_Logs.
5. Voulez-vous rechercher les lignes qui ne correspondent pas ? [N]> Vous pouvez définir cette ligne comme valeur par défaut, sauf si vous devez rechercher tout sauf votre expression régulière Grep.
6. Voulez-vous suivre les journaux ? [N]> Cette option n'est disponible que dans la sortie du grep, si vous la laissez par défaut (N), elle affiche les journaux SHD de la première ligne du fichier courant.
7. Voulez-vous paginer le résultat ? [N]> Si vous sélectionnez "Y", la sortie est la même que la sortie de la commande less, vous pouvez naviguer entre les lignes et les pages et vous pouvez également rechercher à l'intérieur des journaux (Tapez / puis le mot clé et appuyez sur Entrée), pour quitter la vue du journal par le type q.

À partir de FTP :

1. Assurez-vous que FTP est activé depuis GUI > Network > Interfaces.
2. Connectez-vous à SWA via FTP.
3. Le dossier Shd_logs contient les journaux.

Champs du journal SHD

Les champs des journaux SHD sont détaillés :

Numéro de champ	Nom	Identifiant	Description

8	CPULd	Pourcentage % 0 ~ 99	CHARGE CPU Pourcentage total d'UC utilisé sur le système, tel qu'indiqué par le système d'exploitation
10	Unité de bureau	Pourcentage % 0 ~ 99	Utilisation du disque espacé utilisé sur la partition /data
12	RAMUtil	Pourcentage % 0 ~ 99	Utilisation de la RAM Pourcentage de mémoire libre signalé par le système d'exploitation
14	Requêtes	Requête / Secondes	Requêtes Nombre moyen de transactions (demandes) au cours de la dernière minute
16	Bande	Kbit/s	Bande passante économisée Bande passante moyenne économisée au cours de la dernière minute. - Équivalent de la bande passante SNMP moyenne économisée au cours de la dernière minute
18	Latence [1]	Millisecondes (ms)	Latence moyenne (temps de réponse) au cours de la dernière

			minute prend le deuxième champ dans les journaux d'accès, qui indique le temps que prend la connexion TCP de l'utilisateur final à WSA (ou de l'utilisateur final au serveur Web si la connexion n'a pas été déchiffrée) WSA récapitule les durées, pour chaque demande enregistrée dans les journaux d'accès pendant les dernières minutes et divise-les en nombres de ces demandes et obtient une latence moyenne pour SHD
20	CacheAtteint	Numéro #	Moyenne des résultats du cache au cours de la dernière minute. - Équivalent de la moyenne des accès au cache SNMP pour la dernière minute
22	CliConn	Numéro #	Nombre total de connexions client actuelles Des clients à WSA - équivalent au total actuel des connexions client SNMP

24	SrvConn	Numéro #	Nombre total de connexions serveur actuelles De WSA au serveur Web - Équivalent du nombre total actuel de connexions serveur SNMP.
26	MémBuf [2]	Pourcentage % 0 ~ 99	Mémoire tampon Quantité totale actuelle de mémoire tampon proxy libre.
28	SwpPgOut	Numéro #	Nombre de pages qui ont été échangées, comme indiqué par le système d'exploitation. Fichier d'échange ou fichier d'échange, espace sur un disque dur utilisé comme emplacement temporaire pour stocker des informations lorsque la mémoire vive est entièrement utilisée.
30	ProxLd	Pourcentage % 0 ~ 99	La charge du processus prox Processus responsable du traitement de toutes les requêtes entrantes (HTTP/HTTPS/FTP/SOCKS)

32	Wbrs_WucLd	Pourcentage % 0 ~ 99	Chargement de Web Reputation Coring Processus utilisé pour le moteur d'analyse WBRS réel. Le processus proxy interagit avec le processus reqscand pour effectuer des analyses WBRS.
34	LogLd	Pourcentage % 0 ~ 99	Chargement du journal proxy
36	RptLd	Pourcentage % 0 ~ 99	Chargement du moteur de rapport Processus responsable de la création de la base de données Reporting. « reportd » interagit avec « haystackd » pour créer la base de données de suivi Web.
38	WebrootLtd	Pourcentage % 0 ~ 99	Chargement de Webroot Antimalware
40	SophosLd	Pourcentage % 0 ~ 99	Chargement de l'antivirus Sophos
42	McafeeLd	Pourcentage % 0 ~ 99	Chargement Antivirus Mcafee

44	WTTLd	Pourcentage % 0 ~ 99	Robinet Trafic Web
46	AMPLD	Pourcentage % 0 ~ 99	Advanced Malware Protection (AMP)

1. Parfois, on peut s'attendre à voir un pic élevé de latence dans les journaux SHD, par exemple s'il n'y a pas beaucoup de demandes sur WSA et qu'à un moment donné, une connexion de longue durée a été terminée - par exemple plusieurs jours. Ensuite, cette seule demande peut augmenter la latence pendant cette minute lorsqu'elle a terminé et qu'elle s'est connectée aux journaux d'accès.

2. Tel qu'écrit dans :

"Utilisation de la mémoire vive pour un système working peut être supérieure à 90 %, car la mémoire vive qui n'est pas utilisée par le système est utilisée par le cache d'objets Web. Si votre système n'est experiencing problèmes de performances graves et cette valeur n'est pas bloquée à 100 %, le système est operating normalement."

Remarque : la mémoire tampon proxy est un composant qui utilise cette mémoire vive

---

Dépannage avec les journaux SHD

Autre processus à forte charge

Si la charge de l'autre processus est élevée, consultez le tableau 1 de cet article et lisez les journaux associés à ce processus.

Latence élevée

Si vous avez vu une latence élevée dans les journaux SHD, vous devez vérifier les journaux Proxy_track dans /data/pub/track_stats/ . Trouvez la période pendant laquelle la latence est élevée. Dans la piste proxy, vous avez deux enregistrements qui sont liés à la latence. Les nombres devant chaque section correspondent au nombre total d'occurrences depuis le dernier redémarrage. Par exemple, dans ce code :

```
Current Date: Wed, 11 Jun 2022 20:03:32 CEST
...
   Client Time    6309.6 ms    109902
...
Current Date: Wed, 11 Jun 2022 20:08:32 CEST
...
   Client Time    6309.6 ms    109982
```

En 5 minutes, le nombre de demandes de clients ayant pris 6 309,6 ms ou plus est de 80. Vous devez donc soustraire les nombres de chaque période pour obtenir la valeur précise que vous devez prendre en compte ces éléments :

Client Time : temps nécessaire entre le client et SWA.

Heure d'accès : Nombre d'accès au cache : les données demandées se trouvent dans le cache et peuvent être remises au client.

Durée d'absence : absence du cache : les données demandées ne se trouvent pas dans le cache ou ne sont pas à jour et ne peuvent pas être remises au client.

Server Transaction Time : temps nécessaire entre SWA et le serveur Web.

Ces valeurs doivent également être prises en compte lors du processus de contrôle des performances :

temps utilisateur : 160,852 (53,33 %)
heure système : 9,768 (3,256 %)

Dans les journaux de suivi des statistiques, les informations sont consignées toutes les 5 minutes (300 secondes). Dans cet exemple, l'heure utilisateur 160.852 est l'heure (en secondes) à laquelle le processeur a été chargé avec des tâches pour traiter les requêtes des utilisateurs. L'heure système est l'heure à laquelle SWA a traité des événements réseau, tels que la décision de routage, etc. La somme de ces deux pourcentages correspond à la charge totale du processeur sur cette période. Si le temps utilisateur est important, cela signifie que vous devez envisager une configuration de complexité élevée.

Informations connexes

- Notes de version de WSA AsyncOS
- Matrice de compatibilité pour Cisco Secure Email and Web Manager
- Mises à niveau et mises à jour Vérification de connectivité
- Assistance technique et téléchargements Cisco

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.