Configurer le paramètre de performance dans les journaux d'accès

Table des matières

Introduction

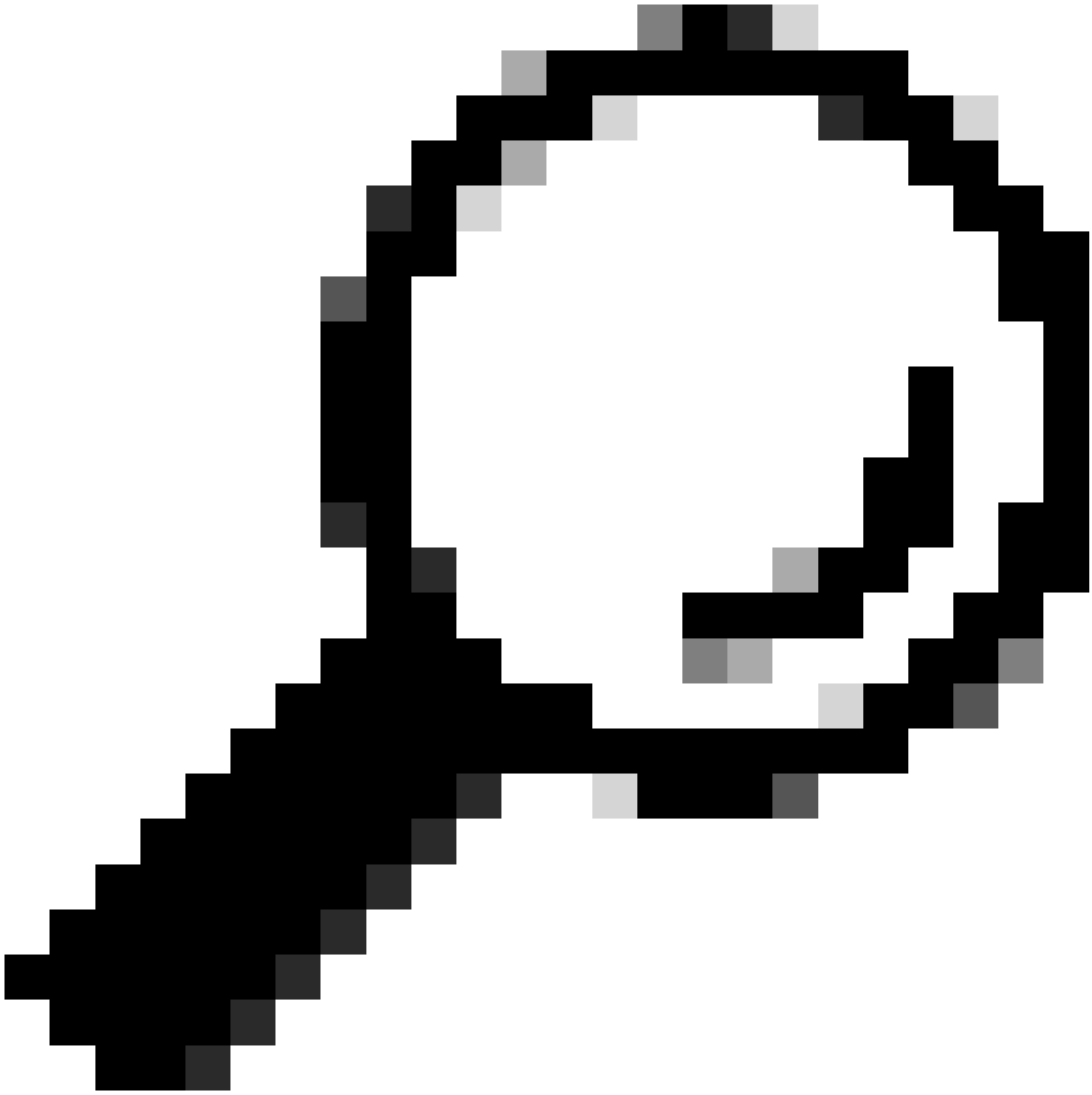
Ce document décrit les étapes à suivre pour ajouter le champ personnalisé du paramètre Performance au journal d'accès de l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès SSH (Secure Shell Protocol) à l'interface de gestion SWA.
- Accès à l'interface graphique utilisateur (GUI) de l'interface de gestion SWA.



Conseil : Il est préférable d'avoir plus de 20 % d'espace disque libre sur la partition de données SWA. Vous pouvez vérifier l'utilisation du disque à partir de l'interface de ligne de commande (CLI) dans le résultat de la commande status detail.

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

En cas de problème de latence et lorsque le trafic est transféré par proxy via un SWA, les journaux d'accès peuvent être utiles pour dépanner la cause première de la latence. Vous pouvez modifier les paramètres actuels des journaux d'accès ou créer de nouveaux journaux d'accès avec des paramètres de performances ajoutés au champ personnalisé.

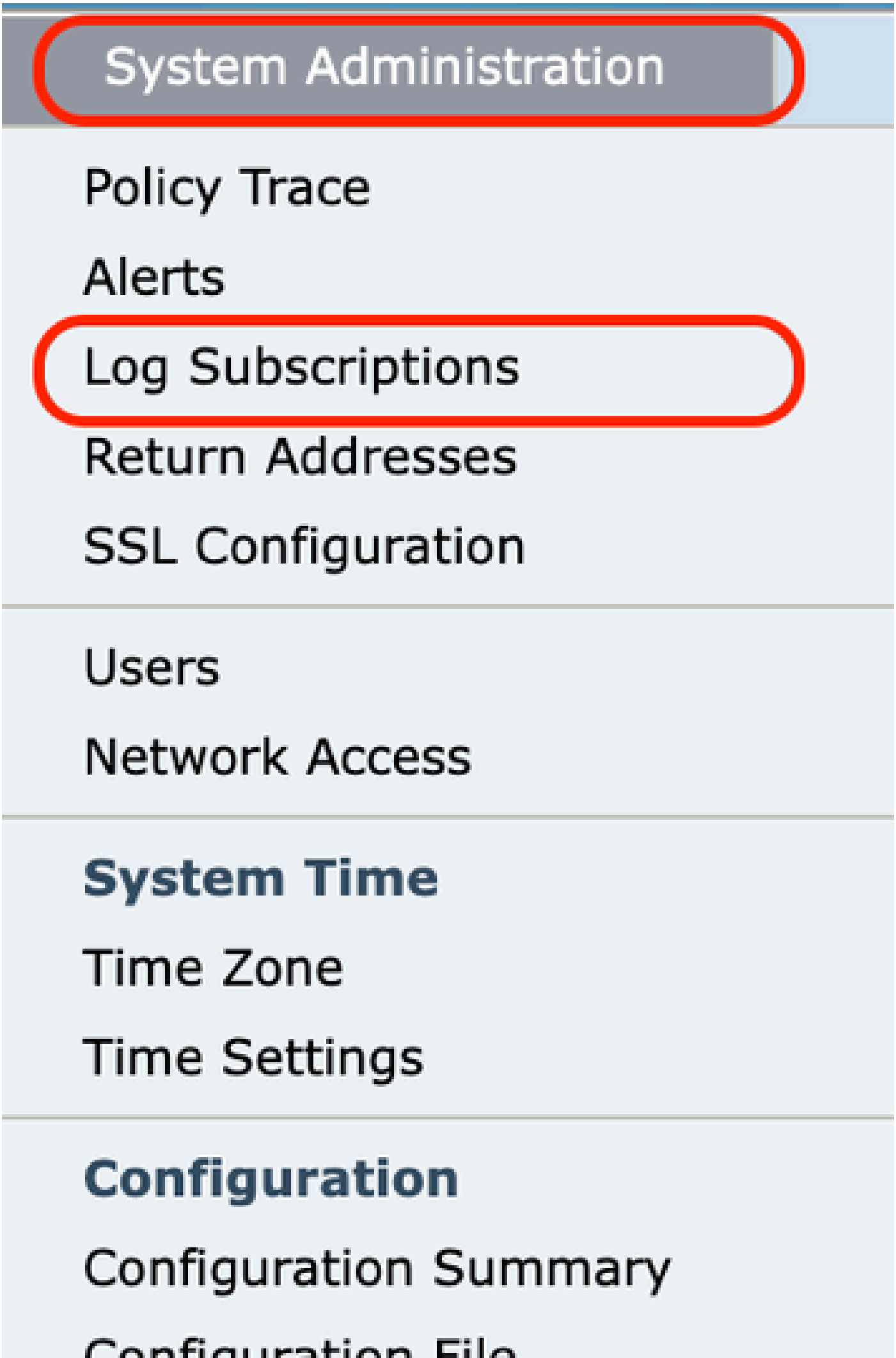
Créer un journal des accès supplémentaires

Dans certaines conditions, en raison de stratégies internes ou d'une autre configuration, il n'est pas possible de modifier le journal d'accès actuel. Pour surmonter cette limitation, vous pouvez créer d'autres journaux Access et ajouter le paramètre Performance personnalisé dans les nouveaux journaux Access.

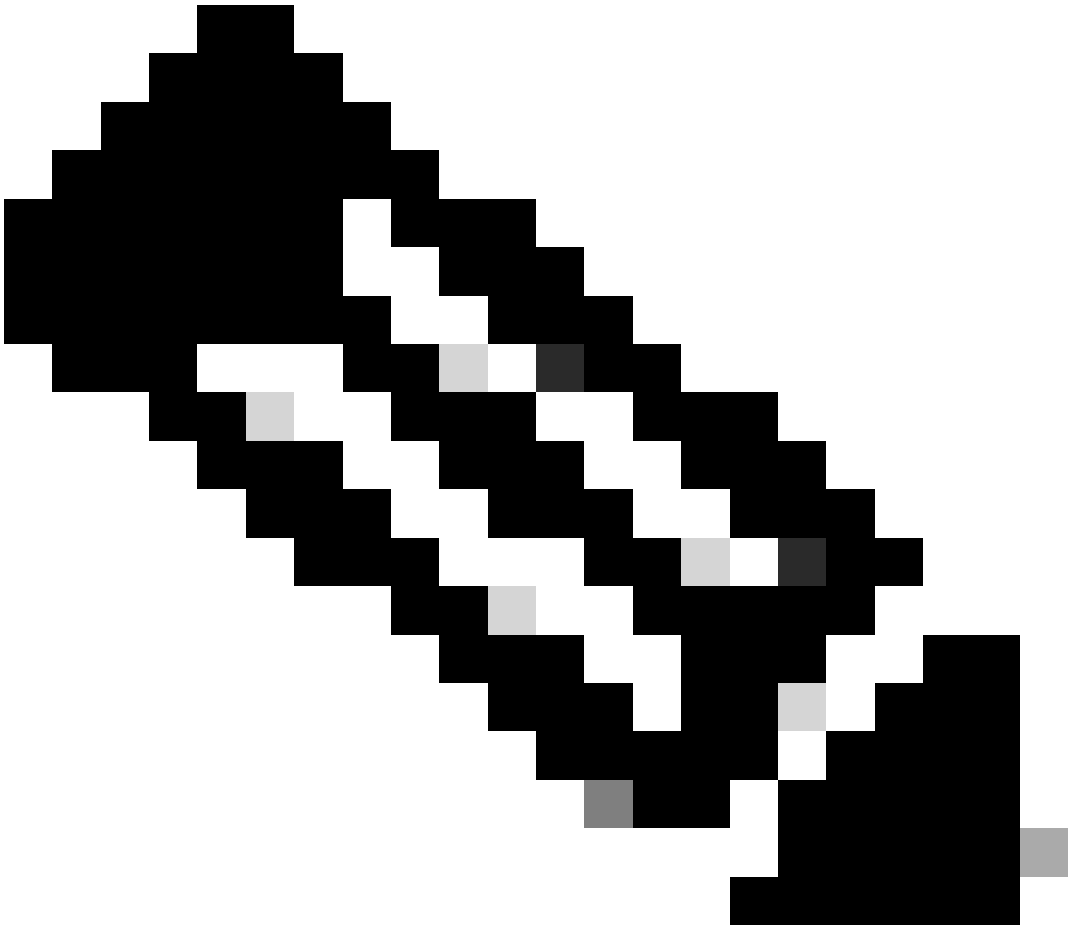
Créer un journal d'accès depuis l'interface graphique

Étape 1. Connectez-vous à l’interface utilisateur graphique.

Étape 2. Dans le menu Administration système, sélectionnez Inscriptions au journal.


System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary

Entrez une valeur comprise entre 102400 (100 kilo-octets) et 10737418240 (10 gigaoctets) pour la taille du fichier (en octets) avant les rôles SWA sur le journal vers un nouveau fichier. Le nombre doit être un entier, et vous pouvez ajouter M pour indiquer la taille en mégaoctets, K pour indiquer la taille du fichier en kilo-octets et G pour gigaoctets.



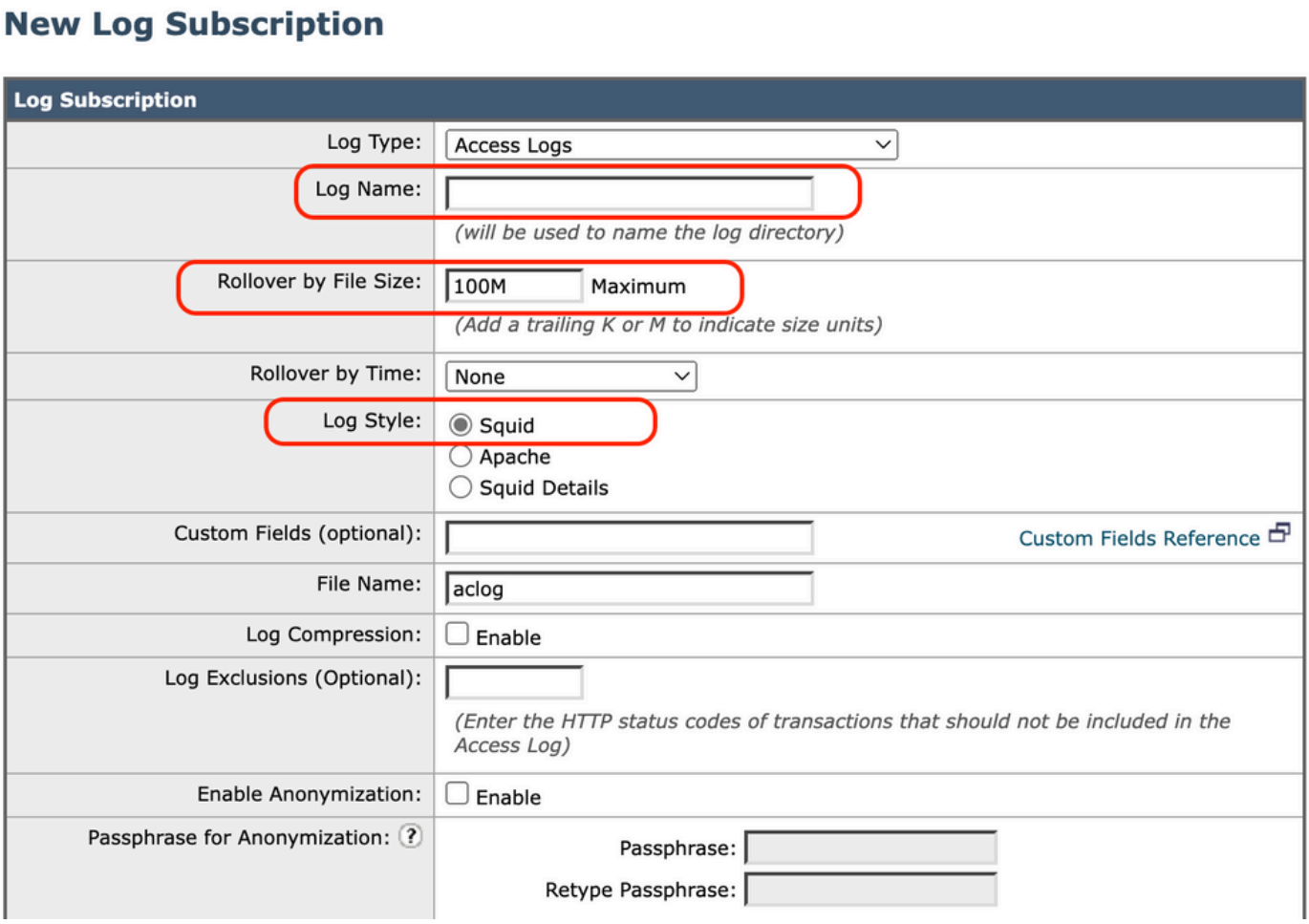
> Remarque : Archive (transfert) les abonnements aux journaux SWA lorsqu'un fichier journal en cours atteint une limite spécifiée par l'utilisateur de taille de fichier maximale ou de durée maximale depuis la dernière substitution.

Étape 7. Choisissez Squid pour le style de journal.

Étape 8. Nom du fichier permet de définir le nom du dossier et le nom du fichier journal pour ce nouveau journal. Il est conseillé d'être identique au nom du journal, qui dans cet exemple était TAC_access_logs.

Étape 9. Vous pouvez activer la compression des journaux pour compresser le fichier journal ou conserver les journaux sous forme de fichier texte.

Étape 10. L'exclusion du journal permet de filtrer le code de réponse HTTP (Hypertext Transfer Protocol). Ne filtrez pas les codes d'état HTTP.



Remplissez les champs obligatoires

Étape 11. Choisissez FTP poll pour conserver les journaux dans le SWA. Tapez 1 et appuyez sur Entrée.

Étape 12. Soumettre et valider les modifications

Configuration du nouveau journal d'accès depuis CLI

Étape 1. Connectez-vous à CLI.

Étape 2. Exécutez logconfig.

Étape 3. Pour créer un nouveau journal, tapez New et appuyez sur Entrée.

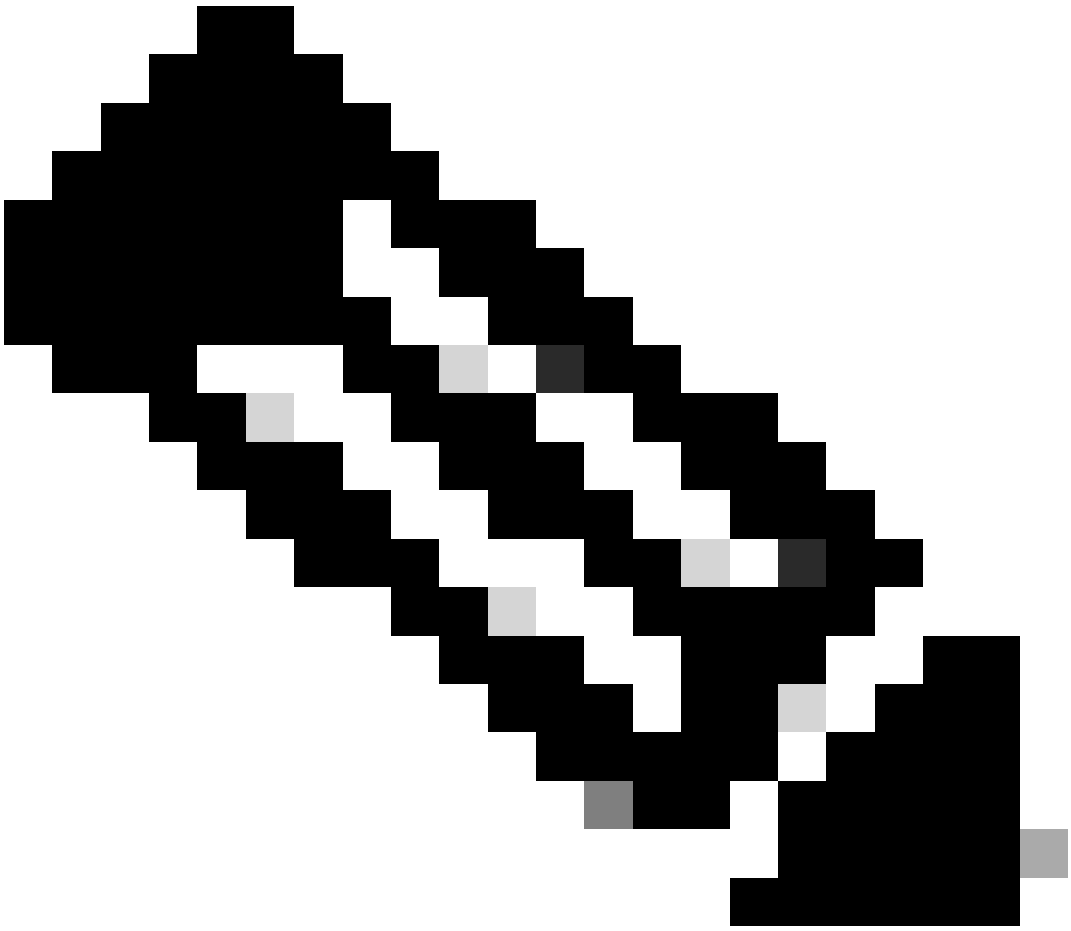
Étape 4. Recherchez les journaux d'accès dans la liste, tapez le numéro associé et appuyez sur Entrée.

Étape 5. Tapez un nom pour le nouveau journal.

Étape 6. Tapez 1 pour choisir Squid comme style de journal pour cet abonnement, puis appuyez sur Entrée.

Étape 7. Ne filtrez pas les codes d'état d'erreur HTTP. Appuyez sur Entrée pour passer à l'étape suivante.

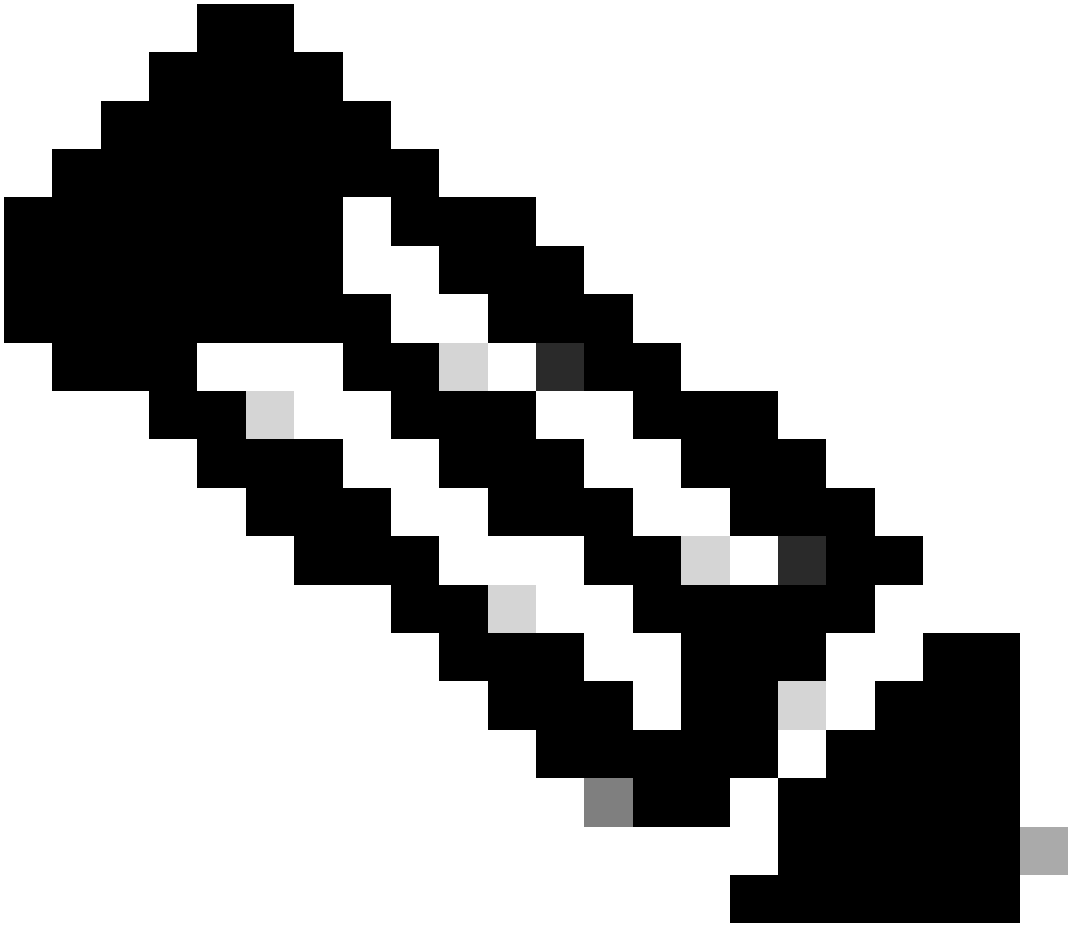
Étape 8. Choisissez FTP poll pour conserver les journaux dans le SWA. Tapez 1 et appuyez sur Entrée.



> Remarque : Afin de pousser les journaux vers le serveur FTP (File Transfer Protocol), le serveur SCP (Secure Copy Protocol) ou le serveur Syslog. Vous pouvez choisir les options qui leur sont associées.

Étape 9. Cette étape consiste à définir le nom du dossier et le nom du fichier pour le nouveau journal. Il est préférable d'être identique au nom du journal et d'appuyer sur Entrée.

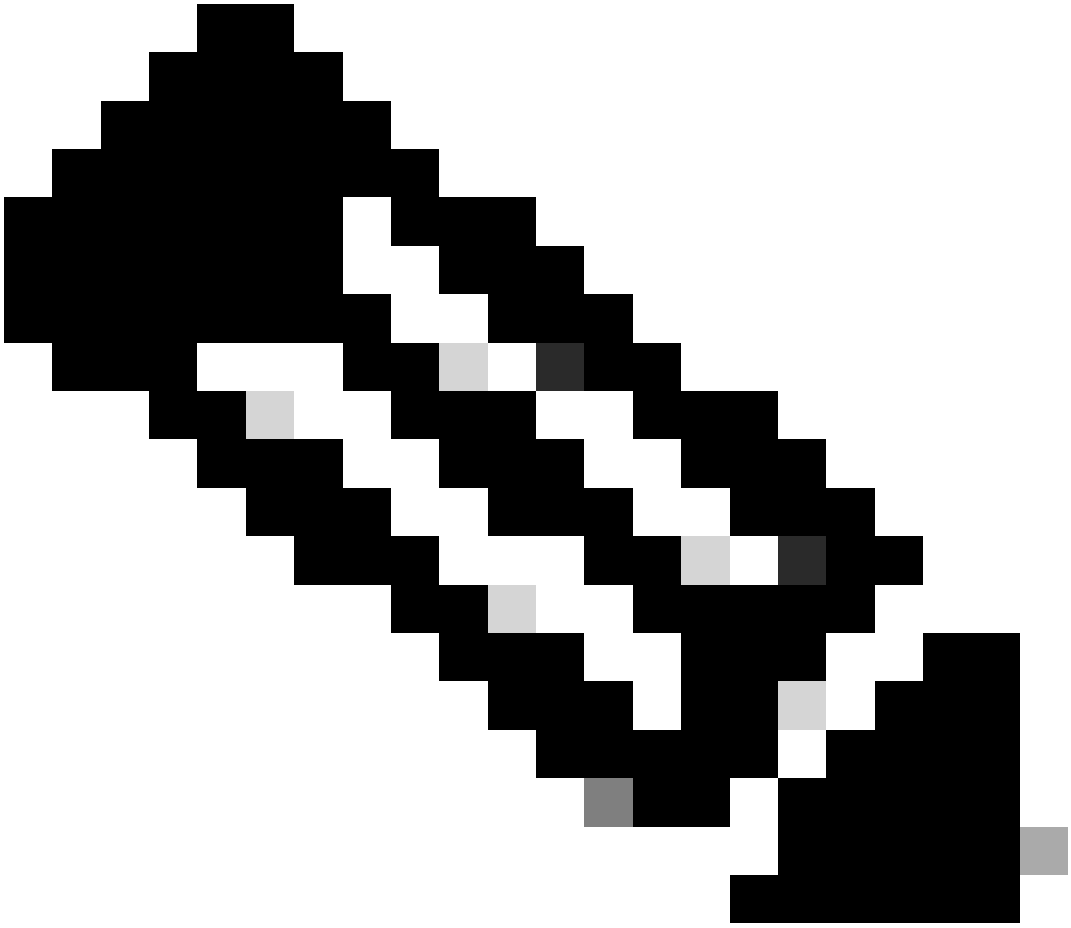
Étape 10. Entrez une valeur comprise entre 102400 (100 kilo-octets) et 10737418240 (10 gigaoctets) pour la taille du fichier (en octets) avant le rôle SWA sur le journal dans un nouveau fichier.



Remarque : Archive (transfert) les abonnements aux journaux SWA lorsqu'un fichier journal en cours atteint une limite spécifiée par l'utilisateur de taille de fichier maximale ou de durée maximale depuis la dernière substitution.

Étape 11. Le nombre maximal de fichiers indique le nombre de fichiers journaux stockés sur le périphérique. Si le nombre total de fichiers journaux a atteint cette valeur, les journaux plus anciens sont supprimés de SWA. La valeur par défaut est 10 fichiers et vous pouvez taper le nombre de journaux, en raison de l'espace disque disponible et d'autres configurations de journaux, puis appuyez sur Entrée.

Étape 12. Au cours de cette étape, vous pouvez choisir de compresser les journaux ou de les conserver en tant que fichier texte. Tapez Y pour Oui et N pour Non et appuyez sur Entrée.



Remarque : Une fois que la taille de fichier a atteint la taille maximale, le fichier est compressé. Le taux de compression dépend du comportement du trafic réseau et peut varier selon les fichiers journaux.

Étape 13. Appuyez sur Entrée pour quitter l'assistant de configuration du journal.

Étape 14. Tapez commit pour enregistrer les modifications.

```
SWA_CLI> logconfig
...
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> NEW

Choose the log file type for this subscription:
1. AVC Engine Framework Logs
```

```
2. AVC Engine Logs
3. Access Control Engine Logs
4. Access Logs
....
58. Webroot Logs
59. Welcome Page Acknowledgement Logs
[1]> <=== type the number assosiated with Access Logs and press Enter

Please enter the name for the log:
[]> <=== Chose desiered name, in this example, TAC_access_logs

Choose the log style for this subscription:
1. Squid
2. Apache
3. Squid Details
[1]> <=== Press Enter to keep the default value

Enter the HTTP Error Status codes (comma separated list of 4xx and 5xx codes) you want to filter out fr
[]> <=== Press Enter to keep the default value

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> <=== Choose FTP poll to keep the logs in the SWA

Filename to use for log files:
[aclog]> <=== It is better to have teh same file name as the log, in this example, TAC_access_logs

Do you want to configure time-based log files rollover? [N]> <=== Enter the desiered answer

Please enter the maximum file size:
[104857600]> <=== Enter the desiered answer, or you can leave as default

Please enter the maximum number of files:
[100]> <=== Enter the desiered answer, it depends on free disk space and log file size

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]> <=== En

Do you want to compress logs (yes/no)
[n]> <=== Enter the desiered answer

Currently configured logs:
1. "Splunk Logs" Type: "Access Logs" Retrieval: FTP Push - Host 10.0.0.1
2. "TAC_access_logs" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
....
40. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
41. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> <=== Press Enter to exit the log configuration wizard

SWA_CLI> commit
Please enter some comments describing your changes:
[]> <=== Type the change description and press Enter
```

Ajouter des champs personnalisés pour le paramètre Performance aux journaux d'accès

Étape 1. Connectez-vous à l’interface graphique utilisateur.

Étape 2. Dans le menu System Administration, sélectionnez Log Subscriptions.

Étape 3. Dans la colonne Nom du journal, cliquez sur Accéder aux journaux ou sur le nom du journal nouvellement créé. Dans cet exemple, TAC_access_logs.

Étape 4. Dans la section Champs personnalisés, collez cette chaîne :

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)

       , Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,

        a; DNS response = %:

         d, WBRS response = %:

           r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respo

            s; AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ] [Client Port = %F, Server IP = %
```

Étape 5. Soumettre et valider les modifications

Vérification des modifications

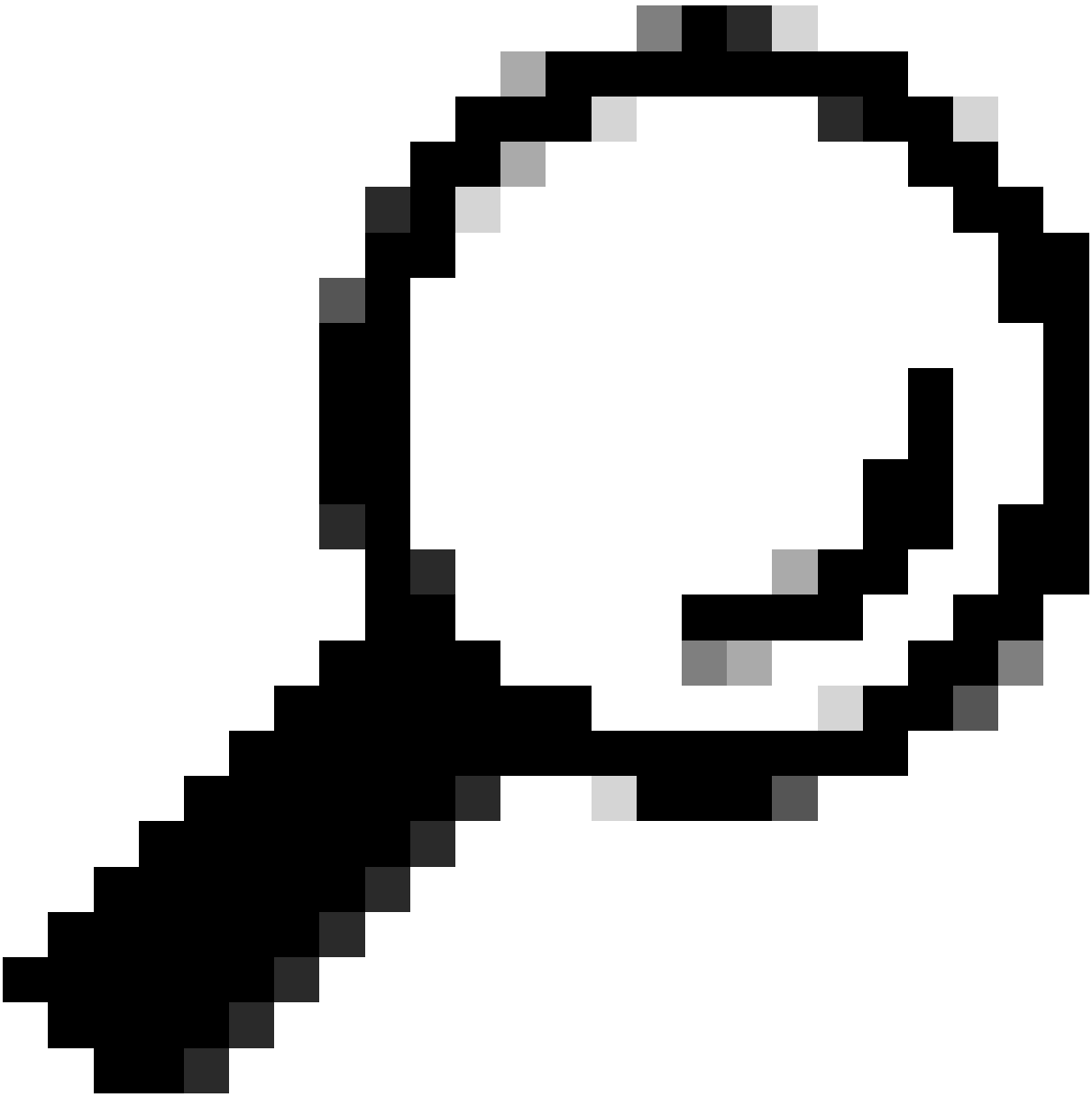
Étape 1. Connectez-vous à CLI.

Étape 2. Tapez tail et appuyez sur Entrée.

Étape 3. Recherchez le numéro associé aux journaux d'accès qui ont ajouté le paramètre Performance. Tapez le numéro et appuyez sur Entrée.

Vous pouvez voir que des informations supplémentaires ont été ajoutées aux journaux d'accès, comme dans cet exemple.

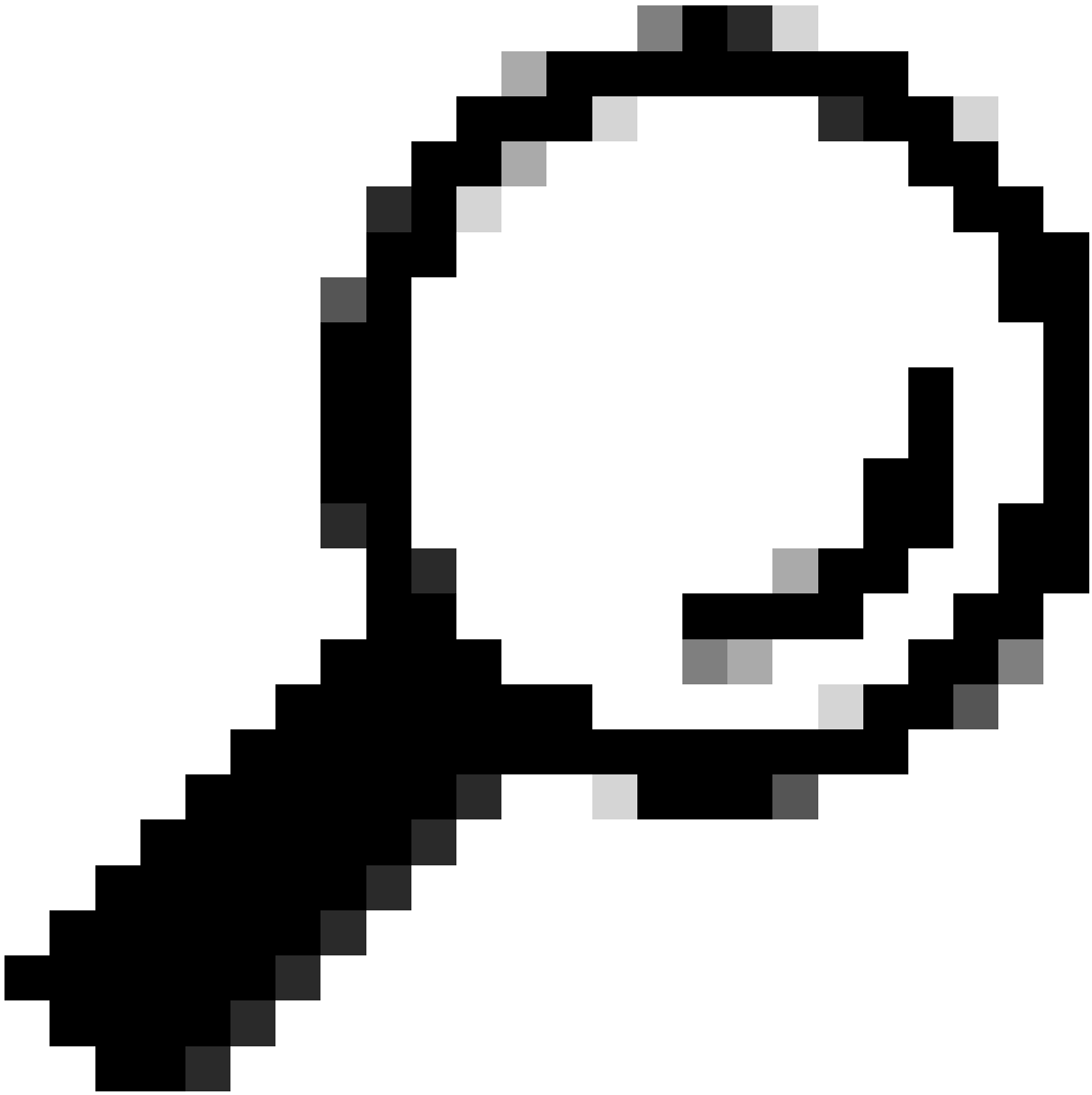
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

        - " [ Request Details: ID = 104, User Agent = "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecl
```



Conseil : Vous pouvez quitter la commande tail lorsque vous maintenez la touche Ctrl enfoncée et que vous appuyez sur C. Si vous n’avez pas quitté la commande tail, tapez q.

Description des champs dans les champs personnalisés

Les valeurs utilisées dans le champ Paramètre de performance personnalisé correspondent aux informations suivantes :



Conseil : Latence = total AMP + total Anti-Spyware + total Webroot + total Sophos + total McAfee + total AVC + total WBRS + total Auth

Nom du champ personnalisé	Champ personnalisé	Description

En-tête de requête	% : <h	Temps d'attente pour l'écriture de l'en-tête de requête sur le serveur après le premier octet.
Demande au serveur	% : <b	Temps d'attente pour écrire le corps de la demande sur le serveur après l'en-tête.
1er octet au client	%:1>	Temps d'attente du premier octet écrit sur le client.
Corps du client	%:b>	Temps d'attente pour le corps complet écrit sur le client.
Temps d'attente Rx (en ms) : 1er octet de requête	%:1<	Durée écoulée entre le moment où le proxy Web commence à se connecter au serveur et le moment où il est en mesure d'écrire pour la première fois sur le serveur. Si le proxy Web doit se connecter à plusieurs serveurs pour terminer la transaction, il s'agit de la somme de ces temps.
En-tête de requête	% : h<	Temps d'attente pour l'en-tête client complet après le premier octet.
Corps du client	% : b<	Temps d'attente pour le corps complet du client.
1er octet de réponse	%:>1	Temps d'attente du premier octet de réponse du serveur.
En-tête de réponse	%:>h	Temps d'attente de l'en-tête du serveur après le premier octet de réponse.
Réponse du serveur	%:>b	Cela signifie essentiellement que SWA a obtenu les en-têtes HTTP du serveur, mais SWA attend les octets de réponse après cela et qui serait le contenu réel du serveur.
Cache disque	%:>c	Temps nécessaire au proxy Web pour lire une réponse à partir du cache disque.
Réponse Auth	% : <a	Délai d'attente pour recevoir la réponse du processus d'authentification du proxy Web, après l'envoi de la demande par le proxy Web.

Total Auth	%:>a	Le délai d'attente pour la réception de la réponse du processus d'authentification du proxy Web comprend le temps nécessaire au proxy Web pour envoyer la demande.
réponse DNS	% : <d	Temps nécessaire au proxy Web pour envoyer la demande DNS (Domain Name Request) au processus DNS du proxy Web.
Total DNS	%:>d	Temps nécessaire au processus DNS du proxy Web pour renvoyer un résultat DNS au proxy Web.
réponse WBRS	% : <r	Délai d'attente pour la réception de la réponse des filtres de réputation de sites Web, après l'envoi de la demande par le proxy Web.
Total WBRS	%:>r	Le délai d'attente pour recevoir le verdict des filtres de réputation Web inclut le temps nécessaire au proxy Web pour envoyer la demande.
réponse de contrôle d'accès	%:A>	Temps d'attente pour recevoir la réponse du processus de visibilité et de contrôle des applications (AVC), après l'envoi de la demande par le proxy Web.
total AVC	% : A<	Le délai d'attente pour recevoir la réponse du processus AVC inclut le temps nécessaire au proxy Web pour envoyer la demande.
réponse DCA	%:C>	Délai d'attente pour la réception de la réponse du moteur d'analyse de contenu dynamique, après l'envoi de la demande par le proxy Web.
Total DCA	% : C<	Le délai d'attente pour recevoir le verdict du moteur d'analyse de contenu dynamique inclut le temps nécessaire au proxy Web pour envoyer la demande.
Réponse de McAfee	%:m>	Délai d'attente pour la réception de la réponse du moteur d'analyse McAfee, après l'envoi de la demande par le proxy Web.
Total McAfee	%:m<	Le délai d'attente pour recevoir le verdict du moteur d'analyse

		McAfee inclut le temps nécessaire au proxy Web pour envoyer la demande.
réponse Sophos	%:p>	Temps d'attente pour recevoir la réponse du moteur d'analyse Sophos, après l'envoi de la demande par le proxy Web.
Total Sophos	%:p<	Le délai d'attente pour recevoir le verdict du moteur d'analyse Sophos inclut le temps nécessaire au proxy Web pour envoyer la requête.
Réponse AMP	%:e>	Délai d'attente pour recevoir la réponse du moteur AMP, après l'envoi de la demande par le proxy Web.
Total AMP	% : e<	Le délai d'attente pour recevoir le verdict du moteur AMP inclut le temps nécessaire au proxy Web pour envoyer la demande.
Latence	%x ; %L	Latence et demande d'heure locale dans un format lisible par l'utilisateur : JJ/MM/AAAA : hh:mm:ss +nnnn. Ce champ est écrit avec des guillemets doubles dans les journaux d'accès. Ce champ vous permet de corréler les journaux avec les problèmes sans avoir à calculer l'heure locale à partir de l'heure de chaque entrée de journal.
Port client	%F	Numéro de port utilisé côté client.
Adresse IP du serveur	%k	Adresse IP du serveur Web.
Numéro de port du serveur	%p	Numéro de port du serveur Web.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance - GD (General Deployment) - Cisco
- Recommandations relatives aux meilleures pratiques pour les appareils de sécurité Web Cisco - 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.