# Utilisation du protocole GREP pour filtrer les journaux d’accès

## Table des matières



## Question :

Environnement : Cisco Web Security Appliance (WSA), toutes les versions d'AsyncOS

Comment puis-je rechercher les journaux d'accès sur l'appliance série S ?

À partir de l'interface de ligne de commande de l'appareil de sécurité Web Cisco, vous pouvez utiliser la commande grep pour filtrer les journaux d'accès et déterminer ce qui est bloqué. Voici un exemple pour montrer tout ce qui est bloqué :

---
TestS650.wsa.com ()> grep

Journaux actuellement configurés :
1. Type "access logs" : Récupération "Access Logs" : Sondage FTP
<...>
18. Type "welcomeack_logs" : "Journaux d'accusé de réception de la page d'accueil"
Récupération : sondage FTP

Saisissez le numéro du journal que vous souhaitez grep.
[]> 1

Entrez l'expression régulière à grep.
[]> BLOC_

Voulez-vous que cette recherche ne respecte pas la casse ? [O]> n

Voulez-vous suivre les journaux ? [N]> n

Voulez-vous paginer le résultat ? [N]> n

(les entrées s'affichent)
---

Pour la question d'expression régulière, vous pouvez entrer BLOCK_ (sans les guillemets) pour

afficher chaque demande que WSA a bloquée. (Avertissement : cette liste peut être très longue) .

Vous pouvez également saisir des parties de l'URL du site si vous souhaitez afficher les entrées de type Access Long associées à un site spécifique. Par exemple : si vous entrez windowsupdate pour l'expression régulière, toutes les entrées du journal d'accès contenant l'URL de Windows Update windowsupdate.microsoft.com s'affichent.

Plus avancé, si vous souhaitez afficher les entrées du journal d'accès d'un site avec windowsupdate dans l'URL, qui ont également été bloquées, vous pouvez utiliser l'expression régulière windowsupdate.*BLOCK_.

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.