Utilizzo di GREP per filtrare i log degli accessi

Sommario

Domanda:

Ambiente: Cisco Web Security Appliance (WSA), tutte le versioni di AsyncOS

Come eseguire ricerche nei log degli accessi sull'accessorio serie S?

Dall'interfaccia della riga di comando di Cisco Web Security Appliance, è possibile utilizzare il comando grep per filtrare i log degli accessi e determinare gli elementi da bloccare. Di seguito è riportato un esempio per mostrare tutto ciò che viene bloccato:

—
TestS650.wsa.com ()> grep

Log configurati:
1. "accesslogs" Tipo: "Access Logs" Recupero: Polling FTP
<.
18. Tipo "welcomeack_logs": "Log di conferma della pagina di benvenuto"
Recupero: polling FTP

Immettere il numero del registro che si desidera conservare.
[]> 1

Immettere l'espressione regolare grep.
[]> BLOCCO_

Non si desidera distinguere tra maiuscole e minuscole nella ricerca? [S]> n

Definire la coda dei registri? [N]> n

Impaginare l'output? [N]> n

(verranno visualizzate le voci)
—

Per la domanda dell'espressione regolare, è possibile immettere BLOCK_ (senza le virgolette) per visualizzare tutte le richieste che WSA ha bloccato. (Attenzione: l'elenco può essere molto lungo).

È inoltre possibile immettere parti dell'URL del sito se si desidera visualizzare voci di accesso estese relative a un sito specifico. Se ad esempio si immette windowsupdate per l'espressione regolare, verranno visualizzate tutte le voci del log degli accessi contenenti l'URL di Windows Update windowsupdate.microsoft.com.

Per ulteriori informazioni, se si desidera visualizzare le voci del log degli accessi di un sito con windowsupdate nell'URL, anch'esso bloccato, è possibile utilizzare l'espressione regolare windowsupdate.*BLOCK_.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).