WSA常見問題：如何檢視Cisco WSA上的日誌？

目錄

簡介

本檔案介紹如何使用**grep**指令從CLI檢視思科網路安全裝置(WSA)上的日誌。

如何檢視Cisco WSA上的日誌？

CLI

1. 為了從CLI檢視日誌，請使用安全外殼(SSH)連線到WSA。 您可以使用puTy等SSH客戶端執行此操作。
2. 登入到CLI後，輸入 **grep** 指令。這將顯示WSA上的日誌清單。
3. 鍵入要運行grep on的日誌訂閱編號，然後按enter。
4. 鍵入要為其搜尋的正規表示式，或將此留空以搜尋所有內容，然後按Enter。
5. 鍵入Y或N以鍵入其餘的提示來修改grep的運行方式。

以下示例說明如何運行grep以在訪問日誌中查詢特定域：

```
wsa.hostname> grep
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
3. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
4. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
5. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
...
42. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
43. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
44. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval:
 FTP Poll
Enter the number of the log you wish to grep.
[]> 1
Enter the regular expression to grep.
[]> domain.com
Do you want this search to be case insensitive? [Y]>
Do you want to search for non-matching lines? [N]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
```

GUI

1. 若要從GUI中檢視日誌，請在HTTP的埠8080（預設）或HTTPS的埠8443（預設）上使用Web瀏覽器連線到WSA。
2. 登入後，按一下**系統管理>日誌訂閱**。
3. 按一下日誌訂閱的FTP連結進行檢視。
4. 選擇要檢視的日誌檔案，其輸出將顯示在瀏覽器中。

附註：預設情況下，WSA在連線到管理介面時將埠21用於FTP。如果此埠已更改，從GUI按一下FTP連結將失敗。若要更正此問題，請在瀏覽器中的URL中的WSA主機名之後為管理介面新增FTP埠。