如何將grep的正規表示式(regex)用於搜尋日誌？

目錄

問題

如何將grep的正規表示式(regex)用於搜尋日誌？

環境

思科網路安全裝置
思科電子郵件安全裝置
思科安全管理裝置

解決方案

當與「grep」命令一起使用時，正規表示式(regex)可以是一個強大的工具，用於搜尋裝置上可用的日誌，例如訪問日誌、代理日誌等。使用CLI命令「grep」時，我們可以根據網站、URL的任何部分或使用者名稱來搜尋日誌。

下面是一些常見場景，您可以在其中結合使用regex和grep來幫助進行故障排除。

案例 1:在訪問日誌中查詢特定網站

最常見的情況是嘗試在思科網路安全裝置(WSA)的訪問日誌中查詢對網站提出的請求。

例如：
通過SSH連線到裝置。收到提示符後，我們可以鍵入「grep」命令列出可用的日誌。

```
CLI> grep
```

輸入您希望「grep」的日誌編號。 []> 1（在此處選擇訪問日誌的編號）
輸入正規表示式為「grep」。 []>**網站\.com**

案例 2:正在嘗試查詢特定副檔名或頂級域

可以使用「grep」命令在URL或頂級域(.com、.org)中查詢特定副檔名(.doc、.pptx)。

例如：
要查詢以.crl結尾的所有URL，可以使用以下正規表示式：**\.crl$**

要查詢包含副檔名.pptx的所有URL，可以使用以下正規表示式：**\.pptx**

案例 3:正在嘗試查詢網站的特定塊

搜尋特定網站時，我們可能也在搜尋特定的HTTP響應。

例如：
如果我們要搜尋domain.com的所有TCP_DENIED/403消息，可以使用以下正規表示式：**tcp_denied/403.*domain\.com**

案例 4:在訪問日誌中查詢電腦名稱

使用NTLMSSP身份驗證方案時，可能會遇到使用者代理（Microsoft NCSI是最常見的）在進行身份驗證時錯誤地傳送電腦憑據而不是使用者憑據的例項。要跟蹤導致此問題的URL/使用者代理，我們可以將regex與「grep」一起使用以隔離發生身份驗證時發出的請求。

如果沒有使用的電腦名，我們可以使用「grep」並查詢所有在使用以下正規表示式進行身份驗證時用作使用者名稱的電腦名：**\$@**

一旦找到發生此問題的行，我們就可以使用下列正規表示式對使用的特定電腦名稱「grep」：**機器名稱\$**

第一個出現的條目應該是使用者使用電腦名稱（而不是使用者名稱）進行身份驗證時提出的請求。

案例 5:在訪問日誌中查詢特定時間段

預設情況下，訪問日誌訂閱將不包含顯示可讀日期/時間的欄位。如果要檢查特定時間段的訪問日誌，可以執行以下步驟：

從http://www.onlineconversion.com/unix_time.htm之類的站點查詢UNIX時間戳。一旦您擁有時間戳，您就可以在訪問日誌中搜尋特定時間。

例如：
Unix時間戳1325419200等於01/01/2012 12:00:00。

我們可以使用以下regex條目在2012年1月1日12:00前後搜尋訪問日誌：13254192

案例 6:搜尋嚴重或警告消息

我們可以使用正規表示式在任何可用日誌（如代理日誌或系統日誌）中搜尋嚴重或警告消息。

例如：
要在代理日誌中搜尋警告消息，我們可以輸入以下正規表示式：

1. **CLI>** grep
2. 輸入您希望「grep」的日誌編號。
   []> 17（在此處選擇代理日誌的編號）
3. 輸入正規表示式為「grep」。
   []> **警告**

其他有用的連結：

正規表示式 — 使用手冊