ESA、SMA和WSA Grep，帶Regex以搜尋日誌

目錄

[簡介](#)
[必要條件](#)
[帶Regex的Grep](#)
[案例 1:在訪問日誌中查詢特定網站](#)
[案例 2:嘗試查詢特定副檔名或頂級域](#)
[案例 3:嘗試查詢網站的特定塊](#)
[案例 4:在訪問日誌中查詢電腦名稱](#)
[案例 5:在訪問日誌中查詢特定時間段](#)
[案例 6:搜尋嚴重或警告消息](#)

簡介

本文說明如何在**grep**命令中使用正規表示式(regex)來搜尋日誌。

必要條件

本文中的資訊係根據以下軟體和硬體版本：

- 思科網路安全裝置(WSA)
- 思科電子郵件安全裝置(ESA)
- 思科安全管理裝置(SMA)

帶Regex的Grep

使用**grep**命令搜尋裝置上的可用日誌（例如訪問日誌、代理日誌等）時，Regex是一個功能強大的工具。您可以使用**grep** CLI命令，根據網站、URL的任何部分以及使用者名稱搜尋日誌。

以下是一些常見情況，您可以在其中將regex與**grep**命令配合使用以協助進行疑難排解。

案例 1:在訪問日誌中查詢特定網站

最常見的情況是當您嘗試在WSA的訪問日誌中查詢對網站發出的請求時。

以下是範例：

通過安全外殼(SSH)連線到裝置。 收到提示後，輸入**grep**命令以列出可用的日誌。

```
CLI> grep
```
輸入您要標籤的日誌的**編號**。

```
[]> 1 (Choose the # for access logs here)
```
輸入正規表示式以**grep**。

```
[]> website\.com
```

案例 2:嘗試查詢特定副檔名或頂級域

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

以下是範例：

若要尋找以.crl結尾的所有URL，請使用以下正規表示式：

```
\.crl$
```
若要查詢包含副檔名.pptx的所有URL，請使用以下正規表示式：

```
\.pptx
```

案例 3:嘗試查詢網站的特定塊

搜尋特定網站時，也可以搜尋特定的HTTP響應。

以下是範例：

如果要搜尋domain.com的所有TCP_DENIED/403消息，請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。若要追蹤導致此問題的URL/使用者代理，請使用regex with **grep**以隔離發生驗證時提出的請求。

如果您沒有使用的電腦名，請使用**grep**並查詢在使用此正規表示式進行身份驗證時用作使用者名稱的所有電腦名：

```
\$@
```
一旦您擁有發生此情況的行，grep表示與此正規表示式一起使用的特定電腦名稱：

```
machinename\$
```

顯示的第一個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，請完成以下步驟：

1. 從站點(如聯機轉換)查詢UNIX時間戳。
2. 一旦您擁有時間戳，請在訪問日誌中搜尋特定時間。

以下是範例：

Unix時間戳1325419200相當於01/01/2012 12:00:00。

您可以使用此regex條目搜尋2012年1月1日12:00附近的訪問日誌：

13254192

案例 6:搜尋嚴重或警告消息

您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。

以下是範例：

要在代理日誌中搜尋警告消息，請輸入以下正規表示式：

```
CLI> grep
```

輸入您要標籤的日誌的編號。

```
[]> 17 (Choose the # for proxy logs here)
```

輸入正規表示式以grep。

```
[]> warning
```