NetAdmin
從技術到決策，掌握IT知識力

✔2011資安回顧

✔平板電腦步入企業應用

網管人

72 January 2012
每月1日出刊
定價280元 特價200元
http://www.netadmin.com.tw

標準式架構興起　維運管理有效率

模組化佈建 蔚為機房主流

解析應用層偵測微細攻擊

資安浪潮推升 IPS走向新世代

網羅常見問題　詳解細部疑難

VMware虛擬化技術 實務問答

PC home 電腦家庭出版集團 PUBLICATION GROUP
ISSN 1990649-8
01
9 771990 649005
集團編號2FNA072書店退書日期2012年3月1日

擺脫csv格式輸出限制

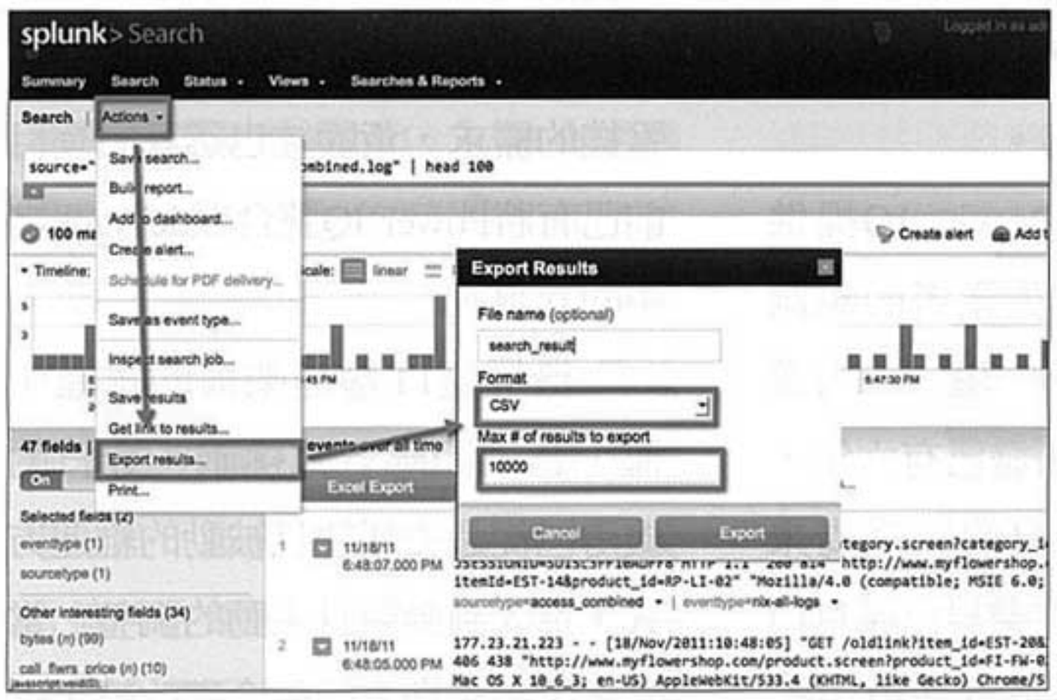
安裝Excel Export 排除難題一次搞定

文◎Owen Lee

Splunk將搜尋結果以csv格式輸出，可以方便進行其他的處理與用途，但是以一般的方式輸出會發生一些意想不到的狀況，以下將借重「Excel Export」應用程式一次解決這些問題。

通常，Splunk可以將搜尋的結果匯出成csv格式，讓使用者拿去做其他的處理。Splunk有許多匯出csv的方式，但是實務應用時卻會碰到各式各樣的限制與麻煩。

譬如，如下圖所示在搜尋頁面點選【Action】→【Export results】，然後選擇csv檔案類型。但是，這個方法有限制，最多只能匯出一萬筆資料，這個限制著實讓人傷腦筋。



而另一個替代方案是，在搜尋語句最後使用outputsv指令，將結果匯出成csv檔案，但問題是Splunk會將檔案放在Splunk Server的某個路徑下，此路徑不能更改，所以若不是該設備的管理人員，可能沒有權限存取到這個目錄。

還有，第三個方案是將搜尋語句儲存成「scheduled saved search」，定時地在背景執行。可以要求Splunk將搜尋結果儲存成csv檔案，並且以電子郵件的方式寄出。這個方案看似不錯，但是使用者收到csv檔案後會發現怎麼多了許多奇怪的欄位。

原來，Splunk不僅僅將搜尋結果打包，還將平時隱藏的一些欄位一起打包寄出，一般使用者對此當然無法接受。因應作法是另外再寫一個Shell Script，將檔案先處理過再寄出。

可是，問題還是沒有解決！使用者會問，為什麼不能用Excel直接開啟csv檔案？一定要用匯入的方式？原因是這又牽涉到另外一些技術問題，例如中文編碼（Splunk使用UTF-8）以及Excel特有的BOM檔頭問題等等。該如何排除以上這些層出不窮的難題呢？

幸好，有一位作者Araitz開發出名為「Excel Export」的App，可以解決以上所有的問題，真可說是造福蒼生。

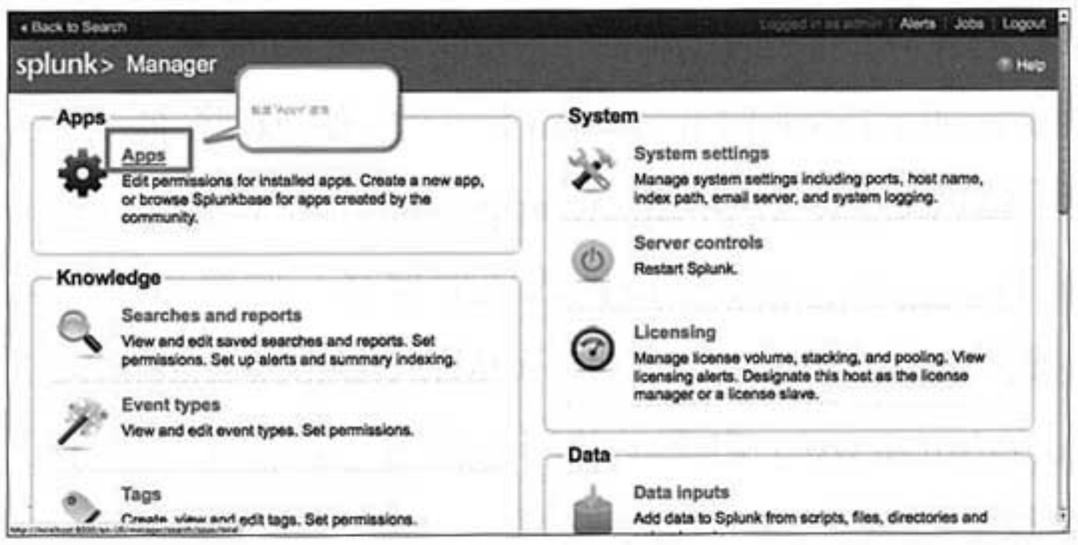
安裝使用Excel Export

「Excel Export」的使用方法很簡單，只須依照

以下的步驟一步一步執行即可：

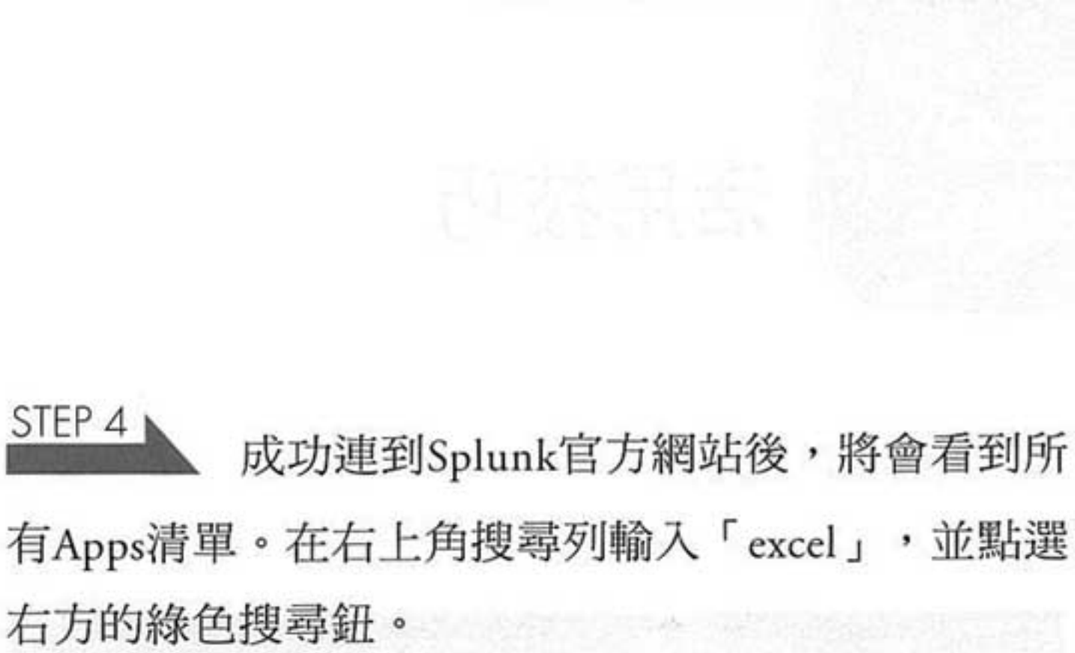
STEP 1 登入Splunk，在任一畫面點選右上角的Manager（管理）連結。

STEP 2 注意左上角Apps連結，然後加以點選。



STEP 3 本頁顯示所有已安裝的Splunk Apps清單，但是這次要安裝一個新的App，名稱為「Excel Export」，所以必須連到Splunk官方網站下載，點選其中的「Find more apps online」。

STEP 4 成功連到Splunk官方網站後，將會看到所有Apps清單。在右上角搜尋列輸入「excel」，並點選右方的綠色搜尋鈕。

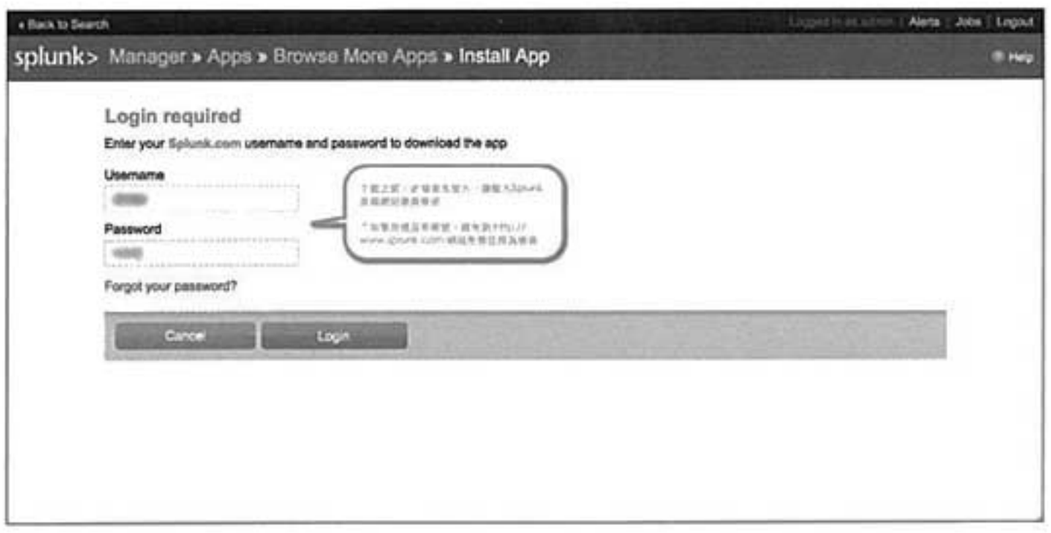


STEP 5 找到一個名為「Splunk for Excel Export」的App，可以查看作者是誰、最新的版本何時發布、版號、被下載的次數以及版權擁有者。它是免費的，不用再花費任何費用。

STEP 6 下方有一個名稱為「Install Free」的綠色按鈕（如果已經安裝過，就不會出現此按鈕），在上面按一下滑鼠左鍵。

STEP 7 此時Splunk會要求驗證你的身分，如果還不是Splunk的會員，請趕快加入，有很多好用或是新

奇的Apps可以免費下載。

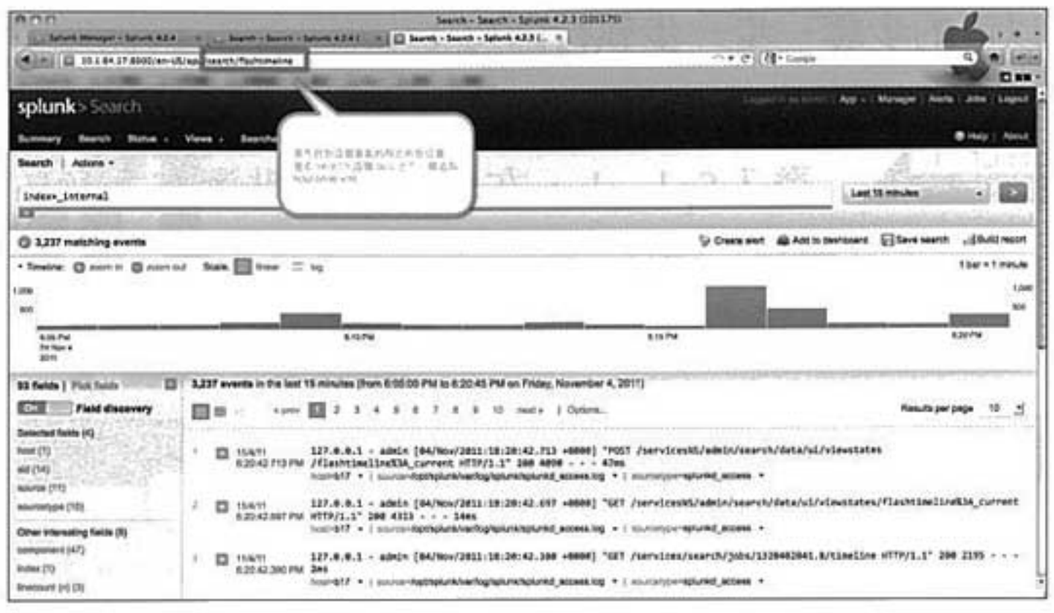


STEP 8 成功登入之後，會自動下載與安裝，這些都在背景執行。安裝成功後會顯示「Restart Splunk」（重新啟動Splunk服務）的訊息，請重新啟動。當然，如果是有其他使用者正在使用，請通知他們一下，勿逕行重啟。

完成以上的步驟就完成了啟用動作，步驟雖多，但是都很簡單，通常在1分鐘內就可以全部完成。

加入Excel Export功能

接著，須決定將Excel Export的功能加入到哪些畫面（Dashboard）上，通常都會想放到Search主畫面上，因為這是最常使用的畫面，Search主畫面其實有個正式的名稱，叫做「flashtimeline」。



接下來，就要找出產生這個畫面的檔案進行修改。這也不難，跟著下面的說明一步步做就好：

STEP 1 參照上圖所示，在上方URL最後的「flashtimeline」就是檔案名稱，由於Splunk的畫面都是由XML檔案組成的，所以確實的檔案名稱是flashtimeline.xml，而存放路徑是在「$SPLUNK_HOME/etc/apps/search/default/data/ui/views/」內。不要直接修改這個檔案，應將這個檔案複製一份到「$SPLUNK_HOME/etc/apps/search/local/data/ui/views/」之下，並修改後者。路徑不存在是正常的，請直接新增這串路徑。

NOTE

$SPLUNK_HOME是指向Splunk安裝的目錄，*NIX系統預設是「/opt/splunk」、Windows系統預設為「c:\program files\splunk」、Mac OS系統則是「/Applications/splunk」。

STEP 2 請用一般文書編輯器打開檔案，在第63行的地方插入以下指令：

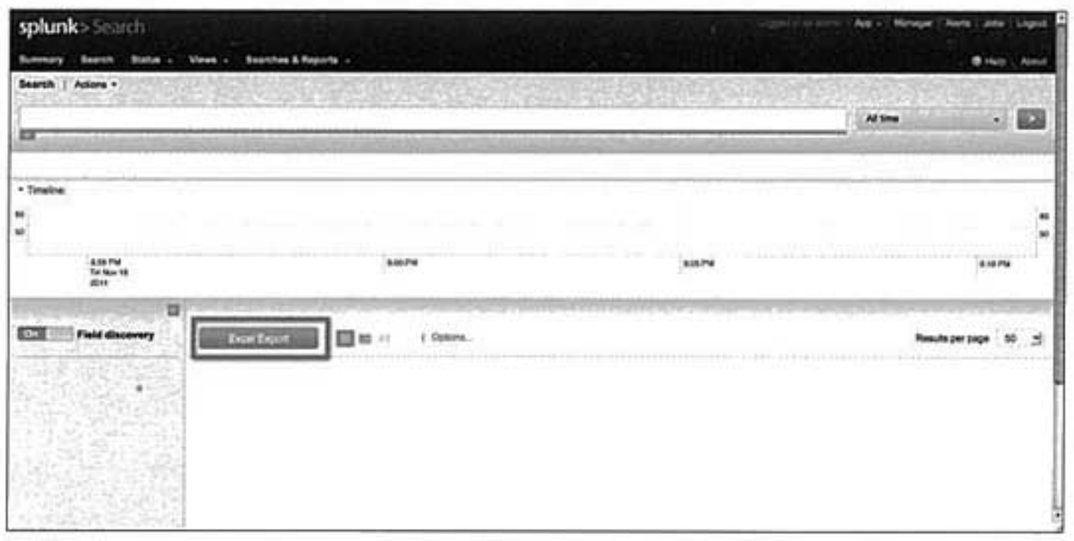
```
<module name="ExcelExport" layoutPanel="PageControls" />
```

flashtimeline.xml

```
48  <param name="options">
49   <list>
50     <param name="text">10</param>
51     <param name="value">10</param>
52    </list>
53    <list>
54     <param name="text">20</param>
55     <param name="value">20</param>
56    </list>
57    <list>
58     <param name="text">50</param>
59     <param name="selected">True</param>
60     <param name="value">50</param>
61    </list>
62  </param>
63  <module name="ButtonSwitcher" layoutPanel="pageControls">
64    <param name="mode">independent</param>
65    <param name="hideChildrenOnLoad">True</param>
66    <param name="selected">splIcon-events-list</param>
67    <param name="disableOnNull">True</param>
68    <module name="ResultsHeader" layoutPanel="resultsHeaderPanel" gro
69      <param name="entityLabel">events</param>
70      <param name="entityLabelSingular">event</param>
71      <param name="entityName">events</param>
72      <module name="Paginator" layoutPanel="pageControls">
73        <param name="entityName">events</param>
74        <param name="maxPages">10</param>
75        <module name="SoftWrap" layoutPanel="resultsOptions">
76          <param name="enable">True</param>
77          <module name="RowNumbers">
78            <module name="MaxLines">
79              <param name="options">
80                <list>
81                  <param name="text">5</param>
82                  <param name="selected">True</param>
83                  <param name="value">5</param>
84                </list>
85                <list>
86                  <param name="text">10</param>
87                  <param name="value">10</param>
```

修改前

STEP 3 回到Splunk搜尋頁面，點選畫面左上角白色Splunk標示，Splunk會自動重新載入剛才修改的Dashboard，如下圖所示，就會看到〔Excel Export〕按鈕了。



STEP 4 按照以往搜尋出資料之後，按一下〔Excel Export〕按鈕，如圖所示，再輸入檔案名稱，選擇輸出筆數。請注意，並沒有1萬筆的上限。接著，就可以將檔案直接下載到本機硬碟，而且使用Excel程式直接開啟。很好用吧！之前的各項限制都解除了。

flashtimeline.xml

```
47  <module name="Count" layoutPanel="pageControls">
48   <param name="options">
49    <list>
50      <param name="text">10</param>
51      <param name="value">10</param>
52     </list>
53     <list>
54      <param name="text">20</param>
55      <param name="value">20</param>
56     </list>
57     <list>
58      <param name="text">50</param>
59      <param name="selected">True</para
60      <param name="value">50</param>
61     </list>
62   </param>
63   <module name="ExcelExport" layoutPanel="pageControls"/>
64   <module name="ButtonSwitcher" layoutPanel="pageControls">
65     <param name="mode">independent</param>
66     <param name="hideChildrenOnLoad">True</param>
67     <param name="selected">splIcon-events-list</param>
68     <param name="disableOnNull">True</param>
69     <module name="ResultsHeader" layoutPanel="resultsHeaderPanel"
70       group="splIcon-events-list" altTitle="Events List">
71       <param name="entityLabel">events</param>
72       <param name="entityLabelSingular">event</param>
73       <param name="entityName">events</param>
74       <module name="Paginator" layoutPanel="pageControls">
75         <param name="entityName">events</param>
76         <param name="maxPages">10</param>
77         <module name="SoftWrap" layoutPanel="resultsOptions">
78           <param name="enable">True</param>
79           <module name="RowNumbers">
80             <module name="MaxLines">
81               <param name="options">
82                 <list>
83                   <param name="text">5</param>
84                   <param name="selected">True</param>
85                   <param name="value">5</param>
86                 </list>
```

修改後

請在第63行插入以下指令

NOTE

上述指令有大小寫的區別，不要打錯，雙引號是英文模式的，不要輸成中文全型的模式，改完後存檔即可。

Splunk App的精神就是，鼓勵熱心、有技術能力的使用者在這個平台上開發各種新的功能，所以在Splunkbase上有許多個人開發的作品，鼓勵各位上去看看有什麼適用的Apps。

<本文作者為精誠資訊協銷代理事業部資深處長，專長為金融、電信應用系統研發>