SYSTEX

splunk>lab

目錄索引

SYSTEX

making it happen 精誠資訊

概要說明

此文件爲精誠資訊所提供，目的爲使客戶第一次使用 Splunk 時可快速完成基本配置

用戶請於 www.splunk.com 登錄帳號，以便下載 Splunk 安裝軟體與相關資源。

請注意此份用戶操作文件依照 Splunk 3.4.6 版本爲製作依據，非此最後版本，請參考以下網址查詢最新安裝方式與相關信息。
www.splunk.com/base

最後更新時間: 2009/4

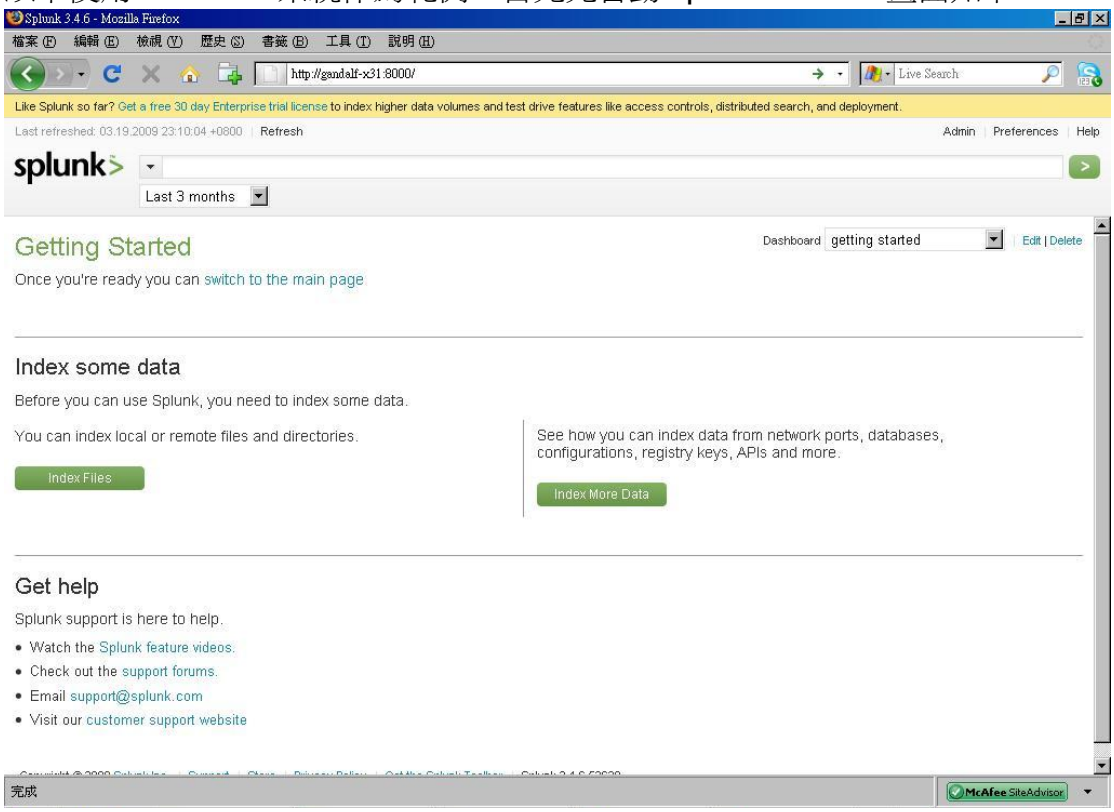
1 使用前注意事項

安裝前請先確認 Splunk 最低硬體與作業系統配置需求，請參考安裝手冊資訊後，進行 splunk 操作。

請使用 Mozilla FireFox 1.5 以上版本爲 Splunk 使用的瀏覽器，並確認有安裝 Adobe Flash 9 功能。

2 操作說明 – Data Input 資料數據導入

以下使用 Windows 系統作爲範例。首先先啓動 Splunk Web UI 畫面如下：



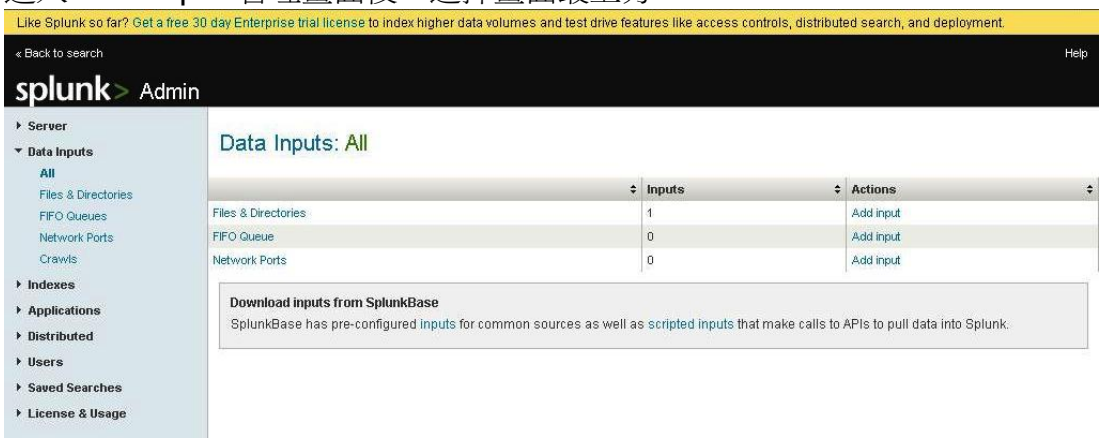
將 Splunk 安裝於 Windows 系統中，預設會導入 Windows Event Log ，在此列舉其他資料數據導入方式：

1. Files & Directories
2. Network ports

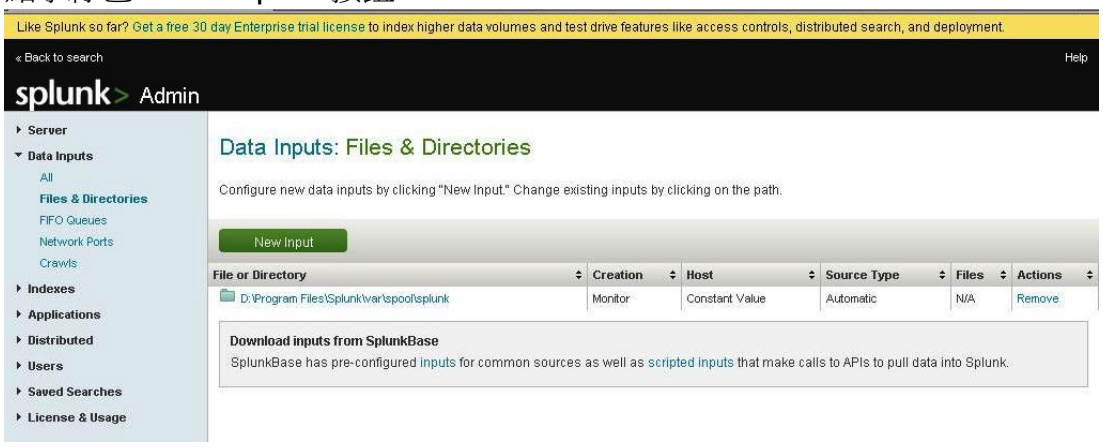
進入資料數據導入頁面，可直接於上圖畫面中綠色按鈕 Index Files 進行資料數據導入，或於 Web UI 右上方 Admin 頁簽進入管理畫面，選擇 Data Input 進行，兩者方式皆相同，可依照喜好進行。

1. Files & Directories

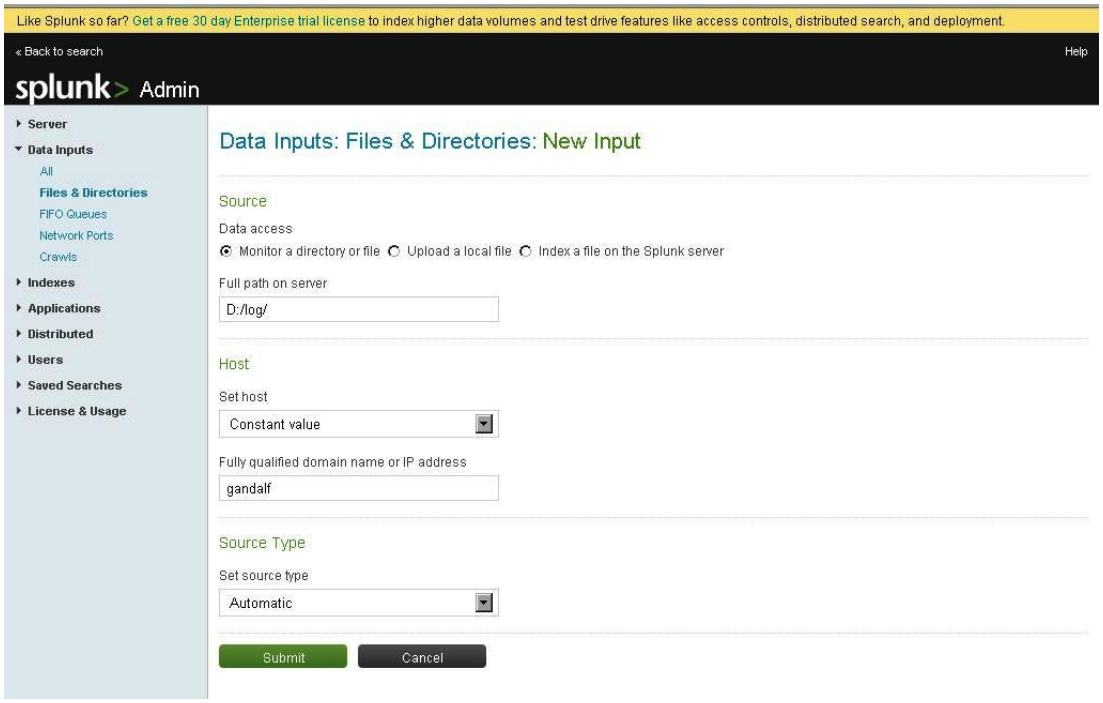
進入 Data Input 管理畫面後，選擇畫面最上方 Files & Directories



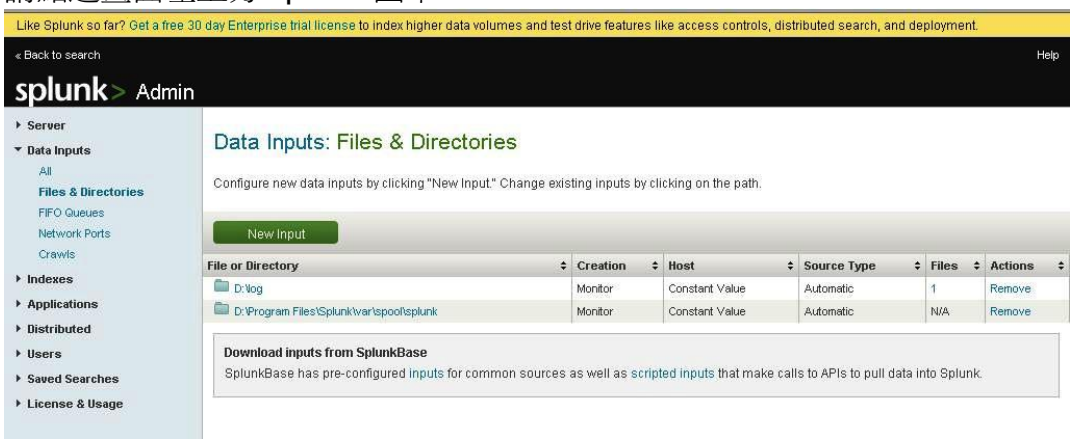
點擊綠色 <New Input> 按鈕



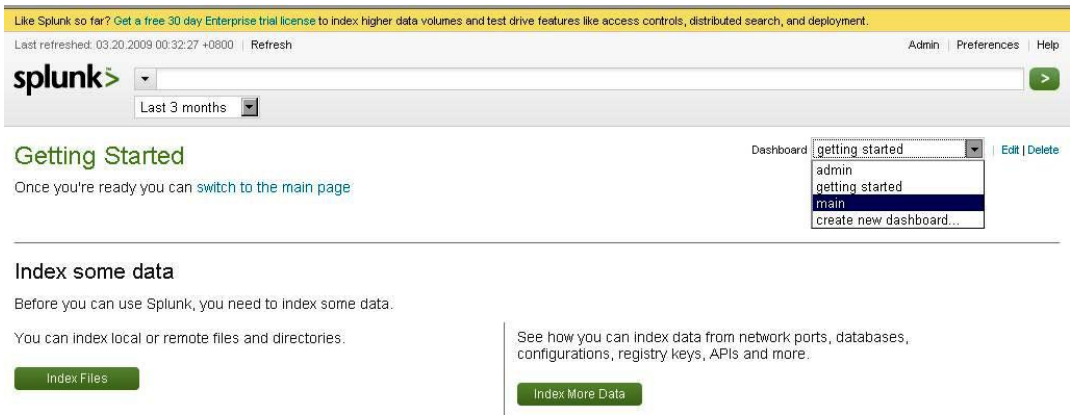
下方 Full path on server 處理 Splunk 本機上 D:/log/ 目錄中的 Log，直接點擊綠色 <Submit> 按鈕完成



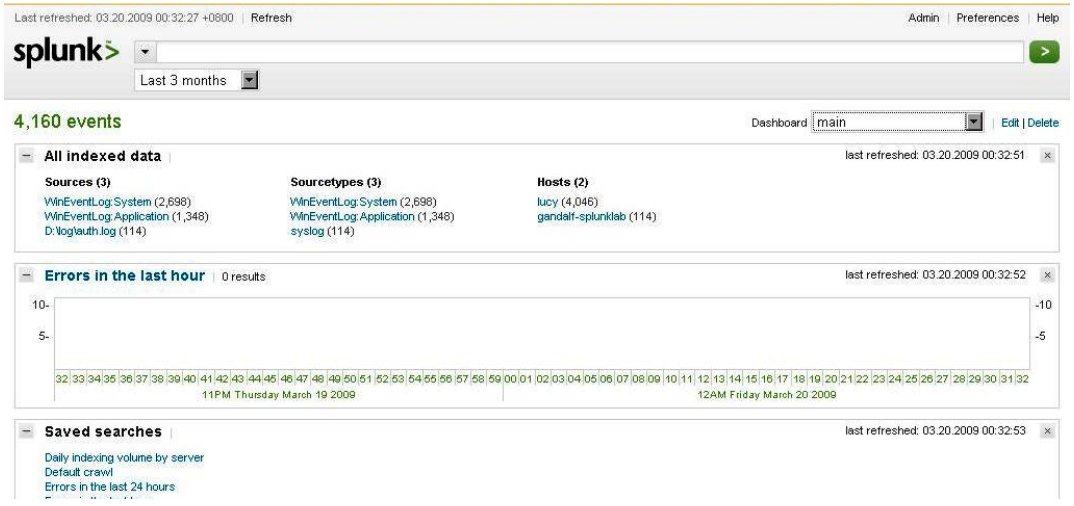
完成設定後會移至以下畫面，請確認剛才輸入的設定中，欄位 Files 數量與您所導入的 Log 檔案數相同，接下來回 Splunk 主畫面確認資料數據導入成功，請點選畫面左上方 Splunk 圖示



回主畫面後，請切換儀表版(Dashboard)至 主要頁面(Main)，點選右上方 Dashboard 下拉選項，進行切換



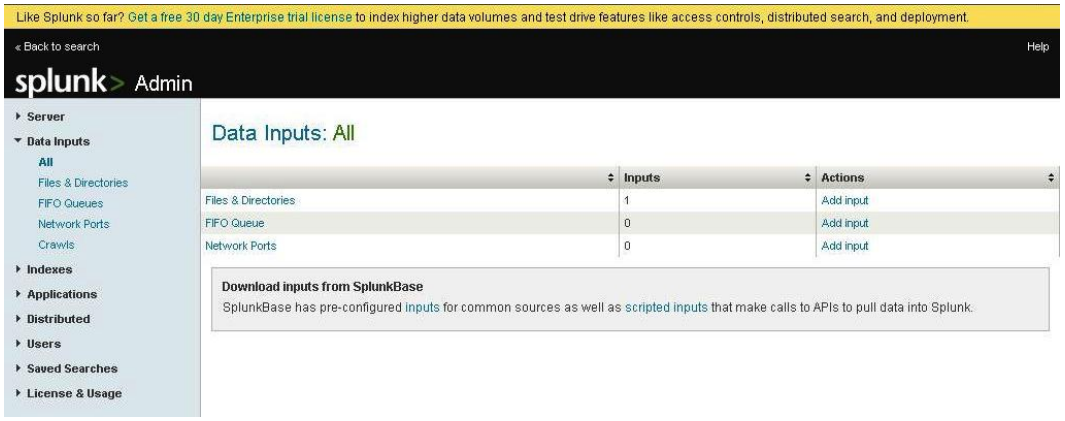
預設主畫面有三個子儀表版，爲 All Indexed data、Error in the last hour 與 Saved Search ，請先檢視 All Indexed data 儀表版中 source 下，是否有您剛剛導入的資訊



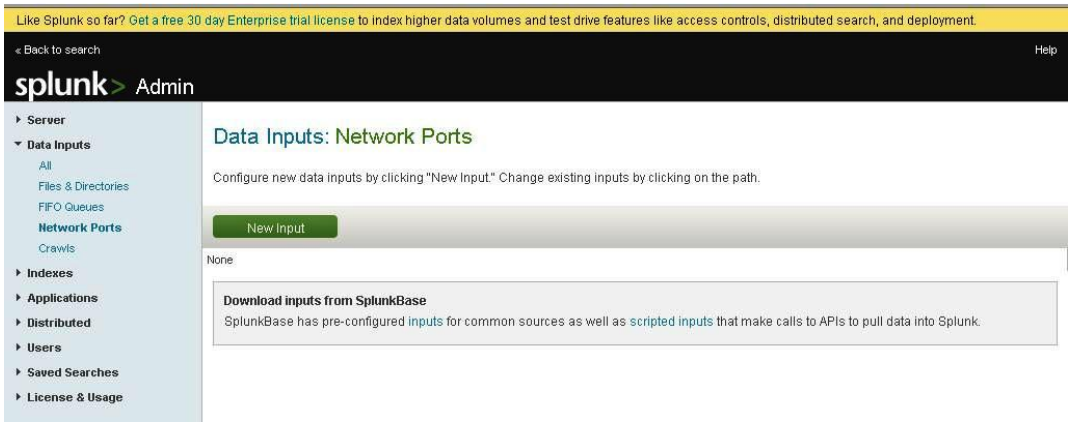
2. Network ports

在此我們舉例導入 syslog (UDP:514) ，請先確認來源設備以經設定 Splunk 爲蒐集 syslog 的主機，相關設定請恰您的系統、網路管理員，或您的協力、服務廠商。

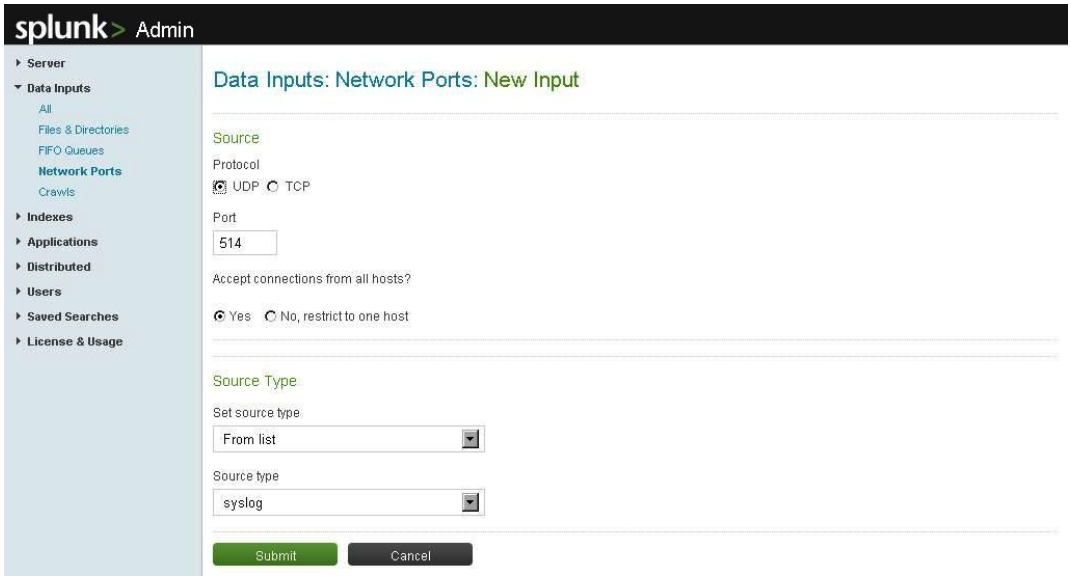
請進入 Data Input 管理畫面，點選 Networks Ports



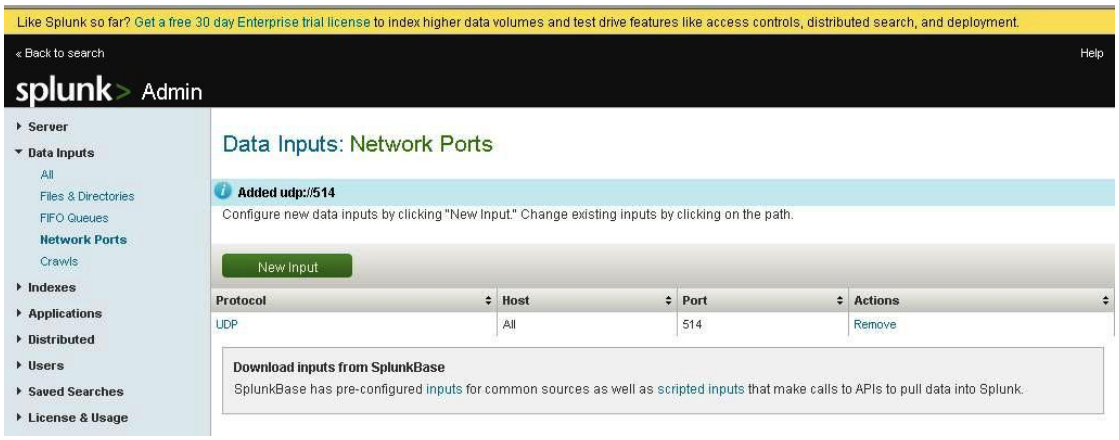
請點擊綠色 <New Input> 按鈕進入



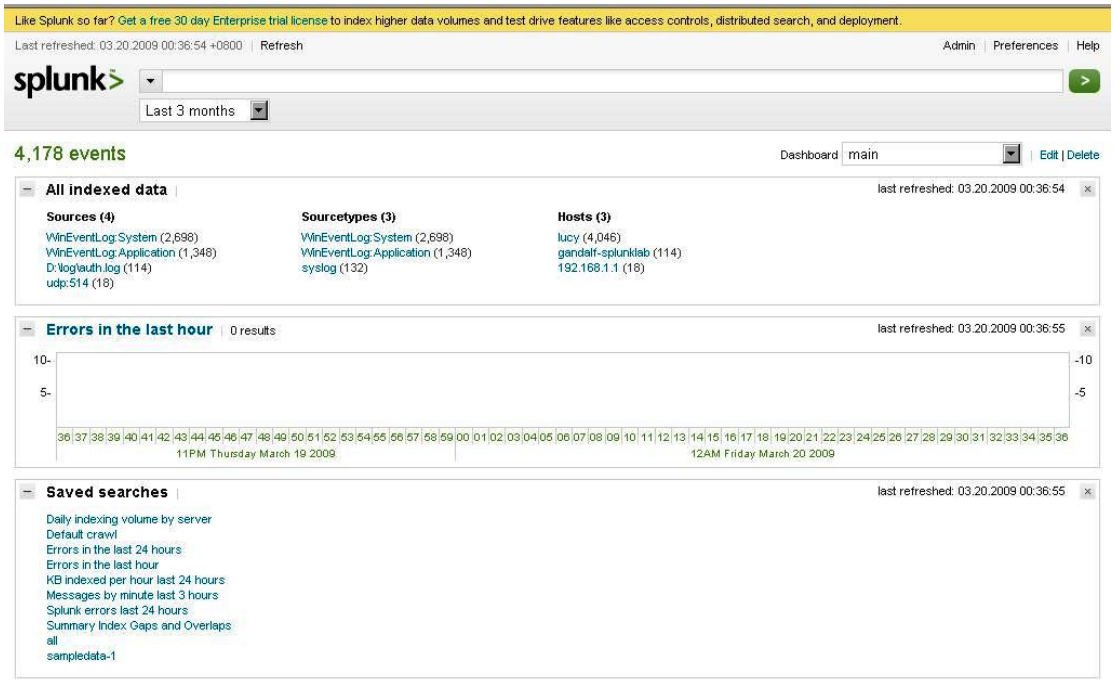
Protocol 選擇 UDP ，點擊綠色 <Submit> 按鈕進行



完成 syslog 蒐集設定如下，點擊左上方 Splunk 圖示回主畫面



檢視 All Indexed data 儀表版中 Hosts 下，是否有您預接收的主機 IP 或名稱，在 Sourcetypes 下是否有 syslog 資訊，於 Sources 下是否有 udp:514 資訊，如以上皆有出現，您已經完成 Network ports SYSLOG 的資料數據導入。



現在您可以進行 Splunk Search

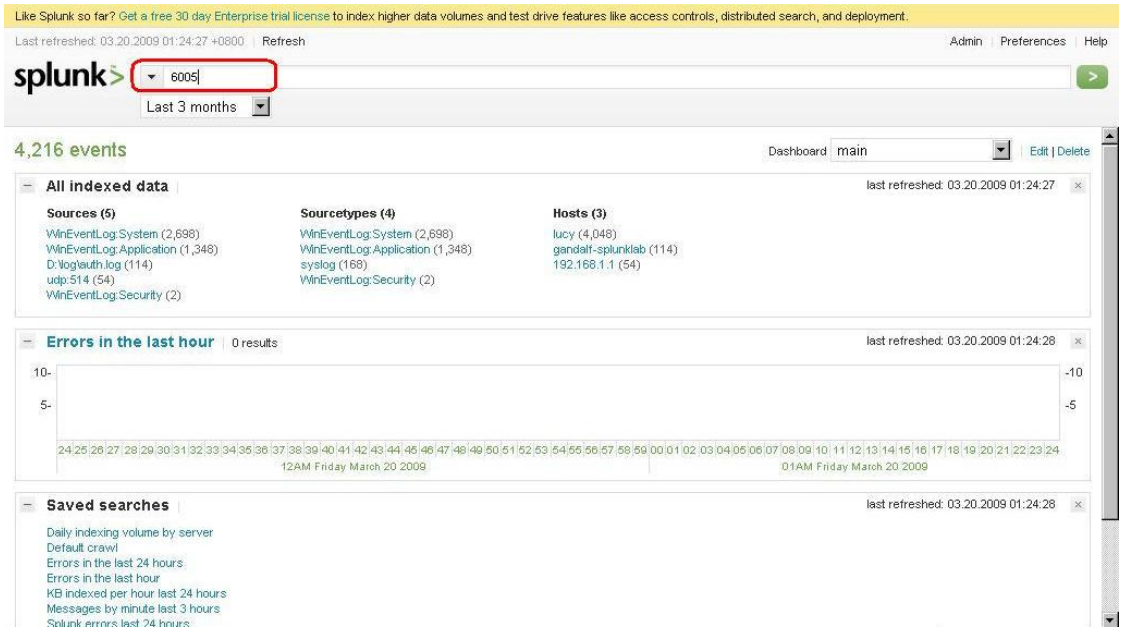
3 操作說明 - Search 搜尋

以下列舉 Windows 與 Linux 上的 Operation 與 Security 搜尋範例：

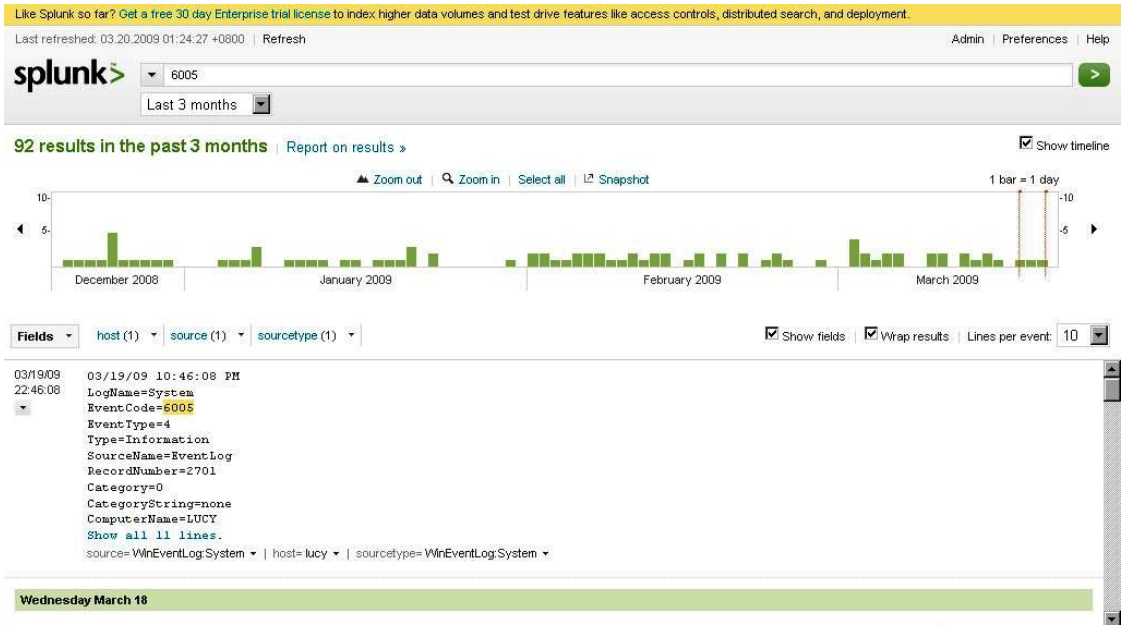
1. Windows Event Code = 6005 事件日誌服務啓動
2. Linux su 使用者權限變換檢視

1. Windows Event Code = 6005 找出系統維運狀態與安全問題

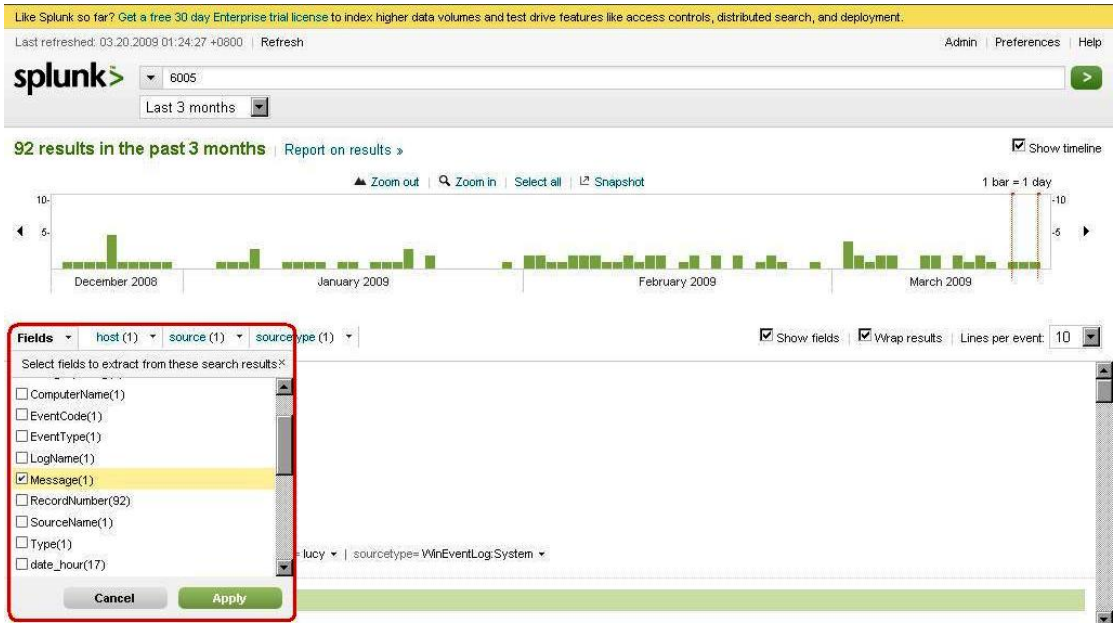
請於 Splunk 搜尋框中，鍵入關鍵字 6005，按壓 Enter 執行搜尋



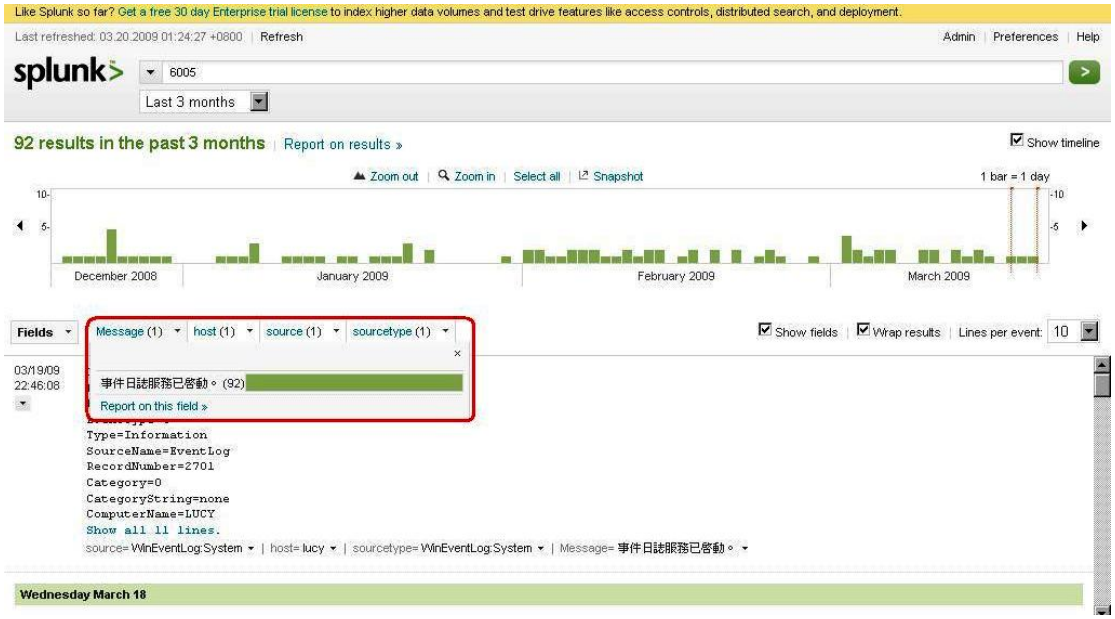
搜尋結束後，Splunk 會先展示一個圖形，以發生 Event Code = 6005 的頻率對應時間，我們既可知道在三個月內發生事件日誌服務啓動(代表系統開機)的頻率。下方爲原始數據內容。



Splunk 會自動判斷日誌欄位，您可以點選下方欄位分析 Fields ，選取您希望展示的欄位



選取後您既可檢視欄位內容，其中資訊包含事件發生頻率

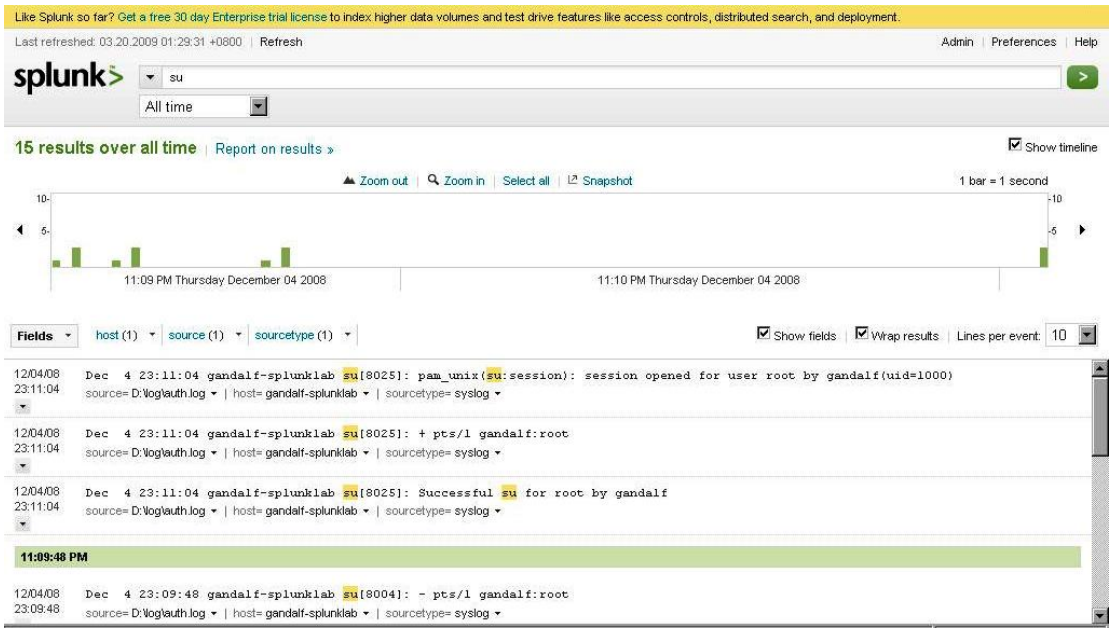


更多 Windows Event ID 查詢，可搜尋網際網路資源。

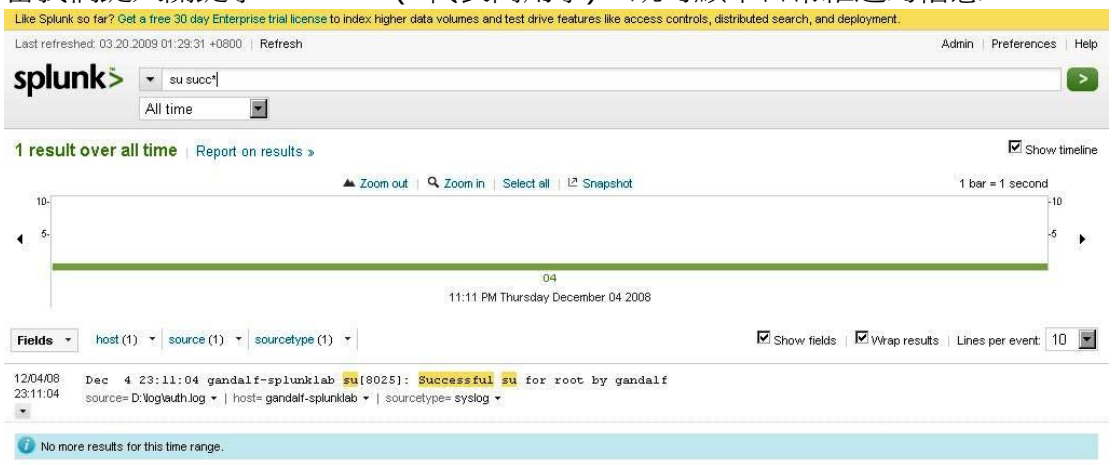
參考網址：www.eventid.net

2. Linux SU 使用者權限變換檢視

SU 指令在日常維運 Linux 系統時經常會使用到，而切換時必須要有權限得以執行，對於 SU 切換成功，我們可以視爲一般性作業，但對於 SU 切換失敗，就有可能是安全問題，以下以 SU 爲核心做搜尋。

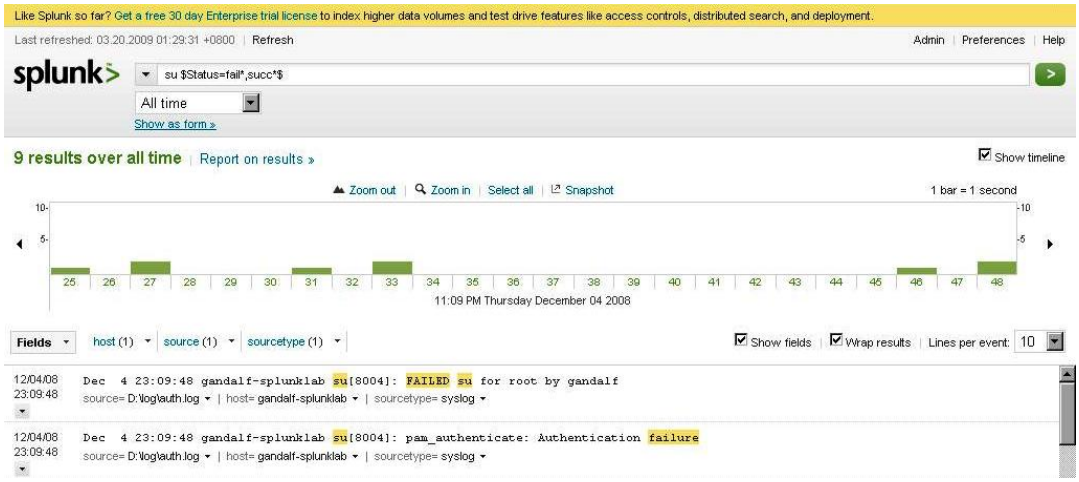


當我們鍵入關鍵字 su succ* (* 代表萬用字)，既可顯示日常維運的信息

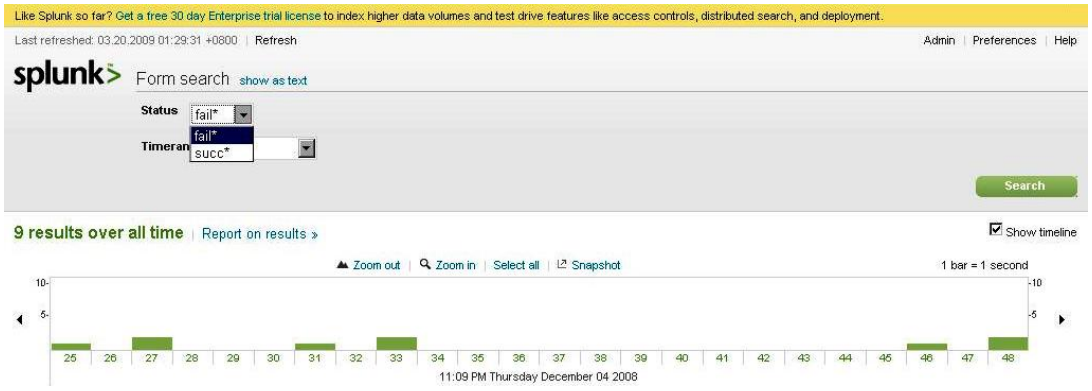


當我們鍵入 su fail* 兩次以上的切換錯誤，就代表可能的安全問題

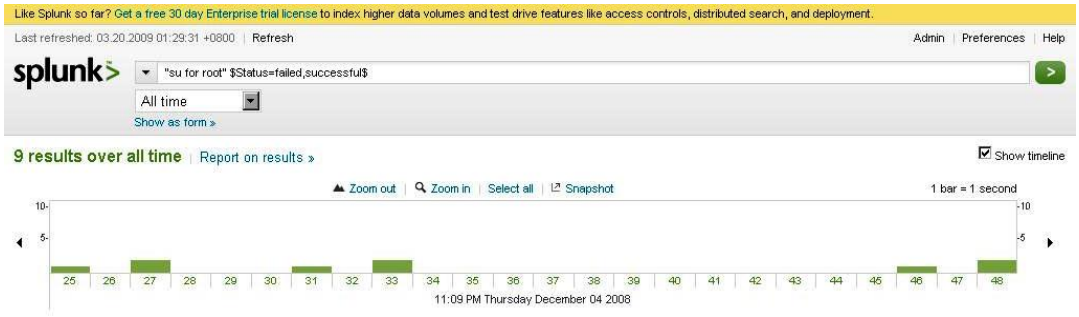
以下使用進階的搜尋方式 show as form。鍵入 su $Status=fail*,succ*$ ($$ 包裹代表啓動 show as form 搜尋)



當我們點選搜尋框下方的 show as form 後，既可得到下圖內容，我們可下拉選單式選擇我們希望搜尋的關鍵字，這可以讓我們將搜尋分享給其他維運者使用。

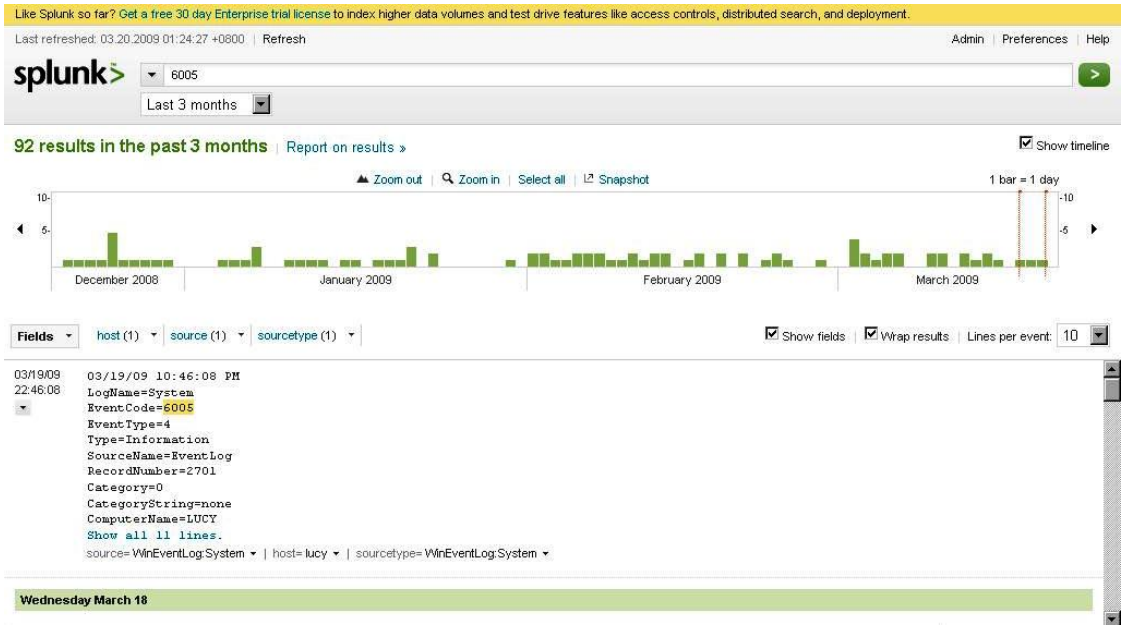


檢視日誌內容，我們可以得到完整的資訊，接下來我們提升搜尋的準確度，鍵入 “su for root” $Status=failed,successful$ (“代表爲字串”) 在 splunk 搜尋框中，空格代表指令 AND (布林代數 AND, OR 與 NOT) ，所以可以精準收斂。

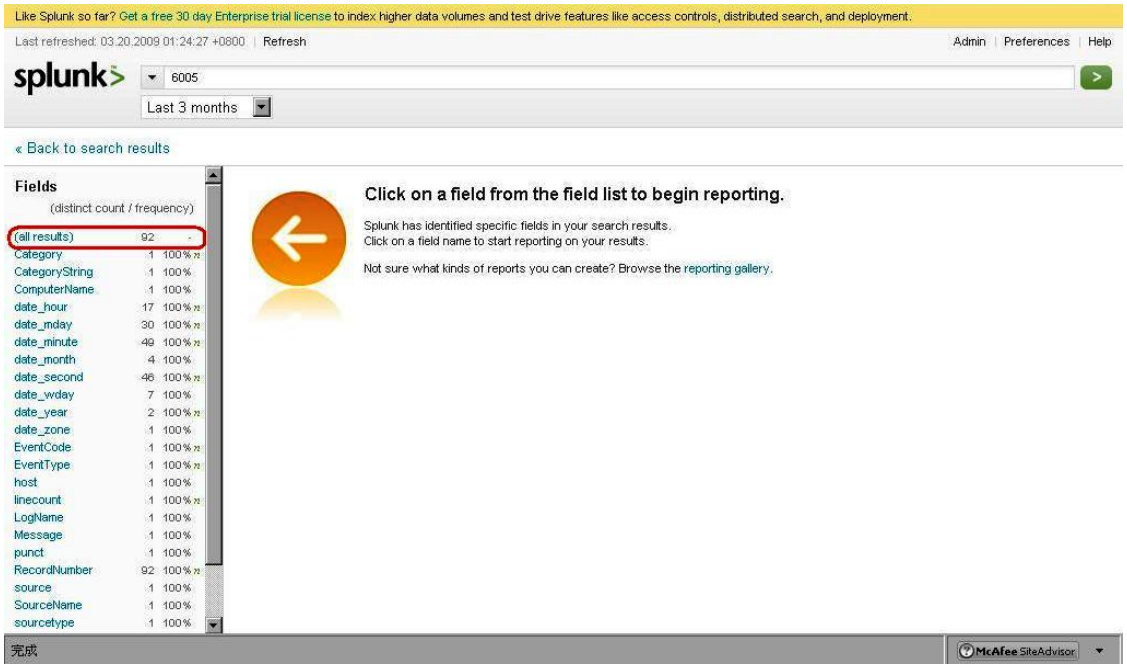


4 操作說明 - Report 報表快速產出

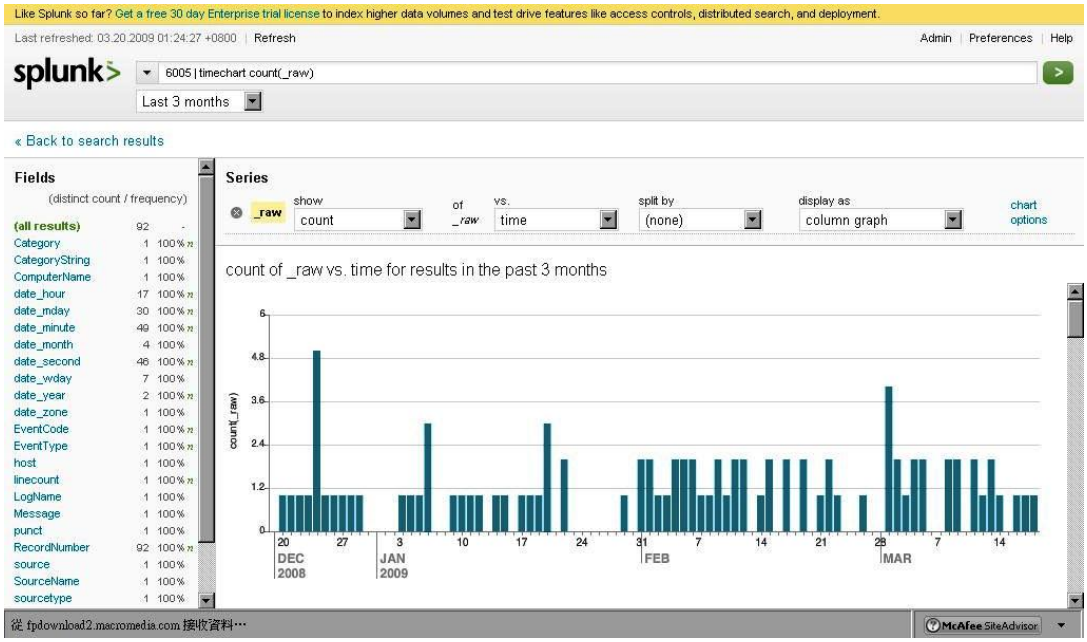
搜尋結束後，Splunk 會先展示一個圖形，以發生 Event Code = 6005 的頻率對應時間，我們可以產出不同的報表格式，請點選 藍色 Report on results > 進入報表模式



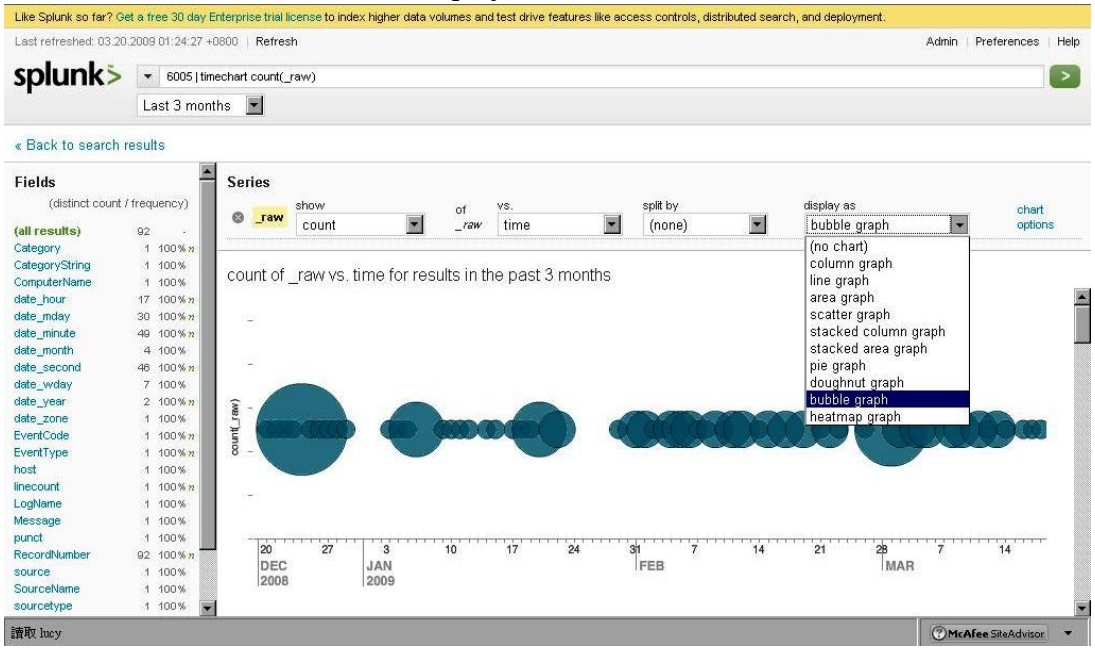
進入報表模式後，請點選左方 (all results)



我們既可產出基本的直方圖



我們亦可使用報表形式切換 <display as>換成我們希望呈現的方式



亦可利用快速鍵做報表合併，Ctrl (鍵盤上) 持續按壓，用滑鼠點選左方欄位，加入欲比較的資料

此份使用手冊僅列舉 Windows 與 Linux 在維運與安全管理的範例，如需其他範例說明，請至 http://www.splunk.com/view/SP-CAAAAGV 參考，其他用戶使用說明，請參考 http://www.splunk.com/base ，或聯繫當地 Splunk 服務供應商取得支援服務。

Happy Splunk

註記

此份用戶手冊爲基於 Splunk 建議而說明。