



目錄索引

1	使用前注意事項	2
2	操作說明 - DATA INPUT 資料數據導入.....	2
3	操作說明 - SEARCH 搜尋.....	7
4	操作說明 - REPORT 報表快速產出.....	11
	註記.....	14



概要說明

此文件為精誠資訊所提供，目的為使客戶第一次使用 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 版本為製作依據，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

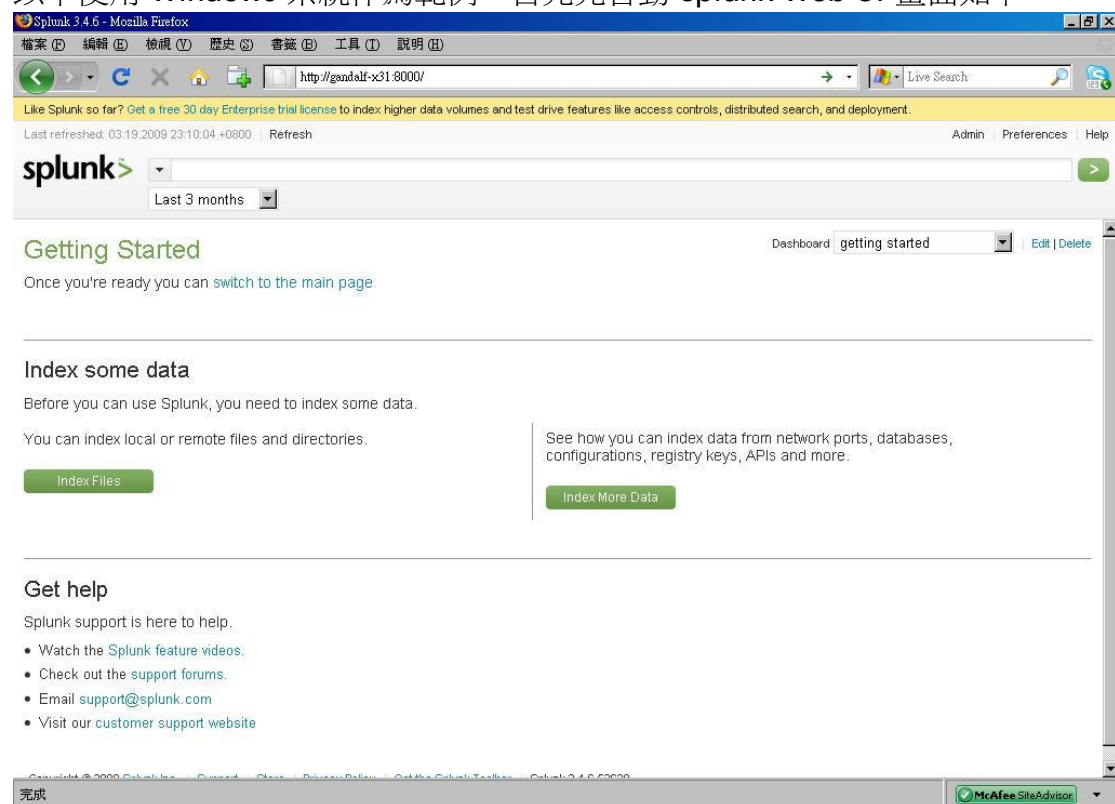
1 使用前注意事項

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 以上版本為 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 系統作為範例。首先先啟動 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 頁籤進入管理畫面，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

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk> Admin

- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: All

	Inputs	Actions
Files & Directories	1	Add input
FIFO Queue	0	Add input
Network Ports	0	Add input

Download inputs from SplunkBase
SplunkBase has pre-configured inputs for common sources as well as scripted inputs that make calls to APIs to pull data into Splunk.

點擊綠色 <New Input> 按鈕

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk> Admin

- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: Files & Directories

Configure new data inputs by clicking "New Input." Change existing inputs by clicking on the path.

New Input

File or Directory	Creation	Host	Source Type	Files	Actions
D:\Program Files\Splunk\var\spool\splunk	Monitor	Constant Value	Automatic	N/A	Remove

Download inputs from SplunkBase
SplunkBase has pre-configured inputs for common sources as well as scripted inputs that make calls to APIs to pull data into Splunk.

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

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk> Admin

- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: Files & Directories: New Input

Source

Data access

☒ Monitor a directory or file ☐ Upload a local file ☐ Index a file on the Splunk server

Full path on server

D:/log/

Host

Set host

Constant value

Fully qualified domain name or IP address

gandalf

Source Type

Set source type

Automatic

Submit Cancel

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

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk> Admin

Server

Data Inputs

- All
- Files & Directories
- FIFO Queues
- Network Ports
- Crawls

Indexes

Applications

Distributed

Users

Saved Searches

License & Usage

Data Inputs: Files & Directories

Configure new data inputs by clicking "New Input." Change existing inputs by clicking on the path.

New Input

File or Directory	Creation	Host	Source Type	Files	Actions
D:\log	Monitor	Constant Value	Automatic	1	Remove
D:\Program Files\Splunk\var\spool\splunk	Monitor	Constant Value	Automatic	N/A	Remove

Download inputs from SplunkBase

SplunkBase has pre-configured inputs for common sources as well as scripted inputs that make calls to APIs to pull data into Splunk.

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

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

Last refreshed: 03.20.2009 00:32:27 +0800 Refresh Admin | Preferences | Help

splunk> Last 3 months

Getting Started

Once you're ready you can [switch to the main page](#)

Dashboard: getting started | Edit | Delete

- admin
- getting started
- main
- create new dashboard...

Index some data

Before you can use Splunk, you need to index some data.

You can index local or remote files and directories.

Index Files

See how you can index data from network ports, databases, configurations, registry keys, APIs and more.

Index More Data

預設主畫面有三個子儀表版，為 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

Last refreshed: 03.20.2009 00:32:27 +0800 Refresh Admin | Preferences | Help

splunk> Last 3 months

4,160 events

Dashboard: main | Edit | Delete

All indexed data

last refreshed: 03.20.2009 00:32:51

Sources (3)

- WinEventLog System (2,698)
- WinEventLog Application (1,348)
- D:\log\auth.log (114)

Sourcetypes (3)

- WinEventLog System (2,698)
- WinEventLog Application (1,348)
- syslog (114)

Hosts (2)

- lucy (4,046)
- gandalf-splunklab (114)

Errors in the last hour

0 results last refreshed: 03.20.2009 00:32:52

10- 5- -10 -5

32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

11PM Thursday March 19 2009 12AM Friday March 20 2009

Saved searches

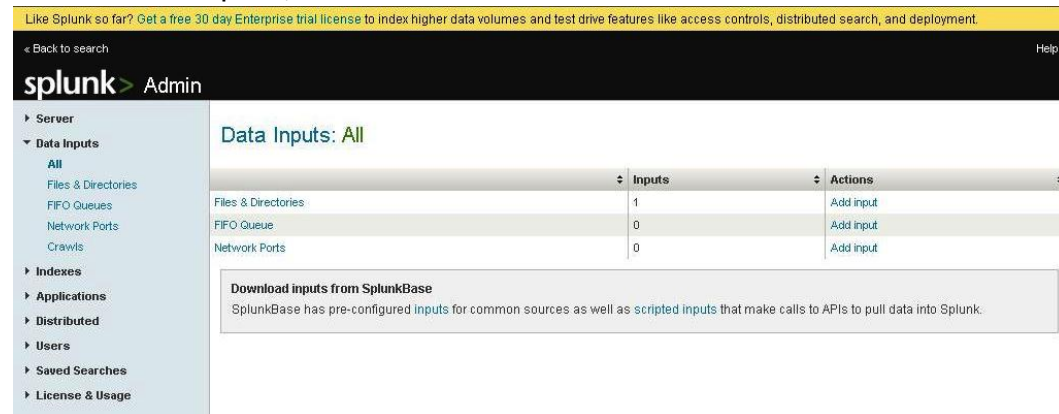
last refreshed: 03.20.2009 00:32:53

- Daily indexing volume by server
- Default crawl
- Errors in the last 24 hours

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** 為蒐集 **syslog** 的主機，相關設定請洽您的系統、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**



Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk > Admin

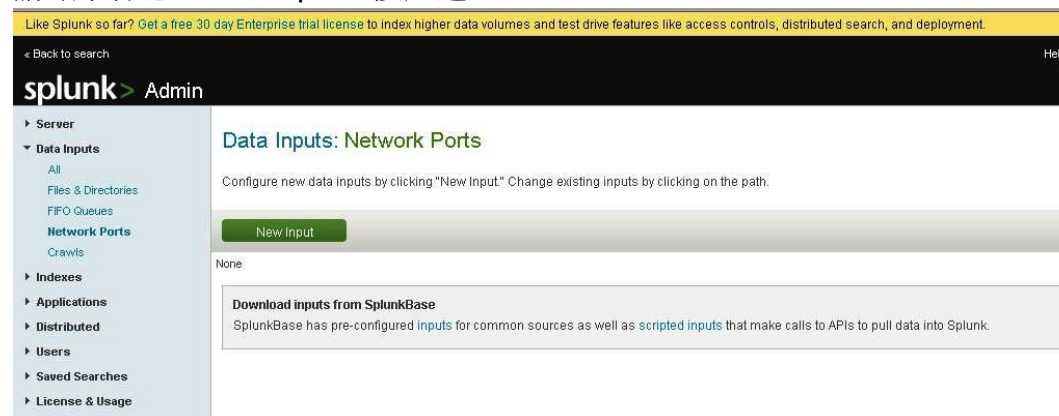
- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: All

	Inputs	Actions
Files & Directories	1	Add input
FIFO Queue	0	Add input
Network Ports	0	Add input

Download inputs from SplunkBase
SplunkBase has pre-configured [inputs](#) for common sources as well as [scripted inputs](#) that make calls to APIs to pull data into Splunk.

請點擊綠色 <New Input> 按鈕進入



Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk > Admin

- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: Network Ports

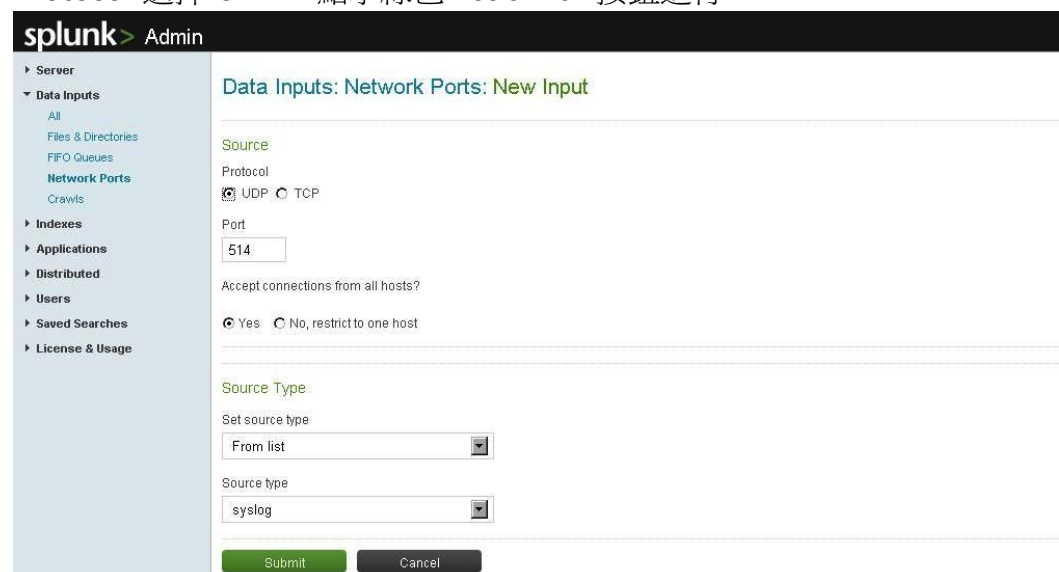
Configure new data inputs by clicking "New Input." Change existing inputs by clicking on the path.

[New Input](#)

None

Download inputs from SplunkBase
SplunkBase has pre-configured [inputs](#) for common sources as well as [scripted inputs](#) that make calls to APIs to pull data into Splunk.

Protocol 選擇 **UDP**，點擊綠色 <Submit> 按鈕進行



splunk > Admin

- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: Network Ports: New Input

Source

Protocol
☒ UDP ☐ TCP

Port
514

Accept connections from all hosts?
☒ Yes ☐ No, restrict to one host

Source Type

Set source type
From list

Source type
syslog

[Submit](#) [Cancel](#)

完成 syslog 蒐集設定如下，點擊左上方 Splunk 圖示回主畫面

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

< Back to search Help

splunk > Admin

- Server
 - Data Inputs
 - All
 - Files & Directories
 - FIFO Queues
 - Network Ports**
 - Crawls
 - Indexes
 - Applications
 - Distributed
 - Users
 - Saved Searches
 - License & Usage

Data Inputs: Network Ports

Added udp:514
Configure new data inputs by clicking "New Input." Change existing inputs by clicking on the path.

[New Input](#)

Protocol	Host	Port	Actions
UDP	All	514	Remove

Download inputs from SplunkBase
SplunkBase has pre-configured [inputs](#) for common sources as well as [scripted inputs](#) that make calls to APIs to pull data into Splunk.

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。

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

Last refreshed: 03.20.2009 00:36:54 +0800 | [Refresh](#) [Admin](#) | [Preferences](#) | [Help](#)

splunk > [>](#)

Last 3 months

4,178 events Dashboard: main | [Edit](#) | [Delete](#)

All indexed data last refreshed: 03.20.2009 00:36:54

Sources (4)

- WinEventLog System (2,698)
- WinEventLog Application (1,348)
- D:\logauth.log (114)
- udp:514 (18)

Sourcetypes (3)

- WinEventLog System (2,698)
- WinEventLog Application (1,348)
- syslog (132)

Hosts (3)

- lucy (4,046)
- gandalf-splunklab (114)
- 192.168.1.1 (18)

Errors in the last hour | 0 results last refreshed: 03.20.2009 00:36:55

Saved searches last refreshed: 03.20.2009 00:36:55

- Daily indexing volume by server
- Default crawl
- Errors in the last 24 hours
- Errors in the last hour
- KB indexed per hour last 24 hours
- Messages by minute last 3 hours
- Splunk errors last 24 hours
- Summary Index Gaps and Overlaps
- all
- sampledata-1

現在您可以進行 Splunk Search

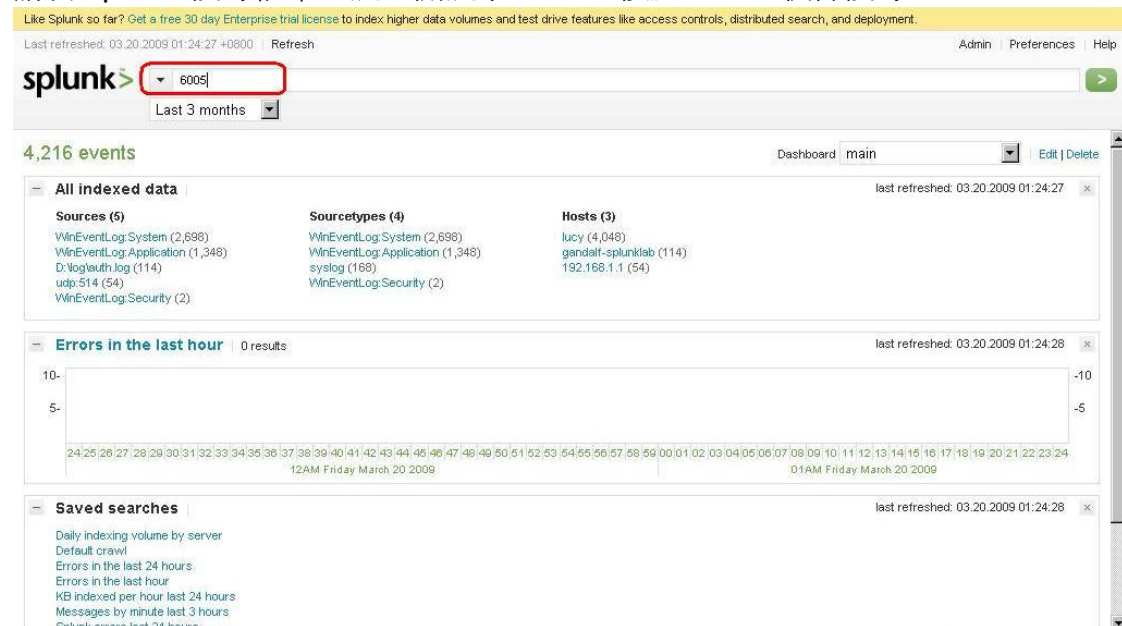
3 操作說明 - Search 搜尋

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

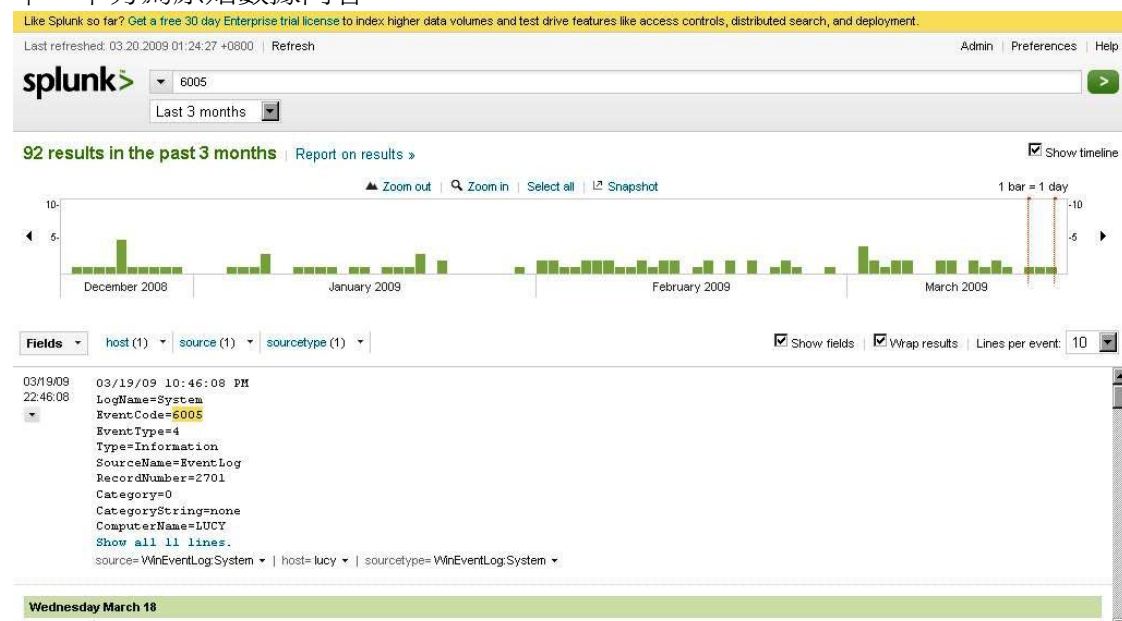
1. Windows Event Code = 6005 事件日誌服務啟動
2. Linux su 使用者權限變換檢視

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啟動(代表系統開機)的頻率。下方為原始數據內容。



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

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

Last refreshed: 03/20/2009 01:24:27 +0800 | Refresh

Admin | Preferences | Help

splunk> 6005

Last 3 months

92 results in the past 3 months | Report on results >

Show timeline

Zoom out | Zoom in | Select all | Snapshot

1 bar = 1 day

Fields | host (1) | source (1) | sourcetype (1)

Select fields to extract from these search results:

- ☐ ComputerName(1)
- ☐ EventCode(1)
- ☐ EventType(1)
- ☐ LogName(1)
- ☒ Message(1)
- ☐ RecordNumber(92)
- ☐ SourceName(1)
- ☐ Type(1)
- ☐ date_hour(17)

Cancel | Apply

lucy | sourcetype=WinEventLog:System

選取後您既可檢視欄位內容，其中資訊包含事件發生頻率

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

Last refreshed: 03/20/2009 01:24:27 +0800 | Refresh

Admin | Preferences | Help

splunk> 6005

Last 3 months

92 results in the past 3 months | Report on results >

Show timeline

Zoom out | Zoom in | Select all | Snapshot

1 bar = 1 day

Fields | Message (1) | host (1) | source (1) | sourcetype (1)

03/19/09 22:46:08

事件日誌服務已啟動。(92)

Report on this field >

Type=Information
SourceName=EventLog
RecordNumber=2701
Category=0
CategoryString=none
ComputerName=LUCY
Show all 11 lines.

source=WinEventLog:System | host=lucy | sourcetype=WinEventLog:System | Message=事件日誌服務已啟動。

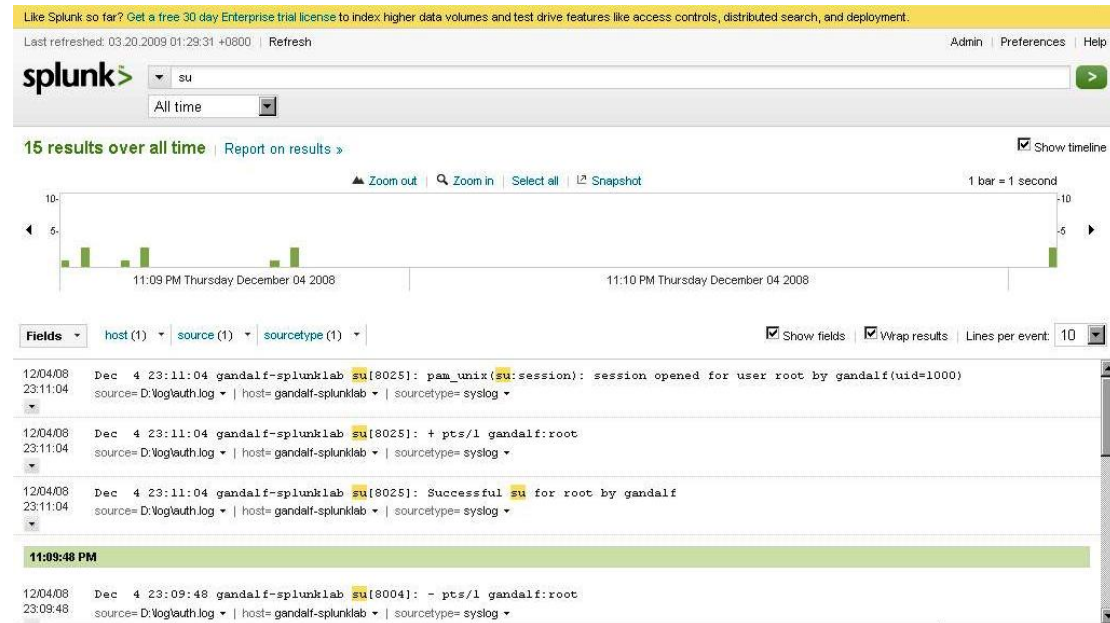
Wednesday March 18

更多 Windows Event ID 查詢，可搜尋網際網路資源。

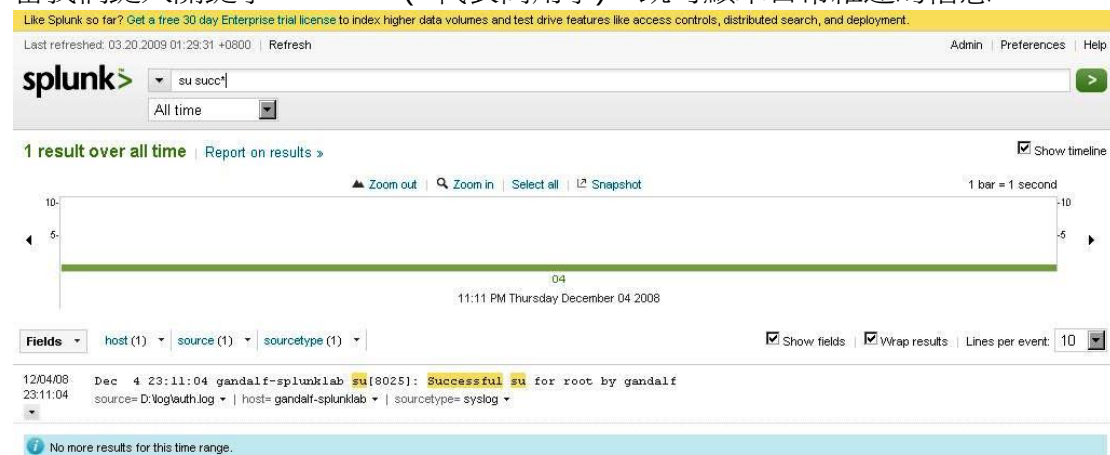
參考網址：www.eventid.net

2. Linux SU 使用者權限變換檢視

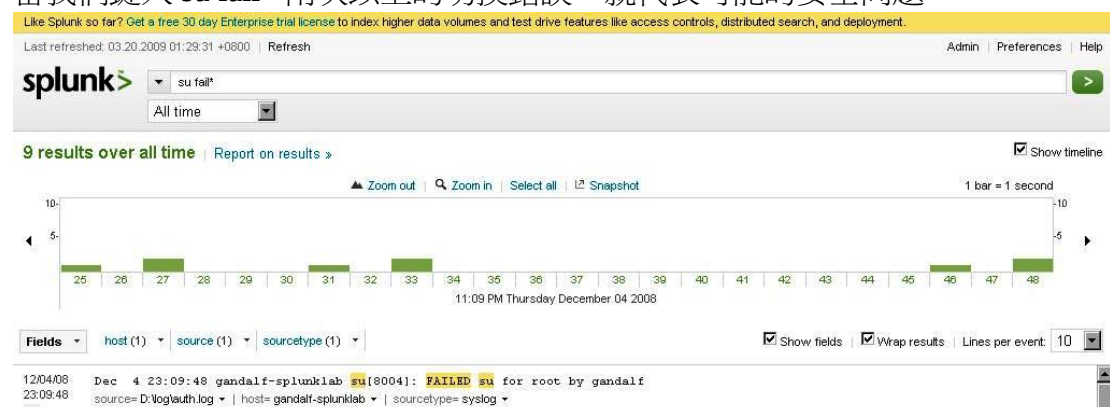
SU 指令在日常維運 Linux 系統時經常會使用到，而切換時必須要有權限得以執行，對於 SU 切換成功，我們可以視為一般性作業，但對於 SU 切換失敗，就有可能是安全問題，以下以 SU 為核心做搜尋。



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 $Status=fail*,succ*$` (\$\$ 包裹代表啟動 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。

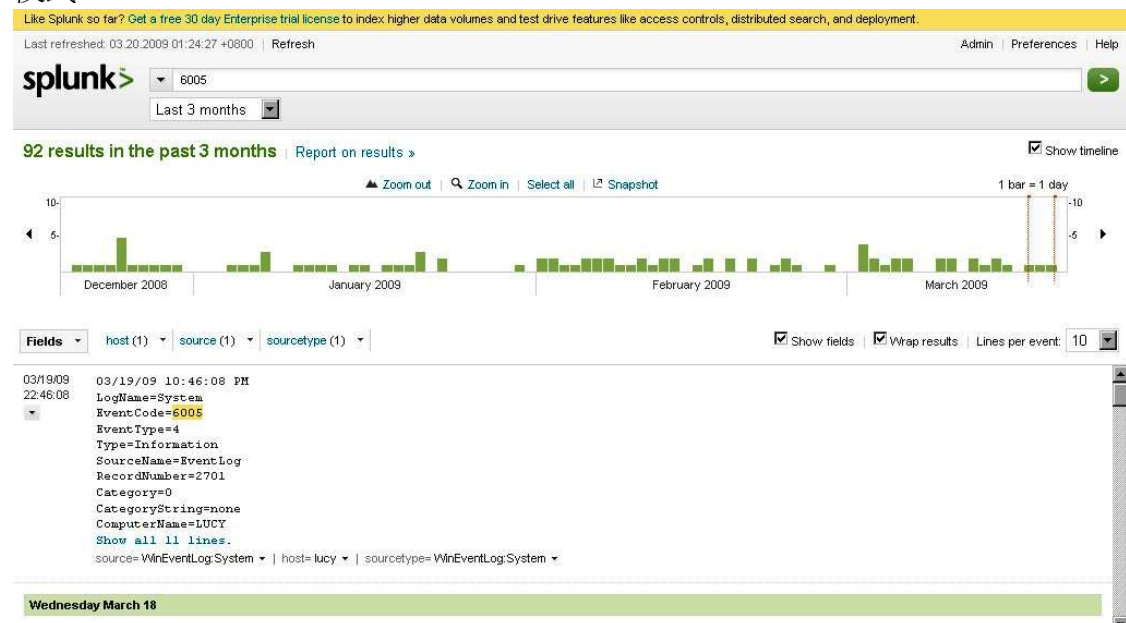


檢視日誌內容，我們可以得到完整的資訊，接下來我們提升搜尋的準確度，鍵入 `"su for root" $Status=failed,successful$` (“代表為字串”) 在 splunk 搜尋框中，空格代表指令 AND (布林代數 AND, OR 與 NOT)，所以可以精準收斂。



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)

Like Splunk so far? Get a free 30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.

Last refreshed: 03.20.2009 01:24:27 +0800 | Refresh

Admin | Preferences | Help

splunk> 6005

Last 3 months

Back to search results

Fields (distinct count / frequency)

(all results)	92	-
Category	1	100%
CategoryString	1	100%
ComputerName	1	100%
date_hour	17	100%
date_mday	30	100%
date_minute	49	100%
date_month	4	100%
date_second	46	100%
date_wday	7	100%
date_year	2	100%
date_zone	1	100%
EventCode	1	100%
EventType	1	100%
host	1	100%
linecount	1	100%
LogName	1	100%
Message	1	100%
punct	1	100%
RecordNumber	92	100%
source	1	100%
SourceName	1	100%
sourcetype	1	100%

Click on a field from the field list to begin reporting.

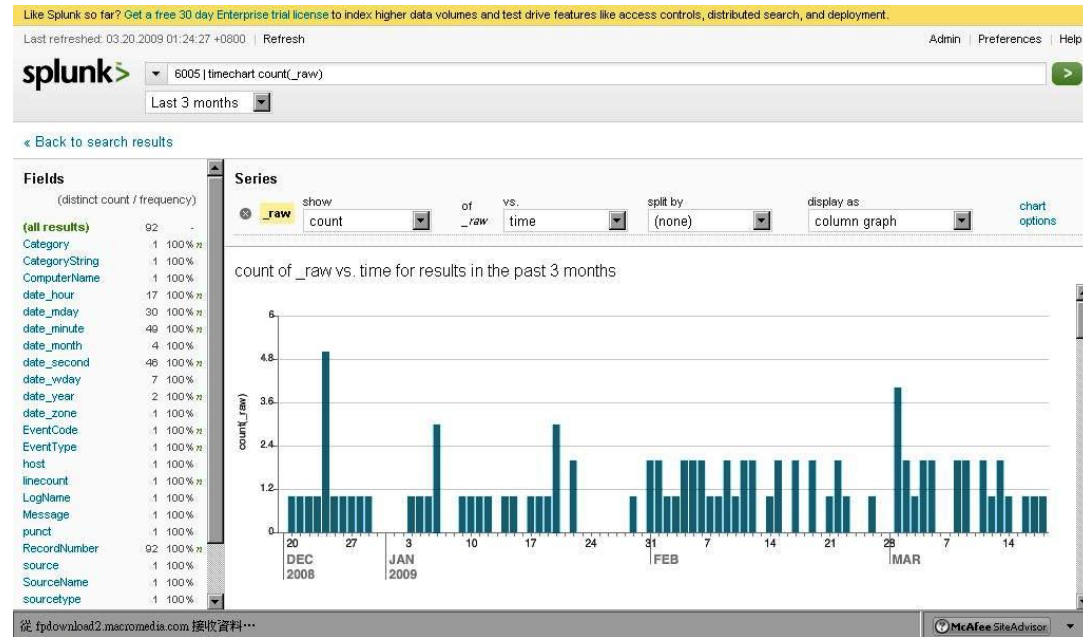
Splunk has identified specific fields in your search results. Click on a field name to start reporting on your results.

Not sure what kinds of reports you can create? Browse the [reporting gallery](#).

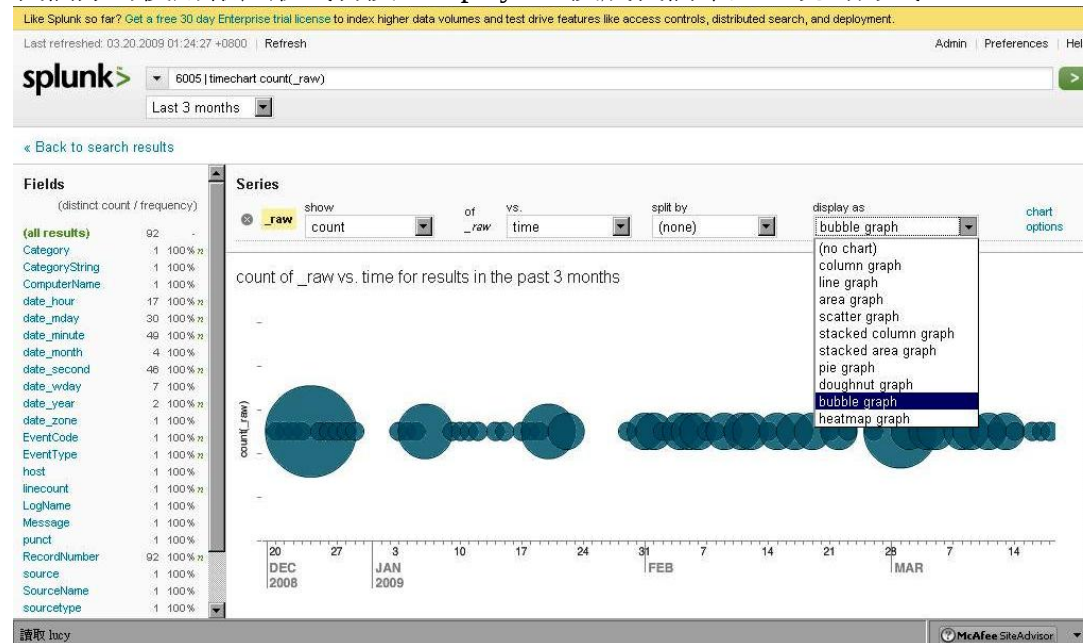
完成

McAfee SiteAdvisor

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

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

此份用戶手冊為基於 **Splunk** 建議而說明。