### SYSTEX splunk>lab

## 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1	1
註記		4

用戶請於 <u>www.splunk.com</u> 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



### 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

THIS DOCUMENT IS INTENDED FOR USE BY THE RELATED BUSINESS PARTIES ONLY. THE INFORMATION CONTAINED HEREIN IS PRIVILEGED AND CONFIDENTIAL. THE RECIPIENT OF THIS DOCUMENT IS REQUIRED TO PROTECT THE CONFIDENTIALITY WITH BEST EFFORT AND HE OR SHE SHOULD NOT USE THE PRIVILEGED INFORMATION TO DISPLACE THE COMPANY'S PROPRIETARY RIGHTS AND COMPETITIVE ADVANTAGES COPYRIGHT © SYSTEX TAIWAN PTE LTD

# 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。首先先啓動 Splunk Web UI 畫面如下:

Spinik 5.4.0 - Mozus	a Firefox			BX
富案 (E) 編輯 (E)	檢視(17) 歴史③ 書籤(18) 工具(11) 説明(14)			
< > - C	🗙 🏠 📑 http://gandalf-x31:8000/	→ • Dive Search	P	8
_ike Splunk so far? Get	t a free 30 day Enterprise trial license to index higher data volume:	s and test drive features like access controls, distributed search, and deployment.		
ast refreshed: 03.19.3	2009 23:10:04 +0800   Refresh	Admin	Preferences	Help
splunk>	•			>
•	Last 3 months			
Gettina St	arted	Dashboard getting started	Edit   Del	lete
Once you're read	y you can switch to the main name			
Index some Before you can us You can index loc	data se Splunk, you need to index some data. al or remote files and directories.	See how you can index data from network ports, databases, configurations, registry keys, APIs and more.		
Index Files		Index More Data		-
Splunk support is	here to help.			
<ul> <li>Watch the Splun</li> </ul>	ik feature videos.			
<ul> <li>Check out the su</li> </ul>	upport forums.			
<ul> <li>Email support@s</li> </ul>	splunk.com			
<ul> <li>Visit our custom</li> </ul>	er support website			
				3
Comministic @ 2000 Cath 記成	unit la company i Change i Debrasse Dellare i Ost Ales Colorelo Ta	Contraction (100) - 100	Afee SiteAdvisor	· •

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

Like Splunk so far? Get a	ree 30 day Enterprise trial license to index higher dat	a volumes and test drive feat	ures like access cor	ntrols, distribute	ed search, and deployment	
« Back to search						Help
splunk> Ad	min					
<ul> <li>Server</li> <li>Data Inputs</li> <li>All</li> </ul>	Data Inputs: All					
Files & Directories		\$	Inputs	\$	Actions	\$
FIFO Queues	Files & Directories		1		Add input	
Network Ports	FIFO Queue		0		Add input	
Crawls	Network Ports		0		Add input	
<ul> <li>Indexes</li> <li>Applications</li> <li>Distributed</li> <li>Users</li> <li>Saved Searches</li> <li>License &amp; Usage</li> </ul>	Download inputs from SplunkBase SplunkBase has pre-configured inputs for	common sources as well as	: scripted inputs that	make calls to <i>i</i>	APIs to pull data into Spluni	K.

### 點擊綠色 <New Input> 按鈕

Like Splunk so far? Get a free 3	0 day Enterprise trial license to index higher data volumes and tes	st drive featur	es li	ke access controls, di	stri	ibuted search, and	dep	oloyme	nt.	
« Back to search										Help
splunk> Admin										
Server     Data Inputs     All     Files & Directories     FIFO Queues     Network Ports	Data Inputs: Files & Directories Configure new data inputs by clicking "New Input" Change exit	sting inputs I	oy cli	icking on the path.						
Crawis	File or Directory 🗧	Creation	\$	Host	¢	Source Type	\$	Files	\$	Actions \$
▶ Indexes	D: Program Files \Splunk \var\spool\splunk	Monitor		Constant Value		Automatic		N/A		Remove
Applications		- 20.		<i>n</i> .		λ	_			
Distributed	Download inputs from SplunkBase		- 4							
Users	SplunkBase has pre-configured inputs for common sources	as well as s	cript	ted inputs that make c	alls	s to APIs to pull da	.a in	to Splu	nk.	
Saved Searches	<del></del>				_		_		_	
▶ License & Usage										

### 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 3	30 day Enterprise trial license to index higher data volumes and test drive features like access controls, distributed search, and deployment.	
« Back to search	н	elp
splunk> Admin	1	
Server     Data Inputs     All     Files & Directories     FiFO Queues     Network Ports	Data Inputs: Files & Directories: New Input Source Data access	
Crawls Crawls Indexes Applications Distributed Users Saved Searches License & license	Monitor a directory or file C Opioad a local file C 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 Cancel 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 feature	es lik	ke access controls, (	dist	ributed search, ar	d de	ployme	nt.		
« Back to search										He	qle
<b>splunk</b> > Admi	n										
Server     Data Inputs     All     FIEs & Directories     FIFO Queues     Network Ports	Data Inputs: Files & Directories Configure new data inputs by clicking "New Input" Change New Input	existing inputs by	y clic	cking on the path.							
Crawls	File or Directory	+ Creation	\$	Host	¢	Source Type	\$	Files	\$	Actions	\$
▶ Indexes	D:Vog	Monitor		Constant Value	_	Automatic		1		Remove	
Applications	D:\Program Files\Splunk\var\spool\splunk	Monitor		Constant Value		Automatic		N/A		Remove	
<ul> <li>Distributed</li> <li>Users</li> <li>Saved Searches</li> <li>License &amp; Usage</li> </ul>	Download inputs from SplunkBase SplunkBase has pre-configured inputs for common source	es as well as sc	cripte	ed inputs that make	call	s to APIs to pull d	ata ir	nto Splu	Jnk.		

# 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

Last refreshed: 03.20.	2009 00:32:27 +0800   Refresh	Admin Preferences Help
splunk>	•	>
	Last 3 months	
Getting St	arted If you can switch to the main page	Deshboard getting started Filt   Deleter admin getting started
		main create new dashboard

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.

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

Index More Data

Last refreshed: 03.2	0.2009 00:32:27 +0800	Refresh		Admin   Preferences   Help
splunk>	• [*]			2
	Last 3 months	•		
4,160 events	5		Das	hboard main Edit   Delete
- All indexe	d data			last refreshed: 03.20.2009 00:32:51 ×
Sources (3)		Sourcetypes (3)	Hosts (2)	
WinEventLog: WinEventLog:/ D:Vog\auth.log	System (2,698) Application (1,348) (114)	WinEventLog:System (2,698) WinEventLog:Application (1,348) syslog (114)	lucy (4,046) gandalf-splunklab (114)	
Errors in t	the last hour   0 res	ults		last refreshed: 03.20.2009 00:32:52 ×
10-				-10
5-				-5
32 33 34 35	36 37 38 39 40 41 42 43 11PM Th	44 45 48 47 48 49 50 51 52 53 54 55 56 57 58 5 ursday March 19 2009	i9 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 12AM Friday M	17 18 19 20 21 22 23 24 26 26 27 28 29 30 31 32 Jarch 20 2009
- Saved sea	volume by server			last refreshed: 03.20.2009 00:32:53 ×
Errors in the la	ist 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

Like Splunk so far? Get a f	ree 30 day Enterprise trial license to index higher d	ata volumes and test drive fea	tures like access co	ntrols, distribut	ted search, and deployme	ent.
« Back to search						Help
splunk > Adr	min					
<ul> <li>▶ Server</li> <li>▼ Data Inputs All</li> </ul>	Data Inputs: All				1	
Files & Directories		\$	Inputs	\$	Actions	\$
FIFO Queues	Files & Directories		1		Add input	
Network Ports	FIFO Queue		0		Add input	
Crawls	Network Ports		0		Add input	
<ul> <li>Indexes</li> <li>Applications</li> <li>Distributed</li> <li>Users</li> <li>Saved Searches</li> <li>License &amp; Usage</li> </ul>	Download inputs from SplunkBase SplunkBase has pre-configured inputs fr	or common sources as well a	s scripted inputs tha	t make calls to	APIs to pull data into Splu	ink.

#### 請點擊綠色 <New Input> 按鈕進入

Like Splunk so far? Get a free 3	0 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	Data Inputs: Network Ports Configure new data inputs by clicking "New Input." Change existing inputs by clicking on the path.	
FIFO Queues Network Ports Crawls Indexes	None	
<ul> <li>Applications</li> <li>Distributed</li> <li>Users</li> </ul>	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.	
<ul> <li>Saved Searches</li> <li>License &amp; Usage</li> </ul>		

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

Server     Data Inputs	Data Inputs: Network Ports: New Input
Files & Directories	Source
Network Ports	Protocol
Crawls	O UDP O TCP
Indexes	Port
Applications	514
Distributed	
Users	Accept connections from all hosts?
Saved Searches	Yes C No, restrict to one host
License & Usage	
	Source Type
	Set source type
	From list
	Source type
	syslog

S	nlun	kΙ	Iser	Man	ual
9	prun	n c	JSCI	man	uuu

### 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	s like access cor	ntrols, distribu	uted search, and deployment.	
« Back to search								Help
splunk > Admir	า							
<ul> <li>Server</li> <li>Data Inputs</li> </ul>	Data Inputs: Net	work Ports						
All Files & Directories FIFO Queues <b>Network Ports</b> Crawls	Added udp://514 Configure new data inputs t New Input	y clicking "New Inf	out." Change exis	ting inputs by	clicking on the p	ath.		
▶ Indexes	Protocol	\$	Host	÷	Port	÷	Actions	÷
Applications     Distributed	UDP		All		514		Remove	
<ul> <li>Users</li> <li>Saved Searches</li> <li>License &amp; Usage</li> </ul>	Download inputs from Sp SplunkBase has pre-conf	<b>lunkBase</b> gured inputs for co	ommon sources	as well as scr	ipted inputs that	make calls t	o APIs to pull data into Splunk.	1

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。

3 00:36:54 +0800         Refresh           ast 3 months         Image: Comparison of the second	Deshboard main last refra Hosts (3) lucy (4,046) gendalf-splunklab (114) 192.168.1.1 (18)	Admin Preferences Help
ta Sourcetypes (3) (2,698) WinEventLog System (2,698) WinEventLog Application (1,348) syslog (132)	Deshboard main last refra Hosts (3) lucy (4,046) gendalf-splunklab (114) 192.168.1.1 (18)	Edit   Delete
ast 3 months Sourcetypes (3) (2,698) winEventLog System (2,698) WinEventLog Application (1,348) syslog (132)	Deshboard main last refre Hosts (3) lucy (4,046) gendalf-splunklab (114) 192.168.1.1 (18)	E   Edit   Delete
ta Sourcetypes (3) n (2,698) WinEventLog:System (2,698) tion (1,348) WinEventLog:Application (1,348) syslog (132)	Dashboard main last refre Hosts (3) lucy (4,046) gendalf-splunklab (114) 192.168.1.1 (18)	Edit   Delete
Sourcetypes (3)           n (2,698)         WinEventLog:System (2,698)           stion (1,348)         WinEventLog:Application (1,348)           syslog (132)         Syslog (132)	last refro Hosts (3) lucy (4,046) gendalf-spluniklab (114) 192.168.1.1 (18)	eshed: 03.20.2009 00:36:54 ×
Sourcetypes (3)           n (2,698)         WinEventLog:System (2,698)           stion (1,348)         WinEventLog:Application (1,348)           syslog (132)         System (2,698)	Hosts (3) lucy (4,046) gendalf-splunklab (114) 192.166.1.1 (18)	
n (2,598) WinEventLog:System (2,598) tition (1,348) WinEventLog:Application (1,348) syslog (132)	lucy (4,046) gandalf-splunklab (114) 192.168.1.1 (18)	
ast hour 0 results	last refre	eshed: 03.20.2009 00:36:55 ×
		-5
42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 00 01 0 11PM Thusday March 19 2009	02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 28 27 12AM Friday March 20 2009	28 29 30 31 32 33 34 35 36
25 by server hours r at 24 hours last 3 hours hours s and Overlaps	last refre	eshed: 03:20.2009 00:36:55 🗙
42 43 4 11P e by ser- hours ir last 24 l last 3 h hours s and Or	al asiao ay asiao iso iso iso iso iso iso iso iso iso is	44 45 49 47 48 49 50 51 52 53 54 55 56 57 58 59 00 0 1 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 M Thusday March 19 2009 12AM Friday March 20 2009 last refr ver hours vertags

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

ast refreshed: 03.20.2009 01:24:27 +0800	)   Refresh			Admin   Prefere	ences   I
plunk > - 6005					(
216 events			Dashboard main		dit I Delete
All indexed data			last refreshe	d: 03.20.2009 01:24	k:27 ×
Sources (5)	Sourcetypes (4)	Hosts (3)			
WinEventLog:System (2,698) WinEventLog:Application (1,348) D:Vogleuth.log (114) udp:514 (54) WinEventLog:Security (2)	WinEventLog:System (2,698) WinEventLog:Application (1,348) systog (168) WinEventLog:Security (2)	lucy (4,048) gandalf-splunklab (114) 192,168,1.1 (54)			
Errors in the last hour 0	results		last refreshe	d: 03.20.2009 01:24	1:28 ×
10-					-10
5-					-5
24 25 26 27 28 29 30 31 32 33 34	36 38 37 38 39 40 41 42 43 44 45 46 47 49 49 50 5 12AM Friday March 20 2009	1 52 53 54 55 56 57 58 59 00 0 1 02 03 0	04 06 06 07 08 09 10 11 12 13 14 15 18 01AM Friday March 20 2009	17 18 19 20 21 22 2	3 24
Saved searches Daily indexing volume by server Default crawl			last refreshe	d: 03.20.2009 01:24	1:28 ×
Errors in the last 24 hours Errors in the last hour KB indexed per hour last 24 hours Messages by minute last 3 hours					

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

Last refreshed: 03.20	2009 01:24:27 +0800   Ref	resh				Adı	nin   Preferences	Help
an lun ki	Beer escore							
spiurik>	▼ 6005							2
	Last 3 months 🔳							
92 results in th	e past 3 months	Report on results »					C Show	timelin
		🔺 Zoom out	Q Zoom in Select all	∣ L <sup>2</sup> Snapshot			1 bar = 1 day	
10-							-11	0
4 5-							-5	•
								100
							5 5	
							an Man	
December	2008	January 2009		February 201	<b>N N #8* *</b>	March 200	<b></b>	
December	2008	January 2009	1 - 18a	February 201	<b>B B mBm m</b> 09	March 200	99	
December	2008	January 2009	1 <u>- 1</u> 11	February 201	<b>8 8 28 4</b>	March 200	<b>19</b>	- 1000
December	2008	January 2009 Derype (1) 👻	<b>1 - 1</b> 8	February 201	09 III and a solution	March 200	Lines per event: 1	0 💌
December Fields + host (1 Select fields to extra	2008 ) * source (1) * sour	January 2009 Perype (1) 🔻	I - II.	February 20	09 Show fi	March 200 elds 🗹 Wrap results	Lines per event: 1	0
Fields     host (1 Select fields to extra ComputerName(1)	2008 )	January 2009		February 201	09 Show fi	March 200	uilla purp 19 Lines per event: 1	0 💌
Fields	2008 ) × source (1) × sour t from these search results	January 2009		February 201	09	March 200	Lines per event: 1	0 💌
Fields v host (1 Select fields to extra ComputerName(1) EventCode(1)	2008 )	January 2009		February 20	09	March 200	Lines per event: 1	0 💌
Fields v host (1 Select fields to extrain ComputerName(1) EventCode(1) EventType(1)	2008 )      v source (1)      source (1)      source (1)	January 2009	M.	February 20	09	March 200	Lines per event.	0 💌
Fields         host (1)           Select fields to extra         ComputerName(1)           EventCode(1)         EventType(1)           LogName(1)         Wessade(1)	2008 ) + source (1) + sour t from these search results	January 2009	1 - 11-	February 20	03 III Show fi	March 200	Lines per event: 1	0 💌
Fields    host (1 Select fields to extra ComputerName(1) EventType(1) LogName(1) Message(1) RecordNumber(92)	2008 )	January 2009	t - pile	February 20	03 I Show fi	March 200	Jines per event 1	0 💌
Fields	2008 )   source (1)   source t from these search results	January 2009	• • •	February 20	Show fi	elds 🗹 Wrap results I	Lines per event: 1	0 💌
Fields  Fields  Fields  Fields to extra ComputerName(1) EventCode(1) EventCode(1) ComputerName(1) ComputerName	2008 )      source (1)      source (1)      source (1)      source (1)	January 2009	8 - pH	February 20	09 I Show ti	March 200	Lines per event 1	0 💌
Fields	2008 )   source (1)   source t from these search results	January 2009	WnEventLog:System •	February 20	03	March 200	Lines per event: 1	0 💌

#### 選取後您既可檢視欄位內容,其中資訊包含事件發生頻率

Last refres	hed: 03.20.2009 01:24:27 +0800   Refresh	Admin   Preterences   He
splu	nk> 🔹 6005	
	Last 3 months	
92 resu	Its in the past 3 months   Report on results »	R Show timelin
	▲ Zoom out   Q Zoom in   Select all   L <sup>2</sup> Snap	shot 1 bar = 1 day
10- • 5-	December 2008 January 2009	-10 -5 + February 2009 March 2009
Fields •	Message (1)  host (1)  hos	Show fields   Wrap results   Lines per event 10
22:46:08	事件日誌服務已啓動。 (92)	
	Type=Information SourceHame=EventLog' RecordNumber=2701 Category=0 CategoryString=none ComputerName=LUCY Show all 11 lines: source=WinEventLog:System *   host=lucy *   sourcetype=WinEventLog:System *   Message=	▶件日誌服務已幣動。 →
Wednesd	Jay March 18	

更多 Windows Event ID 查詢,可搜尋網際網路資源。

參考網址:<u>www.eventid.net</u>

#### 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。

Like Splunk so	o 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 refreshe	ed: 03:20.2009 01:29:31 +0800   Refresh	Admin   Preferences   Help
splun	ik> → su	
	All time	
15 result	s over all time   Report on results »	Show timeline
	Zoom out   Q. Zoom in   Select all   12 Snapsh	not 1 bar = 1 second
10-		-10
4 5-		-6 🕨
	11:09 PM Thursday December 04 2008 11:1	0 PM Thursday December 04 2008
Fields *	host (1) × source (1) × sourcetype (1) ×	Show fields K Wrap results Lines per event: 10
12/04/08 23:11:04	Dec 4 23:11:04 gandalf-splunklab <mark>su</mark> [8025]: pam_unix( <mark>su</mark> :session): sessi source=D:NogNauthlog →   host=gandaf-splunklab →   sourcetype=syslog →	ion opened for user root by gandalf(uid=1000)
12/04/08 23:11:04	Dec 4 23:11:04 gandalf-splunklab <mark>su</mark> [8025]: + pts/l gandalf:root source=D:NogNauthlog +   host=gandaf-splunklab +   sourcetype=syslog +	
12/04/08 23:11:04	Dec 4 23:11:04 gandalf-splunklab <mark>su</mark> [8025]: Successful <mark>su</mark> for root by q source=D:NogWauthlog •   host=gandaf-splunklab •   sourcetype=syslog •	yandalf
11:09:48 PM	1	
12/04/08	Dec 4 23:09:48 gandalf-splunklab <mark>su</mark> [8004]: - pts/l gandalf:root	
23:09:48	source= D: logtauth log +   host= gandalf-splunklab +   sourcetype= syslog +	

### 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

Circ Optanic So Tar : Oo	e a nee so aay c	riterprise trial license to line	iex nigher dat	ta volumes anu te	St unve rea	tui es inte access controls	, distributed search, and d	epioyment.				
Last refreshed: 03.20.	2009 01:29:31 +0	0800 Refresh						i.	Admin	Preference	es	Help
splunk>	▼ su succ*											>
	All time	<b>*</b>										
1 result over a	Il time   Rep	ort on results »								🗹 Sho	vy time	eline
			Zoom out	Q Zoom in Se	elect all	Snapshot			1 bar	= 1 second	ł	
10-											-10	
4 <sup>5-</sup>											-5	F
				10000000000000	04	in annanch						
				11:11 PM Thu	ursday Deci	ember 04 2008						
Fields + host (1	) 🔻 source (1	) 🔹 sourcetype (1) 🔹					☑ Show fields	₩ Wrap results	Lines	per event:	10	
12/04/08 Dec 4 23:11:04 source=)	23:11:04 ga D:\log\auth.log •	an dal f-splunk lab <mark>su</mark>   host=gandalf-splunklak	[8025]: <mark>5</mark> • •   sourcet	uccessful su ype=syslog +	i for roc	t by gandalf						
• O No more results fr	or this time range		xe: 1005/2025									

### 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

splunk>	▼ su fail*			>		
	All time	×				
9 results over :	all time   Re	eport on results »			🗹 Show tirr	nelina
		A Zoom out	Q Zoom in Select all	្ន	bar = 1 second	
10-					- 10	
5-					-5	
			· · · · · · · · · · · · · · · · · · ·			1
25 26	27 28	29 30 31 32 33	34 35 36 37 38 39 40 4 11:09 PM Thursday December 04 2008	11 42 43 44 45 48 41	47 48	
Fields • host (1	) 🔹 source (1)	) • sourcetype (1) •		Show fields   🗹 Wrap results   L	ines per event: 10	
12/04/08 Dec 4	23:09:48 ga	ndalf-splunklab <mark>su</mark> [8004]:	FAILED su for root by gandalf			
23:09:48 source=	): Vog\auth.log 👻	host= gandalf-splunklab +   sourc	etype= syslog 👻			
						1

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)

Like Splunk so far? Ge	t a free 30 day Enterprise trial license to index higher data volumes and test drive feat	ures like access controls, distributed search, and deployment.
Last refreshed: 03.20.	2009 01:29:31 +0800   Refresh	Admin   Preferences   Help
splunk>	▼ su \$Status=fail*,succ*\$	
	All time Show as form >	
9 results over a	all time Report on results »	Show timeline
10.	🔺 Zoom out   🔍 Zoom in   Select all   🗠	Snapshot 1 bar = 1 second
5.	27 28 20 30 31 31 32 33 34 36 38 37	-5 p
	11:09 PM Thursday Dece	mber 04 2008
Fields • host (1	)  v source (1)  v sourcetype (1)  v	Show fields   🗹 Wrap results   Lines per event: 10 💌
2/04/08 Dec 4 23:09:48 source=1	23:09:48 gandalf-splunklab <mark>su</mark> [8004]: <mark>FAILED su</mark> for root by D'NogNauthlog +   host=gandalf-splunkdab +   sourcetype=sysNog +	gandalf.
12/04/08 Dec 4 23:09:48 source=1	23:09:48 gandalf-splunklab <mark>su</mark> [8004]: pam_authenticate: Auth D:Woglauth.log •   host= gandalf-splunklab •   sourcetype=syslog •	nentication <mark>failure</mark>

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。

plunk>	▼ "su for root	t" \$Status=failed,s	uccessful\$					
	All time							
	Show as form »							
esults over	all time Rer	nort on results					I Shov	ev time
esults over	all time Rep	oort on results	»				Nov Show	ev time
esults over	all time   Rep	oort on results :	» 🔺 Zoom out	Q Zoom in Se	elect all 🛛 🗠 Snapshot		☑ Shov 1 bar = 1 second	∾ time
results over :	<b>all time</b>   Rep	oort on results	»	Q Zoom in Se	elect all   년 Snapshot		☑ Shov 1 bar = 1 second	v time
10.	all time   Rep	oort on results :	» 🔺 Zoom out	🔍 Zoom in   Se	elect all   🖾 Snapshot		I bar = 1 second	v time
10. 5.	all time   Rep	oort on results :	» 🔺 Zoom out	Q Zoom in Se	elect all   년 Snapshot		I bar = 1 second	w time -10 -5
results over 1 10- 5-	all time   Rep	oort on results	» 🔺 Zoom out	Q Zoom in Se	elect all   12 Snapshot		I bar = 1 second	•v tim -10 -5

# 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

Like Splunk so far? Ge	a free 30 day Enterprise trial license to in	idex 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
splunks	▼ 6005		
spiainte	Last 3 months		
92 results in th	e past 3 months   Report on	results »	Show timeline
		🔺 Zoom out   🔍 Zoom in   Select all   🗠 Snapshot	1 bar = 1 day
10-			-10
4 5-			-5 🕨
ACCO TANDA COMO TANDA C	a and a constant and a constant a	a seal of the Albertan State of the State of Sta	I Ralla ana
December 2	1008 Janua	ry 2009 February 2009 Mar	ch 2009
Fields • host (1	source (1) V sourcetype (1)	🔽 Show fields 🛛 🔽 Wrap resu	tts Linesperevent: 10 💌
03/19/09 03/19/0 22:46:08 LocNam	)9 10:46:08 PM =Svstem		
• EventC	de= <mark>6005</mark>		
Type=I	pe=4 Mormation		
Sourcel	Jame=EventLog humber=2701		
Catego:	:y=0		
Catego: Computi	yString=none		
Show a.	1 11 lines.		
source=1	VinEventLog:System +   host=lucy +	sourcetype=WinEventLog:System +	
Karana da ana			
Wednesday March	18		
淮入報表	愺弌後,請點選	左方 (all results)	
		<u>/</u>	
Like Spidink SU far / Ge	a free 50 day chilerprise than idense to in	idex nigher data volumes and test drive reatures like access controls, distributed search, and deployment.	Admin   Dreferences   Heln
	000 01.24.27 40000   Neirean		Autini Preferences Thep
splunk>	• 6005		>
	Last 3 months 💻		
« Back to search re	sults		
Fields	*		
(distinct count /	frequency)	Click on a field from the field list to begin reporting.	
(all results)	92 .	Splunk has identified specific fields in your search results.	
Category	1 100% 72		
CategoryString	1 100%	indu sure what whats of reports you can creater provise the reporting gallery.	
date_hour	17 100%2		
date_mday	30 100% 7		
date_minute	49 100% n 4 100%		
date_second	46 100%		
date_wday	7 100%		
date_year	2 100% 2		
EventCode	1 100%		
EventType	1 100% 2		
host	1 100%		
LogName	1 100% 2		
Message	1 100%		
punct	1 100%		
RecordNumber	92 100% n		
SourceName	1 100%		
sourcetype	1 100%		
完成			CMcAfee SiteAdvisor 🔹



# 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

splunk>	🔹 6005   tir	(timechart count(_raw)											>
<b>.</b>	Last 3 mor	nths 📘	-										
Back to search	results												
ields		Ser	ies										
(distinct count	t / frequency)			show			VS		split by		display as		
1.		0	_raw	count		101	time		(none)		hubble graph	ontio	De
all results)	92 -			count		-'"	ume				Dobble graph P	• opiio	110
ategory	1 100% 2										(no chart)		
CategoryString	1 100%	COU	nt of	rawys	time for re	esults in t	he nast 3	8 months			column graph		
omputerName	1 100%	000		_1011110.		vouro mi	no puor	2 monuno			line graph		
ate_hour	17 100% n										area grapri		
ate_mday	30 100%n	- 25									scatter graph		
ate_minute	49 100% 2										stacked column graph		
ate_month	4 100%	1.12									stacked area graph		
ate_second	46 100% 2										deughput graph		
ate_wuay	7 100%		1								hubble graph		
ale_year	2 100 % 7	MB	1		6		6		000		heatman granh	00	
ate_zone	1 100%	12		1000		CON					licatinap graph		1
ventTune	1 100 % 2	no -						-		Mark Car			·
ost	1 100%												
necount	1 100%			-									
ogName	1 100%	-											
lessage	1 100%												
unct	1 100%												2
ecordNumber	92 100% 2		20	27	3	10	17	24	31 7	14	21 28 7	14	
ource	1 100%		DEC		JAN				FEB		MAR		
SourceName	1 100%		2008		12009								
	1 10001												

12

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

Last refreshed: 03.20	1.2009 01:24:27 +0	800 Refresh								Admin   Pr	references	Hel
splunk>	▼ 6005   time	chart count(_raw)	count(EventCode)									
-1	Last 3 month	ns 💌										
« Back to search	results											
Fields	<b>_</b>	Series										
(distinct count	/ frequency)		show		VS.		split by		display as		ch	ant.
and the second	725	😵 _raw	count	■ of _raw	time	-	(none)	-	hubble graph	1		tions
all results)	92 -				Luine		(noney		Papero graph		-	
ategory	1 100% 2	S EventCode	show	of		inh	erited		display as	5		
ategorystring	1 100%	U LIOMODUO	count 🔄	EventCod	9		or red a		bubble graph	1	•	
omputerName	1 100%											
:omputerName late_hour	1 100% 17 100%n					8 G.	3723 5					
omputerName ate_hour ate_mday	1 100% 17 100%n 30 100%n	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ist 3 month	s				
computerName late_hour late_mday late_minute	1 100% 17 100%n 30 100%n 49 100%n	count of _rav	v, count of Eventi	Code vs. tim	e for results	in the pa	ist 3 month	s				
omputerName ate_hour ate_mday ate_minute ate_month	1 100% 17 100%2 30 100%2 49 100%2 4 100%	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	S				
omputerName late_hour late_mday late_minute late_month late_second	1 100% 17 100%n 30 100%n 49 100%n 4 100% 46 100%n	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	S	count(	raw)		1
omputerName ate_hour ate_minute ate_month ate_second ate_wday	1 100% 17 100%n 30 100%n 49 100%n 4 100% 46 100%n 7 100%	count of _rav	v, count of Eventi	Code vs. tim	e for results	in the pa	ast 3 month	S	count[ count]	_raw) EventCode)		]
omputerName ate_thour ate_minute ate_minute ate_second ate_second ate_year	1 100% 17 100%n 30 100%n 49 100%n 4 100% 46 100%n 7 100% 2 100%n	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	S	count(	_raw) EventCode)		
omputerName ate_hour ate_minute ate_month ate_second ate_year ate_year ate_yone	1 100% 17 100%n 30 100%n 49 100%n 4 100%n 4 100%n 7 100% 2 100%n 1 100%	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	S	count(	_raw) EventCode)		
omputerName ate_hour ate_minute ate_month ate_second ate_veday ate_year ate_zone ventCode	1 100% 17 100%n 30 100%n 49 100%n 4 100% 48 100%n 7 100% 2 100%n 1 100% 1 100%n	count of _rav		Code vs. tim	e for results	in the pa	ast 3 month	s	count(	_raw) EventCode)		
omputerName iate_hour ate_mday ate_minute ate_second ate_wday ate_year ate_zone ventCode ventType	1 100% 17 100%n 30 100%n 49 100%n 4 100% 48 100%n 7 100% 2 100%n 1 100%n 1 100%n 1 100%n	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	s <b>Dava</b>	count(	_raw) EventCode)		
omputerName ate_hour ate_minute ate_minute ate_workh ate_second ate_vear ate_vear ate_vear ate_vear ate_cone ventCode ventType ost	1 100% 17 100% 30 100% 49 100% 40 100% 46 100% 7 100% 2 100% 1 100% 1 100% 1 100% 1 100% 1 100%	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	s D.000	count(	raw) EventCode)		
computerName ate_hour ate_inday ate_initute ate_month ate_second ate_vear ate_year ate_year ate_zone ventCode ventCode ost	1 100% 17 100% n 18 100% n 49 100% n 4 100% n 48 100% n 7 100% n 1 000% n 1 100% n 1 100% n 1 100% n	count of _rav		Code vs. tim	e for results	in the pa	ast 3 month	s <b>Dexe</b>	count(	_raw) EventCode)		
omputerName ate_inour ate_inday ate_inouth ate_second ate_wday ate_year ate_zone <b>ventCode</b> ventType ost ost ogName	1 100% 17 100% x 30 100% x 49 100% x 40 100% x 4 100% x 7 100% x 1 100% x 1 100% x 1 100% x 1 100% x 1 100% x	count of _rav		Code vs. tim	e for results	in the pa	ast 3 month	s D.C.C.C.	count(	_raw) EventCode)		
omputerName ate_inour ate_inday ate_ininite ate_second ate_voran ate_zone ventCode ventType ost ost ecount ogName fessage	1         100%           30         100% π           30         100% π           40         100% π           40         100% π           1         100% π	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	s D.000	count(	raw) EventCode)		
omputerName ate_nour ate_mday ate_month ate_second ate_vear ate_vear ate_vear ate_vear ate_vear ate_vear ate_vear ate_cone wentType osecount code essage unct	1         100%           30         100% π           40         100% π           44         100% π           7         100% π           1         100% π	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	s DOX		_raw) EventCode)		
omputerName ate_nour ate_nour ate_nourth ate_second ate_way ate_year ate_year ate_year ate_zone wentCode ventType ost account oogName lessage unct accorthumber	1         100%           7         100% π           30         100% π           40         100% π           40         100% π           2         100% π           1         100% π	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	est 3 month	s D.000 D.000	count(	_raw) EventCode)		
omputerName ate_inour ate_inday ate_ininite ate_second ate_vear ate_zone ventType ost ventType ost lessage unct lessage unct	1         100%           7         100% π           30         100% π           40         100% π           4         100%           4         100%           4         100% π           1         100% π	count of _rav	v, count of Event	Code vs. tim	e for results	in the pa	ast 3 month	s DCC DCCC		_raw) EventCode)		
omputerName date_hour iate_minute date_month date_second date_worday date_word date_word date_word wentType date_tone wentType date_tone wentType date_tone wentCode	1 100% 17 100% 18 17 100% 18 17 100% 18 17 100% 18 17 100% 18 17 100% 17 100\% 17 10\% 17 100\% 17\% 170\% 170	count of _rav	v, count of Event	Code vs. tim		in the pa	ast 3 month	S DOCC DOCC 11	count( count)	_raw) EventCode)		

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 <u>http://www.splunk.com/view/SP-CAAAAGV</u> 參考,其他用戶使用說明,請參考 <u>http://www.splunk.com/base</u>,或聯繫當地 Splunk 服務供應商取得支援服務。

Happy Splunk

Spluit USEL Manual
--------------------

註記

此份用戶手冊為基於 Splunk 建議而說明。