

Splunk 教育訓練 2

7/26 案例主題:作業系統安全事件日誌

更了解Splunk

Splunk 重要專有名詞說明



- Data Input: 資料輸入(例如:檔案、TCP、UDP、WMI、Script、Forwarder、Stream、API...)
- Source type : 來源類別 (例如: apache logs, security log、network log, sensor log...)
- Host: 資料主機 (例如: apache1、apche2, apserver1, firewall1, 10.1.1.2, ...)
- Source: 來源(例如:/opt/apache/log/*.*, udp:514, /bin/current_status.sh)
- Field: 欄位(字段):以正規表示式(Regular Expression) 摄取出欄位(字段)
- Search Language:搜尋語法 (概念: 縮小範圍 -> 運算 -> 結果呈現)
- Saved Search: 儲存搜尋,將搜尋條件存下來,下次可以直接用
- Alert: 告警,當搜尋到特定關鍵字、統計分析達到設定值,可發出警告(即時、排程)
- Report : 報表,將儲存搜尋結果,產出的圖形化報表
- Dashboard : 儀表版 · 將不同報表彙整多個面板 成 儀表版
- Data Model: 資料模型,將機器資料虛擬化的資料結構
- Pivot Analysis: 樞紐分析,提供給一般使用者可以拖拉產生報表和儀表板





- **關鍵字Keywords** 搜尋error, password
- 布林函數Booleans

OR, AND, NOT; AND是默認值不顯示; 必須為大寫, 可將需優先執行條件放入()中 sourcetype=vendor_sales OR (sourcetype=access_combined action=purchase)

• 詞組Phrases

"web error"不同於web AND error

• 欄位搜尋Field serarches

status=404, user=admin

• 萬用字元Wildcards *

status=40* matches 40, 40a, 404 等等。關鍵字前面使用 * 是無效的如*dmin

• 比較Comparisons

=, !=, <, <=, >=, > status>399, user!=admin



搜尋以五個元件組成

- Search terms 你想看什麼?
 - 關鍵字,詞句,布林函數等等
- Command 你想對搜尋結果做些什麼?
 -建立圖表,計算統計,評估與格式化等等
- Function 你想要對搜尋結果做如何圖表,計算與評估
 -加總,取平均值,轉換值等等
- Arguments 有什麼變數要應用到這個功能?

-計算特定欄位的平均值,轉換milliseconds to seconds等等

• Clauses — 你想要如何組合或重新命名搜尋結果中的欄位



使用直立線字元 | 來進行資料的後續處理

搜尋	樞細分析	報告	警示	儀表板				Sea	rch & Rep	orting
へ新	授尋								另存為 ~	關閉
<pre>sourcetype=access_* status=200 action=purchase top categoryId</pre>									昨天 🗸	Q
✓ 623 (1)	✓ 623 個事件 (14/06/23 0:00:00.000 至 14/06/24 0:00:00.000) 工作 ✓ Ⅱ ■ → ± 巻							₹ 智慧模式 ~		
事件	統計資料	ł (7)	視覺化							

毎頁 20 個 ~ 格式 ~ 預覧 ~

categoryId 0	count ≎	percent \diamond
STRATEGY	92	29.299363
ARCADE	67	21.337580
ACCESSORIES	43	13.694268
TEE	41	13.057325
SIMULATION	31	9.872611
SHOOTER	28	8.917197
SPORTS	12	3.821656

搜尋 語言 的 範例



This diagram represents a search, broken into its syntax components







- 搜尋 Buttercup Games 商店的成功購買數
 - sourcetype=access_* status=200 action=purchase
- 搜尋發生錯誤的產生記錄
 - (error OR fail* OR severe) OR (status=404 OR status=500 OR status=503)

- 搜尋昨天購買了多少模擬遊戲
 - sourcetype=access_* status=200 action=purchase categoryId=simulation



Searching and Reporting





- 透過下列練習,熟悉source type 使用下列指令,產生搜尋內容 -table
 - -rename
 - -field
 - -dedup
 - -sort



Searching & Reporting with Splunk

建立表單 Table



想知道網路的 src, dest, app 與 rule的相互關係,如何視覺化

Table命令用來回傳使用參 數列表(src,dest,app,rule))的欄位欄位表格。 sourcetype="pan:threat"

2 | table src,src_port,dest,dest_port,app,rule

src ≑	1	src_port 🗘 🖌	dest ‡	1	dest_port 🗘 🖌	app ‡	1
192.168.0.2		50297	184.106.31.170		80	web-browsing	
72.21.194.1		80	192.168.0.2		59160	web-browsing	
64.39.66.153		80	192.168.0.3		59310	web-browsing	
192.168.0.2		62525	204.232.231.46		80	web-browsing	
192.168.0.2		64276	184.106.31.170		80	web-browsing	
192.168.0.3		8839	74.125.224.195		80	web-browsing	
200.147.33.17		80	192.168.0.2		57451	web-browsing	
222.222.204.67		80	192.168.0.2		50928	web-browsing	
192.168.0.2		59709	213.180.199.61		80	web-browsing	
192.168.0.2		58928	184.106.31.170		80	web-browsing	
192.168.0.2		61425	64.74.223.43		80	web-browsing	
192.168.0.2		57566	184.106.31.170		80	web-browsing	

修改表單欄位名稱 Rename



客戶想知道網路的 src, dest, app 與 rule的相互關係, 如何視覺化

Rename命令用來將table 回傳使用欄位更具意義。

rename	src as 來源位置,
	dest <mark>as</mark> 目的位置
	app as 應用程式,
	rule <mark>as</mark> 規則

1	sourcetype="pan:threat"
2	<pre>table src,src_port,dest,dest_port,app,rule</pre>
3	rename src as 來源位置,
4	dest <mark>as</mark> 目的位置
5	app as 應用程式,
6	rule as 規則

來源位置 ≑	/	目的位置 ≑	1	應用程式 ≑	1	規則 ≑
192.168.0.2		184.106.31.170		web-browsing		rule1
192.168.0.2		64.78.56.109		ssl		rule1
192.168.0.2		204.232.231.46		web-browsing		rule1
192.168.0.2		204.232.231.46		web-browsing		rule1
192.168.0.2		212.193.230.207		web-browsing		rule1
200.147.1.41		192.168.0.2		web-browsing		rule1
192.168.0.2		218.94.11.45		web-browsing		rule1
192.168.0.2		184.106.31.170		web-browsing		rule1

極速搜尋 使用 Fields



欄位萃取是搜尋中最花資源的部分。 使用Field命令可以"包含"或"排 除"特定的欄位,加速搜尋的效果。 使用"包含"會優於"排除"

splunk[®]>

Searching & Reporting with Splunk





客戶想知道網路的 src, dest, app 與 rule的相互關係, 如何視覺化

1	sourcetype="pan:threat"
2	fields src,dest,app,rule
3	table src,dest,app,rule
4	<mark>rename</mark> src as 來源位置,
5	dest as 目的位置
6	app as 應用程式,
7	rule as 規則

rename productId as ProductID
 rename action as "Customer Action"
 rename status as "HTTP Status"

來源位置 ≑	/	目的位置 ≑	/	應用程式 ≑	/	規則 ≑
192.168.0.2		184.106.31.170		web-browsing		rule1
192.168.0.2		64.78.56.109		ssl		rule1
192.168.0.2		204.232.231.46		web-browsing		rule1
192.168.0.2		204.232.231.46		web-browsing		rule1
192.168.0.2		212.193.230.207		web-browsing		rule1
200.147.1.41		192.168.0.2		web-browsing		rule1
192.168.0.2		218.94.11.45		web-browsing		rule1
192.168.0.2		184.106.31.170		web-browsing		rule1

極速搜尋 使用 Fields



客戶想知道上週發生網路問題的狀況,針對user, app,與src_ip上的欄位進行萃取

提升效率----只有萃取特定需要的欄位

Selected Fields	i	<i>i</i> Time Event									
a host 5 a source 5	>	8/3/15 1:59:59.000 PM	Aug 03 13:59: ; logname= ui	sourcetype=linux secure							
a sourcetype 1			host = ip-10-222-	134-157 source = /opt/splunk/	var/s	oool/splunk/auth.ni	x sourcetype = linux_secure	(fail* OR invalid)			
Interesting Fields a action 2	>	8/3/15 1:59:59.000 PM	Aug 03 13:59: host = ip-10-222-	59 acmepayroll sshd[15511 134-157 source = /opt/splunk/]: I var/s	nvalid user ad bool/splunk/auth.ni	fields user, app, src_ip				
a app 3	>	8/3/15 1:59:58.000 PM	Aug 03 13:59: m 10.11.36.38	58 acmepayroll sshd[17757 3 port 40168 ssh2]: F	ailed password	for <mark>invalid</mark> user nagios fro				
a vendor_action 3			host = ip-10-222-	134-157 eouroe = /ont/enlunk/	var/ei						
3 more fields ✿ Extract New Fields	>	8/3/15 1:59:58.000 PM	<pre>shd[14225]: pam_unix(sshd:auth): authentication failure sh ruser= rhost=110.172.158.2 (ast(apuk/ust/auth_buk/usth_buk/auth_buk/apuk/ust/auth_buk/auth buk/auth_b</pre>								
Returned 6,567 results by scanning 6,567 events in 1.425 seconds.			• Extract New Fields	>	8/3/15 1:59:59.000 PM	Aug 03 13:59:59 acmepayroll s host = ip-10-222-134-157 source = /	shd[15511]: Invalid user administrator from 10.11.36.11 /opt/splunk/var/spool/splunk/auth.nix sourcetype = linux_secure				
			-		>	8/3/15 1:59:58.000 PM	Aug 03 13:59:58 acmepayroll s m 10.11.36.38 port 40168 ssh2	shd[17757]: Failed password for invalid user nagios fro			
							host = ip-10-222-134-157 source = /opt/splunk/var/spool/splunk/auth.nix sourcetype = linux_secure				
				>	8/3/15 1:59:58.000 PM	Aug 03 13:59:58 acmepayroll sshd[14908]: Failed password for invalid user operator f rom 10.11.36.29 port 35158 ssh2					
							host = ip-10-222-134-157 source = /opt/splunk/var/spool/splunk/auth.nix sourcetype = linux_secure				

Returned 6,567 results by scanning 6,567 events in 0.753 seconds.

重複資料刪除Dedup



從搜尋的結果移除重複資料

		category ≑	/	app ≑	/	rule ≑	/	action \$
2	sourcetype="pan:threat"	health-and-medicine		web-browsing		rule1		allowed
2	Table category, app, rule, action	business-and-economy		web-browsing		rule1		allowed
		social-networking		web-browsing		rule1		allowed
		malware-sites		web-browsing		rule1		blocked
		any		web-browsing		rule1		blocked
		any		web-browsing		rule1		blocked
		not-resolved		web-browsing		rule1		allowed

| dedup category

category \$	/	app ‡	/
malware-sites		web-browsing	
business-and-economy		web-browsing	
not-resolved		web-browsing	
any		web-browsing	

| dedup category , app

category 🗢	/	app 🗢	/
web-hosting		web-browsing	
web-advertisements		web-browsing	
not-resolved		web-browsing	
malware-sites		web-browsing	





使用升序 + ascending由小到大(預設) 或降序 - descending由大到小 限制回傳結果的數量,使用limit參數

... | sort limit=20 -categoryId, product_name
... | sort 20 count

使用Sort排序結果

由小到大(預設)或由大到小

- 1 sourcetype="pan:threat"
- 2 | table category, app, rule, action
- 3 | dedup category,app
- 4 | sort limit=20 -category,+app,rule,action

category 🗢 🖌	арр 🗘 🖌 🖌	rule 🗢 🛛 🖉	action ‡
web-hosting	ssl	rule1	allowed
web-hosting	web-browsing	rule1	allowed
web-based-email	hotmail	rule1	allowed
web-based-email	mail.ru-base	rule1	allowed
web-based-email	ssl	rule1	allowed
web-based-email	web-browsing	rule1	allowed



 \sim





將搜索結果轉換到Splunk可用於統計的數據表中 需要將搜索結果轉換為可視化

學會使用以下命令及其功能

- -top
- rare
- stats



Searching & Reporting with Splunk

使用top指令



在一個小時前,應用程式使用最多

top指令將搜索結果找到欄位最常見的值並計數,轉換至欄位 -預設回傳最常見的10筆結果

app 🗢	1	count 🗘 🖉	percent 🗘 🖌
web-browsing		119995	93.210135
google-maps		2618	2.033619
ssl		2192	1.702709
facebook-base		1244	0.966319
google-analytics		825	0.640846
flash		419	0.325472
sourceforge		329	0.255562
pandora		275	0.213615
google-safebrowsing		142	0.110303
apple-update		131	0.101759

使用top指令

- 預設輸出顯示為表格格式
- 自動回傳count 與percent列。
- Limit=#回傳這個數量的結果
 -預設顯示10筆最常見的結果
 -limit=0則為顯示全部結果數量

top Help More » Displays the most common values of a field.

Examples

Return the 20 most common values of the "url" field. ... | top limit=20 url

Return top URL values. ... | top url

Return top "user" values for each "host". ... | top user by host

- countfield=字串提供將原本count欄位 的名稱改變成所需的名字。
- **showperc=f**將不建立percent欄位。

使用Top指令

sourcetype="pan:threat"

| top limit=20 threat

2

在一個小時前,產生最多的攻擊事件的前20名威脅是什麼

threat 🗢	/	count 🗘 🖌	percent 🗘 🖌
(9999)		89055	70.975429
Windows Executable (EXE)(52020)		20200	16.099081
PII(60000)		12033	9.590111
Microsoft PE File(52060)		2005	1.597953
(0)		245	0.195261
Adobe Portable Document Format (PDF)(52021)		148	0.117954
256429558(256429558)		129	0.102811
254799658(254799658)		128	0.102014
254796918(254796918)		120	0.095638

(0) 254798198(254798198) 254797738(254797738) Microsoft PE File(52060) Pil(60000) Windows Executable (EXE)(\$2020)



(9999)







在過去一個小時內,哪一個行為最少出現在你的網路環境中?

rare指令將搜索結果找到 欄位最少見的值並計數, 轉換至欄位

-預設回傳最常見的10	筆
-------------	---

結果

-相關參數與 top用法一致

- sourcetype="pan:threat"
- 2 | rare showperc=f limit=20 threat

threat \$	/	count 🗘 🖌
Antivirus 2009 Downloads Antivirus Executable(12466)		1
HTML/Trojan.agent.cqbon(255147)		1
Antivirus-2010 asking download from tbest-antivirus-2010-download.info(12507)		3
Trojan.Win32.Ertfor.A updatesabout.com(12587)		3
Bredolab.Gen Command and Control Traffic(13024)		4
Trojan-Downloader.Win32.Zlob.wwv runtime childhe(12471)		4
Win PC Defender runtime detection(12548)		4
Trojan-Spy.Win32.Zbot.wti(12620)		6
Antivirus-2009 redirect to order page(12402)		14

使用stats指令



- stats讓你可以針對搜尋條件產生的結果 進行統計計算。
- 常見function 包含以下:
- -count -回傳搜尋條件匹配的事件數量
- -sum -回傳數字加總
- -avg —回傳數字平均
- -list –回傳欄位內所有的值
- -values 回傳欄位內的唯一值

stats	Help	More	»
Provides	statistics,	grouped	optionally by field.

Examples

Search the access logs, and return the number of hits from the top 100 values of "referer_domain".

sourcetype=access_combined | top limit=100 referer_domain | stats sum(count)

Return the average for each hour, of any unique field that ends with the string "lay" (for example, delay, xdelay, relay, etc).

... | stats avg(*lay) BY date_hour

Remove duplicates of results with the same "host" value and return the total count of the remaining results.

... | stats distinct_count(host)

使用stats指令count功能



想看到60分鐘有Malware活動的來源IP統計

<pre>1 sourcetype="pan:threat" "tag::eventtype"=malware 2</pre>					
2	Stats count by src	src 🗢	/	count 🗘 🖌	
		112.175.39.123		9	
		187.73.33.50		7	
		188.138.1.135		13	

• 使用as可以將count 欄位名稱改成更易懂的名稱

1 sourcetype="pan:threat" "tag::eventtyp	e"=malware		
2 stats count as 次數 by src 3 rename src as 來源位置	來源位置 ≑	1	次數 ≑ ✓
	112.175.39.123		9
	187.73.33.50		7
	188.138.1.135		13
	205.185.216.10		10
	213.186.33.4		10

使用stats指令count(欄位)



想看到15分鐘前威脅事件,防火牆的威脅對映動作Allow,Block及全部事件統計

- 加一個欄位名稱當做參數,計算相關的事件數量與百分比。
- 使用as可以將count欄位名稱改成更易懂的名稱。

1 2 3 4 5	sourcet stats sort	<pre>type="pan:threat" s count(eval(action="allowed")) as allowed , count(eval(action="blocked")) as blocked , count as Totals by threat - Totals</pre>	Win	allowed other (2) Pilecocco odocw., ¥52020) (9993)	blocked PH(60000) Window_1(53020)	other (22) Microso(82060) Pil(60000) (9999) Window(52020)	Totals
		threat \$	/	allowed 🗘 🖌	blocked 🗘 🖌	Totals 🗘 🖌	
		(9999)		6932	1737	8669	
		Windows Executable (EXE)(52020)		538	1429	1967	
		PII(60000)		457	713	1170	
		Microsoft PE File(52060)		205	0	205	
		(0)		37	0	37	
		254797738(254797738)		17	0	17	

使用stats指令count by 欄位



想看到15分鐘前根據來源與目的分類產生威脅的事件數量

- 經由子句回傳一個指定欄位或欄位組的事件數量統計
- 可使用任意數量的欄位當參數透過by欄位列舉

-與chart/timechart指令基本不同為, chart/timechart可使用的欄位限制為2

1 sourcetype="pan:threat"

2 | stats count as Count by threat, src, dest

3 | sort - Count

Windows Executable (EXE)(52020)	20	0.147.33.19		192.168.0.2		103
Windows Executable (EXE)(52020)	20	0.147.33.17		192.168.0.2		106
(9999)	19	2.168.0.2		17.254.32.16		107
PII(60000)	74	.125.224.200		192.168.0.2		111
(9999)	19	2.168.0.2		64.78.56.109		111
PII(60000)	72	.21.194.1		192.168.0.2		115
(9999)	19	2.168.0.2		208.73.210.29		171
(9999)	19	2.168.0.2		204.232.231.46		1004
(9999)	19	2.168.0.2		184.106.31.170		3436
threat 🗘	/ sr	c \$	1	dest 🗘	/	Count 🗘 🖌

使用stats指令 sum (欄位)



想知道上週使用公司網路使用流量跟連線數

	欄位內容為數字可用sum做加總的	的動作	other (14) 192.168.0.6	other (14) 192.168.0.100
1 2 3	sourcetype="pan:traffic" stats sum(bytes) as Used , count by src sort - Used		10.0.1.20 192.168.0.2	192.168.0.6 192.168.0.3 192.168.0.2
	src ≑	1	Used 🗘 🖉	count 🗢 🖌
	192.168.0.2		99748383	6175
	192.168.0.3		49521977	1149
	10.0.1.20		44225409	34
	192.168.0.6		41225619	686
	192.168.0.100		349508	687
	108.224.90.120		94346	1

使用stats指令avg(欄位)進階 ^{想知道上週使用公司網路使用流量跟平均使用量}



1	sourcetype="pan:traffic"						
2	stats sum(bytes) as Used ,						
3	avg(bytes) as "Avg Used",						
4	count as Sessions by src						
5	sort - Used						

欄位內容為數字可用avg 做計算平均值的動作

src ≑	1	Used 🗘 🖌	Avg Used 🗘 🖌	Sessions 🗘 🖌
192.168.0.2		70580346	11422.61628095161	6179
192.168.0.3		46088543	40393.11393514461	1141
10.0.1.20		45724410	1270122.5	36
192.168.0.6		40119289	60879.04248861912	659
192.168.0.100		336545	494.91911764705884	680
108.224.90.120		94346	94346	1
98.248.152.109		26904	13452	2
192.168.0.1		21370	1017.6190476190476	21
166.205.139.177		5635	1127	5





想知道4小時威脅分數為4,5使用的IP跟User的關係

- 1 sourcetype="pan:threat" app:risk=4 OR app:risk=5
- 2 | stats values(user) as Users ,count by src

src \$	/	Users ≑	/	count 🗢 🖉
10.0.1.20		tng\crusher tng\jordy tng\picard		116
109.201.131.15		crusher tng\crusher		134
109.235.249.163		crusher tng\crusher		53
112.175.39.123		tng\crusher		327
114.108.168.12		crusher tng\crusher		103

資料結構化

- 大多數將搜尋結果可視化,至少會結構 化成兩列的表格。
- 在圖表中
 - -第一列提供X軸的值 -第二列提供Y軸的值

vendor_action ©	count 👳
Accepted	2
FTP LOGIN	6
Failed	29
HANDLING TELNET CALL	2
Invalid user	3
session opened	59





資料結構化chart



- Chart指令可以顯示任何一系列的圖表
- 你可以決定x軸是使用哪個欄位繪製於圖表中
 - --相關的參數顯示視為Y軸,必須要為數字
 - -使用的第一個欄位在over參數後的視為X軸 -使用over與by將數據分成子分組,相關的內容將產 生於該圖表中
- chart avg(bytes) over host
 - -host 值會於X軸
- chart avg(bytes) over host by product_name -host 值會於X軸,在product_name進行x軸拆分

資料結構化chart over欄位



顯示24小時內應用程式類別分析圖

- 1 sourcetype="pan:traffic"
- 2 | chart avg(bytes) over app:category



資料結構化chart over欄位 by 欄位



顯示24小時內根據使用者使用應用程式類別分析圖

- 將app:category做事件分 組後,各分組使用user在 進行事件分類
- sourcetype="pan:traffic"
- 2 | chart avg(bytes) over app:category by user





想看到最近4小時威脅分析大於4的威脅次數,根據各類別及使用者來分析

你會發現圖表裡占比最重的是 Null and Other,但這樣的結果 並不是我們想看到的

sourcetype="pan:threat" app:risk>=4

2 | chart usenull=f useother=f count over user by category





想看到最近4小時威脅分析大於4的威脅次數,根據各類別及使用者來分析

chart與timechart指令預設過濾結果只取最高值前十名顯示 -剩餘的值會被集中到OTHER 要移除empty(null)可使用usernull=f 要移除OTHER可使用userother=f



資料結構化chart限制顯示數量



想看到最近4小時威脅分析大於4的威脅次數,根據各類別及使用者來分析

使用limit參數, limit=0為不限制數量



| chart count over user by category limit=3



時間趨勢圖timechart

想看到24小時內威脅分數為5的趨勢圖



時間趨勢圖timechart



想看到24小時內各使用者威脅分數為5的趨勢分析圖

timechart最多只能選一個欄位作 時間群組後的事件分類

- sourcetype="pan:threat" app:risk>=5
- 2 | timechart count by user



時間趨勢圖timechart 調整採樣間隔



- 1 sourcetype="pan:threat" app:risk>=4
- 2 | timechart span=10m count by user

- Example defaults:
 - Last 60 minutes uses span=1m
 - Last 24 hours uses span=30m
- Adjust the interval using the span argument, i.e. span=15m

_time ‡	counselor 🖌	crusher 🖌
2019-04-17 16:00:00	64	1295
2019-04-17 16:10:00	84	1295
2019-04-17 16:20:00	75	1331
2019-04-17 16:30:00	67	1312
2019-04-17 16:40:00	67	1328
2019-04-17 16:50:00	70	1297
2019-04-17 17:00:00	69	1203
2019-04-17 17:10:00	63	1288

時間趨勢圖timechart 使用統計參數



想看到4小時內從使用者每5分鐘的使用量趨勢分析圖













Search	Datasets Reports	Alerts	Dashbo	bards		Search & Reporting	
Report Report view th	orts s are based on single searches a ne report. Open the report in Pivo	nd can ind ot or Searc	clude visu th to refin	ualizations, sta e the paramet	tistics and/or events. Click ers or further explore the o	:k the name to	
44 Rep	ports	All	Yours	This App's	filter	٩	
i	Title ▼	A	ctions		Next Scheduled Time	◆ 使用者每5分鐘的使用量 Edit ▼ More Info ▼ Add to Dashboar	rd
ŕ	反而音鸣5万姓的反而重	Se	earch			Last 4 hours -	
>	gps distant	O Se	pen in earch	Edit 🔻	None	✓ 11,184 events (4/18/19 12:37:00.000 PM to 4/18/19 4:37:14.000 PM) Job ▼ II ■ O → ● 40,000,000	¥
>	abc	O Se	pen in earch	Edit 🔻	None	30,000,000	
>	Splunk errors last 24 hours	O Se	pen in earch	Edit 🔻	None	20,000,000	elor rusher
>	Orphaned scheduled searches	O Se	pen in earch	Edit •	None	10,000,000 100 PM 130 PM 2:00 PM 2:30 PM 3:30 PM 4:00 PM	rdy card
						Thu Apr 18 2019time	



16

免費試用

- Splunk Enterprise (term)
 - 60 days enterprise full features, then free with limited features
 - 500MB/day
 - Violation = 4 warnings (rolling 30-day period)



- Mission-critical performance, scale, and reliability
- ✓ Splunk Premium Solutions and Apps from Splunkbase

🛓 Free Download







Links Referenced in Exploring Splunk

Chapte	rTopic	Description	Link
2	tutorial	The Splunk Tutorial	docs.splunk.com/Documentation/Splunk/4.2/User/WelcometotheSplunktutorial
2	add_data	Tutorial: how to add sample data	docs.splunk.com/Documentation/Splunk/4.2/User/Adddatatutorial
2	sample_data	Tutorial: link to sample data	www.splunk.com/base/images/Tutorial/Sampledata.zip
3	mining_tips	Mining unfamiliar data	www.innovato.com/splunk/mining.htm
5	auto_fields	More information on automatic field extraction	$docs.splunk.com/Documentation/Splunk/latest/knowledge/Aboutfields \#An_example_of_automatic_field_extraction and the second sec$
5	ifx	More information about the Interactive Field Extractor (IFX)	docs.splunk.com/Documentation/Splunk/4.2/User/InteractiveFieldExtractionExample
5	config_fields	Manually configuring field extractions	$\label{eq:constraint} does.splunk.com/Documentation/Splunk/latest/Knowledge/Managesearch-timefieldextractions$
5	search_fields	Use the search language to extract fields	docs.splunk.com/Documentation/Splunk/4.2/User/ExtractFieldsWithSearchCommands
5	custom_alerts	Creating custom alert scripts	docs.splunk.com/Documentation/Splunk/4.2/admin/ConfigureScriptedAlerts
6	concurrency	The concurrency search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/Concurrency
6	metadata	The metadata search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/metadata
6	streamstats	The streamstats search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/streamstats
6	trendline	The trendline search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/Trendline
8	autolookup	Configuring automatic Lookups	docs.splunk.com/Documentation/Splunk/4.2/User/CreateAndConfigureFieldLookups
8	lookuptutorial	Lookup tutorial	docs.splunk.com/Documentation/Splunk/4.2/User/Fieldlookupstutorial

Splunkbase 有2,053 個安裝套件(App),可免費下載安裝

4

熱門下載:

- Splunk App for Windows
- Splunk for Unix and Linux
- DB Collect
- Splunk for Cisco Firewall
- Splunk for F5
- Splunk for Nagios
- Splunk for Web Intelligence









http://docs.splunk.com

splunk > docs

Get started

Search and report

t

Administer

Develop

Splunk Enterprise Overview

A technical overview of Splunk platform features and documentation.

Release Notes

Includes information about new features, known issues, and fixed problems.

Installation Manual

How to install or migrate Splunk Enterprise. Includes system migration requirements and licensing information.

Search Tutorial

If you are new to Splunk search, start here. Guides you through adding data, searching data, and creating simple dashboards.

Data Model and Pivot Tutorial

Introduction to adding data, building simple data models, and creating new pivots.

Splunk Enterprise Scenarios

Contains scenario-based topics. Each topic illustrates a complex use case that is comprised of several tasks involving multiple product features. Some of these scenarios may involve Splunk apps and add-ons.

Translated Documentation

Some Splunk Enterprise manuals are available in Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Getting Data In

Deploy

How to get your machine data into your Splunk deployment and ensure that it is indexed efficiently and effectively.

研討會、案例、用戶分享



• <u>http://conf.splunk.com</u>



.CONF ARCHIVES

2016 Keynotes, Speakers & Sessions

2015 Highlights Video

2015 Sponsors

2015 Keynotes

2015 Speakers & Sessions

2015 theCube Interviews

2014 Keynotes

2014 Sessions

下載 Splunk Mobile











splunk >enterprise 應用套件 ▼			🥑 Administre
應用套件 ♀管理	哈囉, Administrator		
依名稱搜尋應用奏件 Q	快速连结 一 送表板 最近檢視 由 約建立	超您共用	
Search & Reporting		200 V D	
Splunk Secure Gateway			
EQ Upgrade Readiness App	日 新增資料 EC 從各種常見來源新增資料。	《 授辱您的資料 透過 Splunk 搜尋將資料化為行動。	记录 一根壳化总的资料 建立通合总资料的优表板。
尋找更多應用套件也			
	回 目1911年100 控制誰有權存取角色。	成と11動を自 使用 Splunk Secure Gateway 登入或管理行動 装置。	
	學習和資源		
	€ Splunk 新手嗎? 讓導覽來幫助您使用。	●書用 Splunk 說明文件進一步瞭解 Ⅰ2 在全方位的指引下部署、管理和使用 Splunk 軟體。	页 取得 Splunk 專家的協助 也 Splunk Lantern 客戶成功中心的可操作指南。
	加入 Splunk 社群 ビ 學習、獲得靈感並分享知識。	● 查看其他人如何使用 Splunk ☑ ◎ 瀏覽真實者戶案例。	② 訓練和認證 13 成為經過認證的 Splunk 忍者。



				🔘 Administrator 👻 🚺 訊息 💌	設定▼ 活動▼ 説明▼ 尋找 ▲
		歡迎使用 Connected Experiences	×		
主目錄	在您的裝置中下載 Co 始・	nnected Experiences 應用套件後,請選擇您正在使用的應	用套件以開		+ 新煤炭五 🔮 曾超延知
	splunk>	Splunk Mobile 檢視儀表板並回應營示。			
	Edge	Splunk Edge Hub 從實體環境中簡化「取得資料」・			Action
	ar	Splunk AR 使用操增置增虑理境場資料 •			A #
	splunk>	Splunk for iPad 以模記附註儀表板、作筆記,並檢視對對 iPad 優化的圖			
	splunk>	Splunk TV 和 Splunk TV Companion 在電視留幕上顕示、管理儒表板並與之互動・			
		步一步			
·					



splunk>enterprise 應用套件 ▼		
主目錄 Administration 儀录板★	掃描以登入 ×	
	開放行動磁雲中的 Splunk Mobile 應用套件並將描下列代碼以签入	
Q. 预寻收置或使用音 上大使用拿 請菁菁拿 点用		
類创前 admin Spur		≜
	上一步	









