程式驅動
code-driven

Splunk 教育訓練 1

7/19 案例主題：大型企業門禁系統安全事件日誌

Agenda

- 產品介紹
- 安裝，操作Splunk
- 介面說明

Splunk介紹

Agenda

程式驅動 code-driven

- 確認Splunk能為你解決的問題
- 機器資料能為你產生的商業價值
- Splunk 作為適用於所有機器資料的優勢
- Splunk 如何在企業內部遍地開花
- Splunk 的客戶群體

讓每個人都能存取、使用機器資料
並從中找出價值

機器資料裡包含了關鍵洞察力

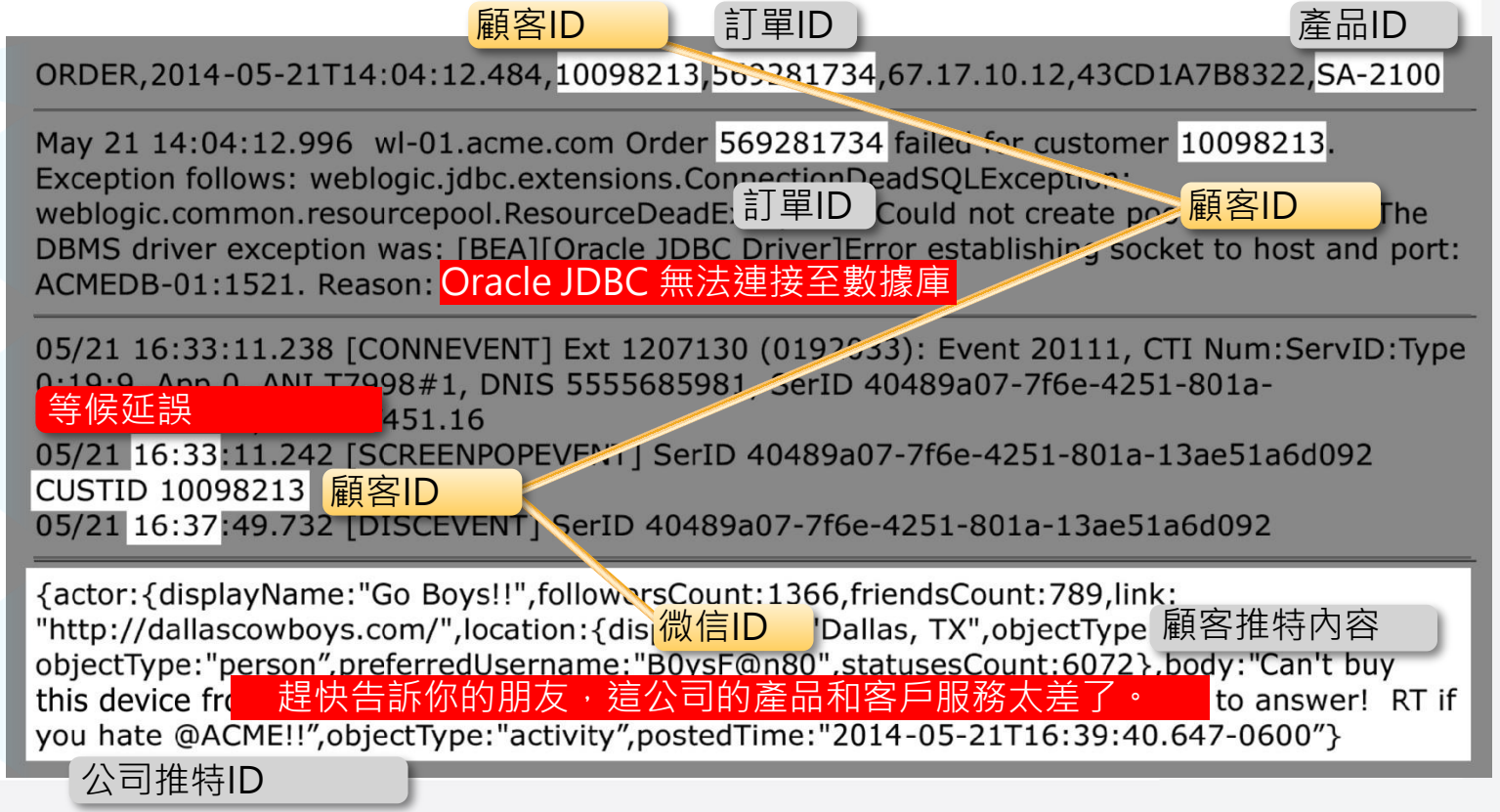
來源

訂單處理

中介軟體

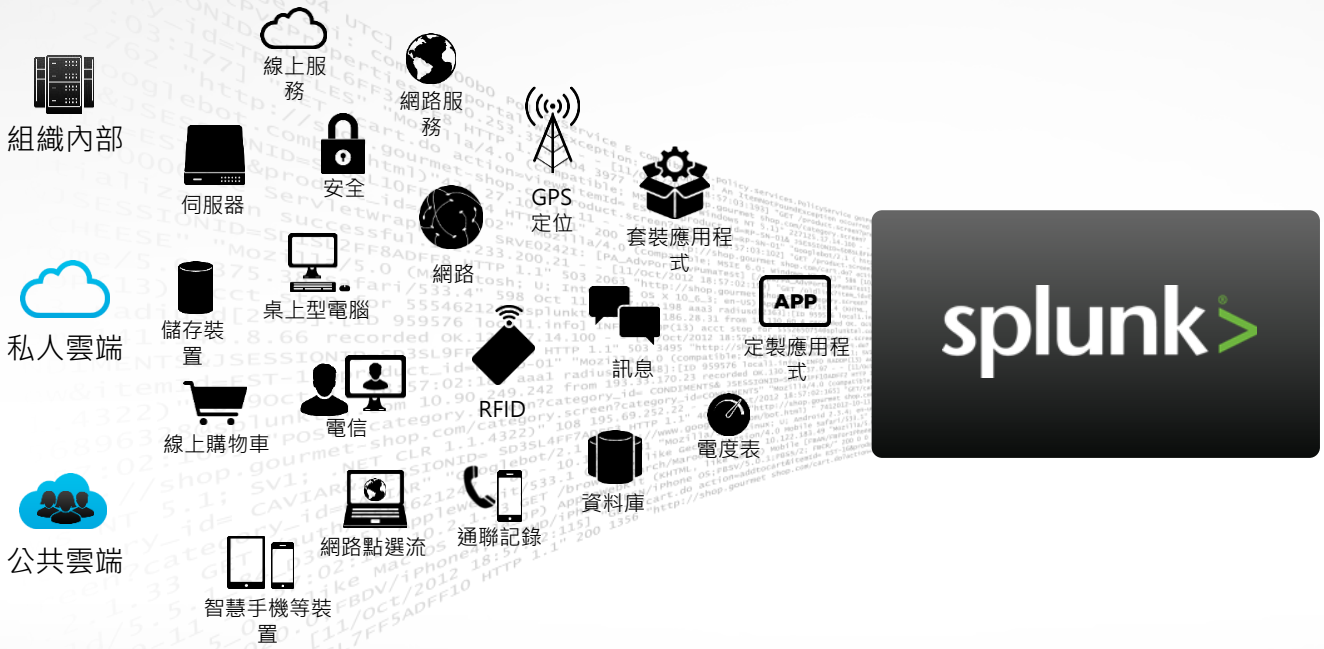
互動式語音回應

Twitter（推特）



將機器資料化為商業價值

索引未曾處理的資料: 不限來源, 種類, 數量



可詢問任何問題

- 應用程式交付
- IT營運
- 安全,合規與詐騙
- 商業分析
- 工業資料與物聯網

領先的機器資料平台

索引未曾處理的資料: 不限來源, 種類, 數量

可詢問任何問題

組織內部

私人雲端

公共雲端

智慧手機等裝置

不論數量、地點或來源

Scheme 動態產生

通用索引

無後端 RDBMS

無須過濾資料

- 應用程式交付
- IT營運
- 合規與詐騙
- 商業分析
- 工業資料與物聯網

Splunk 巨量資料產品

程式驅動 code-driven

Splunk 優質解決專案

- Splunk IT Service Intelligence™
- Splunk Enterprise Security™
- Splunk User Behavior Analytics™

內容豐富的應用程式生態系統

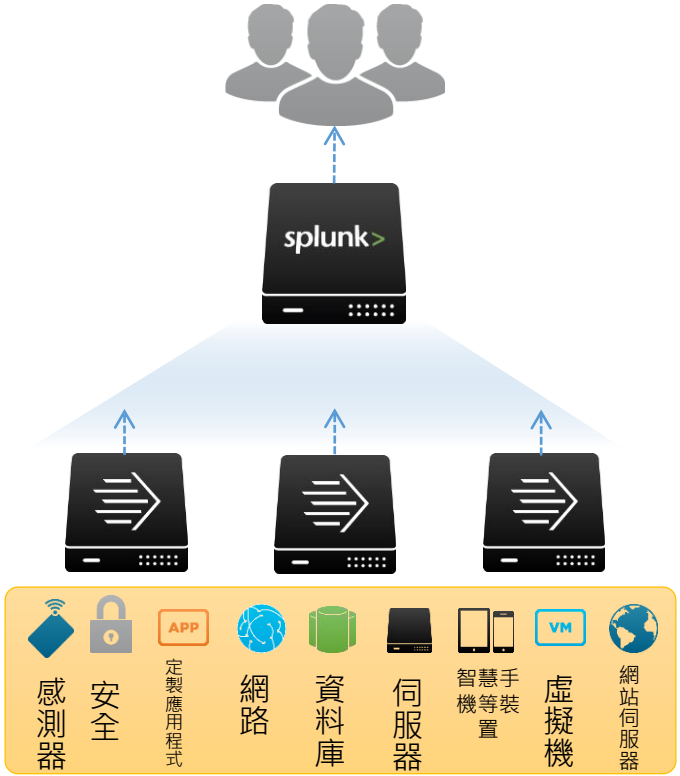
Microsoft .net, Symantec, cisco, salesforce.com, kepware, NetApp, Linux

splunk>enterprise | splunk>cloud | splunk>light | Hunk

splunk> 機器資料平台

Forwarders | 系統日誌/ TCP / 其它 | 行動資料 | 物聯網 | 網路資料 | Hadoop | 資料庫 | Mainframe 資料

幾個簡單步驟即可部署Splunk Enterprise



只要四個步驟：

1. 下載
2. 安裝
3. 轉送資料
4. 搜尋

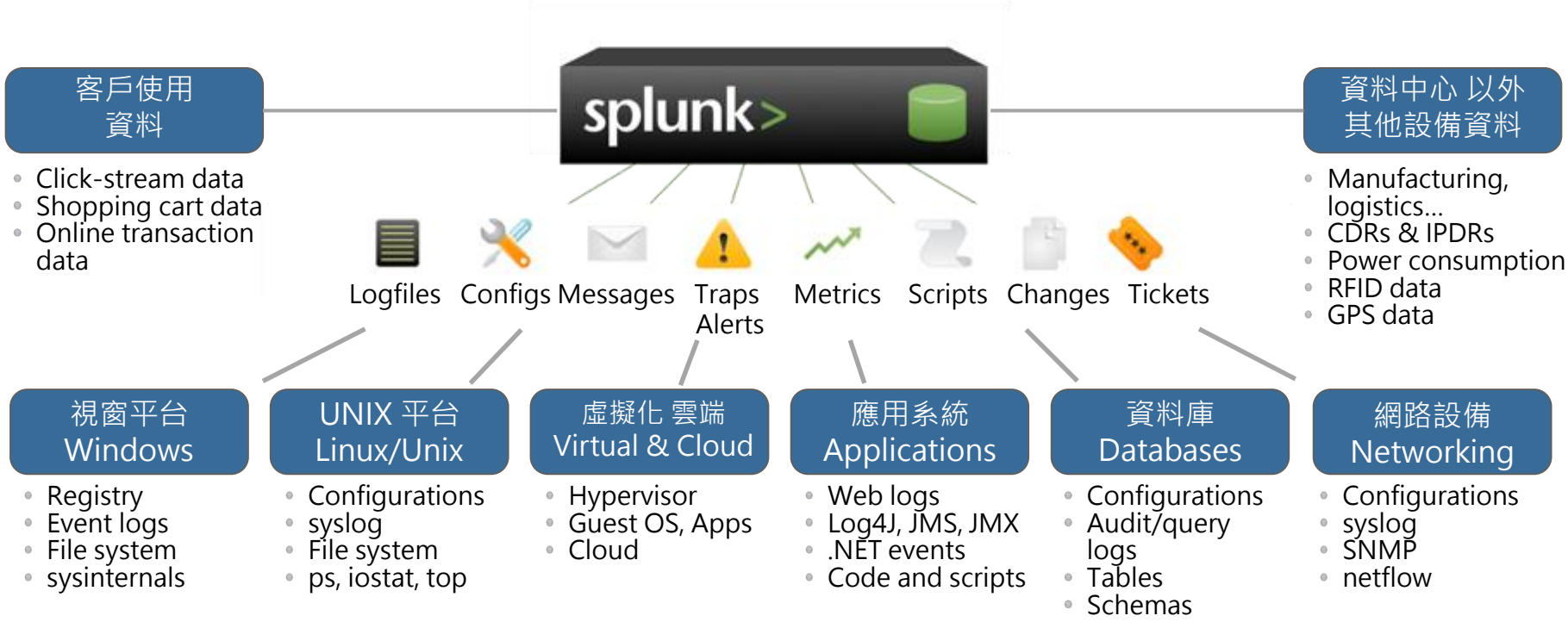
日容量可擴充至數百TB

程式驅動 code-driven

企業級的擴充性、回復能力與相容性

Splunk: 營運智慧平台

不用事先定義 資料欄位，不用 客製化 連接器，不用資料庫，不需要事先過濾



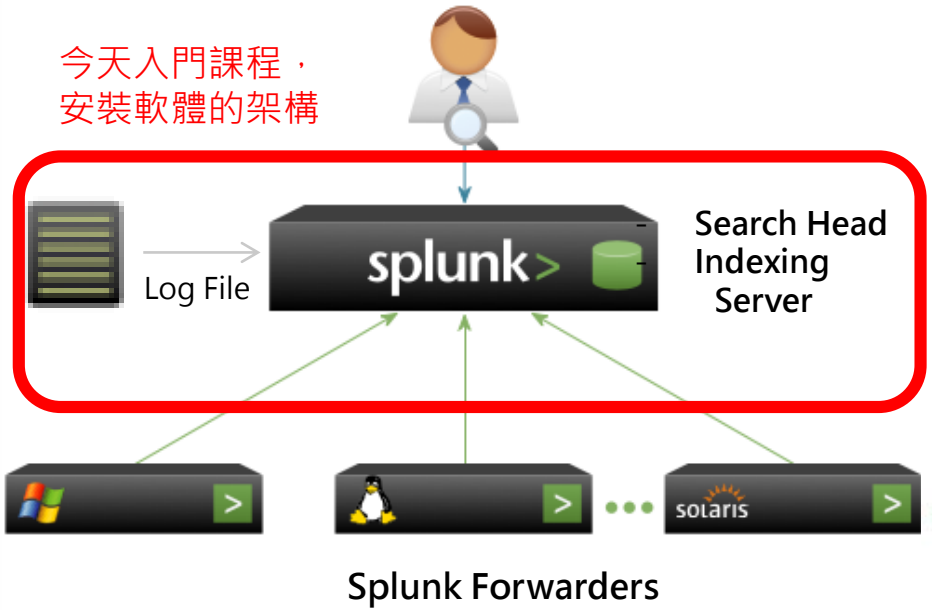
總結

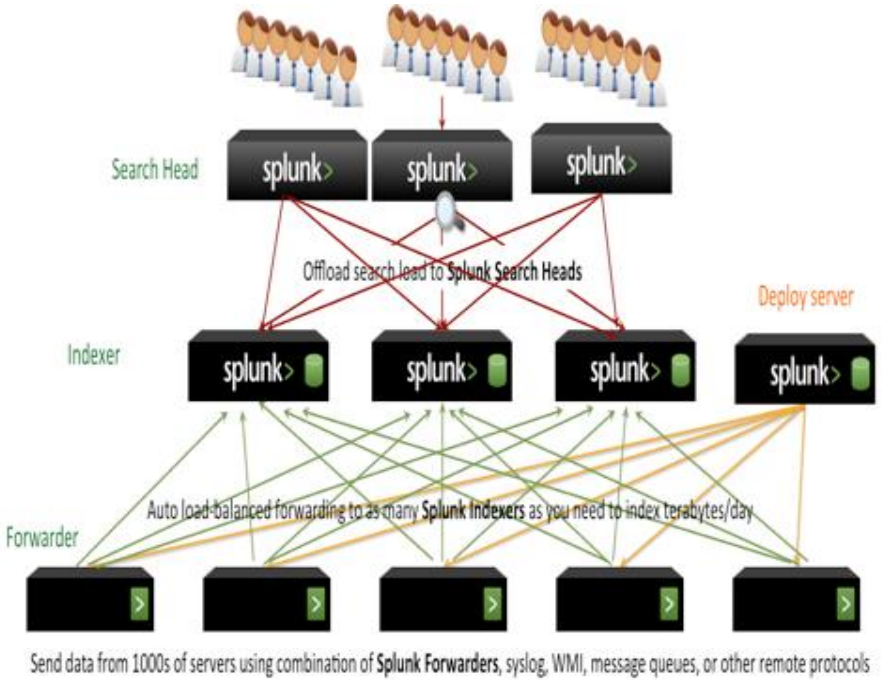
- 適用於所有機器資料的平台
- 即時架構
- Schema on the Fly
- 強大的分析功能和迅速產生警示，報告
- 靈活的擴充性：從單台接需求擴張到叢集
- 快速獲取價值
- 有活力和熱情的用戶群體

安裝Splunk

Splunk 產品，四 個主要元件：

Search Head, Indexer, Forwarder, Deployment Server



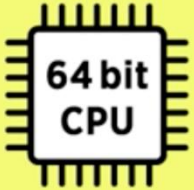


資源需求

程式驅動 code-driven

Search Head

Requirements



x4

4 x 2GHz cores each

- 12GB RAM
- 1GbE NIC
  with optional second NIC for management
- 2 x 10K RPM 300GB SAS drives - RAID 1

資源需求

程式驅動 code-driven

Indexer

Requirements

64 bit CPU x2

6 x 2GHz cores each

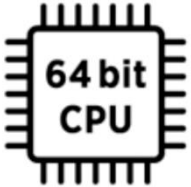
- 12GB RAM
- 1GbE NIC
  with optional second NIC
  for management
- 64-bit Linux/Windows
- 800 IOPS

資源需求

程式驅動 code-driven

Forwarder

Requirements

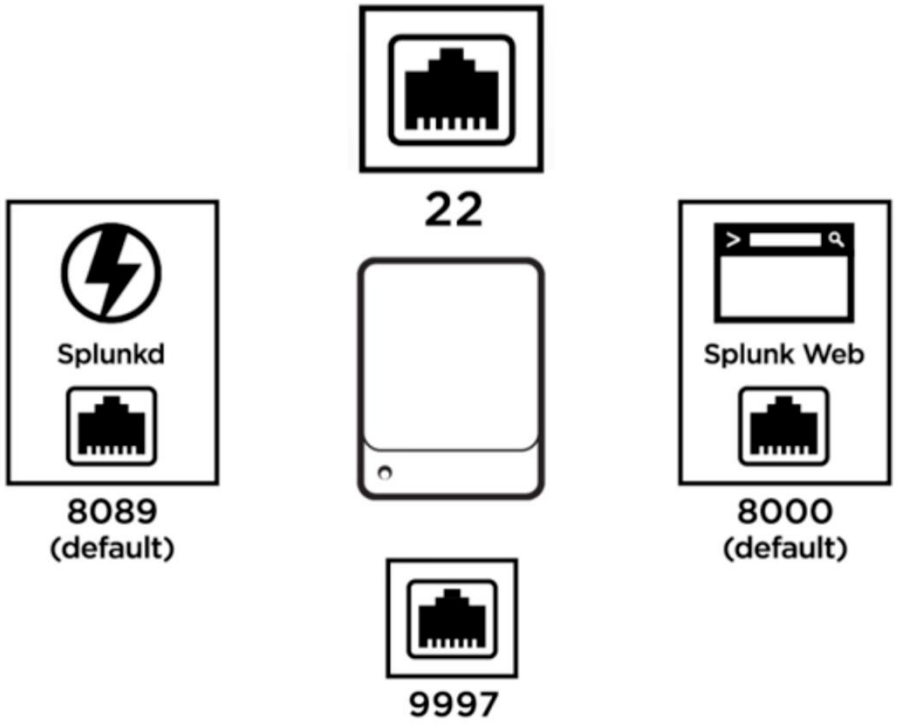


x1

2 x 1.5GHz cores

- 1GB RAM

資源需求



Splunk 兩個主要執行程式之一 ： splunkd

程式驅動 code-driven

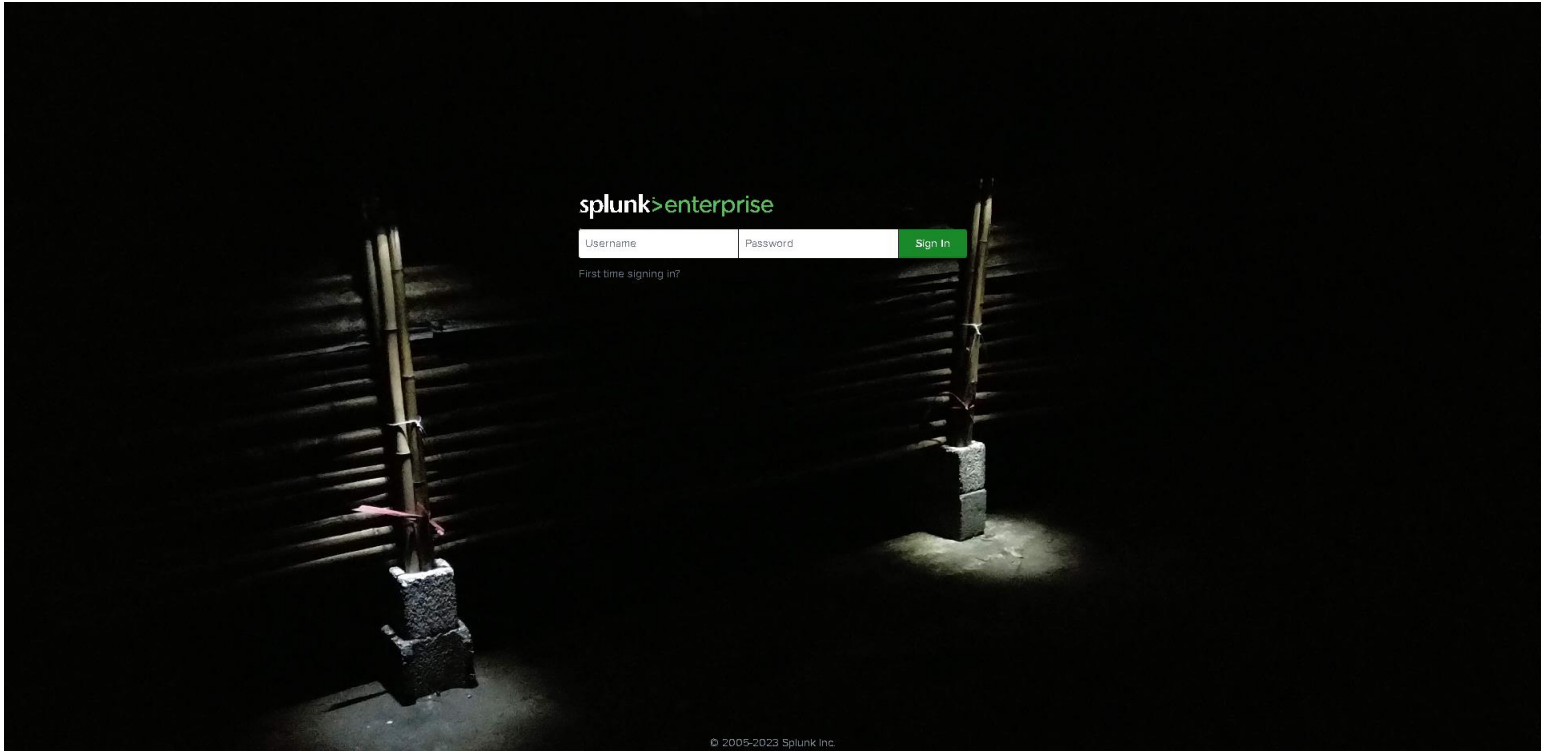
- 全文檢索服務：被查詢、傳回結果、和 將 所有進入的資料 建立索引
- Accesses, processes, and indexes incoming data
- Processes all search requests and returns results
- Runs a web server on port 8089 by default
- Speaks SSL by default
- Splunk helpers run as dependent process(es) of splunkd
  - Splunk helpers run outside scripts, for example:
    - Scripted inputs
    - Scripted alerts

Splunk 兩個主要執行程式之二 ： Splunk Web

程式驅動 code-driven

- Python-based web server, based on CherryPy framework
- Provides both search and management web front end for splunkd process
- Runs on port 8000 by default
- Sets initial login to user: admin password: changeme

LAB 4 you http://splunk.pair.tw:8000



安裝的 作業系統 和 瀏覽器 需求

Splunk works on Windows, Linux, Solaris, FreeBSD, MacOS X, AIX, and HP-UX

Firefox 3, 4, and 8; IE 7, 8, and 9; latest Safari and Chrome

docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements

For Linux -------Production

程式驅動

A 此平台的軟體可從 splunk.com 下載，但未提供對平台的官方支援。
D Splunk 支援此平台與架構，但可能會在未來版本中移除支援。如需有關不建議使用功能的資訊，請參閱《版本資訊》中的<不建議使用的功能>。
† 您必須使用 gnu `tar` 以解除封裝 HP/UX 安裝封存。

Unix 作業系統

作業系統	架構	Enterprise	Free	試用版	通用轉送器
Solaris 10 和 11	x86 (64 位元)	D	D	D	✔
	SPARC				✔
Linux 2.6 及更新版本	x86 (64 位元)	✔	✔	✔	✔
	x86 (32 位元)				D
Linux 3.x 及更新版本	x86 (64 位元)	✔	✔	✔	✔
	x86 (32 位元)				D
PowerLinux 2.6 及更新版本	PowerPC				✔
zLinux 2.6 及更新版本	s390x				✔

For Linux -------Production

程式驅動

A 此平台的軟體可從 splunk.com 下載，但未提供對平台的官方支援。
D Splunk 支援此平台與架構，但可能會在未來版本中移除支援。如需有關不建議使用功能的資訊，請參閱《版本資訊》中的<不建議使用的功能>。
† 您必須使用 gnu `tar` 以解除封裝 HP/UX 安裝封存。

Unix 作業系統

作業系統	架構	Enterprise	Free	試用版	通用轉送器
FreeBSD 9	x86 (64 位元)				✔
FreeBSD 10	x86 (64 位元)				✔
Mac OS X 10.10 和 10.11	Intel		✔	✔	✔
AIX 7.1 和 7.2	PowerPC				✔
AIX 6.1	PowerPC				D
HP/UX† 11i v3	Itanium				✔
ARM Linux	ARM				A

For Linux ------Production

若要在 Linux 系統上安裝 Splunk Enterprise，請將 tar 檔案展開至使用 tar 命令的適當目錄：

tar xvzf splunk_package_name.tgz

預設安裝目錄為目前工作目錄中的 splunk。若要安裝至 /opt/splunk，請使用下列命令：

tar xvzf splunk_package_name.tgz -C /opt

For MAC OS ------Demo or LAB

Mac OS 建置有兩種形式：DMG 套件和 tar 檔案。
如果您需要兩個安裝在相同主機的不同位置上，請使用 tar 檔案。
pkg 安裝程式無法安裝第二個執行個體。
如果已經有一個執行個體，那麼在成功安裝第二個時就會移除該執行個體。

若要在 Mac OS X 上安裝 Splunk Enterprise，請將 tar 檔案展開至使用 tar 命令的適當目錄：

```
tar xvzf splunk_package_name.tgz
```

預設安裝目錄為目前工作目錄中的 splunk。若要安裝至 /Applications/splunk，請使用下列命令：

```
tar xvzf splunk_package_name.tgz -C /Applications
```

For Windows Server OS ---Production

D Splunk 支援此平台與架構，但可能會在未來版本中移除支援。如需有關不建議使用功能的資訊，請參閱《版本資訊》中的＜不建議使用的功能＞。
*** Splunk 支援但不建議在此平台與架構上使用 Splunk Enterprise。

Operating system	Architecture	Enterprise	Free	Trial	Universal Forwarder
Windows Server 2008 R2	x86 (64-bit)	D	D	D	D
Windows Server 2012 and Server 2012 R2	x86 (64-bit)	✔	✔	✔	✔
Windows 8, 8.1, and 10	x86 (64-bit)		✔	✔	✔
	x86 (32-bit)		***	***	✔

For Windows Server OS ---Production

程式驅動 code-driven

使用 PowerShell 安裝
您可以從 PowerShell 視窗安裝 Splunk Enterprise。執行此操作的步驟與從命令提示安裝所使用的步驟相同。

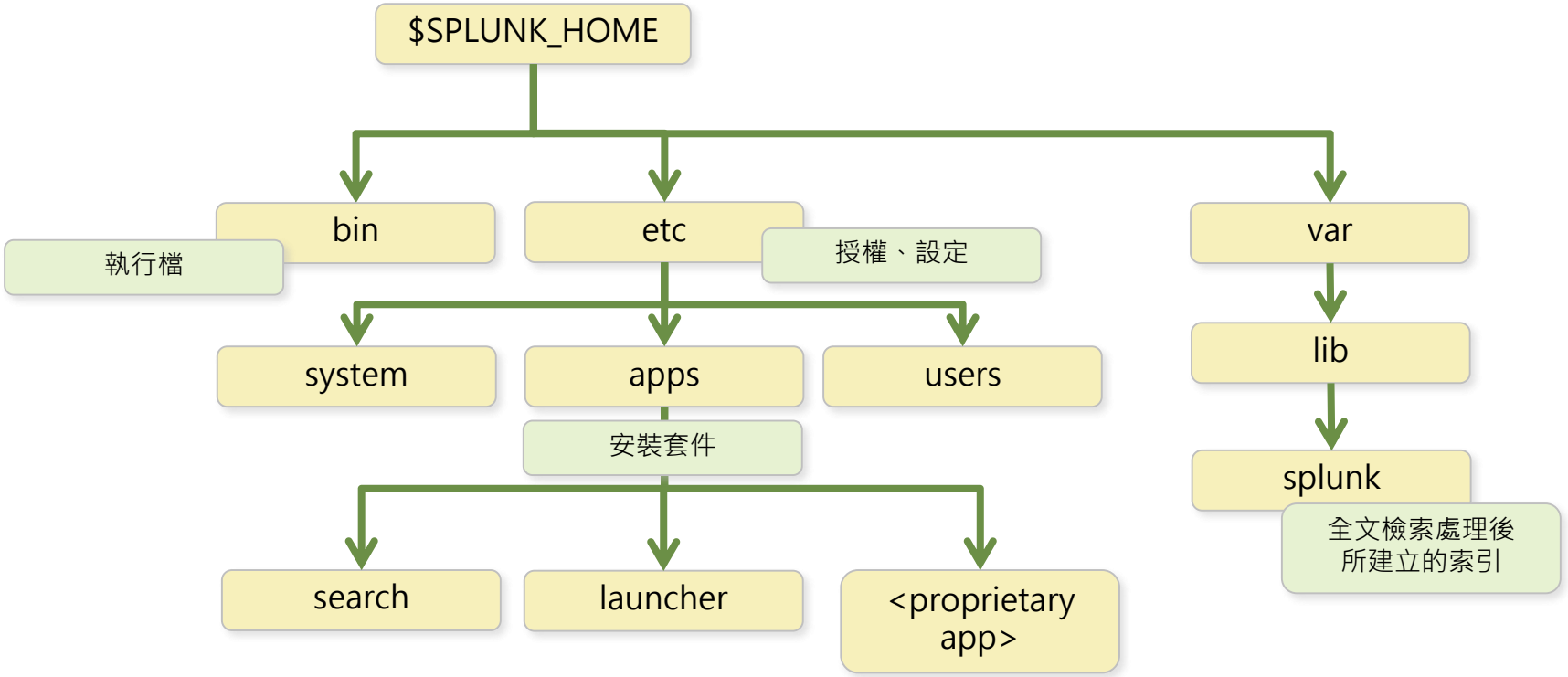
使用 msiexec.exe 以從命令列或 PowerShell 提示安裝 Splunk Enterprise。

針對 64 位元平台，請使用 splunk-<...>-x64-release.msi：

msiexec.exe /i splunk-<...>-x64-release.msi [<flag>]... [/quiet]

C:\>msiexec.exe /lev splunk.log /i splunk-<...>-x64-release.msi /quiet

Splunk 產品的目錄結構

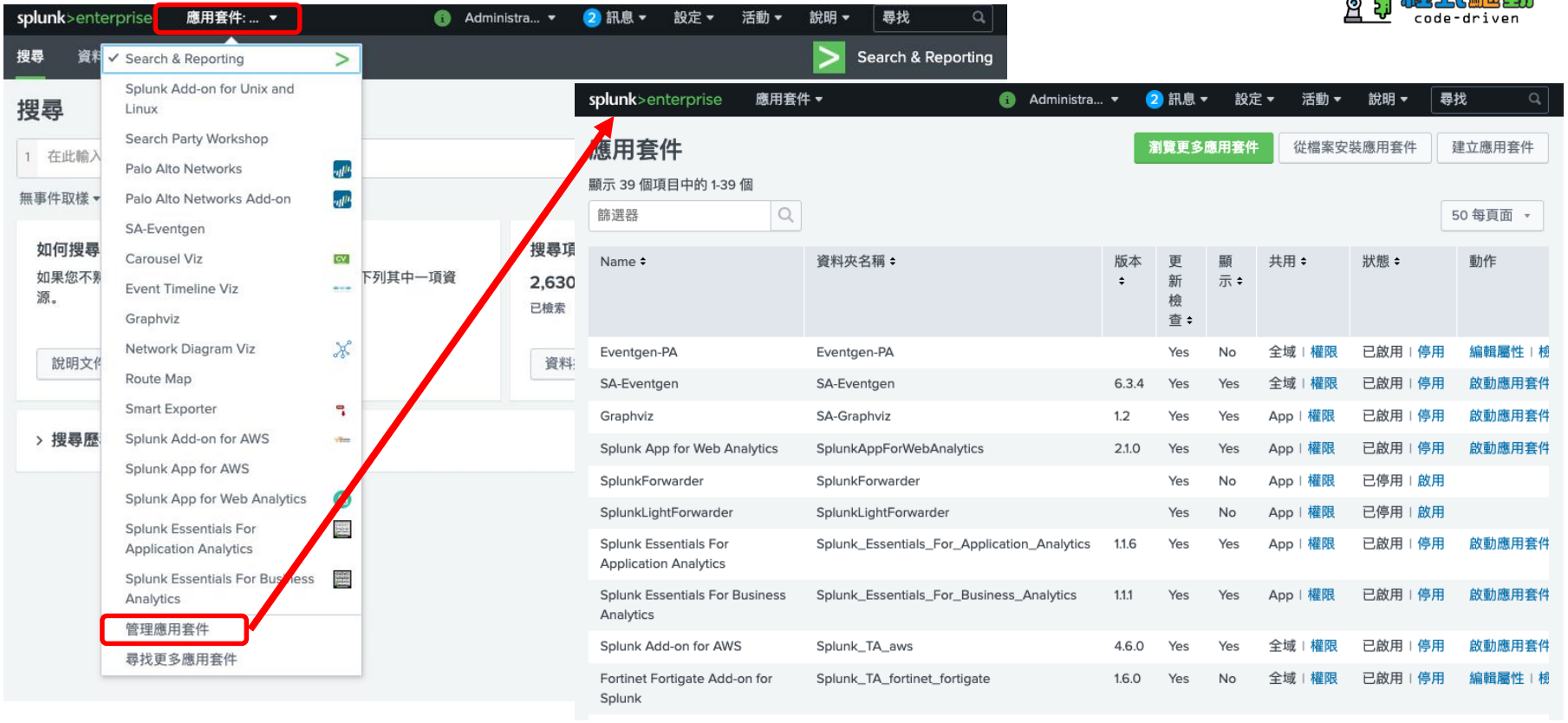


Splunk App 目錄結構

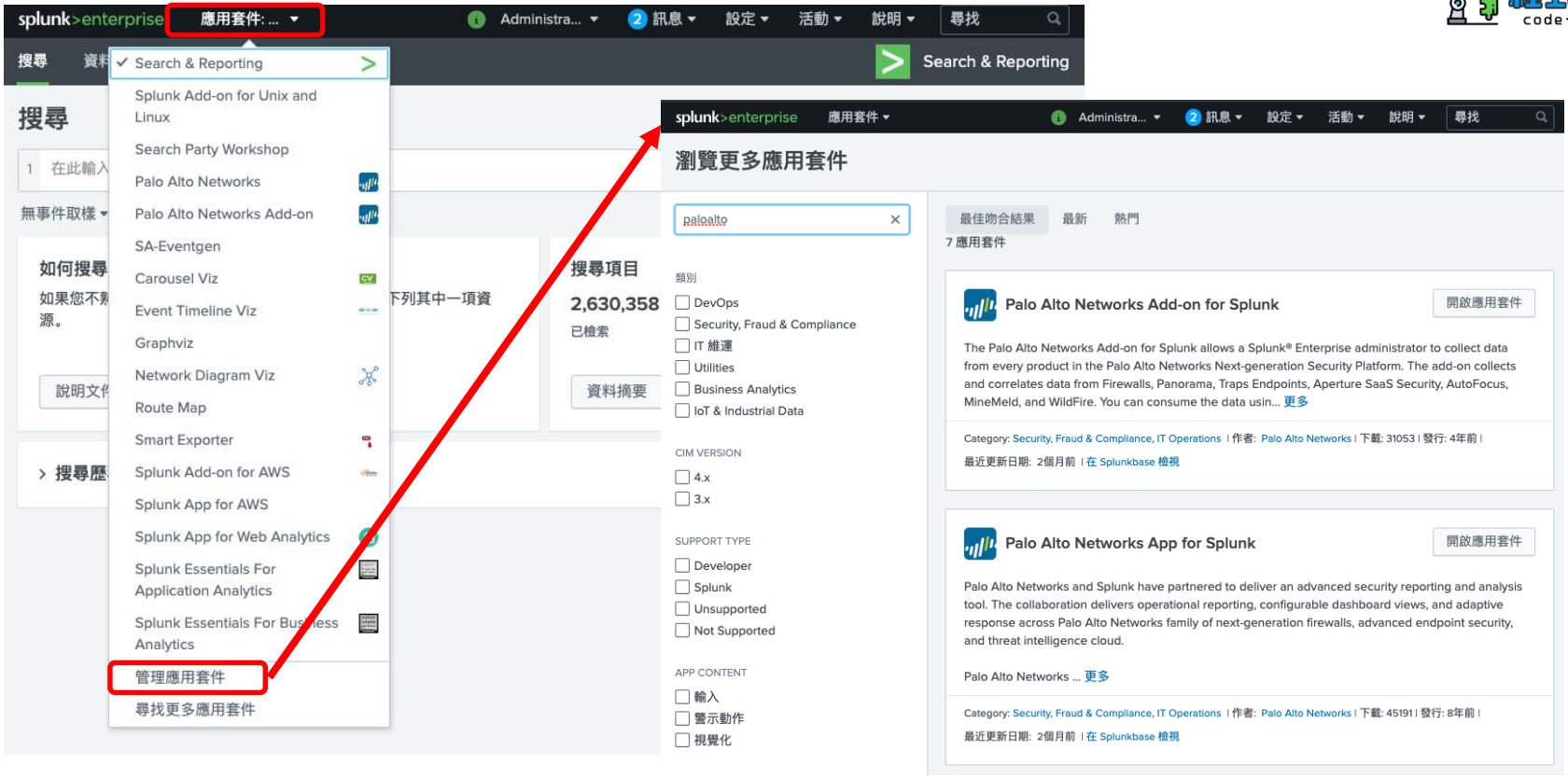
程式驅動 code-driven

```
/opt/splunk/etc/apps/Eventgen-PA ls -alR
total 8
drwxr-xr-x   7 jack  staff   224  4 15 12:28 .
drwx------@ 45 jack  staff  1440  4 18 20:43 ..
drwxr-xr-x@  4 jack  staff   128  4 16 10:17 default
drwxr-xr-x   3 jack  staff    96  4 16 16:01 local
-rw-------   1 jack  staff   229  4 15 11:11 local.meta
drwxr-xr-x   3 jack  staff    96  4 15 12:28 metadata
drwxr-xr-x@ 19 jack  staff   608  4 16 15:53 samples

./default:
total 24
drwxr-xr-x@ 4 jack  staff   128  4 16 10:17 .
drwxr-xr-x  7 jack  staff   224  4 15 12:28 ..
-rw-r--r--@ 1 jack  staff  6148  4 16 10:17 .DS_Store
-rw-r--r--@ 1 jack  staff  3846  8  5  2017 eventgen.conf

./local:
total 24
drwxr-xr-x  3 jack  staff    96  4 16 16:01 .
drwxr-xr-x  7 jack  staff   224  4 15 12:28 ..
-rw-r--r--@ 1 jack  staff  9288  4 16 16:01 eventgen.conf
```

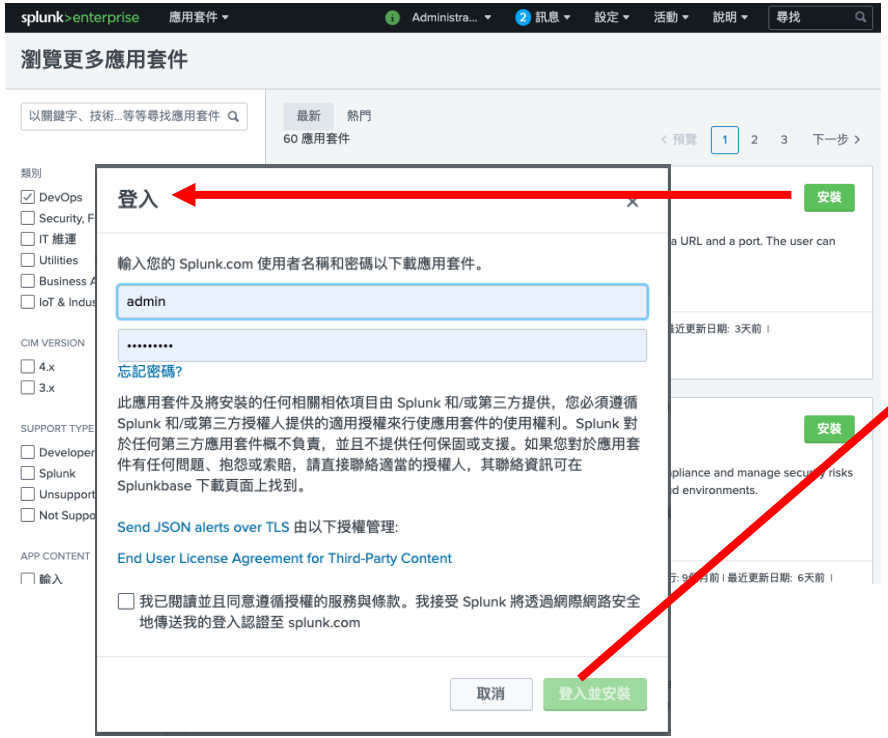
APP and Add-on安裝



APP and Add-on安裝



APP and Add-on安裝



APP and Add-on安裝

程式驅動 code-driven

應用套件

瀏覽更多應用套件 | 從檔案安裝應用套件 | 建立應用套件

顯示 40 個項目中的 1-40 個

篩選器

Name	資料夾名稱	版本	更新檢查
Eventgen-PA	Eventgen-PA		Yes
SA-Eventgen	SA-Eventgen	6.3.4	Yes
Graphviz	SA-Graphviz	1.2	Yes
Splunk App for Web Analytics	SplunkAppForWebAnalytics	2.1.0	Yes
SplunkForwarder	SplunkForwarder		Yes
SplunkLightForwarder	SplunkLightForwarder		Yes
Splunk Essentials For Application Analytics	Splunk_Essentials_For_Application_Analytics	1.1.6	Yes
Splunk Essentials For Business Analytics	Splunk_Essentials_For_Business_Analytics	1.1.1	Yes
Splunk Add-on for AWS	Splunk_TA_aws	4.6.0	Yes
Fortinet Fortigate Add-on for Splunk	Splunk_TA_fortinet_fortigate	1.6.0	Yes
Splunk Add-on for Unix and Linux	Splunk_TA_nix	6.0.2	Yes
Palo Alto Networks Add-on	Splunk_TA_paloalto	6.1.1	Yes
Palo Alto Networks	SplunkforPaloAltoNetworks	6.1.1	Yes
Microsoft Sysmon Add-on	TA-microsoft-sysmon	8.0.0 | 更新為	Yes

```
/opt/splunk/etc/apps ls -al
total 16
drwx------@ 44 jack  staff  1408  4 18 17:24 .
drwxr-xr-x@ 38 jack  staff  1216  4 18 11:33 ..
-rw-r--r--@  1 jack  staff  6148  4 15 10:48 .DS_Store
drwxr-xr-x   7 jack  staff   224  4 15 12:28 Eventgen-PA
drwxr-xr-x  10 jack  staff   320  4 15 10:51 SA-Eventgen
drwx------   8 jack  staff   256  4 17 12:07 SA-Graphviz
drwx------  13 jack  staff   416  4 17 17:20 SplunkAppForWebAnalytics
drwxr-xr-x@  4 jack  staff   128  2  6 10:57 SplunkForwarder
drwxr-xr-x@  4 jack  staff   128  2  6 10:57 SplunkLightForwarder
drwxr-xr-x  10 jack  staff   320  4 17 17:11 Splunk_Essentials_For_Application_Analytics
drwxr-xr-x  10 jack  staff   320  4 17 17:13 Splunk_Essentials_For_Business_Analytics
drwx------  14 jack  staff   448  4 17 14:57 Splunk_TA_aws
drwxrwxr-x  10 jack  staff   320  4  9 14:38 Splunk_TA_fortinet_fortigate
drwx------  12 jack  staff   384  3 26 16:33 Splunk_TA_nix
drwxrwxr-x  15 jack  staff   480  4 15 10:44 Splunk_TA_paloalto
drwxrwxr-x  12 jack  staff   384  4 16 10:15 SplunkforPaloAltoNetworks
drwxr-xr-x   8 jack  staff   256  2 25 09:24 TA-microsoft-sysmon
drwxr-xr-x@  8 jack  staff   256  3 26 12:29 alert_logevent
drwxr-xr-x@  7 jack  staff   224  2  6 10:57 alert_webhook
drwxr-xr-x@  4 jack  staff   128  2  6 10:57 appsbrowser
drwxr-xr-x   8 jack  staff   256  4 17 12:13 carousel-viz
drwx------   2 jack  staff    64  3 26 13:53 default
drwxr-xr-x   9 jack  staff   288  4 17 12:13 event-timeline-viz
```

使用Splunk

Splunk 重要專有名詞說明

程式驅動 code-driven

- 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) 擷取出欄位 (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

Splunk Web介面之管理員：設定Data Input

- Setting up inputs in manager is easy
- Useful for learning inputs and their settings
- Not typically used for setting production inputs, but can be used to create an example inputs.conf

資料輸入 的 類別 – All OS’ s

程式驅動 code-driven

- 檔案和目錄（Files & directories）- Splunk monitors text-based log files
- 網路輸入（TCP and UDP）- Splunk listens on a specified port for data feeds
- 指令碼（Scripts）- Splunk runs a script and indexes the output
- HTTP 事件收集器（HTTP Event Collector）

資料輸入

設定來自檔案與目錄、網路連接埠和指令式輸入的資料輸入。設定來自檔案與目錄、網路連接埠和指令式輸入的資料輸入。若您希望設定兩 Splunk 執行個體間的轉送與接收，請前往轉送與接收。

本機輸入

類型	輸入	動作
檔案與目錄 檢索本機檔案，或監控整個目錄。	15	+ 新增
HTTP 事件記錄器 透過 HTTP 或 HTTPS 接收資料	0	+ 新增
TCP 在 TCP 連接埠上監聽傳入資料，如系統記錄。	0	+ 新增
UDP 在 UDP 連接埠上監聽傳入資料，如系統記錄。	0	+ 新增
指令碼 執行自訂指令碼以收集或產生更多資料。	36	+ 新增
Aperture	0	+ 新增
AutoFocus Export	0	+ 新增
AWS Billing Collect and index billing report of AWS in CSV format located in AWS S3 bucket.	0	+ 新增
AWS Billing (Cost And Usage Report)	0	+ 新增
AWS CloudTrail Collect and index log files produced by AWS CloudTrail. CloudTrail logging must be enabled and published to SNS topics and an SQS queue.	0	+ 新增

指定 資料輸入的 檔案和目錄

選擇 輸入的 檔案 或 目錄 位置 => Source

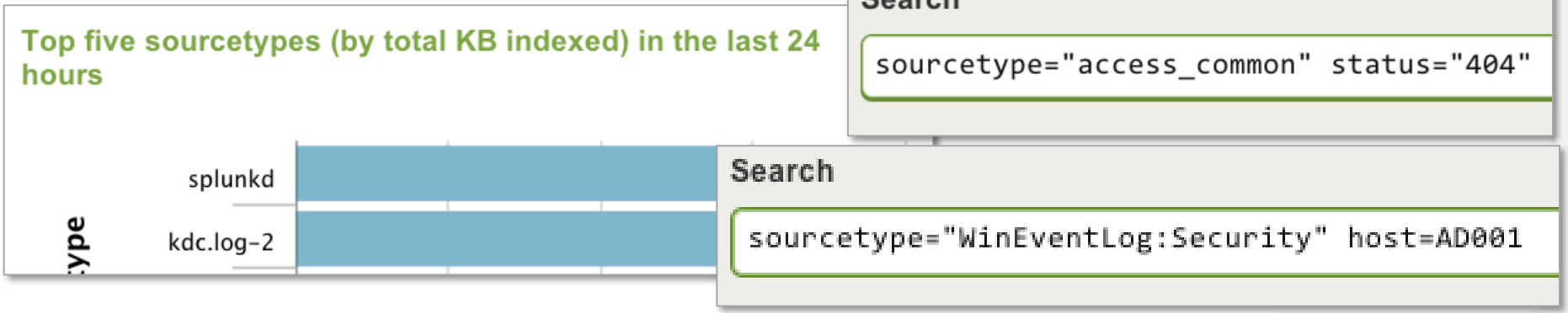
- Specify a file or directory for ongoing monitoring
- Upload a copy of a file
  - Useful for testing and development

選擇 資料輸入的 指定主機 => host

- Specify a constant value if all monitored files in an input are from the same host

選擇 資料輸入的 來源類型 => sourcetype

- Sourcetype is Splunk’ s way of identifying the type of data
- Default and custom data processing during indexing relies heavily on sourcetype
- Also used heavily in searches, reports, dashboards, Apps -- basically the rest of Splunk as well!



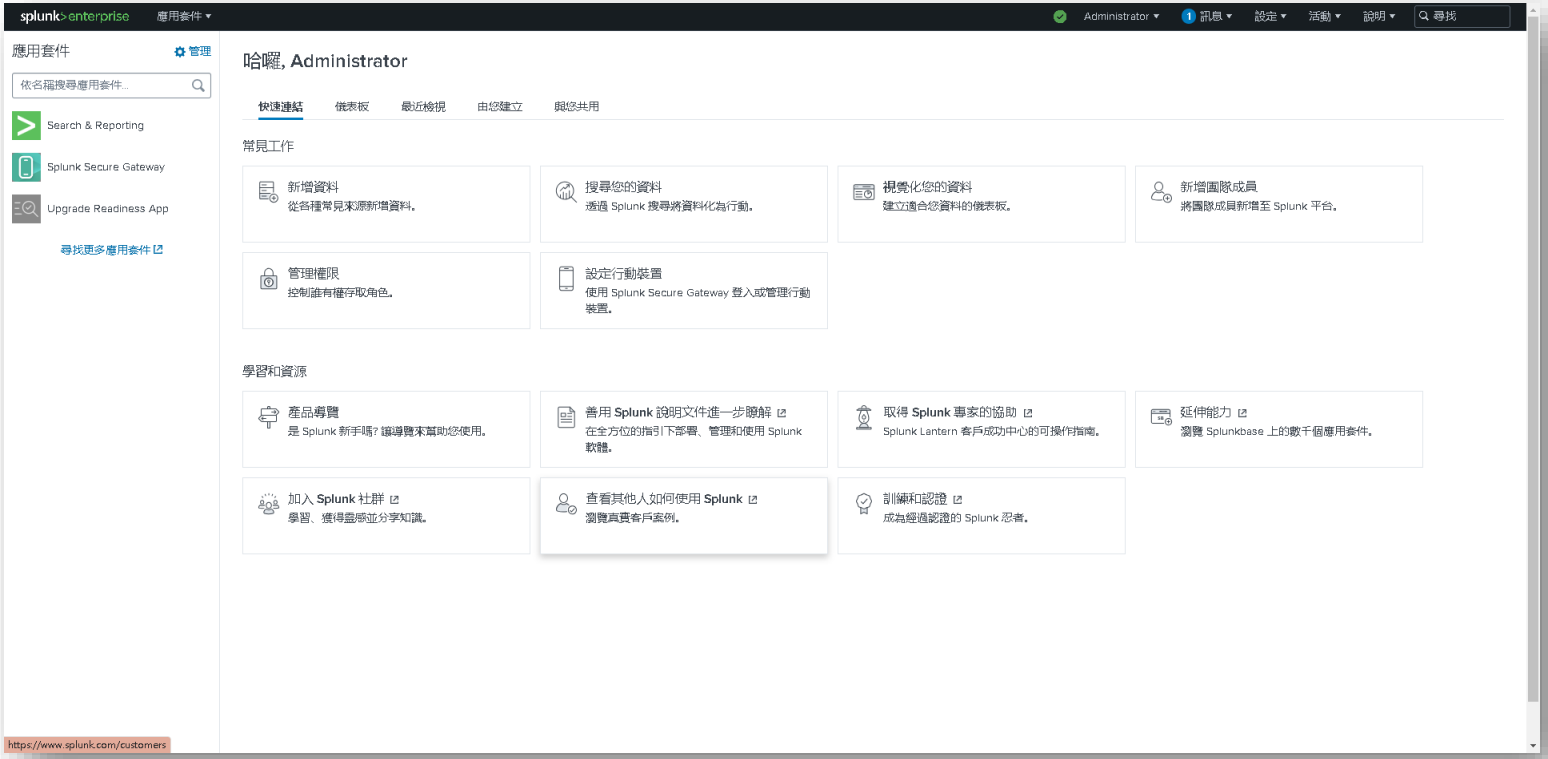
預設可辨識的來源類型，其他可透過下載App、或自行設定

- http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes

Category	Source type(s)
Application servers	log4j, log4php, weblogic_stdout, websphere_activity, websphere_core, websphere_trlog
Databases	mysqld, mysqld_error, mysqld_bin
E-mail	exim_main, exim_reject, postfix_syslog, sendmail_syslog, procmail
Operating systems	linux_messages_syslog, linux_secure, linux_audit, linux_bootlog, anaconda, anaconda_syslog, osx_asl, osx_crashreporter, osx_crash_log, osx_install, osx_secure, osx_daily, osx_weekly, osx_monthly, osx_window_server, windows_snare_syslog, dmesg, ftp, ssl_error, syslog, sar, rpmpkgs
Network	novell_groupwise, tcp
Printers	cups_access, cups_error, spooler
Routers and firewalls	cisco_cdr, cisco_syslog, clavister
VoIP	asterisk_cdr, asterisk_event, asterisk_messages, asterisk_queue
Webservers	access_combined, access_combined_wcookie, access_common, apache_error, iis
Miscellaneous	snort

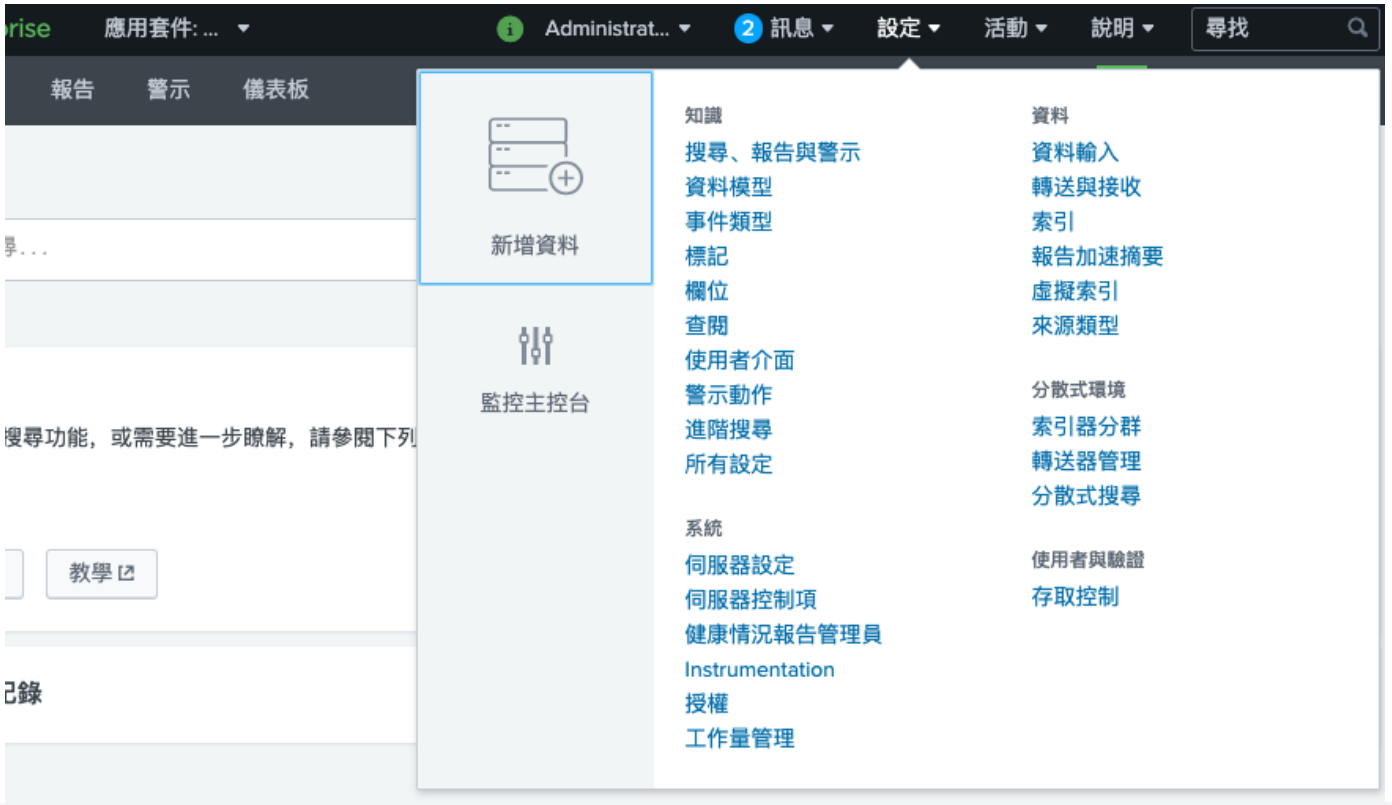
Splunk 登入的首頁

程式驅動 code-driven

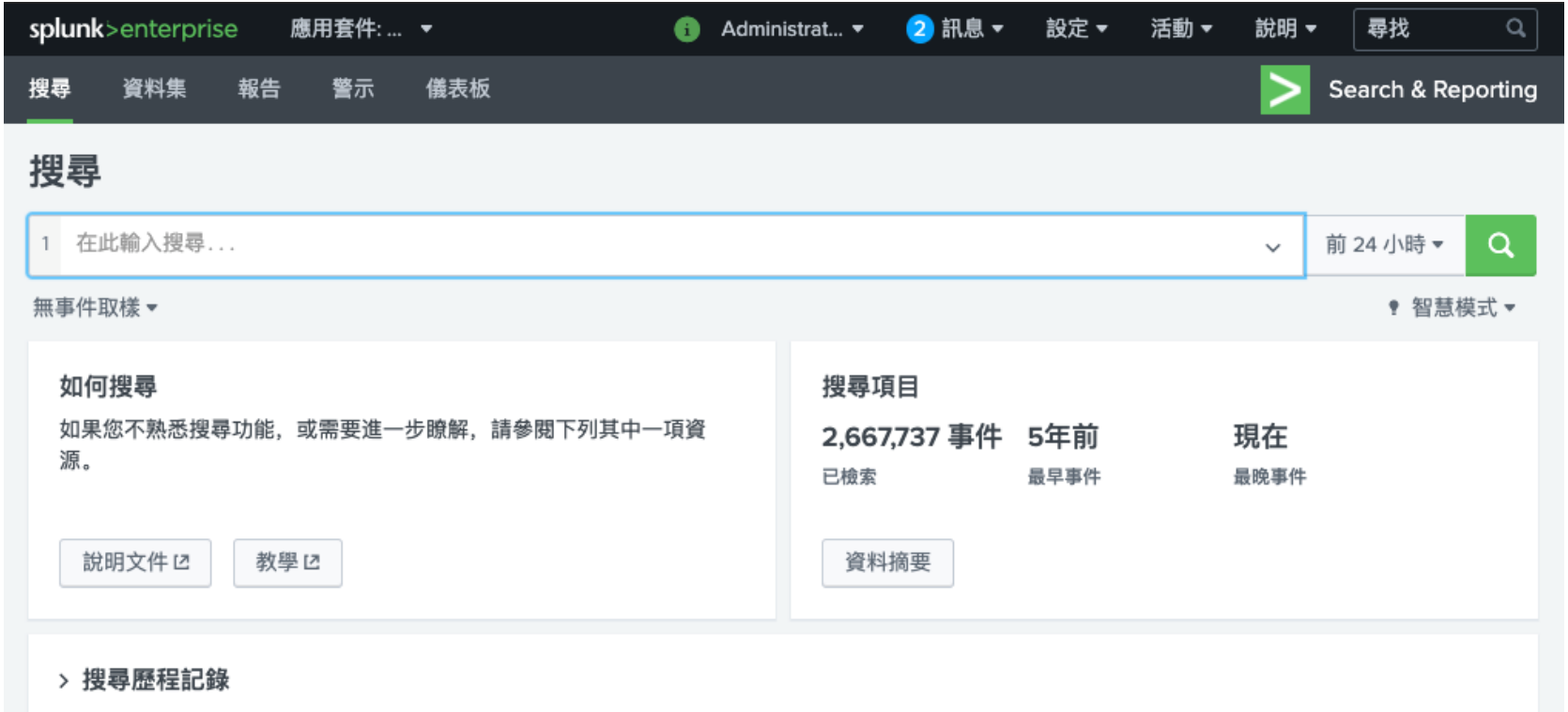


基本 搜尋使用套件（Search App）

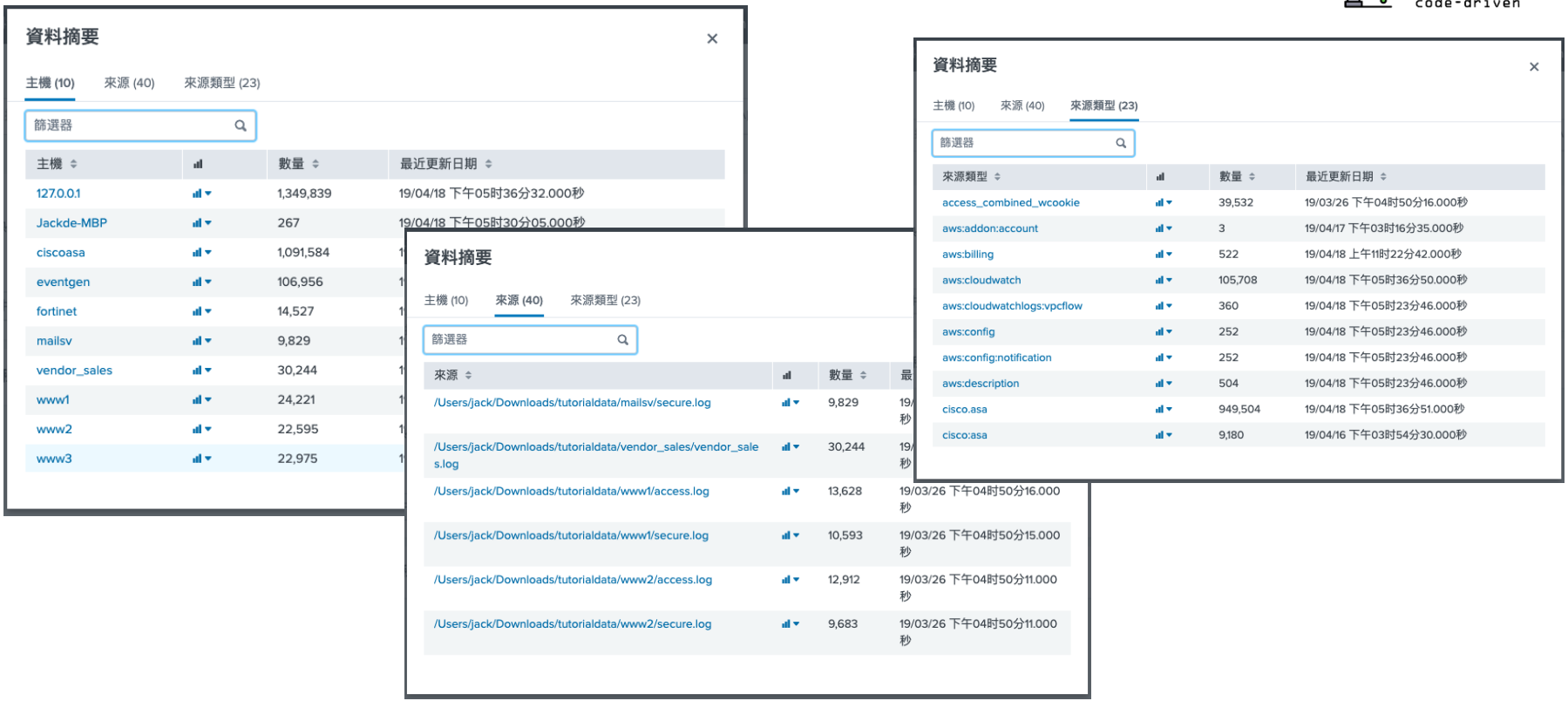
設定的管理介面：知識、資料、系統管理、存取控制



開始使用 Search & Report 應用套件

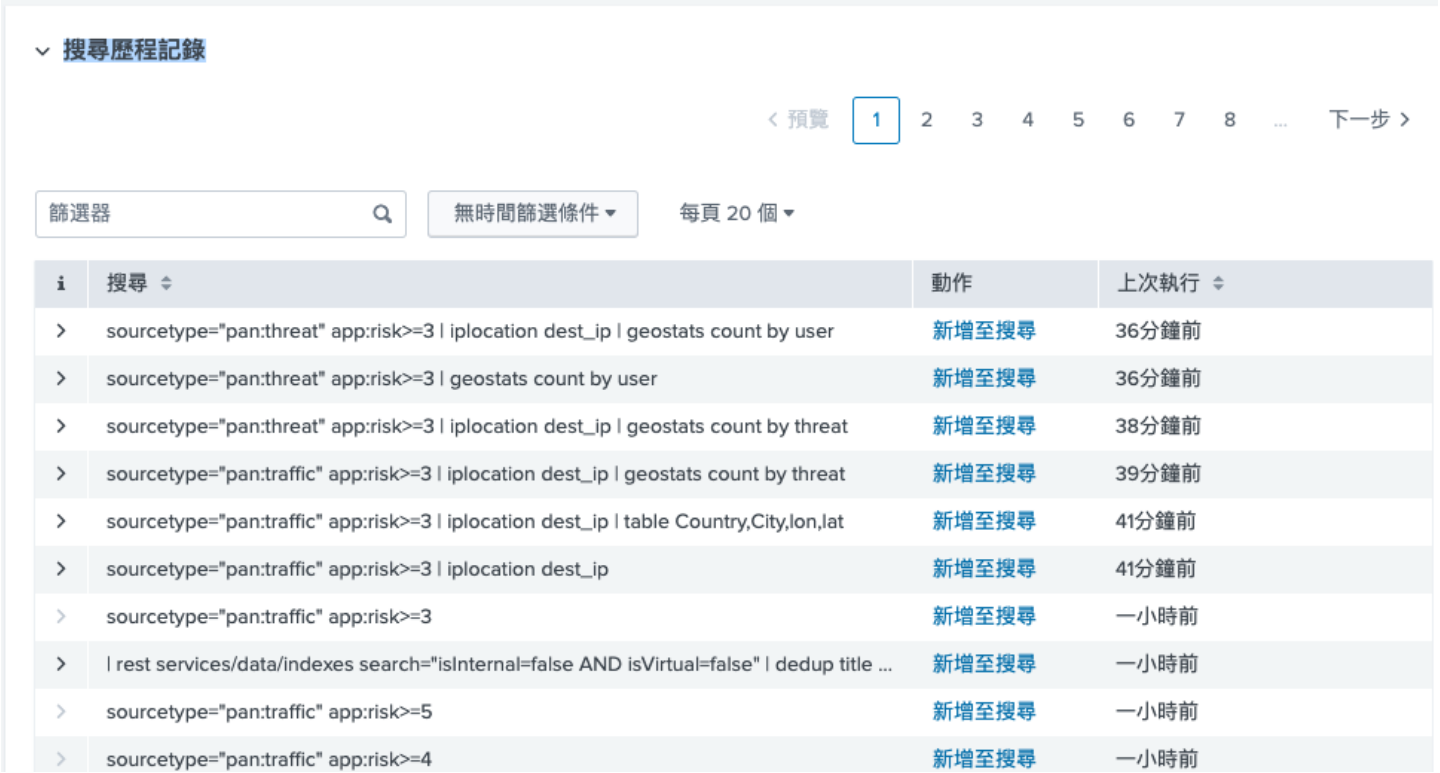


資料摘要 說明


資料摘要
主機 (10)
來源 (40)
來源類型 (23)
篩選器
主機
數量
最近更新日期
127.0.0.1 1,349,839 19/04/18 下午05時36分32.000秒
Jackde-MBP 267 19/04/18 下午05時30分05.000秒
ciscoasa 1,091,584
eventgen 106,956
fortinet 14,527
mailsv 9,829
vendor_sales 30,244
www1 24,221
www2 22,595
www3 22,975
資料摘要
主機 (10)
來源 (40)
來源類型 (23)
篩選器
來源
數量
/Users/jack/Downloads/tutorialdata/mailsv/secure.log 9,829
/Users/jack/Downloads/tutorialdata/vendor_sales/vendor_sales.log 30,244
/Users/jack/Downloads/tutorialdata/www1/access.log 13,628 19/03/26 下午04時50分16.000秒
/Users/jack/Downloads/tutorialdata/www1/secure.log 10,593 19/03/26 下午04時50分15.000秒
/Users/jack/Downloads/tutorialdata/www2/access.log 12,912 19/03/26 下午04時50分11.000秒
/Users/jack/Downloads/tutorialdata/www2/secure.log 9,683 19/03/26 下午04時50分11.000秒
資料摘要
主機 (10)
來源 (40)
來源類型 (23)
篩選器
來源類型
數量
最近更新日期
access_combined_wcookie 39,532 19/03/26 下午04時50分16.000秒
aws:addon:account 3 19/04/17 下午03時16分35.000秒
aws:billing 522 19/04/18 上午11時22分42.000秒
aws:cloudwatch 105,708 19/04/18 下午05時36分50.000秒
aws:cloudwatchlogs:vpcflow 360 19/04/18 下午05時23分46.000秒
aws:config 252 19/04/18 下午05時23分46.000秒
aws:config:notification 252 19/04/18 下午05時23分46.000秒
aws:description 504 19/04/18 下午05時23分46.000秒
cisco.asa 949,504 19/04/18 下午05時36分51.000秒
cisco:asa 9,180 19/04/16 下午03時54分30.000秒

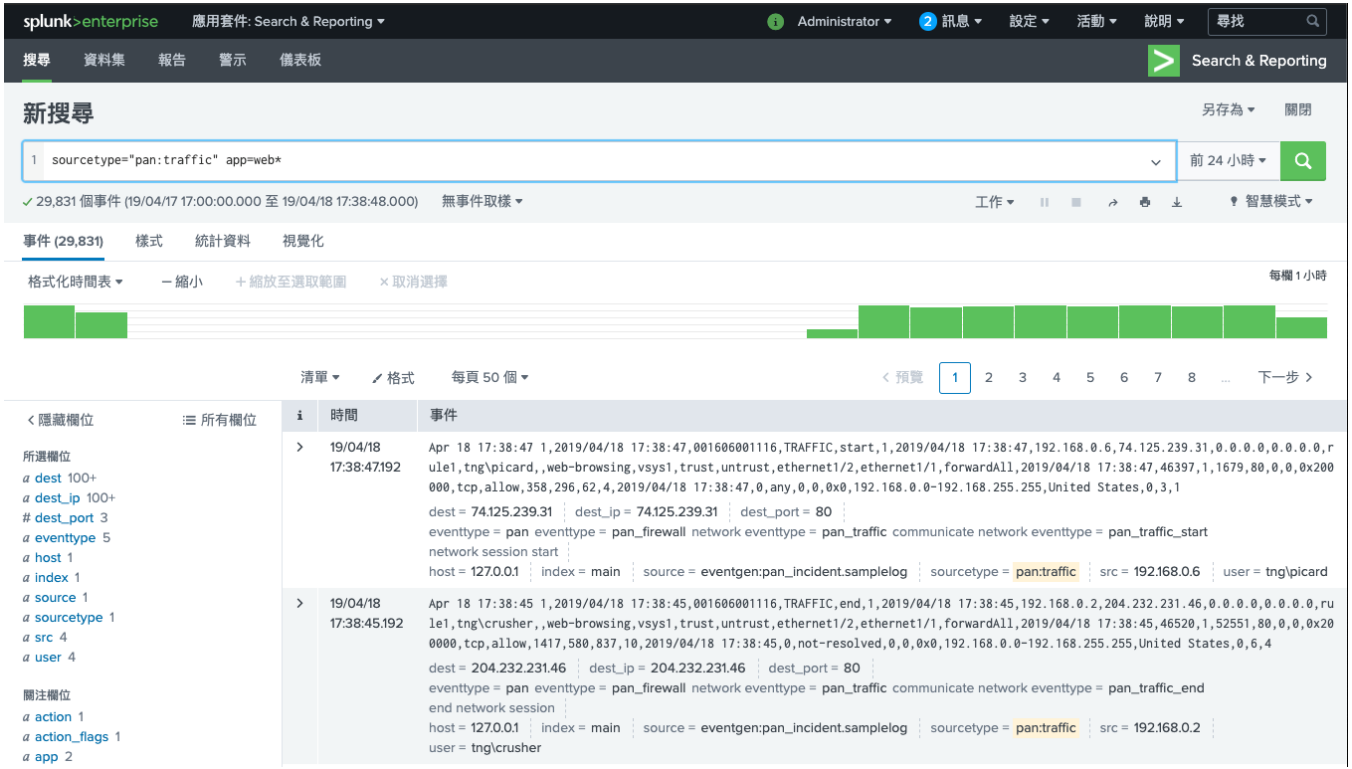
搜尋歷程記錄

程式驅動 code-driven



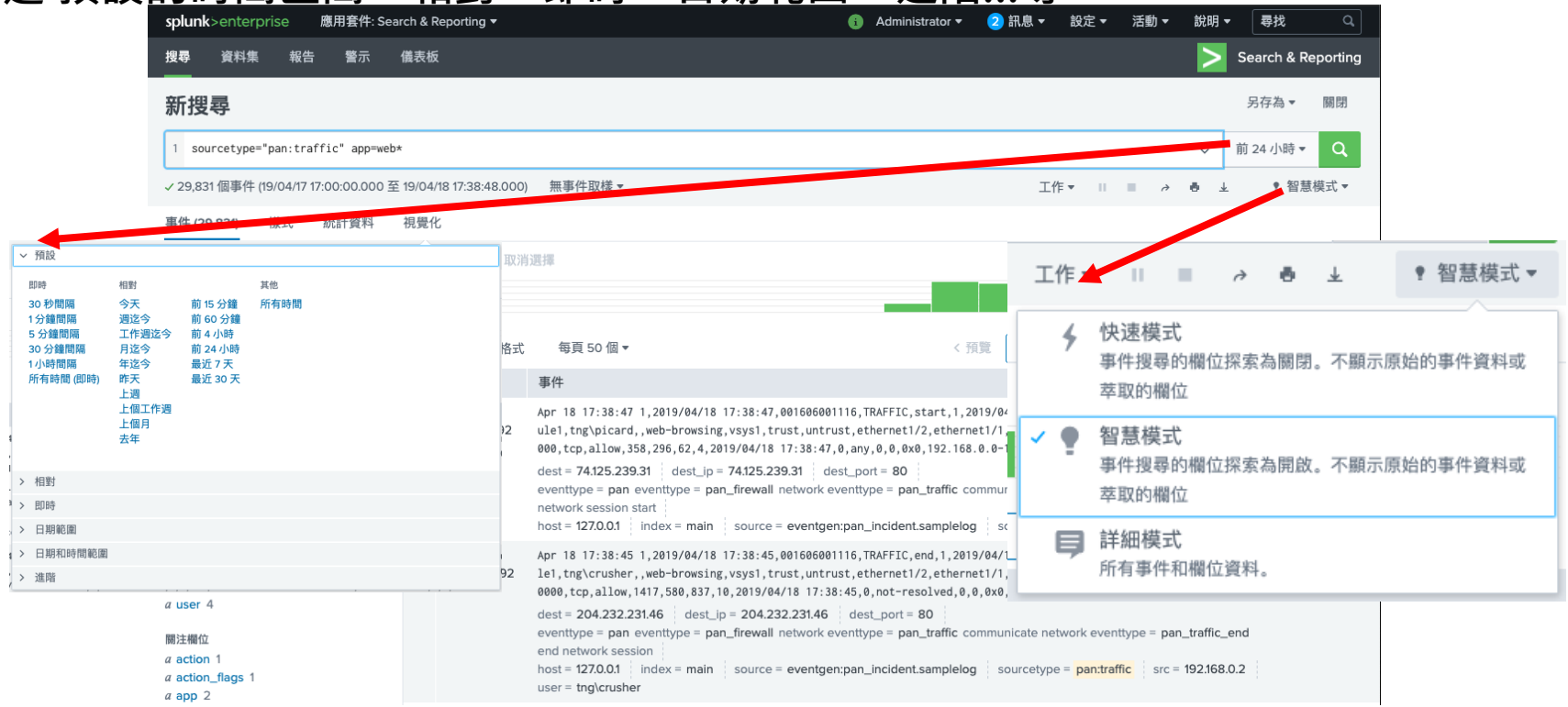
	搜尋	動作	上次執行
>	sourcetype="pan:threat" app:risk>=3 | iplocation dest_ip | geostats count by user	新增至搜尋	36分鐘前
>	sourcetype="pan:threat" app:risk>=3 | geostats count by user	新增至搜尋	36分鐘前
>	sourcetype="pan:threat" app:risk>=3 | iplocation dest_ip | geostats count by threat	新增至搜尋	38分鐘前
>	sourcetype="pan:traffic" app:risk>=3 | iplocation dest_ip | geostats count by threat	新增至搜尋	39分鐘前
>	sourcetype="pan:traffic" app:risk>=3 | iplocation dest_ip | table Country,City,lon,lat	新增至搜尋	41分鐘前
>	sourcetype="pan:traffic" app:risk>=3 | iplocation dest_ip	新增至搜尋	41分鐘前
>	sourcetype="pan:traffic" app:risk>=3	新增至搜尋	一小時前
>	| rest services/data/indexes search="isInternal=false AND isVirtual=false" | dedup title ...	新增至搜尋	一小時前
>	sourcetype="pan:traffic" app:risk>=5	新增至搜尋	一小時前
>	sourcetype="pan:traffic" app:risk>=4	新增至搜尋	一小時前

Search 的結果呈現

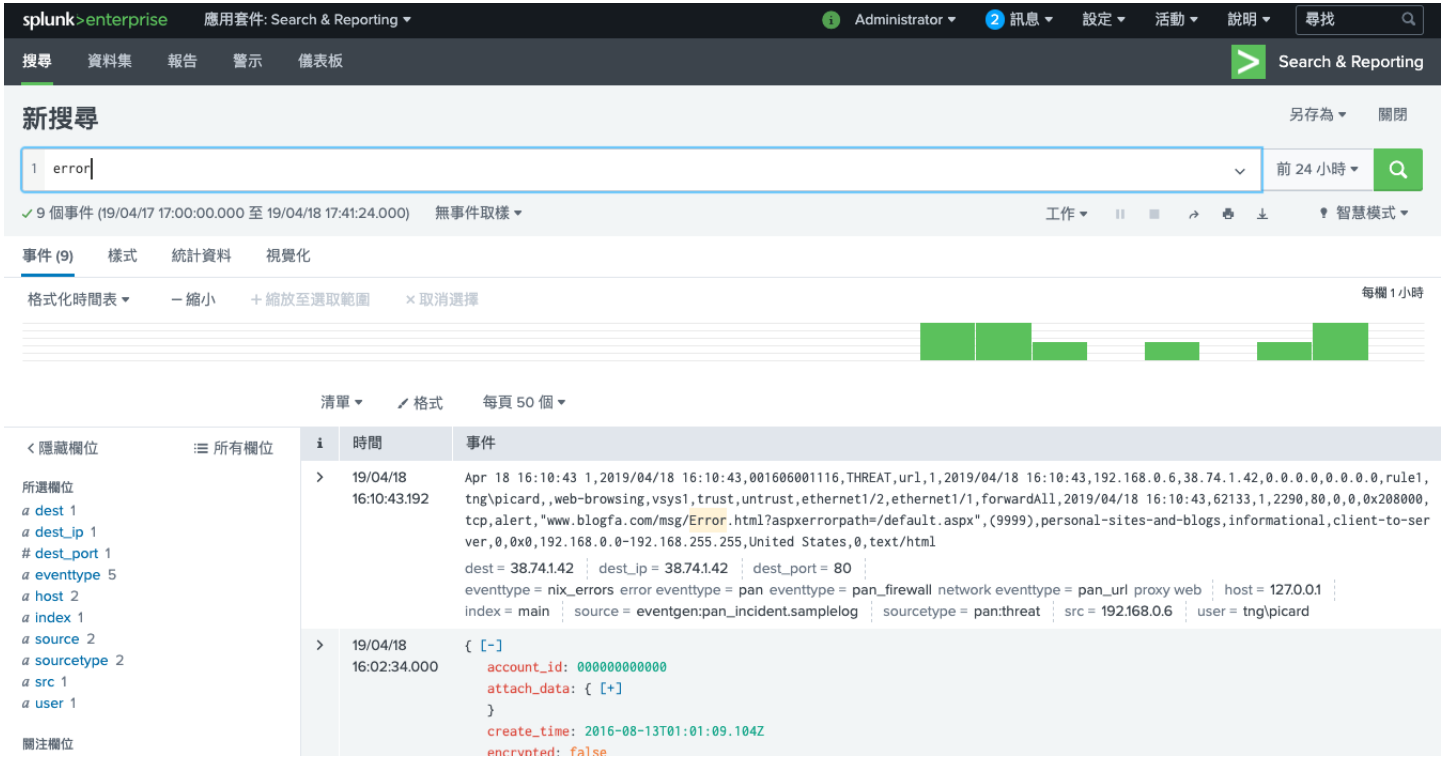


時間範圍挑選器、搜尋模式

可選 預設的時間區間、相對、即時、日期範圍、進階...等



以關鍵字搜尋，可搭配 OR, NOT，可點選 TimeLine 縮小時間
例如： error



資料結果頁籤：事件、樣式、統計資料、視覺化

程式驅動 code-driven

splunk>enterprise 應用套件: Search & Reporting

搜尋 資料集 報告 警示 儀表板

新搜尋

```
1 sourcetype="pan:traffic" app=web*
2 | timechart span=5m sum(bytes) by user
```

✓ 29,972 個事件 (19/04/17 17:00:00.000 至 19/04/18 17:42:22.000) 無事件取樣

事件 樣式 統計資料 (297) 視覺化

每頁 20 個 格式 預覽

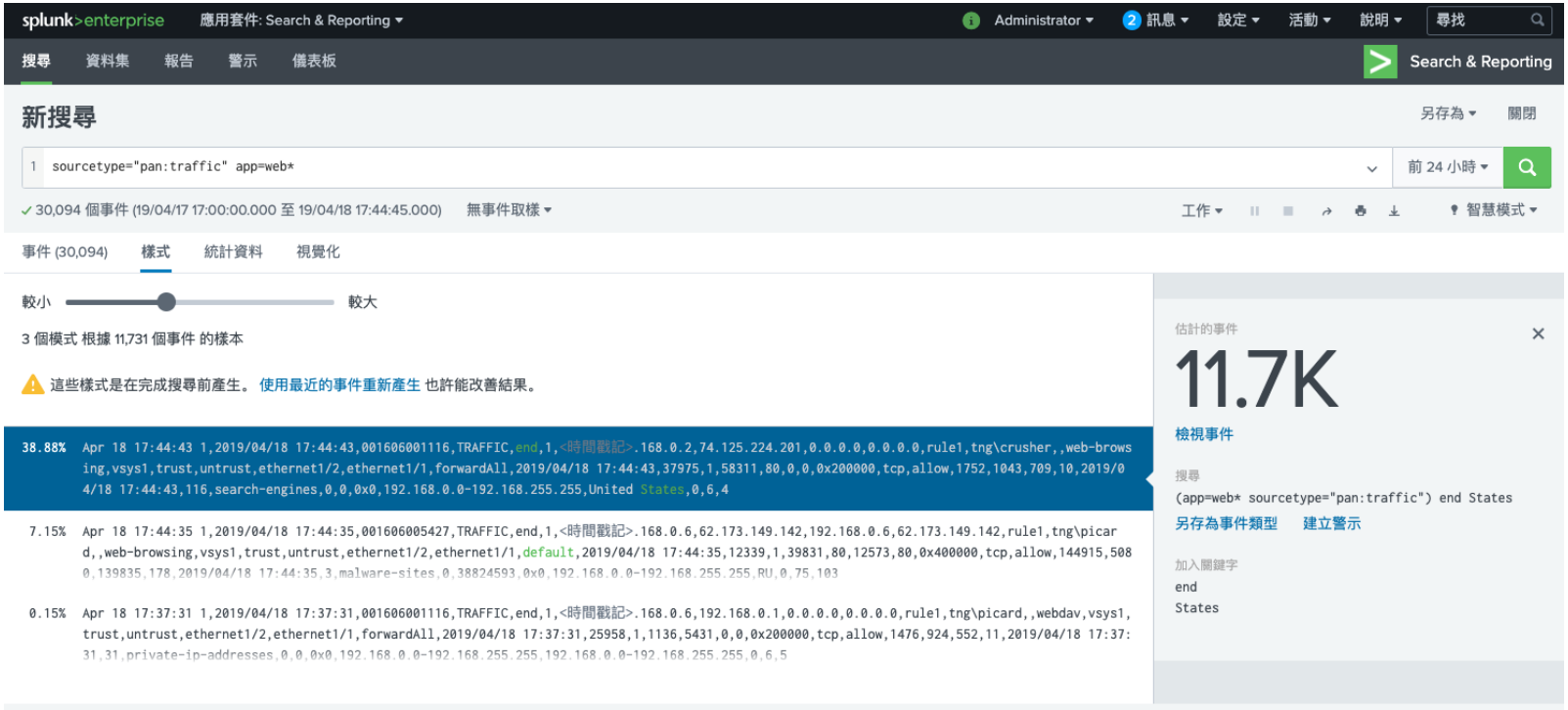
_time	counselor	tng\cr
2019/04/17 17:00:00	187986	
2019/04/17 17:05:00	79080	
2019/04/17 17:10:00	123090	
2019/04/17 17:15:00	327393	
2019/04/17 17:20:00	369821	
2019/04/17 17:25:00	41163	
2019/04/17 17:30:00	293172	
2019/04/17 17:35:00	379140	

1. 搜尋 的事件結果

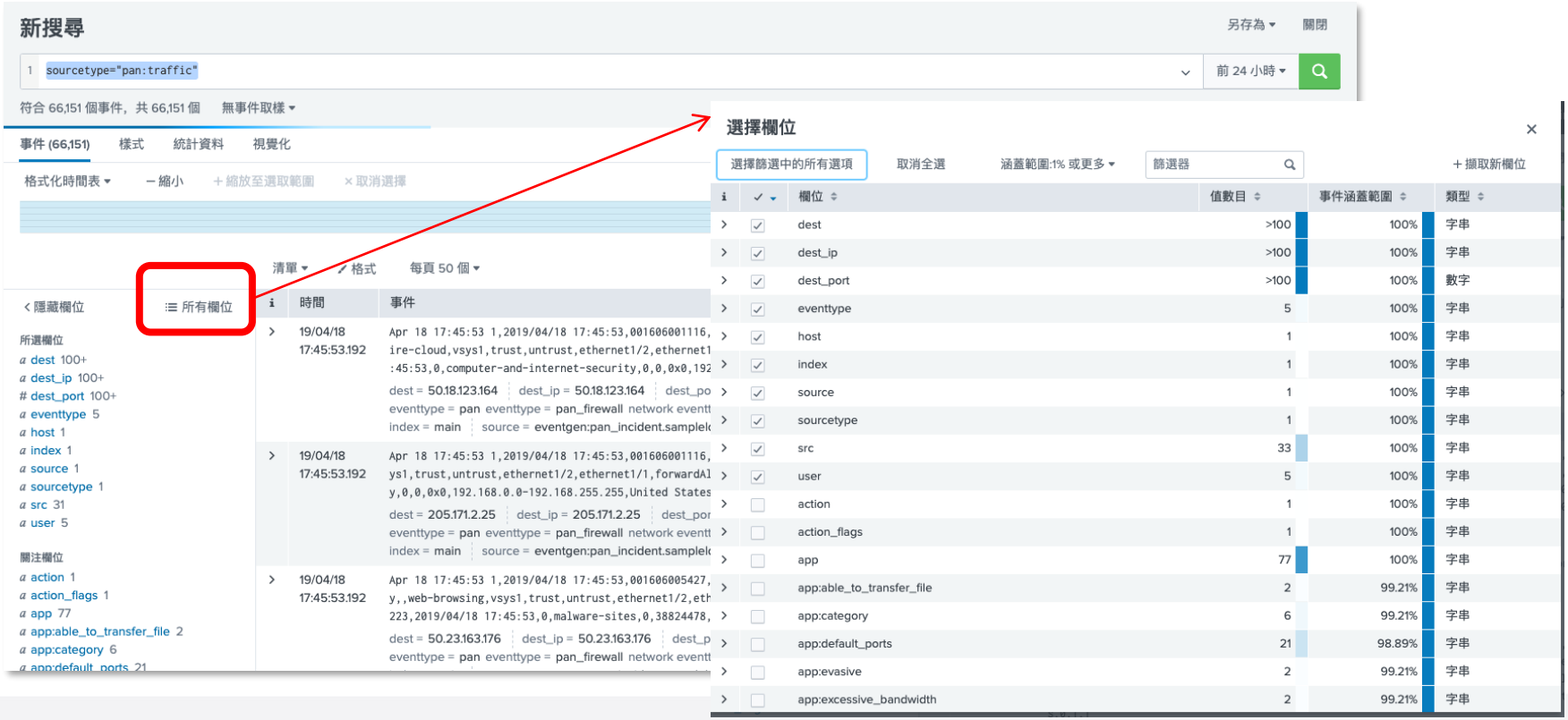
2. 統計分析

3. 視覺化

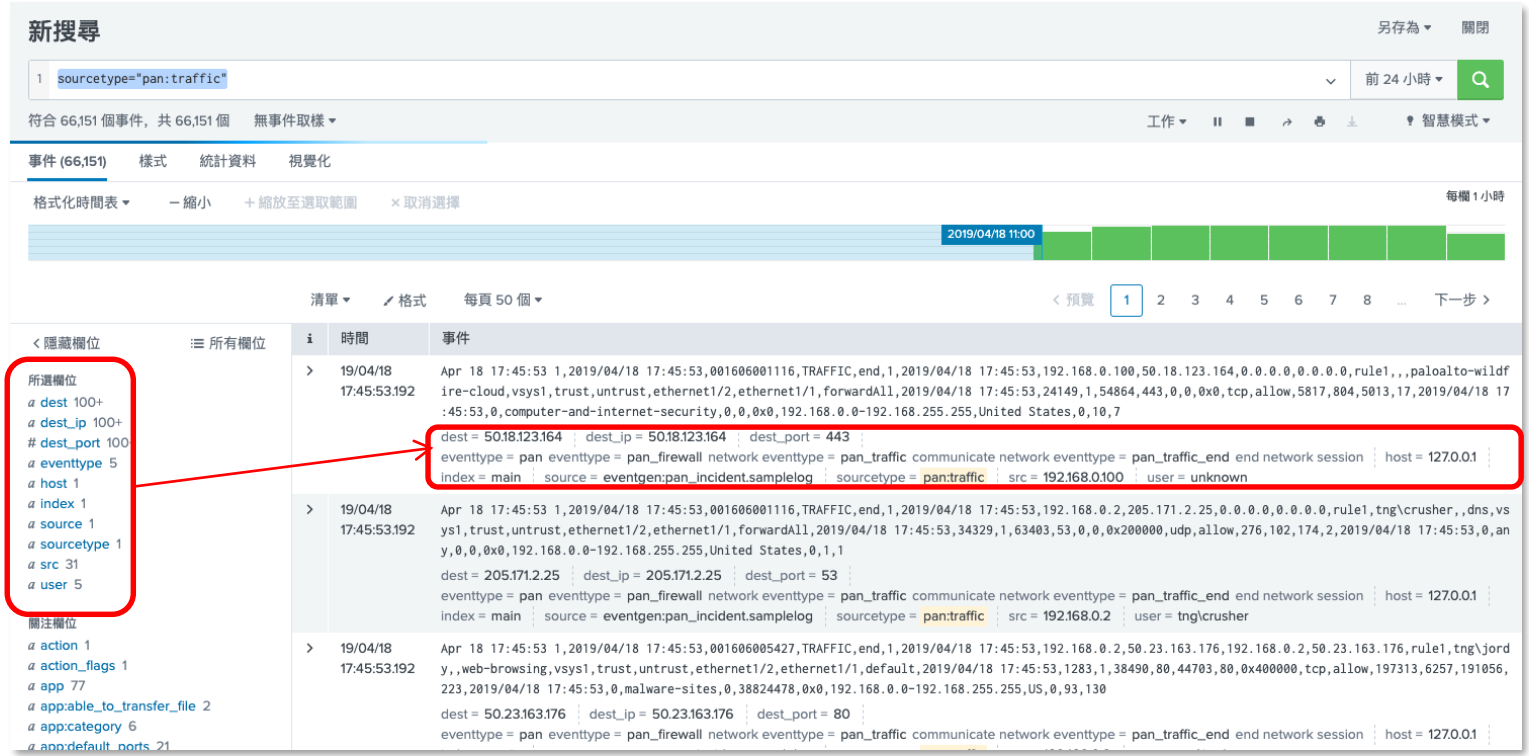
資料結果頁籤：對資料做初步的 Pattern分析



欄位（字段）選擇顯示


新搜尋
另存為
關閉
sourcetype="pan:traffic"
前 24 小時
符合 66,151 個事件，共 66,151 個
無事件取樣
事件 (66,151)
樣式
統計資料
視覺化
格式化時間表
縮小
縮放至選取範圍
取消選擇
清單
格式
每頁 50 個
隱藏欄位
所有欄位
所選欄位
a dest 100+
a dest_ip 100+
dest_port 100+
a eventtype 5
a host 1
a index 1
a source 1
a sourcetype 1
a src 31
a user 5
關注欄位
a action 1
a action_flags 1
a app 77
a app:able_to_transfer_file 2
a app:category 6
a app:default_ports 21
時間
事件
19/04/18 17:45:53.192
選擇欄位
選擇篩選中的所有選項
取消全選
涵蓋範圍:1% 或更多
篩選器
擷取新欄位
欄位
值數目
事件涵蓋範圍
類型
dest >100 100% 字串
dest_ip >100 100% 字串
dest_port >100 100% 數字
eventtype 5 100% 字串
host 1 100% 字串
index 1 100% 字串
source 1 100% 字串
sourcetype 1 100% 字串
src 33 100% 字串
user 5 100% 字串
action 1 100% 字串
action_flags 1 100% 字串
app 77 100% 字串
app:able_to_transfer_file 2 99.21% 字串
app:category 6 99.21% 字串
app:default_ports 21 98.89% 字串
app:evasive 2 99.21% 字串
app:excessive_bandwidth 2 99.21% 字串

欄位（字段）選擇顯示

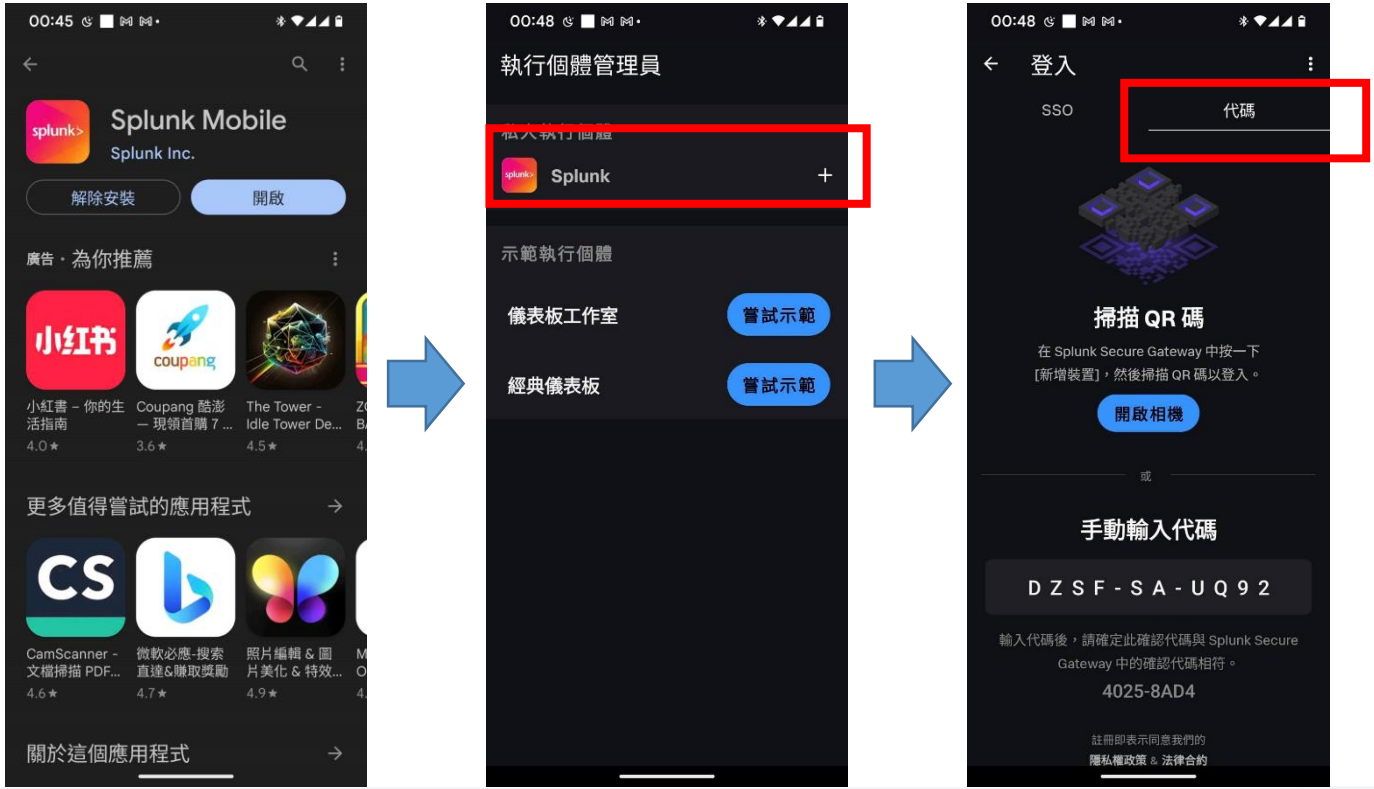

新搜尋
另存為
關閉
sourcetype="pan:traffic"
前 24 小時
符合 66,151 個事件，共 66,151 個
無事件取樣
工作
智慧模式
事件 (66,151)
樣式
統計資料
視覺化
格式化時間表
縮小
縮放至選取範圍
取消選擇
每欄 1 小時
2019/04/18 11:00
清單
格式
每頁 50 個
預覽
下一步
隱藏欄位
所有欄位
所選欄位
a dest 100+
a dest_ip 100+
dest_port 100
a eventtype 5
a host 1
a index 1
a source 1
a sourcetype 1
a src 31
a user 5
關注欄位
a action 1
a action_flags 1
a app 77
a app:able_to_transfer_file 2
a app:category 6
a app:default_ports 21
時間
事件
19/04/18 17:45:53.192
Apr 18 17:45:53 1,2019/04/18 17:45:53,001606001116,TRAFFIC,end,1,2019/04/18 17:45:53,192.168.0.100,50.18.123.164,0.0.0.0,0.0.0.0,rule1,,,paloalto-wildfire-cloud,vsys1,trust,untrust,ethernet1/2,ethernet1/1,forwardAll,2019/04/18 17:45:53,24149,1,54864,443,0,0,0x0,tcp,allow,5817,804,5013,17,2019/04/18 17:45:53,0,computer-and-internet-security,0,0,0x0,192.168.0.0-192.168.255.255,United States,0,10,7
dest = 50.18.123.164 dest_ip = 50.18.123.164 dest_port = 443
eventtype = pan eventtype = pan_firewall network eventtype = pan_traffic communicate network eventtype = pan_traffic_end end network session host = 127.0.0.1
index = main source = eventgen:pan_incident.samplelog sourcetype = pan:traffic src = 192.168.0.100 user = unknown
19/04/18 17:45:53.192
Apr 18 17:45:53 1,2019/04/18 17:45:53,001606001116,TRAFFIC,end,1,2019/04/18 17:45:53,192.168.0.2,205.171.2.25,0.0.0.0,0.0.0.0,rule1,tng\crusher,,dns,vsys1,trust,untrust,ethernet1/2,ethernet1/1,forwardAll,2019/04/18 17:45:53,34329,1,63403,53,0,0,0x200000,udp,allow,276,102,174,2,2019/04/18 17:45:53,0,any,0,0,0x0,192.168.0.0-192.168.255.255,United States,0,1,1
dest = 205.171.2.25 dest_ip = 205.171.2.25 dest_port = 53
eventtype = pan eventtype = pan_firewall network eventtype = pan_traffic communicate network eventtype = pan_traffic_end end network session host = 127.0.0.1
index = main source = eventgen:pan_incident.samplelog sourcetype = pan:traffic src = 192.168.0.2 user = tng\crusher
19/04/18 17:45:53.192
Apr 18 17:45:53 1,2019/04/18 17:45:53,001606005427,TRAFFIC,end,1,2019/04/18 17:45:53,192.168.0.2,50.23.163.176,192.168.0.2,50.23.163.176,rule1,tng\jordy,,web-browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,default,2019/04/18 17:45:53,1283,1,38490,80,44703,80,0x400000,tcp,allow,197313,6257,191056,223,2019/04/18 17:45:53,0,malware-sites,0,38824478,0x0,192.168.0.0-192.168.255.255,US,0,93,130
dest = 50.23.163.176 dest_ip = 50.23.163.176 dest_port = 80
eventtype = pan eventtype = pan_firewall network eventtype = pan_traffic communicate network eventtype = pan_traffic_end end network session host = 127.0.0.1

檢視『欄位摘要』


清單
格式
每頁 50 個
預覽
1
2
3
4
5
6
7
8
下一
隱藏欄位
所有欄位
所選欄位
a dest 100+
a dest_ip 100+
dest_port 100+
a eventtype 5
a host 1
a index 1
a source 1
a sourcetype 1
a src 33
a user 5
關注欄位
a action 1
a action_flags 1
a app 77
a app:able_to_transfer_file 2
a app:category 6
a app:default_ports 21
a app:evasive 2
時間
事件
19/04/18 17:45:53.192
Apr 18 17:45:53 1,2019/04/18 17:45:53,001606001116,TRAFFIC,end,1,2019/04/18 17:45
.168.0.100,50.18.123.164,0.0.0.0,0.0.0.0,rule1,,,paloalto-wildfire-cloud,vsys1,tr
,1,54864,443,0,0
net-security,0,0
user
5 值, 100% 的事件
已選取
是
否
報告
最高值
依時間的最高值
罕見值
具有此欄位的事件
值
數量
%
tng\crusher
68,292
72.521%
counselor
10,688
11.35%
unknown
7,762
8.243%
tng\picard
7,241
7.689%
tng\jordy
186
0.198%
sourcetype = pan:traffic
src = 192.168.0.2
user = tng\crusher

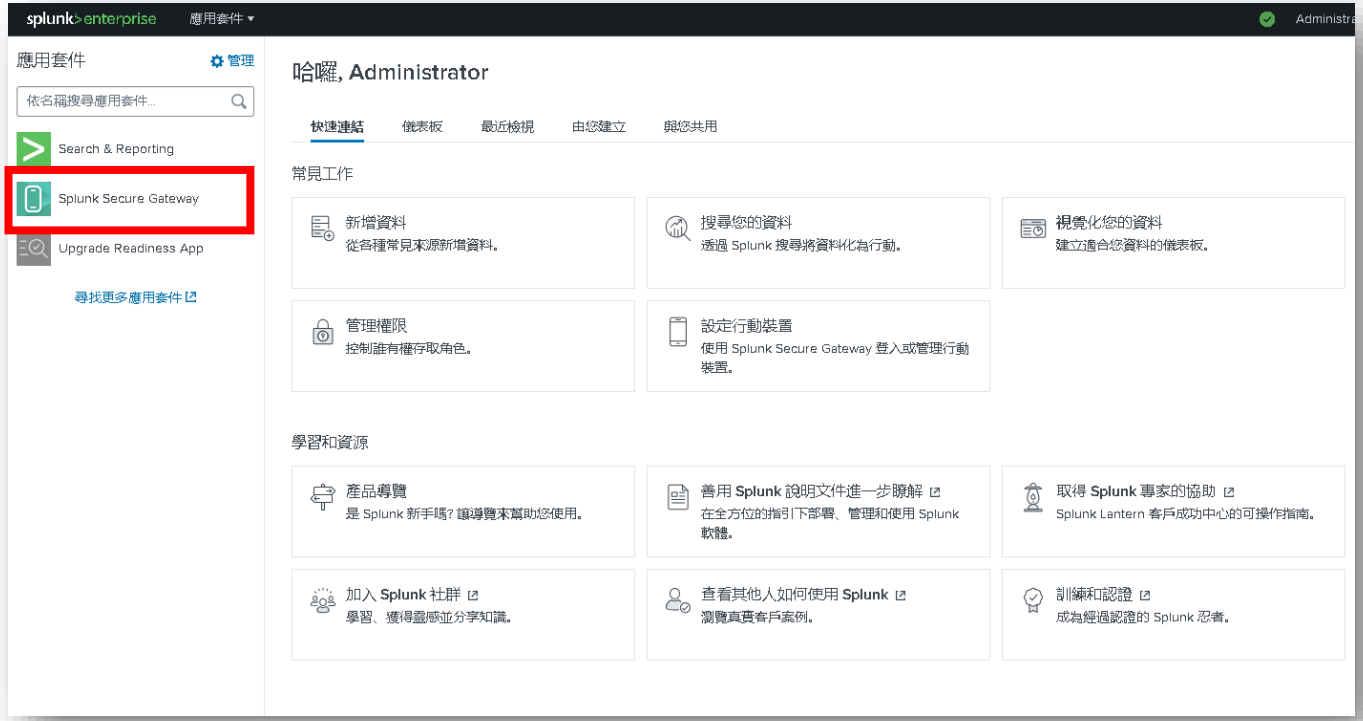
Splunk Secure Gateway

下載 Splunk Mobile

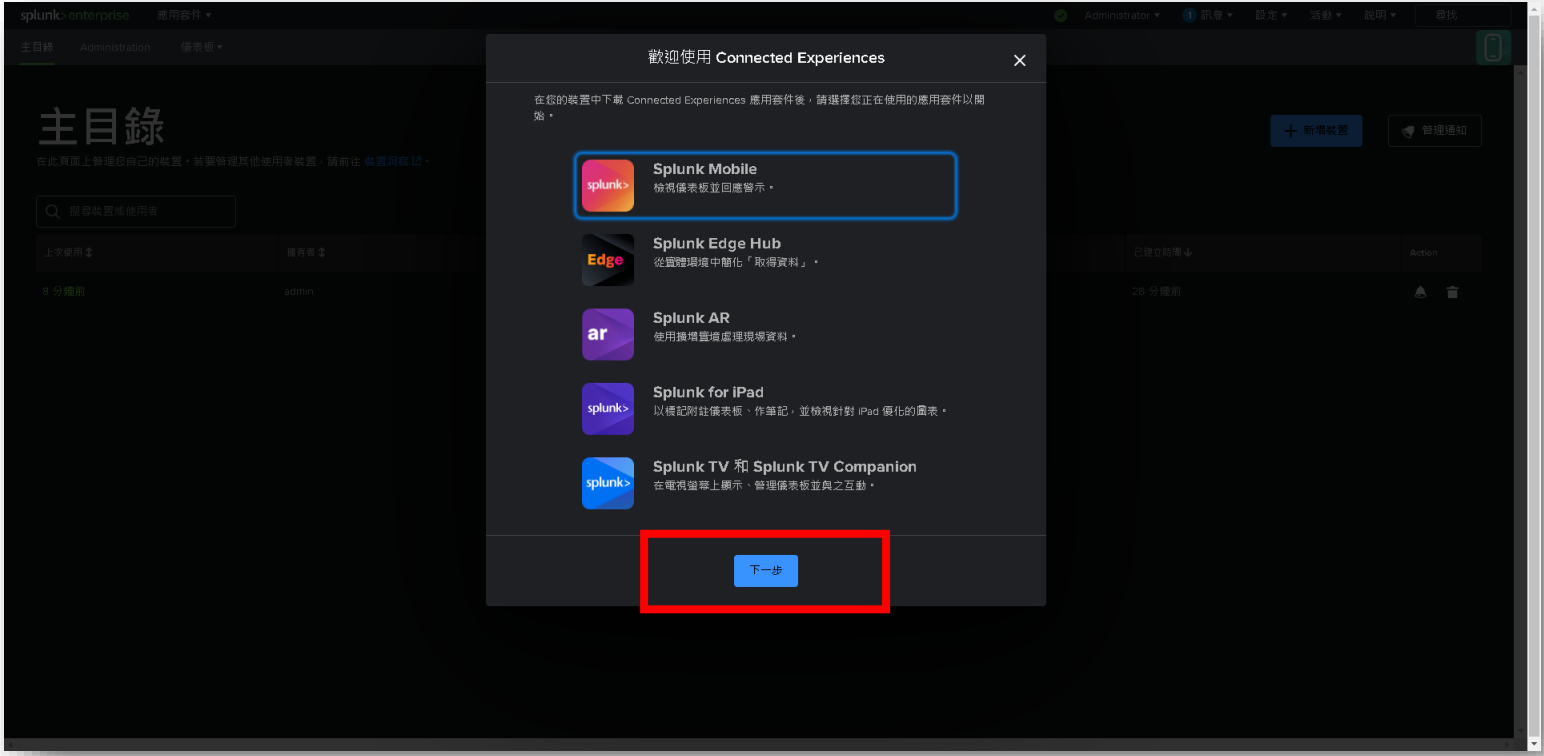


Splunk Secure Gateway

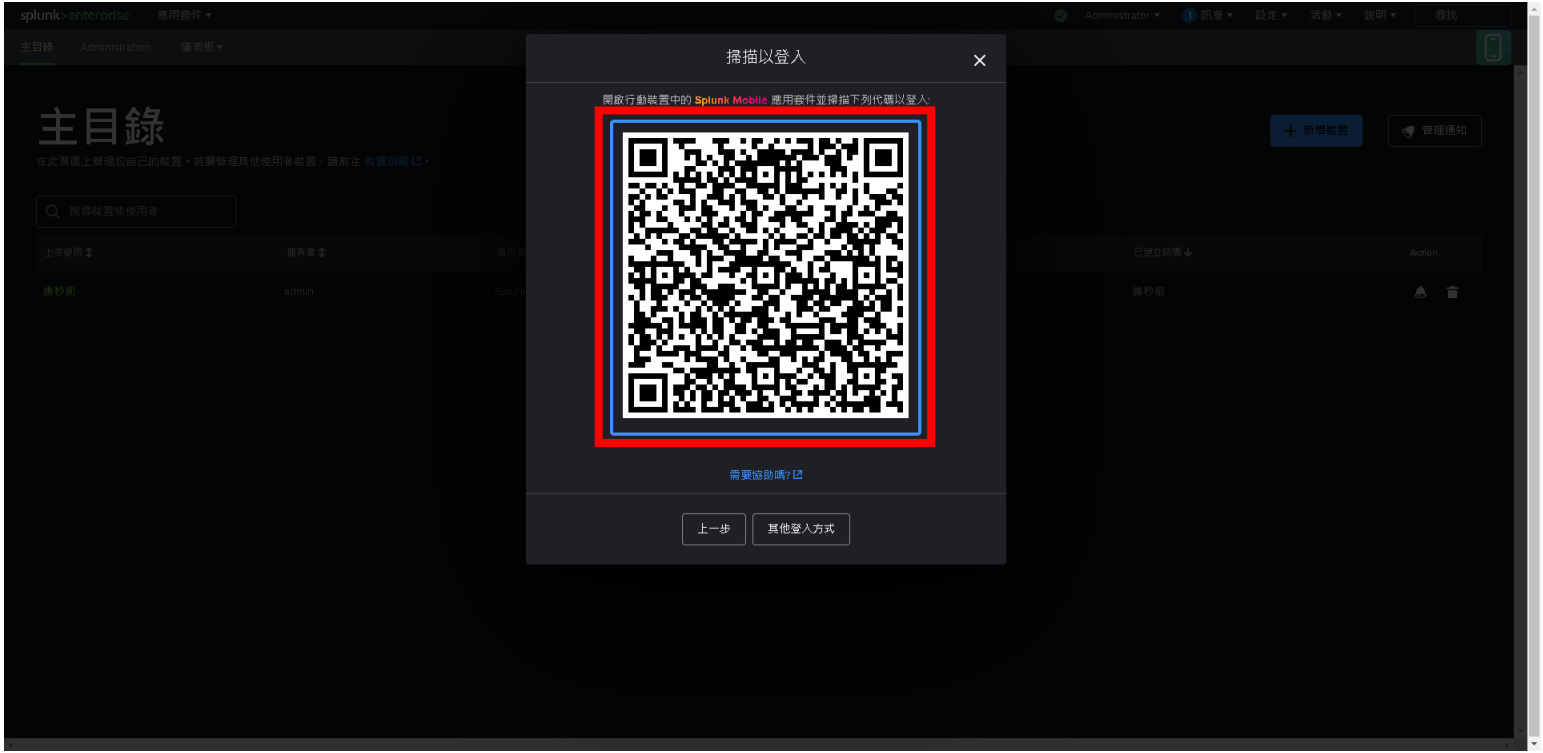
程式驅動 code-driven



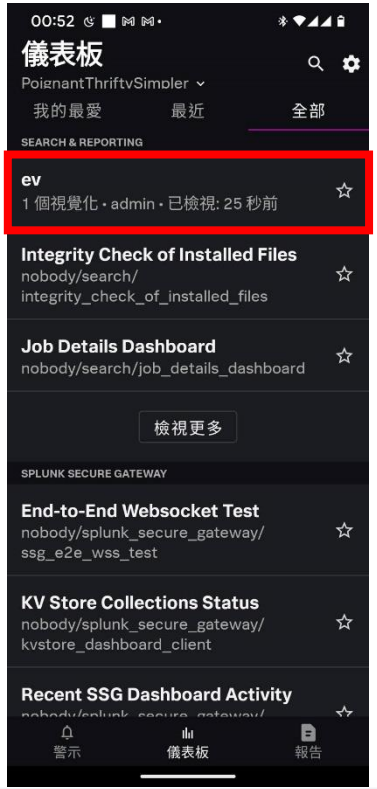
Splunk Secure Gateway

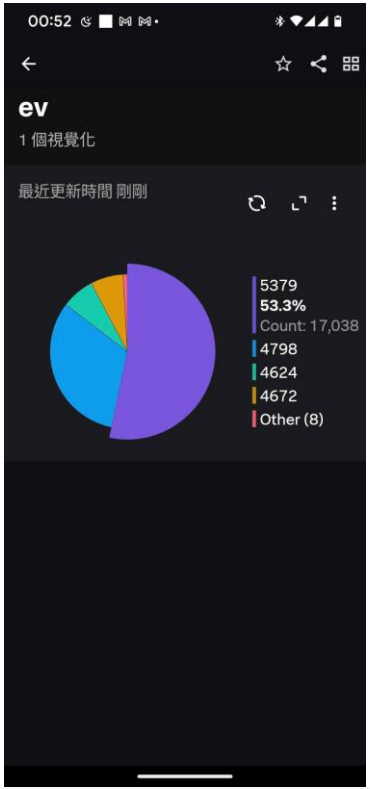


Splunk Secure Gateway



Splunk Secure Gateway





Thank you.

程式驅動

code-driven