

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



- 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

splunk

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



顧客ID

訂單ID

產品ID

ORDER,2014-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

訂單處理

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.



中介軟體

Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: 訂單ID Could not create pool 顧客ID The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Oracle JDBC 無法連接至數據庫



互動式語音
回應

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192933): Event 20111, CTI Num:ServID:Type 0:19:9 App 0 ANI T7998#1, DNIS 5555685981 SerID 40489a07-7f6e-4251-801a- 等候延誤 451.16

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

CUSTID 10098213 顧客ID

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092



Twitter (推特)

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:"http://dallascowboys.com/",location:{displayname:"Dallas, TX",objectType:"person",preferredUsername:"B0vsF@n80",statusesCount:6072},body:"Can't buy this device from 趕快告訴你的朋友，這公司的產品和客戶服務太差了。 to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2014-05-21T16:39:40.647-0600"}

公司推特ID

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

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

無須過濾資料
合規與詐騙

商業分析

工業資料與物聯網

Splunk 巨量資料產品



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



salesforce.com



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

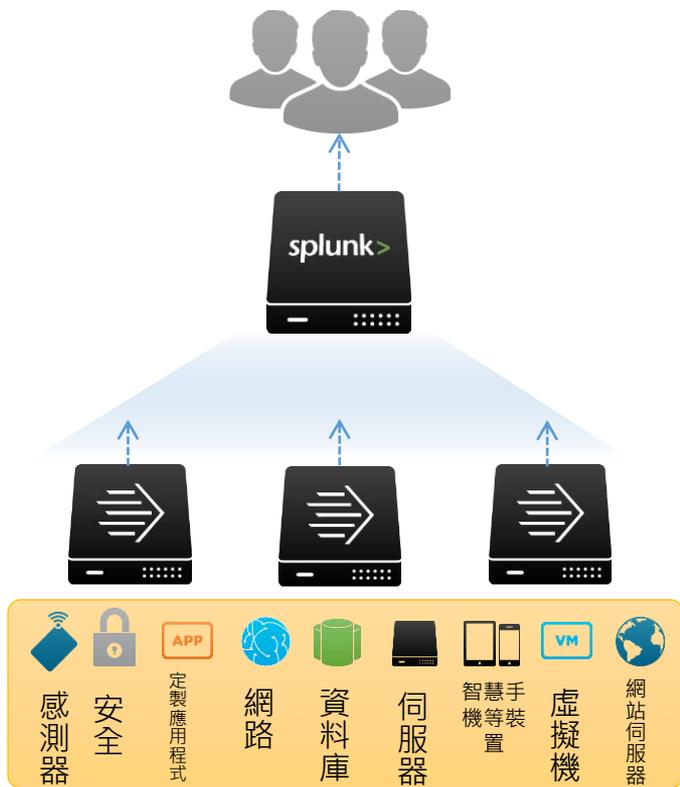


資料庫



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

企業級的擴充性、回復能力與相容性



將搜尋負載卸載至Splunk Search Head



自動平衡轉送到Splunk索引器的負載



使用任何一種組合的Splunk轉送器，傳送來自數千個伺服器的資料

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



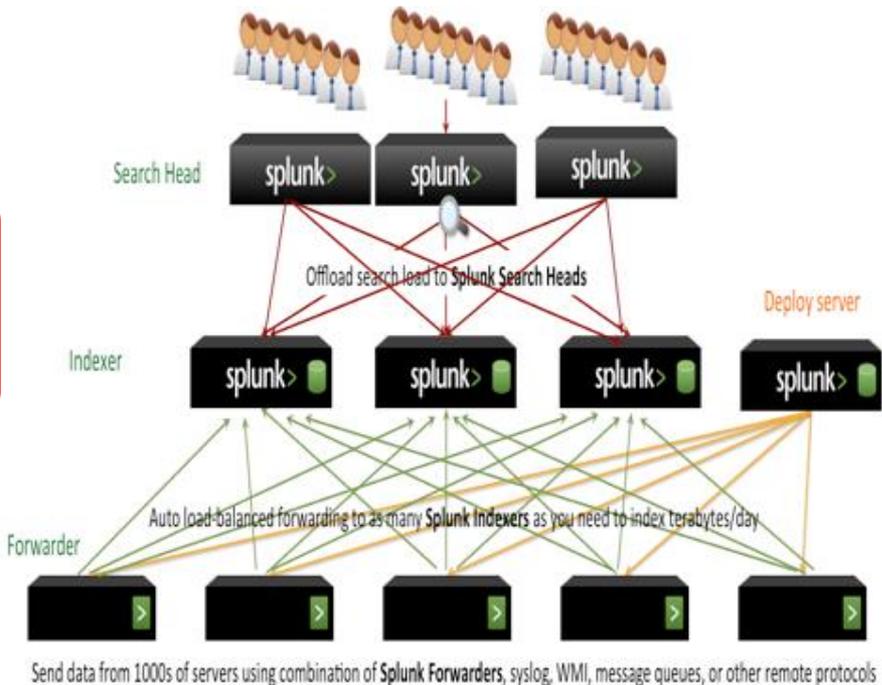
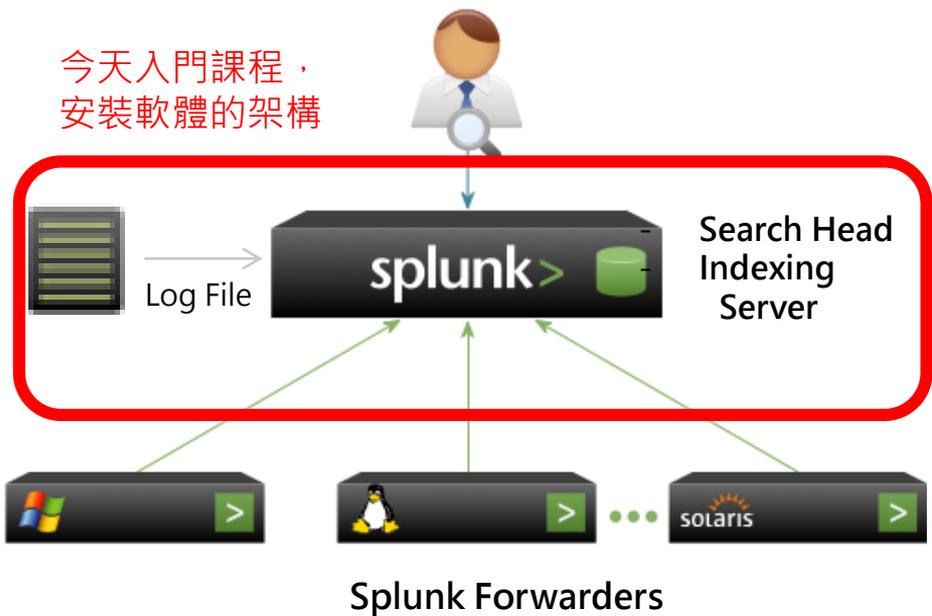
- 適用於所有機器資料的平台
- 即時架構
- Schema on the Fly
- 強大的分析功能和迅速產生警示，報告
- 靈活的擴充性：從單台接需求擴張到叢集
- 快速獲取價值
- 有活力和熱情的用戶群體

安裝Splunk

Splunk 產品，四個主要元件： Search Head, Indexer, Forwarder, Deployment Server



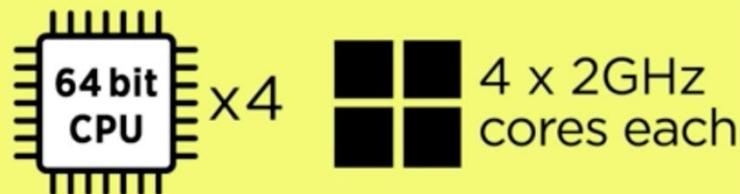
今天入門課程，
安裝軟體的架構





Search Head

Requirements



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



Indexer

Requirements

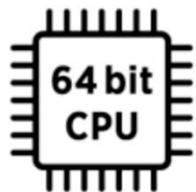


- 12GB RAM
- 1GbE NIC
with optional second NIC
for management
- 64-bit Linux/Windows
- 800 IOPS



Forwarder

Requirements



x1



2 x 1.5GHz
cores

- 1GB RAM

資源需求



Splunkd

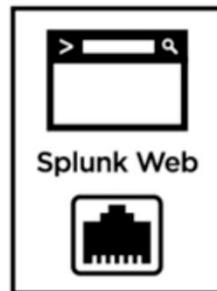
8089
(default)



22



9997



Splunk Web

8000
(default)

Splunk 兩個主要執行程式之一：

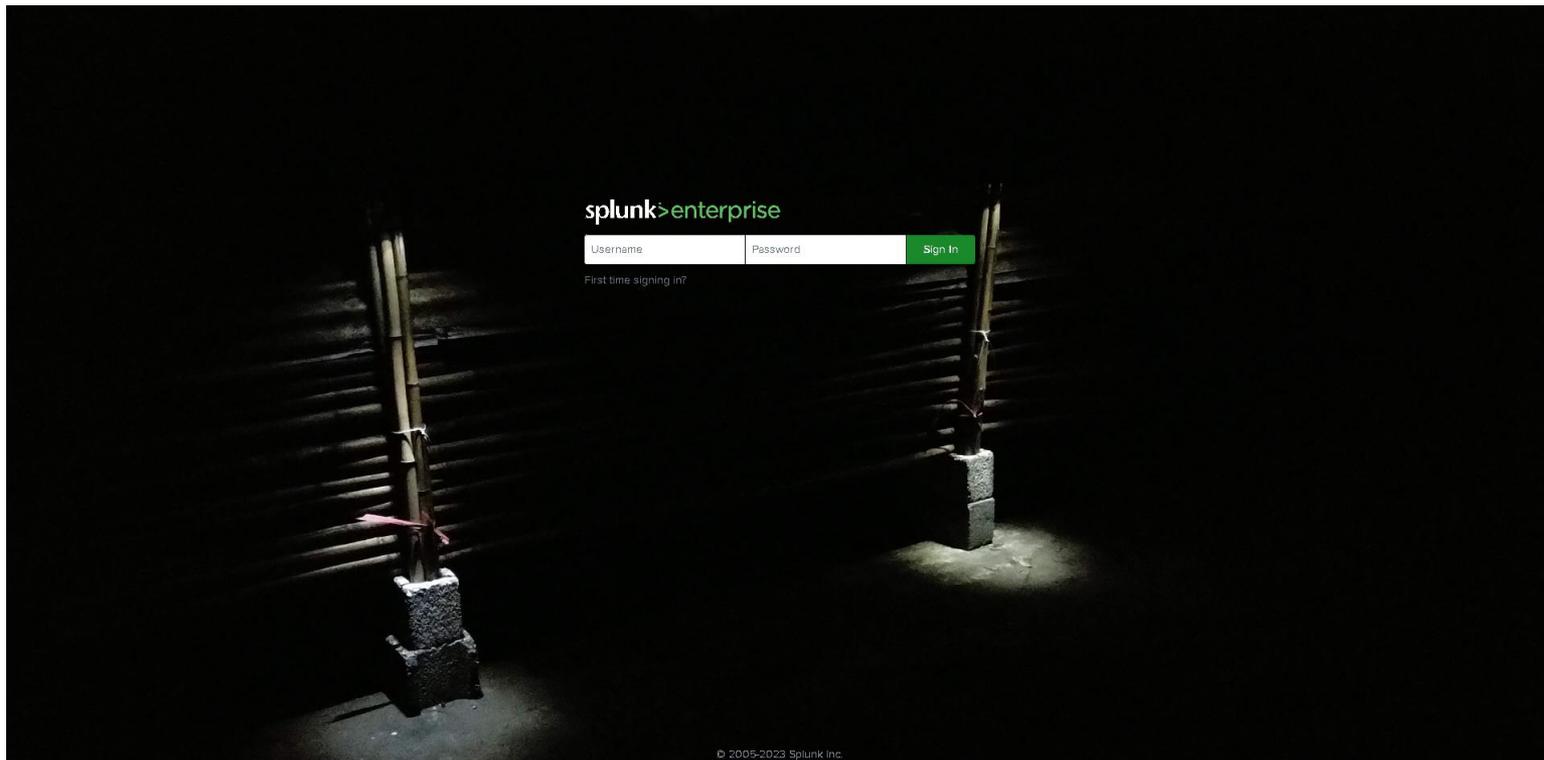
- 全文檢索服務：被查詢、傳回結果、和將所有進入的資料建立索引
- Accesses, processes, and indexes incoming data
- Processes all search requests and returns results
- Runs a web server on port **8089** by default
- Speaks SSL by default
- Splunk helpers run as dependent process(es) of splunkd
 - Splunk helpers run outside scripts,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



Unix 作業系統

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。

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



Unix 作業系統

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。

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



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。

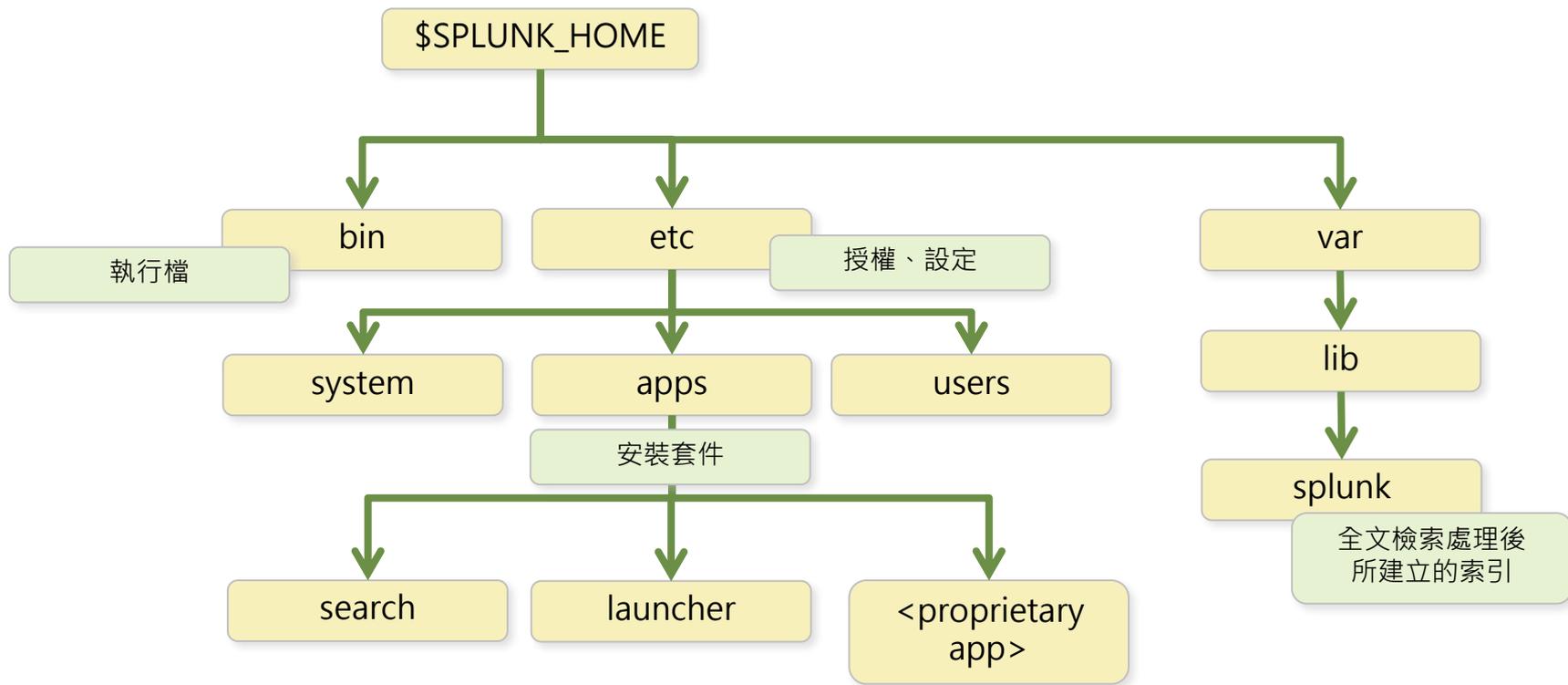
針對 64 位元平台，請使用 `splunk- \langle ... \rangle -x64-release.msi`：

```
msiexec.exe /i splunk- $\langle$ ... $\rangle$ -x64-release.msi [ $\langle$ flag $\rangle$ ]... [/quiet]
```

```
C:\> msiexec.exe /lev splunk.log /i splunk- $\langle$ ... $\rangle$ -x64-release.msi /quiet
```



Splunk 產品的目錄結構



Splunk App 目錄結構



```
/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



splunk>enterprise 應用套件: ...

Administr... 2 訊息 設定 活動 說明 尋找

Search & Reporting

Search & Reporting

應用套件

顯示 39 個項目中的 1-39 個

篩選器

50 每頁面

Name	資料夾名稱	版本	更新檢查	顯示	共用	狀態	動作
Eventgen-PA	Eventgen-PA		Yes	No	全域 權限	已啟用 停用	編輯屬性 核
SA-Eventgen	SA-Eventgen	6.3.4	Yes	Yes	全域 權限	已啟用 停用	啟動應用套件
Graphviz	SA-Graphviz	1.2	Yes	Yes	App 權限	已啟用 停用	啟動應用套件
Splunk App for Web Analytics	SplunkAppForWebAnalytics	2.1.0	Yes	Yes	App 權限	已啟用 停用	啟動應用套件
SplunkForwarder	SplunkForwarder		Yes	No	App 權限	已停用 啟用	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App 權限	已停用 啟用	
Splunk Essentials For Application Analytics	Splunk_Essentials_For_Application_Analytics	11.6	Yes	Yes	App 權限	已啟用 停用	啟動應用套件
Splunk Essentials For Business Analytics	Splunk_Essentials_For_Business_Analytics	11.1	Yes	Yes	App 權限	已啟用 停用	啟動應用套件
Splunk Add-on for AWS	Splunk_TA_aws	4.6.0	Yes	Yes	全域 權限	已啟用 停用	啟動應用套件
Fortinet Fortigate Add-on for Splunk	Splunk_TA_fortinet_fortigate	1.6.0	Yes	No	全域 權限	已啟用 停用	編輯屬性 核

管理應用套件

尋找更多應用套件

APP and Add-on安裝



splunk>enterprise 應用套件: ...

Administr... 2 訊息 設定 活動 說明 尋找

Search & Reporting

Search & Reporting

- Splunk Add-on for Unix and Linux
- Search Party Workshop
- Palo Alto Networks
- Palo Alto Networks Add-on
- SA-Eventgen
- Carousel Viz
- Event Timeline Viz
- Graphviz
- Network Diagram Viz
- Route Map
- Smart Exporter
- Splunk Add-on for AWS
- Splunk App for AWS
- Splunk App for Web Analytics
- Splunk Essentials For Application Analytics
- Splunk Essentials For Business Analytics
- 管理應用套件**
- 尋找更多應用套件

splunk>enterprise 應用套件

瀏覽更多應用套件

paloalto

搜尋項目 2,630,358 已檢索

類別

- DevOps
- Security, Fraud & Compliance
- IT 維運
- Utilities
- Business Analytics
- IoT & Industrial Data

CIM VERSION

- 4.x
- 3.x

SUPPORT TYPE

- Developer
- Splunk
- Unsupported
- Not Supported

APP CONTENT

- 輸入
- 警示動作
- 視覺化

最佳吻合結果 最新 熱門

7 應用套件

Palo Alto Networks Add-on for Splunk

開啟應用套件

The Palo Alto Networks Add-on for Splunk allows a Splunk® Enterprise administrator to collect data from every product in the Palo Alto Networks Next-generation Security Platform. The add-on collects and correlates data from Firewalls, Panorama, Traps Endpoints, Aperture SaaS Security, AutoFocus, MineMeld, and WildFire. You can consume the data usin... [更多](#)

Category: Security, Fraud & Compliance, IT Operations | 作者: Palo Alto Networks | 下載: 31053 | 發行: 4年前 | 最近更新日期: 2個月前 | [在 Splunkbase 檢視](#)

Palo Alto Networks App for Splunk

開啟應用套件

Palo Alto Networks and Splunk have partnered to deliver an advanced security reporting and analysis tool. The collaboration delivers operational reporting, configurable dashboard views, and adaptive response across Palo Alto Networks family of next-generation firewalls, advanced endpoint security, and threat intelligence cloud.

Palo Alto Networks ... [更多](#)

Category: Security, Fraud & Compliance, IT Operations | 作者: Palo Alto Networks | 下載: 45191 | 發行: 8年前 | 最近更新日期: 2個月前 | [在 Splunkbase 檢視](#)

APP and Add-on安裝



splunk>enterprise 應用套件

Administrat... 2 訊息 設定 活動 說明 尋找

瀏覽更多應用套件

以關鍵字、技術...等尋找應用套件

最新 熱門
60 應用套件

< 預覽 1 2 3 下一步 >

類別

- DevOps
- Security, F
- IT 維護
- Utilities
- Business A
- IoT & Indus

CIM VERSION

- 4.x
- 3.x

SUPPORT TYPE

- Developer
- Splunk
- Unsupport
- Not Suppo

APP CONTENT

- 輸入

登入

安裝

輸入您的 Splunk.com 使用者名稱和密碼以下載應用套件。

admin

.....

[忘記密碼?](#)

此應用套件及將安裝的任何相關相依項目由 Splunk 和/或第三方提供，您必須遵循 Splunk 和/或第三方授權人提供的適用授權來行使應用套件的使用權利。Splunk 對於任何第三方應用套件概不負責，並且不提供任何保固或支援。如果您對於應用套件有任何問題、抱怨或索賠，請直接聯絡適當的授權人，其聯絡資訊可在 Splunkbase 下載頁面上找到。

[Send JSON alerts over TLS](#) 由以下授權管理:

[End User License Agreement for Third-Party Content](#)

我已閱讀並且同意遵循授權的服務與條款。我接受 Splunk 將透過國際網路安全地傳送我的登入認證至 splunk.com

取消 登入並安裝

完成

Send JSON alerts over TLS 已安裝成功。

[開啟應用套件](#)

[返回主目錄](#)

完成

APP and Add-on安裝



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

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	11.6	Yes
Splunk Essentials For Business Analytics	Splunk_Essentials_For_Business_Analytics	11.1	Yes
Splunk Add-on for AWS	Splunk_TA_aws	4.6.0	Yes
Fortinet Fortigate Add-on for Splunk	Splunk_TA_fortinet_fortigate	16.0	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	Yes

更新
新加

```
/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
drwxr-xr-x 8 jack staff 256 4 17 12:07 force_directed_viz
```

使用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) 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](#)

splunk> 應用套件 ▾

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

[新增資料](#)

類型

檔案與目錄
上傳檔案、檢索本機檔案，或監控整個目錄。

TCP
在 TCP 連接埠上監聽傳入資料，如系統記錄。

UDP
在 UDP 連接埠上監聽傳入資料，如系統記錄。

指令碼
執行自訂指令碼以收集或產生更多資料。

Wire data
Passively capture wire data from network traffic.

資料輸入的類別 – All OS' s



- 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



add new input

edit existing input

您資料的完整路徑	設定主機	來源類型	索引
\$SPLUNK_HOME/etc/apps/SplunkAppForWebAnalytics/samples/apache.log	常數值	access_combined	default
\$SPLUNK_HOME/etc/apps/SplunkAppForWebAnalytics/samples/iis.log	常數值	iis	default
\$SPLUNK_HOME/etc/splunk/version	常數值	splunk_version	_internal
\$SPLUNK_HOME/var/log/introspection	常數值	自動	_introspection
\$SPLUNK_HOME/var/log/splunk			
\$SPLUNK_HOME/var/log/splunk/license_usage_summary.log			

新增資料

選擇來源 設定來源類型 輸入設定 檢閱 完成

檔案和目錄
上傳檔案、檢索本機檔案，或監控整個目錄。

HTTP 事件記錄器
設定用戶端可用來透過 HTTP 或 HTTPS 傳送資料之 Token。

TCP / UDP
設定 Splunk 平台以監聽網路連接埠。

指令碼
透過指令碼從任何 API、服務或資料庫取得資料。

Aperture

AutoFocus Export

AWS Billing
Collect and index billing report of AWS in CSV format located in AWS S3 bucket.

AWS Billing (Cost And Usage Report)

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.

設定此執行個體可監控資料的檔案和目錄。若要監控目錄中的所有物件，請選擇目錄。Splunk 平台會監控單一來源類型，並將該類型指派給目錄中的所有物件。如果目錄中有不同的物件類型或資料來源，則這可能導致問題。若要將多個來源類型指派給相同目錄中的物件，請設定那些物件的個別資料輸入。 [進一步瞭解](#)

檔案或目錄? 瀏覽

在 Windows 上: c:\apache\apache.error.log 或
%SystemName%\apache\apache.error.log。在 Unix 上: /var/log 或
/mnt/www01/var/log。

白名單?

黑名單?

常見問答集

- > Splunk 平台可檢索哪些種類的檔案?
- > 我無法存取要檢索的檔案。為什麼?
- > 我如何將遠端資料傳送至我的 Splunk 平台執行個體?
- > 除了監控檔案的內容，我是否還能監控這些檔案的變更?

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

設定此執行個體可監控資料的檔案和目錄。若要監控目錄中的所有物件，請選擇目錄。Splunk 平台會監控單一來源類型，並將該類型指派給目錄中的所有物件。如果目錄中有不同的物件類型或資料來源，則這可能導致問題。若要將多個來源類型指派給相同目錄中的物件，請設定那些物件的個別資料輸入。[進一步瞭解](#)

檔案或目錄 ?

 瀏覽

在 Windows 上: c:\apache\apache.error.log 或
\\hostname\apache\apache.error.log。在 Unix 上: /var/log 或
/mnt/www01/var/log。

持續監控

檢索一次

白名單 ?

黑名單 ?

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

輸入設定

選擇為此資料輸入設定其他輸入參數，如下所示：

來源類型

來源類型是 Splunk 平台指派給所有傳入資料的其中一個預設欄位。它會告知 Splunk 平台您已取得的資料種類，讓 Splunk 平台可在檢索期間明智地格式化資料。它也是分類資料的一種方式，讓您可以輕易搜尋資料。

應用套件範疇

應用套件範疇是 Splunk 平台執行個體中的資料夾，包含適用於資料的特殊使用案例或領域的設定。應用套件範疇可改善輸入和來源類型定義的管理能力。Splunk 平台會根據優先順序規則來載入所有應用套件範疇。 [進一步瞭解](#)

主機

Splunk 平台檢索資料時，每個事件會接收一個「主機」值。主機值應為事件來源之機器的名稱。您選擇的輸入類型會決定可用的設定選項。 [進一步瞭解](#)

索引

Splunk 平台會在選擇的索引中將傳入的資料儲存為事件。若在判定資料的來源類型時發生問題，請考慮使用「沙箱」索引。沙箱索引可讓您疑難排解設定而不致影響生產索引，您稍後可以隨時變更此設定。 [進一步瞭解](#)

自動 選擇 新增

應用套件範疇 Apps Browser (appsbrowser) ▾

- 常數值
- 路徑上的規則運算式
- 路徑中的區段

主機欄位值 Jackde-MBP

索引 預設 ▾ 建立新索引

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!

Top five sourcetypes (by total KB indexed) in the last 24 hours

sourcetype	KB indexed
splunkd	[Bar]
kdc.log-2	[Bar]

Search

```
sourcetype="access_common" status="404"
```

Search

```
sourcetype="WinEventLog:Security" host=AD001
```

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



splunk enterprise 應用套件

Administrator 訊息 設定 活動 說明 尋找

應用套件 [管理](#)

依名稱搜尋應用套件...

[Search & Reporting](#)

[Splunk Secure Gateway](#)

[Upgrade Readiness App](#)

[尋找更多應用套件](#)

哈囉, Administrator

[快速連結](#) [儀表板](#) [最近檢視](#) [由您建立](#) [與您共用](#)

常見工作

- 新增資料**
從各種常見來源新增資料。
- 搜尋您的資料**
透過 Splunk 搜尋將資料化為行動。
- 視覺化您的資料**
建立適合您資料的儀表板。
- 新增團隊成員**
將團隊成員新增至 Splunk 平台。
- 管理權限**
控制誰有權存取角色。
- 設定行動裝置**
使用 Splunk Secure Gateway 登入或管理行動裝置。

學習和資源

- 產品專覽**
是 Splunk 新手嗎? 讓導覽來幫助您使用。
- 善用 Splunk 說明文件進一步瞭解**
在全方位的指引下部署、管理和使用 Splunk 軟體。
- 取得 Splunk 专家的協助**
Splunk Lantern 客戶成功中心的可操作指南。
- 延伸能力**
瀏覽 Splunkbase 上的數千個應用套件。
- 加入 Splunk 社群**
學習、獲得靈感和分享知識。
- 查看其他人如何使用 Splunk**
瀏覽真實客戶案例。
- 訓練和認證**
成為經過認證的 Splunk 忍者。

<https://www.splunk.com/customers>

基本 搜尋使用套件 (Search App)



splunk>enterprise 應用套件: ... i Administrat... 2 訊息 設定 活動 說明 尋找

搜尋 資料集 報告 警示 儀表板 > Search & Reporting

搜尋

1 在此輸入搜尋... 前 24 小時 🔍

無事件取樣

🔗 智慧模式

如何搜尋

如果您不熟悉搜尋功能，或需要進一步瞭解，請參閱下列其中一項資源。

[說明文件](#)

[教學](#)

搜尋項目

2,667,737 事件

已檢索

5年前

最早事件

現在

最晚事件

[資料摘要](#)

> [搜尋歷程記錄](#)

設定的管理介面：知識、資料、系統管理、存取控制



The screenshot shows the 'rise' application settings management interface. The top navigation bar includes 'Administrat...', '2 訊息', '設定', '活動', '說明', and a search bar. The left sidebar contains '報告', '警示', '儀表板', and '新增資料' (highlighted with a blue box). The main content area is divided into three columns: '知識', '資料', and '系統'. The '知識' column includes '搜尋、報告與警示', '資料模型', '事件類型', '標記', '欄位', '查閱', '使用者介面', '警示動作', '進階搜尋', and '所有設定'. The '資料' column includes '資料輸入', '轉送與接收', '索引', '報告加速摘要', '虛擬索引', '來源類型', '分散式環境', '索引器分群', '轉送器管理', '分散式搜尋', '使用者與驗證', and '存取控制'. The '系統' column includes '伺服器設定', '伺服器控制項', '健康情況報告管理員', 'Instrumentation', '授權', and '工作量管理'. A '教學' button is visible in the bottom left corner.

開始使用 Search & Report 應用套件



splunk>enterprise 應用套件: ... i Administrat... 2 訊息 設定 活動 說明 尋找

搜尋 資料集 報告 警示 儀表板 > Search & Reporting

搜尋

1 在此輸入搜尋...

前 24 小時



無事件取樣

智慧模式

如何搜尋

如果您不熟悉搜尋功能，或需要進一步瞭解，請參閱下列其中一項資源。

[說明文件](#)

[教學](#)

搜尋項目

2,667,737 事件

已檢索

5年前

最早事件

現在

最晚事件

[資料摘要](#)

> [搜尋歷程記錄](#)

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	最近更新日期
/Users/jack/Downloads/tutorialdata/mailsv/secure.log	9,829	19/03/26 下午04時50分16.000秒
/Users/jack/Downloads/tutorialdata/vendor_sales/vendor_sales.log	30,244	19/03/26 下午04時50分15.000秒
/Users/jack/Downloads/tutorialdata/www1/access.log	13,628	19/03/26 下午04時50分11.000秒
/Users/jack/Downloads/tutorialdata/www1/secure.log	10,593	19/03/26 下午04時50分11.000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:vpclflow	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



搜尋歷程記錄

< 預覽 1 2 3 4 5 6 7 8 ... 下一步 >

篩選器



無時間篩選條件 ▾

每頁 20 個 ▾

i	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,Ion,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



splunk>enterprise 應用套件: Search & Reporting Administrator 2 訊息 設定 活動 說明 尋找

搜尋 資料集 報告 警示 儀表板 Search & Reporting

新搜尋

另存為 關閉

1 sourcetype="pan:traffic" app=web* 前 24 小時

✓ 29,831 個事件 (19/04/17 17:00:00.000 至 19/04/18 17:38:48.000) 無事件取樣

工作 智慧模式

事件 (29,831) 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

清單 格式 每頁 50 個

< 預覽 1 2 3 4 5 6 7 8 ... 下一步 >

< 隱藏欄位	≡ 所有欄位	i	時間	事件
所選欄位 a dest 100+ a dest_ip 100+ # dest_port 3 a eventtype 5 a host 1 a index 1 a source 1 a sourcetype 1 a src 4 a user 4		>	19/04/18 17:38:47:192	Apr 18 17:38:47 1,2019/04/18 17:38:47,001606001116,TRAFFIC,start,1,2019/04/18 17:38:47,192.168.0.6,74.125.239.31,0.0.0.0.0.0.0.0,rule1,tng\picard,,web-browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,forwardAll,2019/04/18 17:38:47,46397,1,1679,80,0,0,0x20000,tcp,allow,358,296,62,4,2019/04/18 17:38:47,0,any,0,0,0x0,192.168.0.0-192.168.255.255,United States,0,3,1 dest = 74.125.239.31 dest_ip = 74.125.239.31 dest_port = 80 eventtype = pan eventtype = pan_firewall network eventtype = pan_traffic communicate network eventtype = pan_traffic_start network session start host = 127.0.0.1 index = main source = eventgen:pan_incident.samplelog sourcetype = pan:traffic src = 192.168.0.6 user = tng\picard
關注欄位 a action 1 a action_flags 1 a app 2		>	19/04/18 17:38:45:192	Apr 18 17:38:45 1,2019/04/18 17:38:45,001606001116,TRAFFIC,end,1,2019/04/18 17:38:45,192.168.0.2,204.232.231.46,0.0.0.0.0.0.0.0,rule1,tng\crusher,,web-browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,forwardAll,2019/04/18 17:38:45,46520,1,52551,80,0,0,0x200000,tcp,allow,1417,580,837,10,2019/04/18 17:38:45,0,not-resolved,0,0,0x0,192.168.0.0-192.168.255.255,United States,0,6,4 dest = 204.232.231.46 dest_ip = 204.232.231.46 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 index = main source = eventgen:pan_incident.samplelog sourcetype = pan:traffic src = 192.168.0.2 user = tng\crusher

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



splunk>enterprise 應用套件: Search & Reporting

Administrator 訊息 設定 活動 說明 尋找

搜尋 資料集 報告 警示 儀表板 Search & Reporting

新搜尋

1 error | 前 24 小時

✓ 9 個事件 (19/04/17 17:00:00.000 至 19/04/18 17:41:24.000) 無事件取樣

事件 (9) 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

清單 格式 每頁 50 個

< 隱藏欄位	≡ 所有欄位	i	時間	事件
所選欄位 a dest 1 a dest_ip 1 # dest_port 1 a eventtype 5 a host 2 a index 1 a source 2 a sourcetype 2 a src 1 a user 1		>	19/04/18 16:10:43.192	Apr 18 16:10:43 1,2019/04/18 16:10:43,001606001116,THREAT,url,1,2019/04/18 16:10:43,192.168.0.6,38.74.1.42,0.0.0.0,0.0.0.0,rule1,tng\picard,,web-browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,forwardAll,2019/04/18 16:10:43,62133,1,2290,80,0,0,0x208000,tcp>alert,"www.blogfa.com/msg/Error.html?aspxerrorpath=/default.aspx",(9999),personal-sites-and-blogs,informational,client-to-server,0,0x0,192.168.0.0-192.168.255.255,United States,0,text/html dest = 38.74.1.42 dest_ip = 38.74.1.42 dest_port = 80 eventtype = nix_errors error eventtype = pan eventtype = pan_firewall network eventtype = pan_url proxy web host = 1270.0.1 index = main source = eventgen:pan_incident.samplelog sourcetype = pan:threat src = 192.168.0.6 user = tng\picard
關注欄位		>	19/04/18 16:02:34.000	{ [-] account_id: 000000000000 attach_data: { [+] } create_time: 2016-08-13T01:01:09.104Z encrypted: false

資料結果頁籤：事件、樣式、統計資料、視覺化



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	

新搜尋

```
1 sourcetype="pan:traffic" app=web*
```

符合 5,273 個事件, 共 5,328 個 無事件取樣

事件 (5,273) 樣式 統計資料 視覺化

格式化摘要 縮小 顯示全部取樣 取消選擇

時間	事件
19/04/18 17:42:49.1	204.232.231.65
19/04/18 17:42:49.2	204.232.231.65

1. 搜尋的事件結果



2. 統計分析

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

✓ 30,019 個事件 (19/04/17 17:00:00.000 至 19/04/18 17:42:36.000) 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
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

3. 視覺化



欄位 (字段) 選擇顯示



新搜尋 另存為 ▾ 關閉

1 `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

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

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 appable_to_transfer_file` 2
`a app:category` 6
`a app:default_ports` 21
`a app:excessive_bandwidth` 2

i	✓ ▾	欄位 ▾	值數目 ▾	事件涵蓋範圍 ▾	類型 ▾
>	<input checked="" type="checkbox"/>	dest	>100	100%	字串
>	<input checked="" type="checkbox"/>	dest_ip	>100	100%	字串
>	<input checked="" type="checkbox"/>	dest_port	>100	100%	數字
>	<input checked="" type="checkbox"/>	eventtype	5	100%	字串
>	<input checked="" type="checkbox"/>	host	1	100%	字串
>	<input checked="" type="checkbox"/>	index	1	100%	字串
>	<input checked="" type="checkbox"/>	source	1	100%	字串
>	<input checked="" type="checkbox"/>	sourcetype	1	100%	字串
>	<input checked="" type="checkbox"/>	src	33	100%	字串
>	<input checked="" type="checkbox"/>	user	5	100%	字串
>	<input type="checkbox"/>	action	1	100%	字串
>	<input type="checkbox"/>	action_flags	1	100%	字串
>	<input type="checkbox"/>	app	77	100%	字串
>	<input type="checkbox"/>	appable_to_transfer_file	2	99.21%	字串
>	<input type="checkbox"/>	app:category	6	99.21%	字串
>	<input type="checkbox"/>	app:default_ports	21	98.89%	字串
>	<input type="checkbox"/>	app:evasive	2	99.21%	字串
>	<input type="checkbox"/>	app:excessive_bandwidth	2	99.21%	字串

欄位 (字段) 選擇顯示



新搜尋 另存為 ▾ 關閉

1 `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 1 2 3 4 5 6 7 8 ... 下一步 >

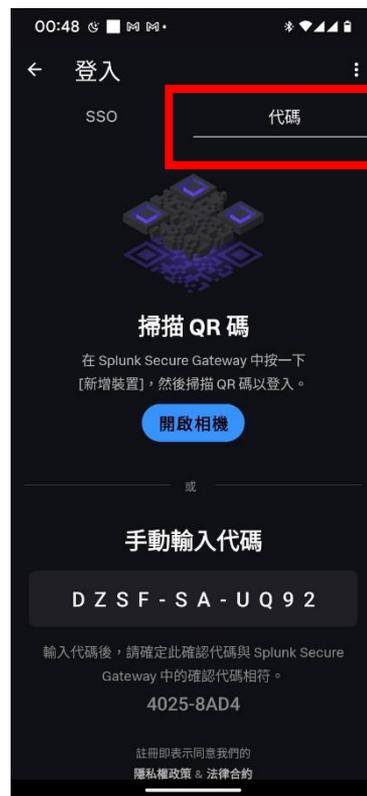
< 隱藏欄位	≡ 所有欄位	i	時間	事件
<div style="border: 2px solid red; padding: 5px;"><p>所選欄位</p><ul style="list-style-type: none">a dest 100+a dest_ip 100+# dest_port 100a eventtype 5a host 1a index 1a source 1a sourcetype 1a src 31a user 5</div>		>	19/04/18 17:45:53.192	Apr 18 17:45:53 1,2019/04/18 17:45:53,001606001116,TRAFFIC,end,1,2019/04/18 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 <div style="border: 2px solid red; padding: 5px;"><code>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 = 1270.0.1 index = main source = eventgen:pan_incident.samplelog sourcetype = pan:traffic src = 192.168.0.100 user = unknown</code></div>
		>	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 <code>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 = 1270.0.1 index = main source = eventgen:pan_incident.samplelog sourcetype = pan:traffic src = 192.168.0.2 user = tng\crusher</code>
		>	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 <code>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 = 1270.0.1</code>

關注欄位

- a action 1
- a action_flags 1
- a app 77
- a appable_to_transfer_file 2
- a app:category 6
- a app:default_ports 21

Splunk Secure Gateway

下載 Splunk Mobile

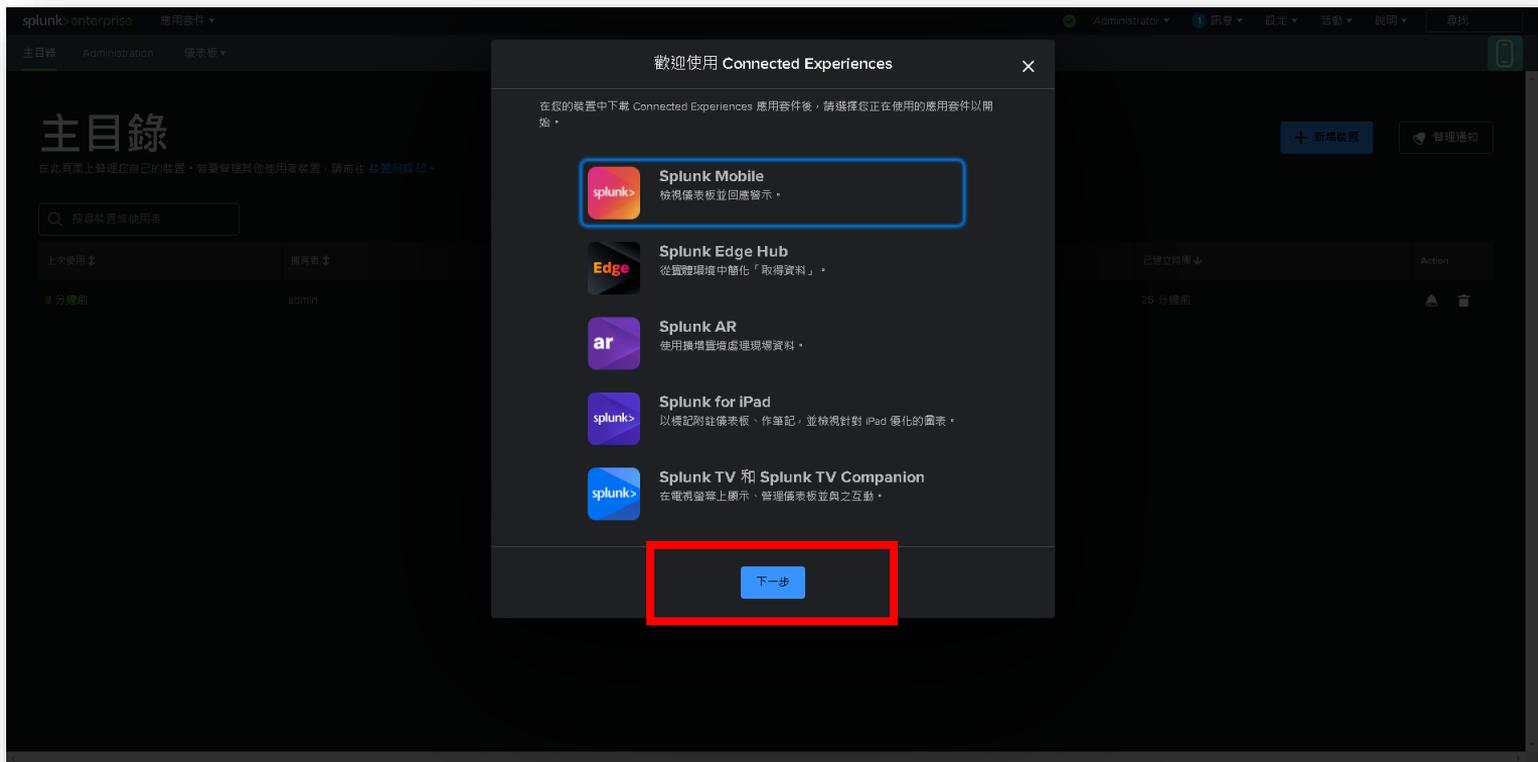


Splunk Secure Gateway



The screenshot shows the Splunk Enterprise Admin console interface. The top navigation bar includes 'splunk enterprise' and '應用套件' (Applications). The left sidebar, titled '應用套件', contains a search bar and a list of applications: 'Search & Reporting', 'Splunk Secure Gateway' (highlighted with a red box), and 'Upgrade Readiness App'. Below the sidebar is a link to '尋找更多應用套件'. The main content area is titled '哈囉, Administrator' and features a '快速連結' (Quick Links) section with tabs for '儀表板', '最近檢視', '由您建立', and '與您共用'. The '常見工作' (Common Tasks) section includes: '新增資料' (Add data), '搜尋您的資料' (Search your data), '視覺化您的資料' (Visualize your data), '管理權限' (Manage permissions), and '設定行動裝置' (Set up mobile devices). The '學習和資源' (Learn and Resources) section includes: '產品導覽' (Product tour), '善用 Splunk 說明文件' (Use Splunk documentation), '取得 Splunk 專家的協助' (Get Splunk expert help), '加入 Splunk 社群' (Join Splunk community), '查看其他人如何使用 Splunk' (See how others use Splunk), and '訓練和認證' (Training and certification).

Splunk Secure Gateway



The screenshot displays the Splunk Enterprise administration interface. A modal dialog titled "歡迎使用 Connected Experiences" is open in the center. The dialog contains the following text and options:

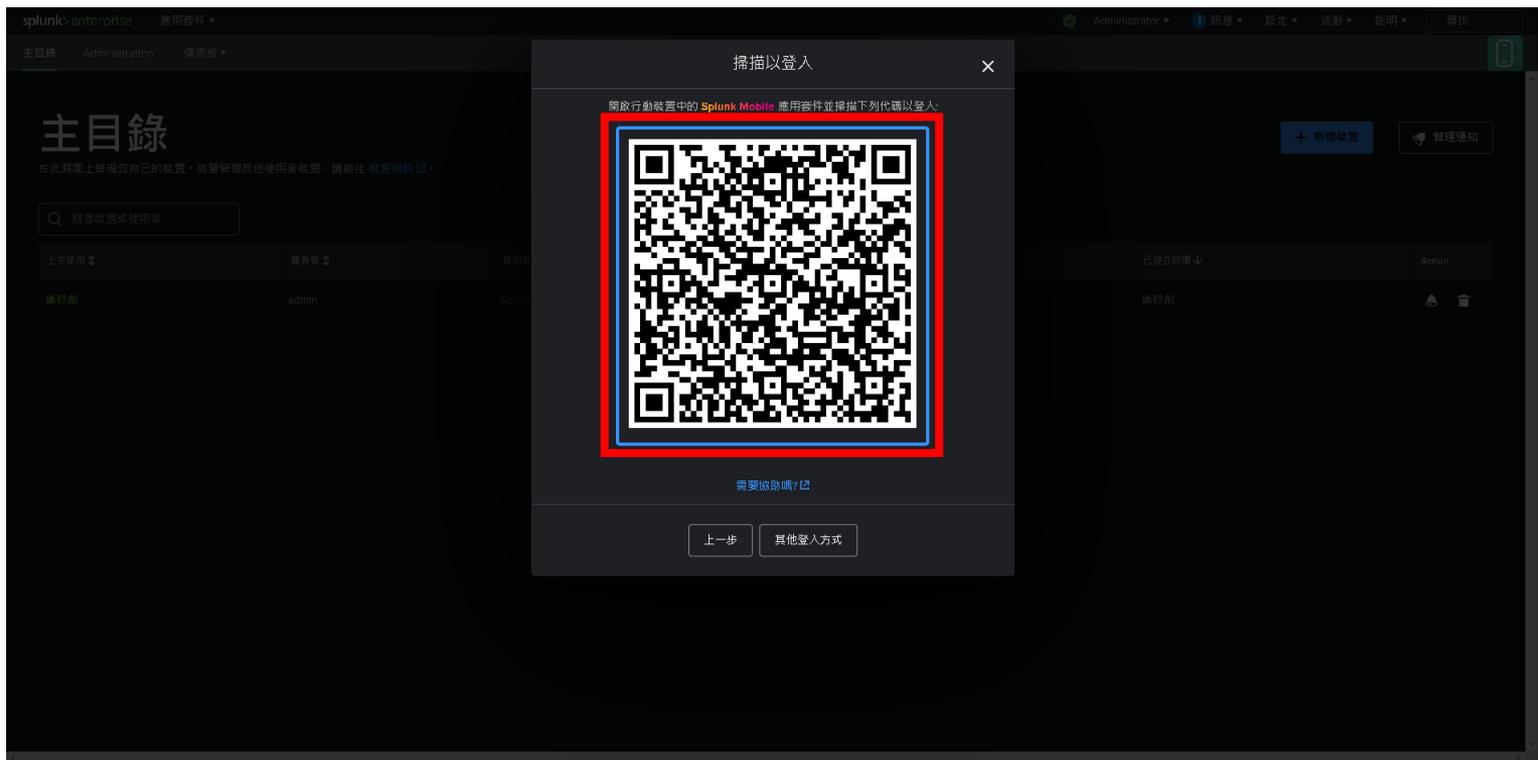
歡迎使用 Connected Experiences

在你的裝置中下載 Connected Experiences 應用套件後，請選擇你正在使用的應用套件以開始。

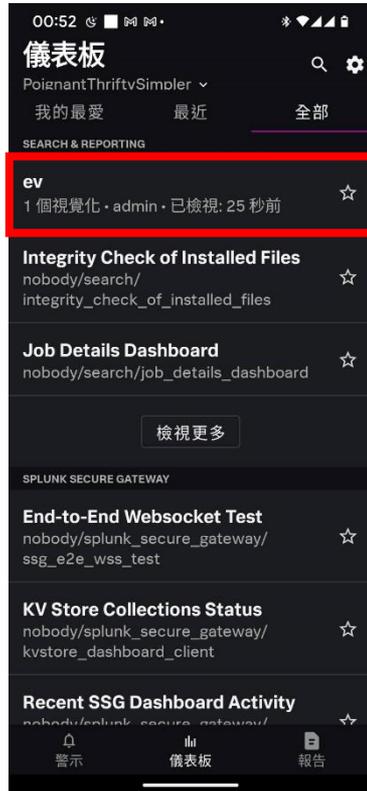
- Splunk Mobile**
檢視儀表板並回應警訊。
- Splunk Edge Hub**
從實體環境中簡化「取得資料」。
- Splunk AR**
使用擴增實境處理現場資料。
- Splunk for iPad**
以標記附註儀表板、作筆記，並檢視針對 iPad 優化的儀表。
- Splunk TV 和 Splunk TV Companion**
在電視螢幕上顯示、管理儀表板並與之互動。

At the bottom of the dialog, a blue button labeled "下一步" (Next) is highlighted with a red rectangular box. In the background, the main interface shows a "主目錄" (Home) section with a search bar and navigation options.

Splunk Secure Gateway



Splunk Secure Gateway



Thank you.

