SPL2 Splunk - 實作入門

Splunk Hands-on Training Level 2

時數：14小時 | 費用：39,800元 | 點數：12點 | 教材：Splunk原廠專用教材 | 各地開課時間：P.173~P.200

課程目標　第一部分共五個小時的課程，教您使用Splunk進行搜尋、檢視、標記、建立告警、簡易報表以及dashboard。第二部分共九小時的課程，深入Splunk搜尋語法與報表製作。使用情境模擬、實務演練方式，讓學員運用搜尋、報表、圖表等方式去解決問題。

適合對象　適合企業內部使用Splunk做系統管理、日誌分析、問題查找等人員

課程內容

Part I

Lesson 1 - 開始搜尋
- Splunk簡介、使用Search App
- 使用基本搜尋功能
- 如何解讀搜尋結果
- 控制搜尋工作的執行方式
- 使用時間範圍做搜尋
- 使用搜尋結果做進一步的搜尋

Lesson 2 - 儲存搜尋結果與指令
- 瀏覽搜尋結果
- 儲存與分享搜尋結果
- 儲存搜尋指令
- 定時執行搜尋

Lesson 3 - 使用「欄位」
- 什麼是「欄位」
- 使用「欄位」做搜尋
- 使用「欄位」瀏覽區

Lesson 4 - 標記與事件類型
- 什麼是標記
- 建立與使用標記
- 什麼是事件類型
- 建立與使用事件類型

Lesson 5 - 建立告警
- 什麼是告警
- 建立告警
- 檢視已觸發的告警

Lesson 6 - 建立報表
- 建立報表與圖表
- 建立組合視頁並嵌入報表
- 建立與修改組合視頁

Part II

Lesson 1 - 基礎搜尋
- 何謂搜尋
- 了解搜尋語法
- 了解欄位並使用fields指令
- 建立表格
- 何謂多值欄位

Lesson 2 - 統計分析
- 了解stats指令
- 找出某個欄位的top與rare值
- 使用stats指令並建立統計表

Lesson 3 - 格式化與計算
- 了解eval指令
- 使用運算指令
- 使用convert,round,format指令
- 使用邏輯判斷指令

Lesson 4 - 繪圖
- 建立圖表與time charts
- 分割圖表
- 過濾null值以及other值
- 使用統計相關指令

Lesson 5 - 關連分析
- 何謂transaction
- 關連事件
- 建立transaction報表

Lesson 6 - 使用參照功能加入更多資訊
- 建立參照表
- 定義參照
- 建立自動參照與使用時間參數做參照

Lesson 7 - 彙總索引
- 定義彙總索引
- 執行搜尋並產生彙總索引
- 了解彙總索引的gap與overlap

Lesson 8 - 巨集
- 管理巨集
- 建立並使用巨集
- 定義巨集參數

備註事項　上課時間：AM09:00 ~ PM17:00

SPL3 Splunk - 中階應用與管理

Splunk Hands-on Training Level 3

時數：15小時 | 費用：69,800元 | 點數：20點 | 教材：Splunk原廠專用教材 | 各地開課時間：P.173~P.200

課程目標　第一部分共七小時的課程專門提供給Splunk系統管理者熟悉Splunk管理工作。包含：各種instances安裝方式、注意事項、參數設定、各種資料匯入、資料傳收、資料管理、使用者帳號管理、授權管理、基本的問題查找與排除方式以及Splunk本身運作的各種監控機制。
第二部分共八小時的課程提供給Splunk App開發者學習如何建立Splunk App，開發dashboards、search forms、search views，學習如何使用Splunk提供的各種UI模組，如何打包App提供使用者下載。

適合對象　Splunk系統管理者、Splunk App開發者

預備知識　本課程為中階課程，學員需上過「SPL2：Splunk-實作入門」（敬請參考SPL2：Splunk-實作入門課程內容）

課程內容

Part I

Lesson 1 - 安裝Splunk
- 標準安裝需求
- 安裝
- 啟動、停止、重起Splunk 服務

Lesson 2 - 如何取得日誌
- 如何取得日誌
- 使用Apps取得日誌
- 日誌來源設定說明

Lesson 3 - 匯入資料
- 手動匯入資料
- 說明Splunk匯入資料的幾種方式與差異
- 資料匯入參數說明

Lesson 4 - 匯入Windows 日誌
- 了解與Windows相關的日誌
- 設定Windows日誌匯入參數

Lesson 5 - Forwarders
- Forwarder種類比較
- 了解使用Forwarder的好處
- 部署與設定Forwarders

Lesson 6 - 了解資料處理
- Splunk如何傳收資料
- 設定資料型態
- Splunk如何使用時區設定
- 設定搜尋期間的欄位擷取

Lesson 7 - Splunk儲存資料方式
- 設定索引
- 資料備份說明
- 備份參數說明
- 回復備份的資料

Lesson 8 - 使用者權限
- 了解使用者與角色
- 建立角色
- 「delete role」說明

Lesson 9 - 授權
- 授權的種類
- 何謂違反授權
- 授權群組、授權池、授權堆疊
- 增加或是移除授權

Lesson 10 - 日常維護作業
- 何謂「job」，管理job的方式
- 何謂「告警」以及設定方式
- 何謂知識物件與權限
- 問題檢視方法
- 如何取得外部支援

Lesson 11 - 版本更新
- 了解Splunk版本更新模式
- 如何取得Splunk更新訊息
- 版本更新建議步驟

Part II

Lesson 1 - 何謂Apps
- 何謂Apps
- 使用者權限與Apps

Lesson 2 - 建立與編修組合視頁
- 在Search App建立一個組合視頁
- 使用編輯器編修組合視頁

Lesson 3 - 簡易XML選項
- 何謂簡易XML選項
- 編修簡易XML

Lesson 4 - 建立 App
- 了解App的目錄結構
- 建立App

Lesson 5 - Form Searches
- 何謂Form Search視頁
- 建立Form Search視頁
- 權限設定

Lesson 6 - 進階視頁
- 了解進階視頁與XML架構
- 了解視頁外觀
- 將簡易XML轉換為進階XML

Lesson 7 - 何謂模組
- 模組的定義
- 使用進階XML模組建立視頁

Lesson 8 - 組合視頁
- 通用模組說明
- 使用進階XML模組建立組合視頁

Lesson 9 - 流程
- 何謂流程
- 在搜尋結果中使用流程功能

Lesson 10 - 選單與圖示
- 建立選單
- 建立App的圖示
- 套用CSS
- 使用IFrame與server side includes 改變呈現方式

Lesson 11 - 包裝Apps
- 如何部署Apps
- 如何打包Apps

備註事項　上課時間：AM09:00 ~ PM17:30

關於Splunk

Splunk是專門設計給企業使用的IT搜尋引擎(Search Engine)，它將雅虎、Google的搜尋技術與概念發揚光大，如今企業可以用Splunk來管理複雜的IT 系統。Splunk能自動收集由各種伺服器、網路設備和軟體產生的資料與日誌。

Splunk的設計與使用概念就像是Google一樣，它打破過去傳統IT管理的方式，企業一旦安裝Splunk的IT Search Engine之後，IT人員就可以透過Browser使用Splunk並對企業的各種IT Data進行關鍵字(Keyword)搜尋，快速地得到所需要的資料，此外Splunk本身還具有計算(Computing)能力，管理者可以透過Splunk將搜尋所得的結果立即做運算處理，進行分析與產生各種報告、圖表與警示，而且還可以設定Splunk進行排程定時搜尋，並將結果以Alert方式通知相關人員。