# 完美風暴 vs 完美投資
# 集中化日誌管理平台

隨著科技的蓬勃發展以及萬物連網的時代，企業環境中充滿著各式各樣的設備及應用程式，這些設備及應用程式都是資料 (Data、Log、Event) 的來源。在過去的時代，企業著重於公司的基礎發展；如今，在軟硬體發展成熟的時代，這些曾經被忽略的巨量資料開始成為大家關注的焦點之一。

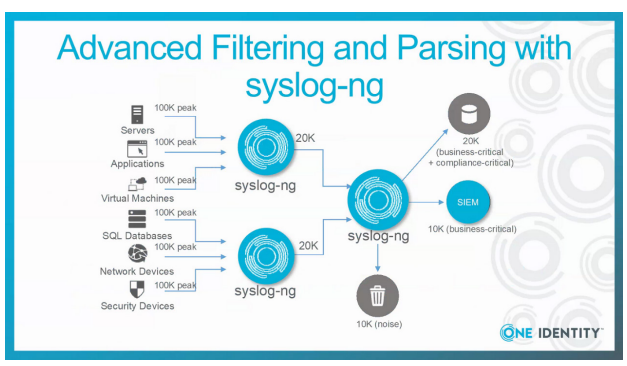
“Log”這個詞大家都不陌生，從設備、系統到應用程式等，每分每秒所記錄的變化都可以是 log 的一種，雖然這些文字訊息非常繁瑣甚至格式多樣化，但卻是設備或程式最即時、最真實的反應。近年來，因為網路的快速發展，駭客入侵企業的資安事件頻傳，而企業該如何面對危機事件的處理、透過設備的 log 來查看入侵者的足跡以及動了什麼手腳。投資日誌管理平台或許對公司企業沒有明顯的變化或效益呈現，但隨著日誌管理、收集、分析及加值應用，集中化日誌管理平台可以讓企業多一層保護，更可以改善營運效率。

## syslog-ng

syslog-ng 是一款強大的開源日誌收集軟體，也被稱為 Syslog-Next Generation，從 1998 年開始歷經了 20 幾年的發展，除了保有開源的版本之外，目前也提供商業化版本，其功能更加完善且擁有原廠的技術支援。

syslog-ng 的設計是為了讓使用者有效率的收集資料，因此在處理高資料流的時候也不會有太多的資源消耗，在環境佈署上所需的資源不高，但可擴展性高，在資料呈現的部分也提供了 Web 介面讓使用者可以快速查詢重要的事件。

許多著名的資安事件管理平台 (SIEM) 例如 Splunk、ArcSight、ELK 等，這些事件管理平台擁有強大的事件分析功能以及華麗的儀表板，用於做資料的加值呈現，但在前端的資料收集往往成為其效能瓶頸及預算的黑洞，因此近年來這些大廠開始出現一些議題 - 關於 syslog-ng 做為前端的資料收集與這些 SIEM 做高度整合，syslog-ng 自始至終為一個日誌集中化管理平台，並非分析軟體也不是 SIEM 平台，但它的特性足以成為企業資料加值應用的基石。



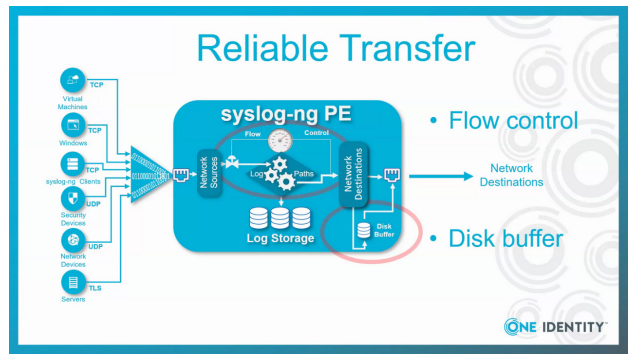

syslog-ng 架構圖

## 擴展性

syslog-ng 解決方案不僅支援傳統的伺服器、網路設備及安全性設備等多達五十多個作業系統平台，甚至可以在端點上作為單點日誌管理解決方案。透過正確的配置，syslog-ng 每秒可以管理超過 650,000 條日誌消息，而單一台 syslog-ng server 可以管理數千個日誌來源，若想分散單台 syslog-ng server 的流量負擔，也可以使用多台 Relay 來實現高可擴展性。為了應付來自各來源的複雜日誌格式，syslog-ng 提供了完整的篩選過濾及分類功能，可以將不必要的日誌訊息過濾，並分類重要的數據，從而減輕網路和 SIEM 上的負載。

## 可靠性

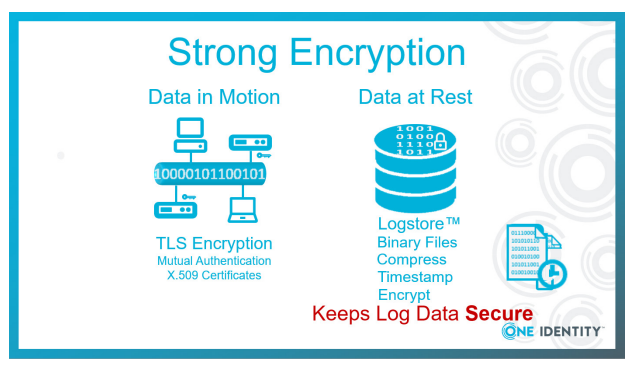
為了確保日誌管理的可靠性，syslog-ng Premium Edition 結合了多項獨特功能，以確保日誌消息的零丟失。首先，syslog-ng 除了通過 TCP 傳輸協定來支援訊息傳輸的可靠性之外，還使用了可靠日誌傳輸協議 (ALTP) 來確保日誌伺服器端已收到來自客戶端的消息。當日誌伺服器因為某些原因停止運作時，客戶端可以使用故障轉移確保日誌訊息可以發送到備用伺服器，並將訊息寫入本地端的磁碟緩衝區保存，確保日誌伺服器恢復之前日誌不會流失，來達到日誌管理的高可靠性。




資料可靠傳輸

## 安全性

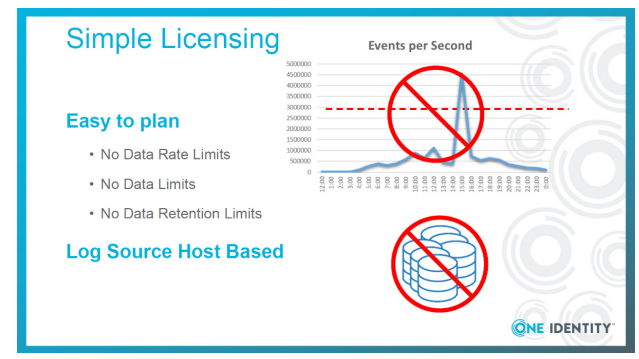
當設備不透過外部網路傳輸的情況下，syslog-ng 可透過 TLS 的相互身分驗證將事件日誌安全的轉發到中央的 SIEM。在資料的安全性中，syslog-ng 將收集的日誌消息儲存進行加密並可加上時間戳記，來防止資料被惡意篡改，進而提升日誌收集管理的安全性。基於日誌的存取控制，syslog-ng 也可以整合 LDAP 來達到日誌存取權限的控制。




資料加密儲存

## 建置成本

在整個日誌管理的生命週期中使用階段性的導入尤佳，在建置前先了解客戶端的需求目的以及未來發展走向，因此建置初期將企業環境的目標主機列舉出來再依序收集，當重要的目標主機日誌集中收容完成後，企業必須開始思考如何將這些繁瑣的文字轉變為有價值的利用；多數企業會希望導入 SIEM 來做日誌的分析或儀表板呈現等加值應用，但這些加值應用的前提是必須有效的將日誌集中化管理以及確保日誌的完整性，syslog-ng 的日誌相容性及高度整合性能夠扮演好日誌加值應用的基石。而在企業導入過程中，導入成本也是重要的考量之一，syslog-ng 的計價方式為 Log Source Host，而非以資料流量或資源使用率來計價，此計價方式再搭配上高度彈性的 Filter 可以協助企業降低整體日誌集中管理的建置成本。




計價方式

## Use Case

### 製造業

在 syslog-ng 的使用案例中，多為因應法規要求，以及企業須乘載高流量的日誌處理環境。以台灣某製造業為例，該企業被上游廠商要求須遵循 ISO27001 等相關法規才能符合代工的規範，而在製造業廠區的生產環境每天產生出數以萬計的日誌資料，因此客戶在比較眾多日誌管理平台，基於用途、需求以及建置成本後，選擇使用 syslog-ng 來完成此重責大任。

syslog-ng 秉持著易佈署及輕量化的產品特性，能夠符合製造業的生產環境來收集廠區中的巨量資料，不論在單一廠區甚至跨地區的資料傳輸，syslog-ng 憑藉著高度擴展性的優勢將原本四散各地的設備日誌做到集中化控管，不但符合稽核法規也讓使用者能夠即時掌握設備的狀態，甚至達到突發事件即時告警的作用。

### 醫療業

日誌集中化管理解決方案不只用於製造業的工業環境中，在醫療業方面，也作為應用管理的幕後推手，台灣某知名醫院採用 syslog-ng 日誌集中化管理平台協助其業務運作。隨著資訊蓬勃發展，醫院的掛號、門診等便民服務中含括了許多應用系統，這些應用系統必須 24 小時正常運作，以維持良好的醫療服務提供品質，因此院區中的資訊部門必須透過系統日誌的收集來判斷整體醫療系統的正常運作。

在導入期間，客戶將最重要的資料庫及核心系統的應用程式日誌集中收集，並使用 syslog-ng 的資料篩選功能，將重要的日誌資訊集中至單一視覺化呈現介面，讓系統管理人員快速查詢關鍵資訊，也將資料篩選條件做事件即時告警。除了做資料集中化收集外，藉由 syslog-ng 的高度擴展性結合 ELK、Grafana 等第三方資料視覺化平台，來做設備狀態的監控或圖表呈現。透過 syslog-ng 的整合方案，降低了原有的資料收集瓶頸，也提高了資料收集品質和完整性。

威雲科技 WeiCloudTech
威雲科技股份有限公司
台北總公司：114 台北市內湖區瑞光路 335 號 5 樓 / (02)7721-8168
台中分公司：403 台中市西區忠明南路 62 號 6 樓之 2 / (04)2328-5588