Syslog-ng Store Box

日誌集中管理的最佳解決方案

面對 IT 基礎建設中，各項設備所產生巨量的日誌紀錄，管理即是一種重要手段；尤其面對法令合規性與資安事件預防及追查，日誌紀錄管理趨勢也朝向集中化方式，以達到事半功倍的效果，節省企業人力與金錢的成本支出。

在 Unix / Linux 平台上，One-Identity 推出一個最佳圖形化的日誌收集解決方案:

Syslog-ng Store Box。

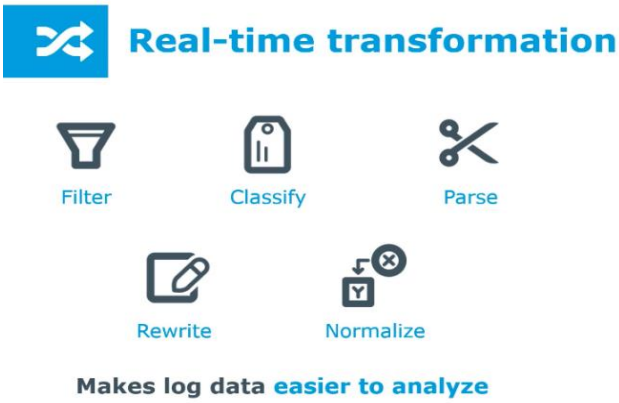
日誌紀錄的首要，即是進行集中化管理。

集中收集一般具有幾個特點：

本篇文章版權為倍力資訊股份有限公司所有，未經書面同意，嚴禁複製、轉載

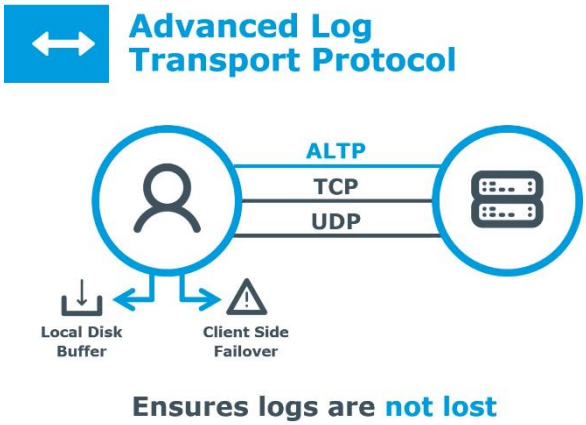
1. 分散處理
2. 多平台支援
3. 彈性化途徑

以上三個特點，均可以使日誌紀錄達成可及性運用之目的。

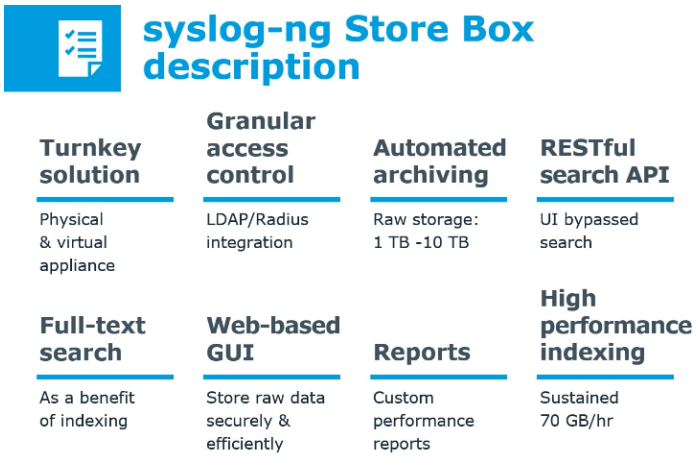


資料集中化管理後，則須進行預先處理。為使資料能容易進行分析，我們可透過過濾、分類、剖析、編寫、標準化這些方法，將資料預先處理，使資料達到可用性運用之目的。

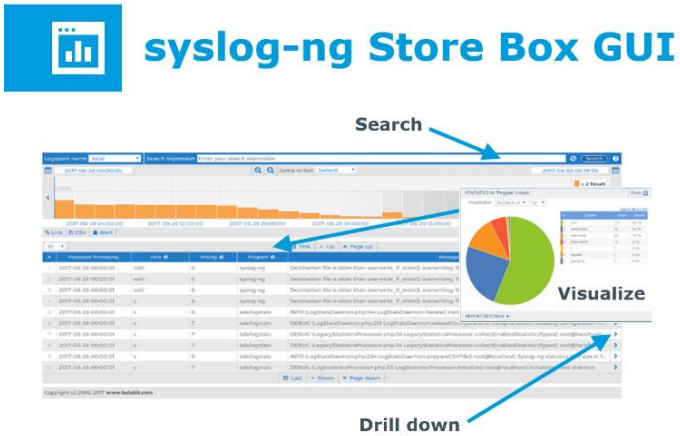
Syslog-ng Store Box 利用基於可信任之流量控制、磁碟緩衝容錯技術的先進日誌紀錄傳輸協定(ALTP)，加上既有之 TCP 與 UDP 傳輸協定，就能確保日誌紀錄不會因通訊距離而遺失。



本篇文章版權為倍力資訊股份有限公司所有，未經書面同意，嚴禁複製、轉載

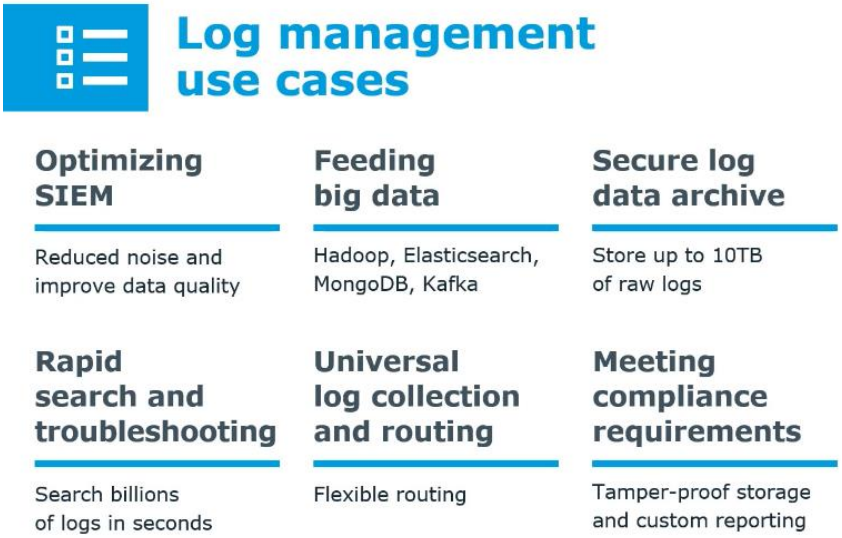


Syslog-ng Store Box 提供了一站式佈建解決方案，並支援 LDAP/Radius 驗證整合、自動封存機制、全文檢索、網頁 GUI 介面、自訂報表、高效索引以及提供 RESTful API 以整合其他檢索方式。



Syslog-ng Store Box 之圖形查詢介面，提供了高效率的搜尋功能，並且提供圖形統計報表，以供進一步資料分析研究。

本篇文章版權為倍力資訊股份有限公司所有，未經書面同意，嚴禁複製、轉載



總結 Syslog-ng Store Box 之優勢：

- 優化資料（SIEM）: 過濾資料並提高可用性。
- 提供大數據分析之穩定資料：支援 Hadoop、Elasticsearch、MongoDB、Kafka。
- 加密保存日誌：提供日誌儲存加密、時間戳記及數位簽章功能。
- 快速搜尋：在幾秒鐘內搜索數十億條日誌。
- 日誌收容：可搭配 Relay 機制，以提供靈活的收容配置。
- 滿足合規要求：提供防止竄改儲存機制和自訂報表功能。

◎如您有任何問題，歡迎隨時與我們聯繫：

系統服務部

副理 廖文志 Albert

02-27316868 分機 420 / albertliao@mpinfo.com.tw

本篇文章版權為倍力資訊股份有限公司所有，未經書面同意，嚴禁複製、轉載