syslog-ng™ Store Box

高效能日誌管理設備

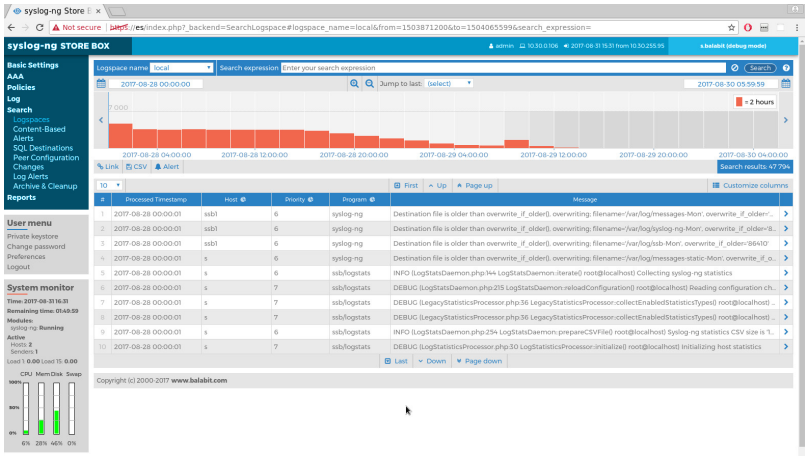
syslog-ng™ Store Box (SSB) 是一款能夠發揮 syslog-ng™ Premium Edition 強大能力的高效能且高可靠性的日誌管理設備。你可利用 SSB 收集和索引日誌資料、執行複雜的搜尋、以分級存取政策確保敏感資訊安全、產出報表以證明遵循資料法規、以及將日誌資料轉傳至第三方分析工具。

功能特性

- 高效能收集與索引
- 過濾、解析、改寫、正規化
- 快速搜尋數億訊息
- 透過自動化搜尋能力以發送警報
- 藉由 REST API 輕易整合第三方工具
- 安全、加密傳輸與儲存
- 分級 role-based 存取控制
- 多重日誌空間搜尋

詳細資訊

- Syslog-ng™ Store Box 詳細資訊
- 產品評估
- 與我聯絡



以前所未見的速度收集和索引

SSB 使用 syslog-ng™ Premium Edition 作爲日誌收集代理。安裝程式涵蓋 50 種以上的平台，包括最普及的 Linux 發行版、商業版 UNIX 和 Windows 。依照組態的不同， syslog-ng™ 每秒可收集多達 650,000 訊息。

syslog-ng™ Store Box 的檢索引擎採效能優化設計。依照實際組態的不同，一台 syslog-ng™ Store Box 可以持續每秒收集和索引多達 100,000 訊息。如果部署成 client relay 組態，一台單一的 SSB 可以從超過 10,000 個日誌來源收集日誌訊息。

搜尋、偵錯和報表

SSB 的全文搜尋功能讓你可以在數秒內，藉由直覺式的 Web 使用者介面搜尋數億日誌。你可以利用萬用字元和布林運算式，執行複雜的搜尋和縮小範圍查詢。它提供一種自動化搜尋功能，以便於更快速偵測異常活動：SSB 可以搜尋傳送進來的日誌資料，並於偵測到關鍵事件時發出預警。

使用者可以輕易建立客製化報表，以證明對於標準和資料法規的遵循，例如 PCI-DSS、ISO 27001、SOX 和 HIPAA。

過濾器與正規化

SSB 提供以訊息 metadata 和訊息內容爲基礎的彈性過濾功能，以減少高流量環境和區段資料所產生的雜訊，達到更好的搜尋和分析。

PatternDB™ 能夠根據訊息內容，對傳送進來的日誌進行即時分類，從非結構化日誌訊息擷取資訊單元，讓你可以匯集不同的日誌格式以便於搜尋和統計。

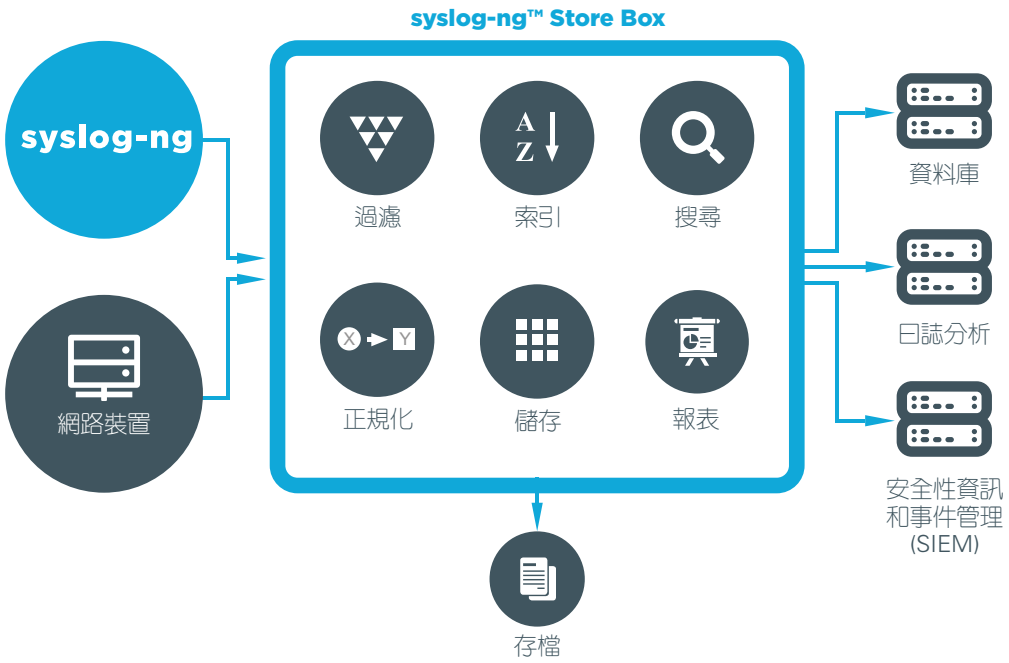
解析和改寫功能可供你根據過濾器和 PatternDB 結果，轉換和正規化日誌，以實現有效的搜尋與分析。

確保日誌資料安全

日誌可以使用 **Transport Layer Security (TLS)** 加密，從 syslog-ng™ Premium Edition clients 傳輸到 SSB ，以保護任何敏感資料。 TLS 在主機和伺服器之間使用 X.509 憑證進行相互驗證。

SSB 的 **Logstore** 將日誌資料儲存在加密、壓縮並且加上時間戳記的二進位檔案，且只允許授權的人員存取。

認證、授權與稽核 (Authentication, Authorization and Accounting) 設定**提供分級存取控制**，根據使用者群組權限限制 SSB 組態和存檔日誌的存取。SSB 可以和 LDAP 及 Radius 資料庫相整合。



儲存和轉傳

SSB 讓你可以儲存大量日誌資料，建立自動留存政策，以及將資料備份到遠端伺服器。最大的 SSB 設備可儲存多達 10 TB 未壓縮資料。

SSB 可以**自動將資料歸建到遠端伺服器**。遠端伺服器上面的資料同樣可接受存取和搜尋，你可以從 SSB 的 Web 介面存取數 TB 的稽核記錄。SSB 藉由 Network File System (NFS) 或 Server Message Block (SMB/CIFS) 協定，利用遠端伺服器當成一台網路驅動器。

你也可以將日誌轉傳至第三方分析工具或藉由其 **REST API** 從 SSB 擷取資料。你可以在 HTTPS 之上使用一個 RESTful 協定存取該 API，亦即你可使用任何能存取 RESTful HTTPS client 的程式語言，將 SSB 整合到你的環境，包括普及的語言例如 Java 和 Python。

搜尋多重日誌空間、設備與地點

SSB 將日誌收集和索引到一個稱爲日誌空間 (logspaces) 的虛擬容器，讓企業能夠以任意數量的準則，區分他們的日誌資料，以及根據使用者權限內容對日誌施以存取限制。多重日誌空間搜尋功能可供你搜尋位於多重日誌空間的日誌資料，不論是在相同的 SSB 設備上或者在遠端地點的不同設備。多重設備搜尋能力讓企業能以一種符合成本效益的方式增加設備，彈性的延展他們的日誌管理。

授權與支援

授權方式是以傳送日誌到 SSB 的 Log Source Hosts (LSH) 主機數量及其硬體組態爲基礎。資料的處理或儲存數量與速率沒有授權上的限制，簡化企業的專案預算。 SSB 客戶可以存取超過 50 種伺服器平台的 syslog-ng™ Premium Edition (PE) 二進位安裝檔。產品支援(包括 7x24支援)採年度合約制，內容包含軟體升級與硬體汰換。

高可用性

SSB 的部署方式可以採用高可用性組態。在此情形下，二台 SSB (其中一台爲 master，另一台爲 slave) 以相同組態同時運作。Master 和 slave 節點分享所有資料，如果 master 停止運轉，另一台將立即接管，進入 active 狀態，因此伺服器可繼續接受存取。SSB T4 和更大容量版本也配備雙重電源。

硬體規格

Product	Unit	Redundant PSU	Processor	Memory	Useful Capacity	RAID	IPMI
SSB T-1	1	No	Intel(R) Xeon(R) X3430 @ 2.40GHz (4 cores)	2 x 4 GB (DDR3)	1 TB	Software raid	Yes
SSB T-4	1	Yes	Intel(R) Xeon(R) E3-1275V2 @ 3.50GHz (4 cores)	2 x 4 GB (DDR3)	4 TB	LSI MegaRAID SAS 9271-4i	Yes
SSB T-10	2	Yes	2 x Intel(R) Xeon(R) E5-2630V2 @ 2.6GHz (6 cores)	8 x 4 GB (DDR3)	10 TB	LSI MegaRAID SAS 9271-4i	Yes

虛擬設備

SSB-VA	Virtual Appliance	VMWare ESXi/ESX	Microsoft Hyper-V	Amazon Web Services	Microsoft Azure

關於 One Identity

One Identity 協助企業建立正確的身分識別與存取管理 (IAM)。我們提供獨特的方案組合，包括身分識別管理組合、存取管理、特權管理、以及身分識別即服務方案，讓企業能夠充分發揮潛能而不會因爲安全問題而受到阻礙，同時有效的防範威脅。詳細資訊請參觀：OneIdentity.com