syslog-ng™ Store Box

高效能日誌管理應用裝置

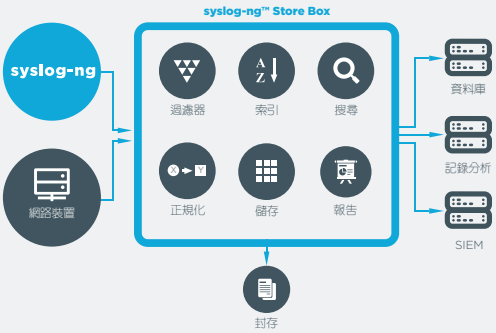
syslog-ng™ Store Box (SSB) 是一款高效能又可靠的日誌管理應用裝置，具備 syslog-ng™ Premium Edition 的優勢。使用 SSB 就能收集日誌資料並爲其編製索引、執行複雜的搜尋、以分級存取政策確保敏感資訊安全、產生報告以符合法規遵循，還能將日誌資料轉送至第三方分析工具。

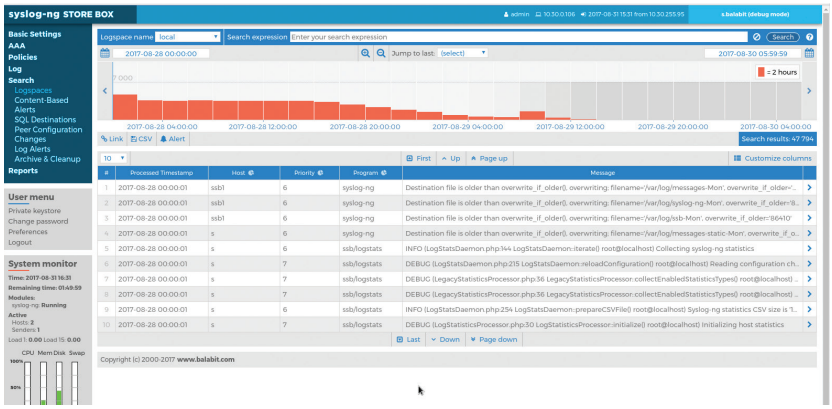
特色

- 高效能收集和編製索引功能
- 過濾、解析、改寫、正規化
- 快速在數十億則訊息中搜尋
- 根據自動化搜尋查詢發出警示
- 透過 REST API 輕鬆與第三方工具整合
- 安全 且經過加密的傳輸和儲存空間
- 精細的角色型存取控制
- 多重日誌空間搜尋功能

深入瞭解

- 深入瞭解有關 syslog-ng™ Store Box
- 索取試用版
- 與我聯絡





以無可匹敵的高速收集日誌資料並爲其編製索引

SSB 使用 syslog-ng™ Premium Edition 做爲日誌收集代理程式。安裝程式可用於 50 多個平台，包括最受歡迎的 Linux 發行版本、UNIX 和 Windows 的商用版本。依照組態的不同， syslog-ng™ 每秒可收集多達 650,000 訊息。

syslog-ng™Store Box 的索引編製引擎已針對效能進行最佳化。依照實際組態的不同，一台syslog-ng™ Store Box 最多可以持續每秒收集和索引多達 100,000 訊息。如果部署成 client relay 模式，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、故障診斷和回報

使用 SSB 全文搜尋功能，就能透過直觀的網頁式使用者介面在幾秒鐘內搜尋數十億筆日誌。萬用字元和 Boolean 運算子可以讓您執行複雜的搜尋並深入查看搜尋結果。它提供了自動搜尋功能，可以更快偵測異常狀況：SSB 能夠搜尋傳入的日誌資料，並在偵測到嚴重事件時傳送警示。

使用者可以輕鬆建立自訂報告，在法規遵循方面展現自身符合 PCI-DSS、ISO 27001、SOX 和 HIPAA 等標準和法規。

過濾與正規化

SSB 根據訊息中繼資料和訊息內容提供靈活的過濾功能，可以減少高流量環境和區段資料產生的雜訊，藉此改善搜尋和分析結果。

PatternDB™ 可以根據訊息內容來爲傳入的日誌即時分類、從非結構化日誌訊息擷取已命名的資訊元素，讓您可以匯總不同的日誌格式以搜尋和產生統計資料。

解析和改寫功能可以讓您根據過濾條件和 PatternDB™ 結果轉換和正規化日誌，藉此進行有效的搜尋和分析。

儲存和轉送

使用 SSB 就能儲存大量日誌資料、建立自動化保留原則、將資料備份到遠端伺服器。最大的 SSB 應用裝置可以儲存多達 10 TB 的未壓縮資料。

SSB 爲遠端伺服器提供自動資料封存。您仍然可以存取和搜尋遠端伺服器上的資料，也可以從 SSB 網頁介面存取數個 TB 的稽核線索。SSB 透過網路檔案系統 (NFS) 或伺服器訊息區 (SMB/CIFS) 通訊協定將遠端伺服器視爲網路磁碟機。

您也可以將日誌轉送至第三方分析工具，或透過其 REST API 從 SSB 擷取資料。您可以透過 HTTPS 使用 RESTful 通訊協定存取 API，這表示您可以使用對 RESTful HTTPS 用戶端具有存取權的任何程式設計語言，將 SSB 整合到您的環境，包括廣爲採用的 Java 和 Python。

保護您的日誌資料

您可以使用傳輸層安全性 (TLS) 加密將日誌從 syslog-ng™ Premium Edition 用戶端傳輸到 SSB，保護任何敏感資料。TLS 可讓主機和伺服器使用 X.509 憑證相互驗證。

SSB 的 Logstore 將日誌資料儲存在經過加密、壓縮且具有時間戳記的二進位檔案中，並僅供獲得授權的人員存取。

認證、授權與稽核(Authentication, Authorization and Accounting)設定提供分級存取控制，可根據使用者群組權限，限制對SSB 設定和存檔日誌的存取。SSB 可與 LDAP 和 Radius 資料庫整合。

可在多個日誌空間、應用裝置和位置進行搜尋

SSB 在所謂日誌空間的虛擬容器中收集日誌並爲其編製索引，這些虛擬容器可讓組織根據任意數目的準則分割日誌資料，並根據使用者設定檔限制使用者對日誌的存取。使用多重日誌空間搜尋功能，就能在多重日誌空間搜尋日誌資料，不論日誌資料是位在相同 SSB 應用裝置上，或是位於遠端位置的不同應用裝置上。可以在多個應用裝置之間搜尋的功能，讓組織能夠選擇以符合成本效益的方式，添購額外應用裝置，擴充其日誌管理。

授權與支援

授權方式是以傳送日誌到 SSB 的 Log Source Hosts (LSH) 主機數量及其硬體設定爲基礎。我們沒有對處理或儲存的資料量或速率設定授權限制，這點讓您在編列專案預算更加輕鬆。

高可用性

SSB 可以部署在高可用性設定中。在此情況下，兩個具有相同設定的 SSB 單元 (主機和從屬) 會同時運作。

硬體規格

產品	單元	備援 PSU	處理器	記憶體	可用儲存空間	RAID	IPMI
3000	1	是	Intel Xeon E3-1275 3.60 Ghz 4 核心	2 個 16 GB	6 TB	LSI MegaRAID SAS 9361-4	2.0
3500	1	是	2 個 Intel Xeon Silver 4110 2.1 Ghz 8 核心	8 個 8 GB	12 TB	LSI Avago CacheVault Power Module 02 (CVPM02) Kit	2.0

虛擬裝置支援平台

SSB-VA	虛擬裝置	VMWare ESXi/ESX	Microsoft Hyper-V	Amazon Web Services	Microsoft Azure

關於 One Identity

One Identity 協助組織正確處理身分識別與存取管理 (IAM)。組織使用我們獨特的產品組合 (包括身分識別管理、存取管理、特殊權限管理產品組合與身分識別即服務解決方案)，可以充分發揮潛力，不受安全性限制，又能抵禦威脅、確保安全。詳情請見 OneIdentity.com

© 2019 One Identity LLC 著作權所有，保留一切權利。One Identity 與 One Identity 標誌皆爲 One Identity LLC 在美國及/或其他國家/地區的商標和註冊商標。如需 One Identity 商標的完整清單，請瀏覽我們的網站：www.oneidentity.com/legal。所有其他商標、服務標誌、註冊商標及註冊服務標誌爲其個別擁有者之財產。
ssb_uc_flyer_en08_RS_A4_41702