syslog-ng™ Premium Edition

企業級日誌管理

syslog-ng™ Premium Edition 提供你掌握 IT 環境動態的關鍵日誌資料。不論使用者活動、效能尺度、網路流量或其他任何日誌資料，syslog-ng™ 都能鉅細靡遺的收集並建立集中化管理。你可以藉此移除資料孤島，並且掌握 IT 環境的完整能見度。

功能特性

- 高效能資料收集
- 零流失的訊息傳輸
- 即時過濾、解析、改寫、正規化
- 型態比對與關聯
- 以外部資料庫的鍵值對 (key-value pairs) 來豐富資料內容
- 以 Python 語言編寫你自己的語法分析器和樣板
- 使用 TLS 進行安全傳輸
- 防竄改的加密儲存
- 超過 50 種伺服器平台 (包括 Windows) 的安裝程式
- 無需安裝代理程式即可收集 Windows 事件日誌
- 將日誌資料直接傳送到 Apache Hadoop、Elasticsearch、MongoDB 和 Apache Kafka
- 使用 Puppet 執行中央配置管理
- 藉由企業整合功能以簡化自我監控

詳細資訊

- Syslog-ng™ Premium Edition 詳細資訊
- 產品評估
- 與我聯絡

擴展日誌管理

依照組態的不同，一台 syslog-ng™ 伺服器每秒可以從數千個日誌來源收集超過 50 萬日誌訊息。一台單一的中央伺服器可從 5,000 台以上的日誌來源主機收集日誌訊息，而如果部署成 client relay 組態，則可以從數萬個來源收集日誌。

確保日誌資料安全

加密傳輸與儲存可確保日誌不會遭竄改，維護數位監控鏈的完整性。TLS 加密技術可預防第三方存取日誌資料。Premium Edition 的 syslog-ng™ 可以將日誌訊息安全的儲存在加密、壓縮並且加上時間戳記的二進位檔案，確保任何敏感資料只允許持有加密金鑰的授權人員存取。

彈性路由日誌

syslog-ng™ 可以從廣泛來源收集日誌訊息，並且彈性的將它們路由到多重目標。

syslog-ng™ Premium Edition 能本地收集和處理從任何裝置藉由 syslog 協定、SQL 資料庫、Microsoft Windows 平台傳送的日誌訊息，以及 JSON 格式訊息或文字檔。它也可以處理多行日誌訊息，例如 Apache Tomcat 訊息。

許多大型企業組織需要將他們的日誌傳送到多重日誌分析工具。大多數日誌分析和 SIEM 方案都可以接收syslog訊息。syslog-ng™ 應用程式可以將日誌直接傳送到 SQL 資料庫、Elasticsearch (包括支援Shield安全部署)、MongoDB、Apache Kafka 和 Hadoop Distributed File System (HDFS) 節點，或使用 Standard Network Management Protocol (SNMP) 和 Simple Mail Transfer Protocol (SMTP) 傳送至其他目標。

Flexible Architecture

MAPR Certified Technology Partner

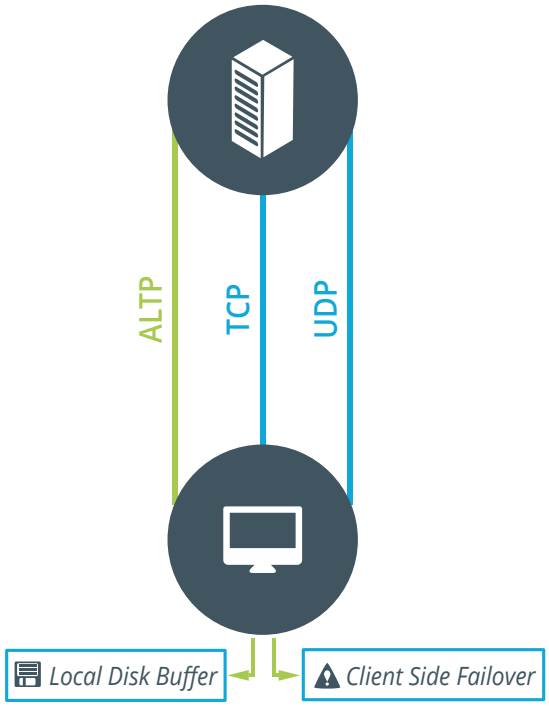
Hortonworks Certified HDP

對於分析、鑑識和資料法規遵循需求的基底資料有信心

syslog-ng™ 利用本地磁碟緩衝、客戶端故障轉移，以及應用層確認，確保零丟失的日誌訊息傳輸。

如果中央日誌伺服器或網路連線無法使用時，syslog-ng™ 會將訊息儲存在本地硬碟機。一旦連線恢復，syslog-ng™ 應用程式會自動依照原先訊息收受的順序，將儲存的訊息傳送到伺服器。

syslog-ng™ Premium Edition 支援 Advanced Log Transport Protocol (ALTP)，這項協定可以爲接受到的訊息提供應用層承認。駐留在伺服器的 syslog-ng™ 應用程式「承認」收到從用戶端 syslog-ng™ 應用程式傳送的日誌訊息，確保當發生傳輸層錯誤時不會造成訊息流失。



萬用日誌收集降低維護與部署成本

syslog-ng™ 可以作爲代理，部署在各類的主機，並且彈性的將日誌路由到多重分析工具或資料庫，免除在伺服器部署多重代理的需要。syslog-ng™ Premium Edition 爲超過 50 種伺服器平台提供經過測試的二進位檔案，節省安裝與維護時間。

優化分析工具

syslog-ng™ 提供強大的過濾、解析、改寫和分類選項，可以在遠端主機轉換日誌，減少轉傳至分析工具例如 SIEM 的日誌資料量與複雜性，降低整體擁有成本。

PatternDB™ 功能提供即時的日誌資料關聯，以及和預定義模式比對日誌訊息內容。

彈性的組態語言，讓使用者能以簡單的規則在遠端主機建構強大而複雜的日誌處理系統。

集中化組態管理

syslog-ng™ 支援 Puppet 組態管理軟體。你可以從一個套件庫安裝 syslog-ng™、升級 syslog-ng™ 至較新版本、從主機刪除 syslog-ng™、從中央套件庫更新遠端主機的 syslog-ng™ PE 組態檔、以及爲你的 syslog-ng™ 組態檔建立備份，並在需要時回復。

授權與支援

授權方式是以 Log Source Hosts (LSH) 數量爲基礎。授權內容對於處理或儲存的資料數量或速率皆無限制，簡化客戶的專案預算。 syslog-ng™ Premium Edition 客戶可以存取超過 50 種伺服器平台的二進位安裝檔。產品支援(包括 7x24 支援)採年度合約制。

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