CASE STUDY

使用 syslog-ng™ 進行彈性的日誌管理

syslog-ng™ Premium Edition

Magyar Telekom

Magyar Telekom 隸屬於德國電信集團，以 T-Home、T-Mobile 和 T-Systems 品牌提供固網和行動通訊、互聯網和 IPTV 服務以及 IT 服務。 Magyar Telekom 的收入超過 20 億美元，員工超過 11,000 人，是匈牙利最大的 ICT 供應商。

挑戰

作為一家通訊和互聯網服務供應商，Magyar Telekom 需要處理大量個人資料。為了遵守歐盟和國家政府資料保護法規，並保護其客戶的個人資料，Magyar Telekom 的 IT 安全政策要求必須收集所有處理個人資料的系統的日誌訊息，並將其發送到安全資訊與事件管理 (SIEM) 工具進行分析。客戶資料處理系統由各種伺服器操作系統、應用程式、資料庫和中介軟體組成。

由於 Magyar Telekom 的 IT 環境規模龐大且複雜，他們需要有效率的解決方案，以將多個來源端的日誌收集整合到一個單一、集中的日誌管理解決方案中。資安團隊以每秒大約 30,000 條訊息的處理速度，需要從超過 10,000 多個來源端收集、集中和管理日誌。如果每天處理超過 20 億條消息還不夠困難的話，這些日誌訊息還需要可靠、安全地傳輸和儲存，以便維持提供給 SIEM 的日誌資料的完整性。

不僅有日誌數量的問題，日誌來源端的多樣性和日誌格式的多變性也讓收集和集中管理變得更加困難。IT 資安團隊需要存取來自各種伺服器、操作系統、資安設備、標準和自定義應用程式，以及多種類型的資料庫的日誌訊息。

參考資訊

- Read more about syslog-ng™
- Request an evaluation
- Request pricing

“ 如果沒有 syslog-ng 的獨特功能，我們就無法收集和集中大量日誌。在 One Identity 的專業服務的幫助下，我們能夠部署高度可靠且安全的日誌基礎架構來處理數十億條日誌訊息。”

Magyar Telekom 資訊安全長
Krisztian Hary

解決方案

有了使用 syslog-ng™ 開源版良好的體驗後，Magyar Telekom 尋求 One Identity 來幫助他們設計和實施高度可靠的集中式日誌管理解決方案。syslog-ng™ Premium Edition 為 IT 資安團隊提供了解決方案，在將遠端主機上的日誌傳輸到中央日誌伺服器之前，先對其進行過濾和結構化。為避免爆炸式的大量日誌資料，Magyar Telekom 使用 syslog-ng™ 以幾乎即時的方式推送日誌訊息，而不是從中央伺服器拉取日誌，這也消除了遠端存取日誌來源主機的需求。

由於消費者的敏感性資料，Magyar Telekom 需要確保日誌在收集和傳輸到中央伺服器的過程中不會遺失。為了實現可靠的傳輸，syslog-ng™ Premium Edition 在網路連接或日誌目的地不可用的情況下，將訊息儲存在日誌來源端主機上。透過可靠資料傳輸原理 (RLTP™)，一種應用程式傳輸協定，syslog-ng™ 會檢測接收端最後收到的訊息，然後從該時間點開始重新發送訊息，確保在連接中斷的情況下接收端不會重覆收到訊息。

為了集中管理日誌資料的流量，syslog-ng™ 客戶端將日誌訊息傳輸到具有單個 IP 位址的負載平衡 Cisco ACE 路由器。在負載平衡器的背後，Magyar Telekom 部署了syslog-ng™ Premium Edition 作為群集配置的中央日誌伺服器，以提供 N+1 冗餘。 使用 syslog-ng™ 作為其集中式日誌管理解決方案，Magyar Telekom 能夠將日誌收集整合至一個可擴充、可靠的日誌管理工具中，使分析工具能夠專注於較小、更可靠的日誌資料集。

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為安全問題而受到阻礙，同時有效的防範威脅。
更多詳細資訊 OneIdentity.com