SYSLOG-NG BASED LOGGING INFRASTRUCTURE

Szabolcs Szigeti, sziqi@ik.bme.hu
Péter Adamkó, adamko@ik.bme.hu
Ádám Gábor, gadam@it2.bme.hu
BME Innovation and Knowledge Centre of Information Technology

Csaba Major, major@balabit.hu
BalaBit IT Security Ltd,

Logging is fundamental in the operation of information technology systems. Traditionally, the syslogd tool and protocol is used for logging. In today's large and complex information systems not only gathering and transporting logs is a complex task, but managing the logging infrastructure is a challenge.
The open source syslog-ng tool of Balabit ltd. is a popular substitute for the original syslogd tool. It provides enhanced features and performance. At the Innovation and Knowledge Centre of Information Technology at Budapest University of Technology and Economics in cooperation with Balabit Ltd. a development project was aimed at developing a tool for implementing a log gathering infrastructure. The system is comprised of software and hardware components. It is a centrally manageable, scalable logging solution. The paper describes the R&D work at the Innovation and Knowledge Centre of Information Technology and the logging system developed here.