

NAPLÓZÓ INFRASTRUKTÚRA SYSLOG-NG-VEL

Szigeti Szabolcs, szigi@ik.bme.hu

Adamkó Péter, adamko@ik.bme.hu

Gábor Ádám, gadam@it2.bme.hu

BME Információtechnológia Innovációs és Tudásközpont

Major Csaba, major@balabit.hu

BalaBit IT Security Kft,

Informatikai rendszerek üzemeltetésének alapvető része a megbízható, hatékony naplózás. Hagyományosan a syslog programra és protokollra alapozott naplózó megoldások szolgálnak. A mai nagyméretű informatikai rendszerekben, hálózatokban nem csak a napló események gyűjtése és továbbítása jelent feladatot, de magának a naplózó infrastruktúrának a menedzselése is.

A Balabit Kft. syslog-ng nevű nyílt forráskódú eszköze népszerű helyettesítője az eredeti syslogd programnak, mivel teljesítményben és funkciókban jelentősen felülmúlja. A Budapesti Műszaki és Gazdaságtudományi Egyetem Információtechnológia Innovációs és Tudásközpont (BME IT2) a Balabit Kft-vel együttműködve kifejlesztett egy, a syslog-ng-n alapuló komplex naplózó infrastruktúrát megvalósító eszközt. A szoftver és hardver komponensekből álló rendszer központilag menedzselhető, skálázható naplózó megoldást tesz lehetővé.

Az előadás bemutatja az IT2 keretében folyó fejlesztőmunkát és a kifejlesztett eszközt.