



## ▪ LogLogic

### Log-menedzsment eszközök

Az informatikai biztonsági kockázatok csökkentésének, a jogi szabályozás által támasztott követelmények biztosításának, vagy akár az üzemeltetés során felmerülő problémák megoldásának érdekében szükség lehet a legkülönbözőbb rendszereken eltárolt naplóinformációk közötti hatékony keresésre. Mindezek feltétele a hálózatban szétszórta naplók összegyűjtése.

A fent említett okoknál fogva szükségessé válhat a felhasználók tevékenységéről, rendszerek működéséről, hozzáférési jogosultságok változásairól szóló bejegyzések begyűjtésén túl ezen információk akár határozatlan idejű, kereshető formátumú tárolása, mely egyben a jelentések elkészítését is támogatja. A LogLogic teljesíti ezeket az információ-kezelési igényeket: egy nagymértékben skálázható, rendkívül nagy teljesítményű, másodpercenként több tízezer naplóbejegyzést feldolgozni képes rendszert nyújt. Fő feladata a teljes hálózaton fellelhető összes naplóinformáció begyűjtése és biztonságos tárolása, illetve bármely esemény után az információ keresése egyszerű lekérések vagy formázott riportok segítségével.

A hálózaton megjelenő információ gyűjtése és monitorozása céljából egy meglévő IT infrastruktúra esetén nem megengedhető a jól működő eszközök és alkalmazások leselejtezése és cseréje. A LogLogic megoldásait éppen ezért úgy tervezték, hogy megoldást nyújtsanak bármely eszköz vagy alkalmazás naplóinak gyűjtésére - még ha az saját fejlesztésű is -, kliens telepítése nélkül, vagy akár azzal is.

A LogLogic eszközök között két termékcsaláddal találkozhatunk, a LogLogic ST-vel, amely a logok gyűjtésére és tárolására specializálódott, illetve a LogLogic LX-el, mellyel gyors riportokat lehet készíteni.

### LogLogic ST

A LogLogic ST családba tartozó eszközök alapvető funkciója a különböző rendszerekből a logok összegyűjtése valamint tárolása. A gépeket a tároló- valamint feldolgozó-képességük szerint csoportosítják. Egyes termékek akár 11 évig is tudják tárolni az adatokat, valamint hálózati tároló is kapcsolható hozzájuk. A tárolt adatokban való keresés egyszerűsített, mivel a fő cél itt a nagy adathalmazban történő hatékony keresés.

### LogLogic LX

A LogLogic LX család eszközei az ST tulajdonságait kiegészítendő, a rövidebb ideig történő tárolás (maximum 90 nap) és az ebből történő részletes jelentéskészítés, a valós idejű riasztások és figyelések biztosítására kerültek kifejlesztésre. Az ST és az LX eszközök együttes alkalmazása homogén környezetet biztosít az inhomogén rendszerek naplózásának hatékony felügyeletére.

#### ▪ A LogLogic ST család jellemzői:

- Akár 75000 üzenet / másodperc feldolgozási kapacitás
- Tömörítési arány maximum 12:1
- Tárolási kapacitás: max. 2.8TB
- CPU: AMD Opteron 2xx család
- Táp: 2x350 watt
- 1db 10/100 Ethernet port management célokra
- Gigabit Ethernet port/portok az adatok gyűjtésére
- Hálózati adattárolási lehetőség: NAS, SAN

#### ▪ A LogLogic LX család jellemzői:

- Akár 4000 üzenet / másodperc feldolgozási kapacitás
- Tömörítési arány maximum 12:1
- Tárolási kapacitás: max. 936GB
- CPU: AMD Opteron 2xx család
- Táp: 2x350 watt
- 1db 10/100 Ethernet port management célokra
- Gigabit Ethernet port/portok az ST egységtől jövő adatok fogadására
- Gyorskeresés az indexelt adatbázis segítségével
- Gyors riportolási lehetőség több fájlformátumba történő exportálás segítségével
- Valós idejű riasztási lehetőség