KÖZPONTI NAPLÓZÓSZERVER HETEROGÉN KÖRNYEZETBE

syslog-ng Store Box

naplók megbízható gyűjtése és tárolása

- Központi naplózószerver berendezés
- Titkosított, aláírt, tömörített és időpecséttel ellátott tárolás
- Web alapú konfigurációs felület és üzenetkeresés
- Gyors keresési lehetőség a naplóüzenetek indexelése révén
- Teljes napló-életciklus menedzsment
- Üzenetek továbbítása külső adatbázisnak vagy SIEM eszköznek
- Akár 10 Terabyte hasznos lemezterület
- Másodpercenként több mint 100.000 üzenet gyűjtése és 75.000 üzenet indexelése valós időben

Egyszerű megoldást keres naplóüzenetei tárolására? Meg akarja akadályozni, hogy illetéktelenek férjenek hozzá az üzeneteihez? Egy megbízható platformra van szüksége magas rendelkezésre állással és kitűnő terméktámogatással? A naplózó infrastruktúrája meg kell, hogy feleljen valamilyen külső szabályozásnak?

A világszerte vállalatok ezrei által használt syslog-ng alkalmazásra épülő syslog-ng Store Box (SSB) egy hatékony és könnyen konfigurálható berendezés a naplóüzenetek gyűjtésére és tárolására. Az SSB az operációs rendszerek és hálózati eszközök széles skálájáról képes naplóüzeneteket fogadni, feldolgozni és biztonságosan tárolni.

Biztonságos és megbízható üzenettovábbítás

A syslog-ng Store Box a hálózati eszközök és alkalmazások által mind a hagyományos BSD-syslog protokollal, mind a legújabb syslog protokoll szabványokkal küldött üzeneteket egyaránt képes feldolgozni és osztályozni. Az SSB az UDP, TCP és TLS hálózati protokollon érkező üzeneteket fogadja. A TLS-titkosított csatornák kölcsönös autentikálása biztosítja a továbbított információ bizalmasságát és integritását. Ha az üzenetek továbbítására syslog-ng-t használ, akkor még hálózati vagy hardverhiba esetén is elkerülheti az üzenetvesztést.

Web alapú konfiguráció és hozzáférés vezérlés

Az SSB böngészőből konfigurálható egy egyszerű, letisztult felhasználó felület segítségével. A naplóüzenetek – beleértve a távoli szerveren tárolt üzeneteket is – az SSB felületén keresztül elérhetőek és kereshetőek. Az SSB továbbá teljesen testre szabható hozzáférés vezérléssel rendelkezik: pontosan meghatározhatja, hogy az SSB különböző beállításait ki módosíthatja, vagy a tárolt üzenetekhez ki férhet hozzá. A felhasználócsoportok és jogosultságok akár egy LDAP (például Microsoft Active Directory) szervertől is lekérdezhetőek. A beállítások változásait az SSB automatikusan naplózza.

Extrém terhelhetőség

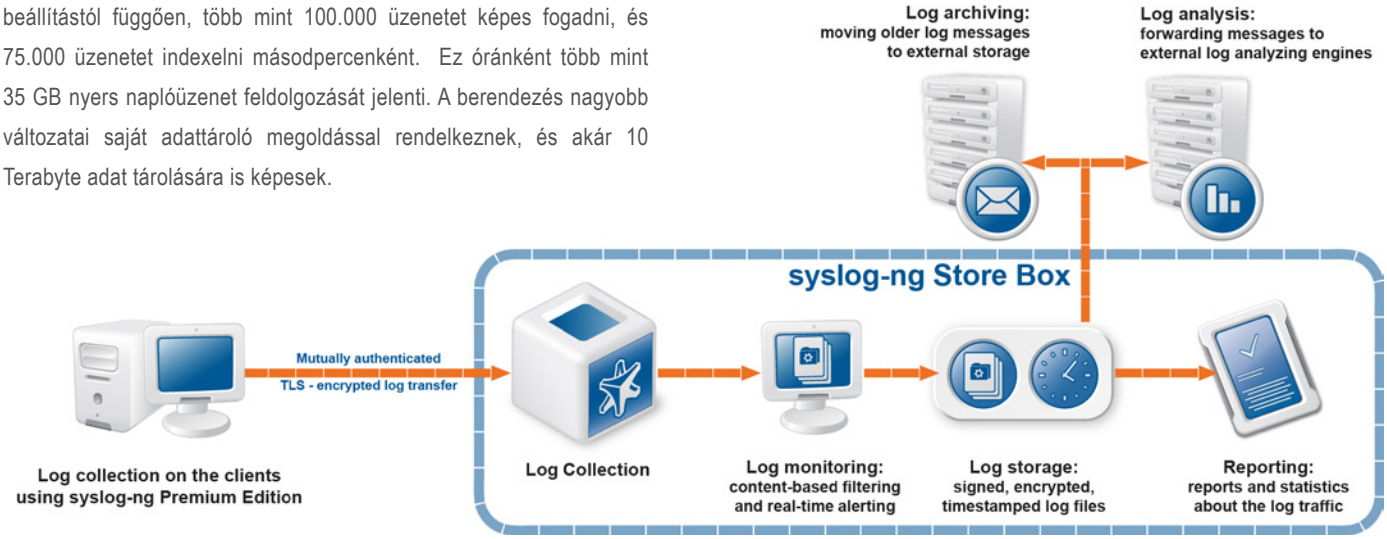
A syslog-ng Store Box egy teljesítményre optimalizált eszköz, és elképesztő mennyiségű üzenet feldolgozására képes. Pontos beállítástól függően, több mint 100.000 üzenetet képes fogadni, és 75.000 üzenetet indexelni másodpercenként. Ez óránként több mint 35 GB nyers naplóüzenet feldolgozását jelenti. A berendezés nagyobb változatai saját adattároló megoldással rendelkeznek, és akár 10 Terabyte adat tárolására is képesek.

Aláírt, időpecsételt tárolás

A syslog-ng Store Box a naplóüzeneteket titkosított, tömörített és digitálisan aláírt bináris fájlokban is képes tárolni. Ez biztosítja, hogy érzékeny adatokhoz csak az erre jogosult, a megfelelő titkosítási kulcsokkal rendelkező személyek férhetnek hozzá. A naplófájlok egy-egy részét a többi résztől függetlenül el lehet látni időpecséttel; az időpecsétet külső szolgáltatótól (Timestamping Authority, TSA) is lehet kérni. A naplófájlok tartalma indexelt, akár több Terabyte adat is online kereshető. Az SSB minden adatot tükrözött RAID meghajtókon tárol, hogy megelőzze az esetleges hardverhiba miatt fellépő adatvesztést. Két SSB egység magas rendelkezésre állást biztosító fürtként is használható, ami egyszerű és kényelmes módja a folytonos naplógyűjtés biztosításának.

Licenc és támogatás

A syslog-ng Store Box megvásárlása lehetővé teszi a syslog-ng Premium Edition letöltését, és naplógyűjtő kliensként való használatát az összes elérhető platformra. A szoftverkövetést – SSB és syslog-ng PE frissítések, javítások – az ár egy évig tartalmazza. A hardvertámogatás kiterjed a teljes helyszíni támogatásra egy éven keresztül. A termékhez 7x24 órás éves támogatás is vásárolható.



Közvetlen adatbázis elérés

Az SSB natívan támogatja az SQL adatbázisforrásokat, lehetővé téve a naplóüzenetek direkt elérését MySQL, Microsoft SQL (MSSQL), Oracle és PostgreSQL adatbázisokból. Emellett az SSB nem csak lokálisan tudja tárolni a naplóüzeneteket, hanem továbbíthatja azokat külső adatbázisba, távoli szerverre, vagy akár egy naplóelemző alkalmazásnak is.

Naplógyűjtő kliens számos platformra

Az SSB a syslog-ng Premium Edition alkalmazást használja a naplóüzenetek gyűjtésére a különböző operációs rendszereken és hardver platformokon, beleértve a régi és modern Linux-, Unix rendszereket, a BSD, Sun Solaris, HP-UX, IBM AIX, IBM System i, Tru64 és a Microsoft XP, Server 2003, Vista, Server 2008, Windows 7 platformokat.

Ha szeretné kipróbálni a syslog-ng Store Boxot, igényeljen egy tesztverziót a HTTP://WWW.BALABIT.COM/MYBALABIT/ oldalon.