BIZTONSÁGOS, TITKOSÍTOTT NAPLÓTOVÁBBÍTÁS ÉS TÁROLÁS

syslog-ng:

naplók megbízható gyűjtése, feldolgozása és tárolása

- TLS-titkosított üzenettovábbítás
- Közvetlen adatbázis elérés
- Titkosított, tömörített, és időpecséttel ellátott tárolás
- Üzenetek pufferelése merevlemezre
- Több mint 40 támogatott platform
- Üzenetek klasszifikálása valós időben

Az Ön naplózó infrastruktúrája biztonságos? Megfelelően kezeli az érzékeny információkat? Biztosítani szeretné, hogy megkap minden fontos naplóüzenetet? Elképesztően sok naplóüzenete keletkezik? Szeretne egy helyre gyűjteni minden naplóüzenetet?

syslog-ng Premium Edition
SECURITY IS KNOWING NOW

syslog-ng Premium Edition

BalaBit IT Security

www.balabit.hu

A syslog-ng megoldás a naplózókliensek, naplótovábbító eszközök (relay-ek) és naplózószerverek funkcióit egy megbízható, multiplatform naplózóinfrastruktúrába egyesíti. A syslog-ng összegyűjti és osztályozza az operációs rendszerek és alkalmazások naplóüzeneteit, és egy titkosított, megbízható csatornán keresztül a nagyteljesítményű naplózószerverre továbbítja, ahol az üzenetek további feldolgozása és biztonságos, titkosított fájlokban vagy adatbázisban tárolása történik. A megbízható transzportprotokollok, az üzenetek pufferelése, valamint a kliensoldalon megadható redundáns szerverek támogatása révén a syslog-ng minimálisra csökkenti az üzenetvesztés kockázatát, megfelelve a különböző szabályozások, így például a PCI-DSS előírásainak.

A syslog-ng Premium Edition a népszerű nyíltforrású változat alapjaira építve kínál olyan fejlett szolgáltatásokat, mint a titkosított és időpecséttel ellátott naplófájlok, a közvetlen adatbázis elérés, a merevlemezre történő pufferelés, a natív SSL titkosítás, vagy a Microsoft Windows és IBM System i platformokon futó kliensalkalmazások.

Megbízható, titkosított üzenettovábbítás

A syslog-ng lehetővé teszi, hogy a naplóüzeneteket távoli szerverekre továbbítsa a legújabb syslog protokollok felhasználásával. Az üzenetek merevlemezre történő pufferelése segít megelőzni az üzenetvesztést, ha a hálózat vagy a naplózószerver elérhetetlenné válik. A kölcsönösen autentikált, TLS-titkosított csatornák használata pedig biztosítja, hogy a továbbított információhoz illetéktelenek nem férhetnek hozzá.

Aláírt, időpecsételt tárolás

A syslog-ng Premium Edition a naplóüzeneteket titkosított, tömörített, indexelt, és időpecséttel ellátott bináris fájlokban is képes tárolni. Az érzékeny adatokhoz így csak az erre jogosult, a megfelelő titkosítási kulcsokkal rendelkező személyek férhetnek hozzá. Az időpecsétet külső szolgáltatótól (Timestamping Authority, TSA) is lehet kérni.

Több mint 40 támogatott platform

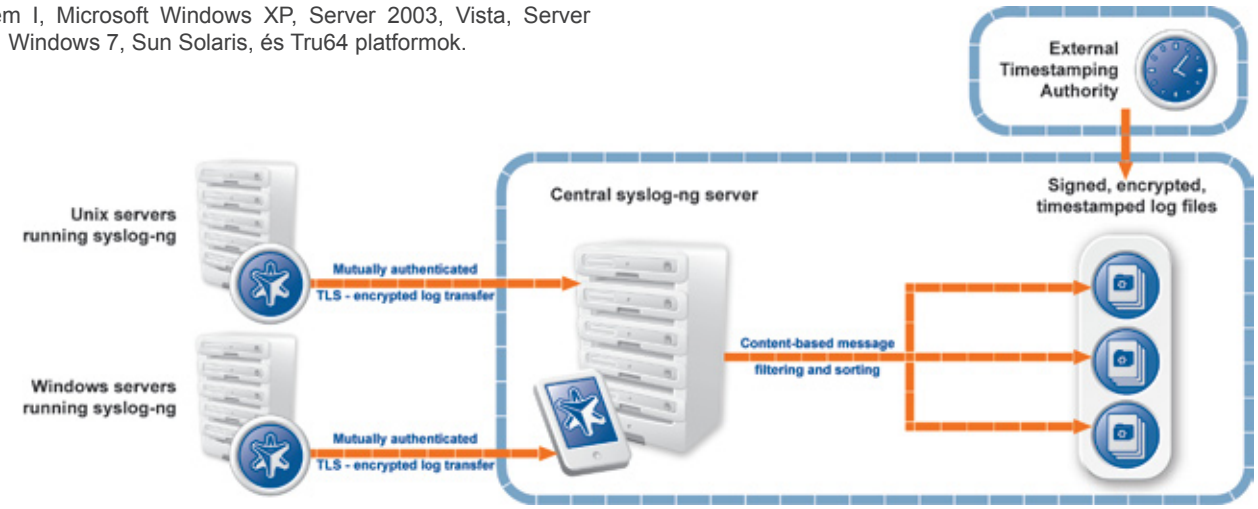
A syslog-ng alkalmazás több mint 40 platformot támogat, így ideális választás olyan környezet naplóüzeneteinek gyűjtésére, amely sok különböző operációs rendszert és hardver platformot használ. A támogatott rendszerek között szerepelnek a régi és modern Linux- és Unix rendszerek, a BSD, HP-UX, IBM AIX, IBM System I, Microsoft Windows XP, Server 2003, Vista, Server 2008, Windows 7, Sun Solaris, és Tru64 platformok.

Szűrés, szegmentálás, módosítás

Válogassa szét a bejövő naplóüzeneteket különböző paramétereik alapján, mint a küldő szerver, alkalmazás, vagy az üzenet prioritása. A syslog-ng az üzenetek részeit képes név-érték párokra vagy mezőkre tagolni, majd a mezők értékét módosítani, és így például az üzenetekből az érzékeny adatokat eltávolítani. A könyvtárak, fájlok és adatbázis táblák makrók segítségével dinamikusan hozhatóak létre, de akár az üzenetek is átformázhatók. A reguláris kifejezéseket és logikai műveleteket felhasználó komplex szűrések szinte korlátlan rugalmasságot nyújtanak, hogy csak a valóban fontos üzeneteket továbbítsa a megfelelő rendeltetési helyekre.

Üzenetek klasszifikálása

A syslog-ng alkalmazás képes minta-adatbázisok alapján osztályozni az üzeneteket. Az azonosított üzenetek címkézhetők és tartalmuk alapján szűrhetők, míg az ismeretlen üzenetek külön kategóriába kerülnek, lehetővé téve az artificial ignorance módszer alkalmazását. Az üzenetek klasszifikálása valós időben történik. Az üzenetminták könnyen bővíthetők további alkalmazásokhoz is.



Közvetlen adatbázis elérés

A naplóüzenetek adatbázisban tárolása révén az üzenetek gyorsan kereshetőek, és naplóelemző alkalmazásokkal is könnyű az együttműködés. A syslog-ng a következő adatbázisokat támogatja: MySQL, Microsoft SQL (MSSQL) , Oracle, PostgreSQL, és SQLite.

Extrém terhelhetőség

A syslog-ng a teljesítményre optimalizált alkalmazás, és elképesztő mennyiségű üzenet feldolgozására képes. Pontos beállításaitól függően valós időben másodpercenként akár 150000 üzenetet, vagy óránként több mint 24 GB nyers naplóüzenetet is képes feldolgozni belépőszintű szerverhardveren.

HA SZERETNÉ KIPRÓBÁLNI A SYSLOG-NG PREMIUM EDITION ALKALMAZÁST, IGÉNYELJEN EGY TESZTVERZIÓT A HTTP://WWW.BALABIT.HU/MYBALABIT/ OLDALON