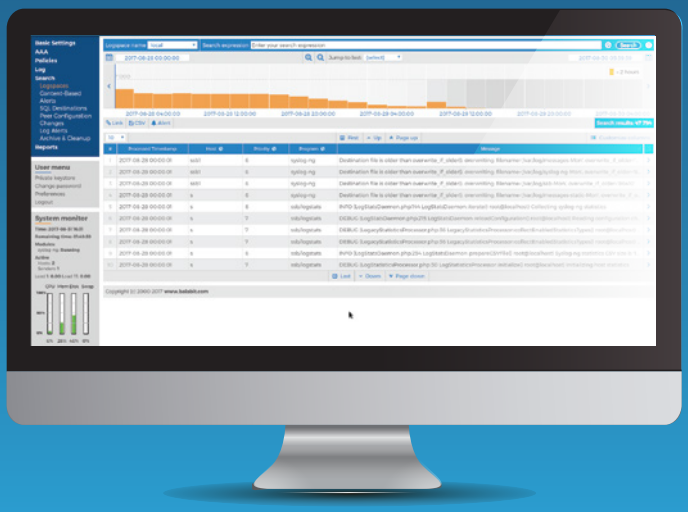
BALASYS

One Identity syslog-ng Store Box

Nagy teljesítményű naplókezelő eszköz

ELŐNYÖK

- Nagy teljesítményű naplógyűjtés és indexelés
- Szűrés, parszolás, újraírás és normalizálás
- Gyors keresés akár több milliárd üzenetben
- Automatikus kereséseken alapuló figyelmeztetések
- Könnyű integráció külső eszközökhöz REST API segítségével
- Biztonságos, titkosított naplótovábbítás és tárolás
- Részletes, szerep-alapú hozzáférés vezérlés
- Univerzális keresőfunkció



ÁTTEKINTÉS

A syslog-ng™ Store Box (SSB) egy nagy teljesítményű, magas megbízhatóságú naplókezelő eszköz, amely a syslog-ng Premium Edition erősségeire épít. Az SSB segítségével naplófájlokat gyűjthet, indexelhet, és komplex kereséseket hajthat végre a naplóüzenetek között, miközben részletes hozzáférés kezeléssel biztosíthatja az érzékeny információk védelmét. Az SSB jelentéskészítő funkciója segíti a törvényi előírásoknak való megfelelést. A naplóüzenetek külső elemző eszközök számára is továbbíthatók.

Páratlan sebességű napló gyűjtés és indexelés

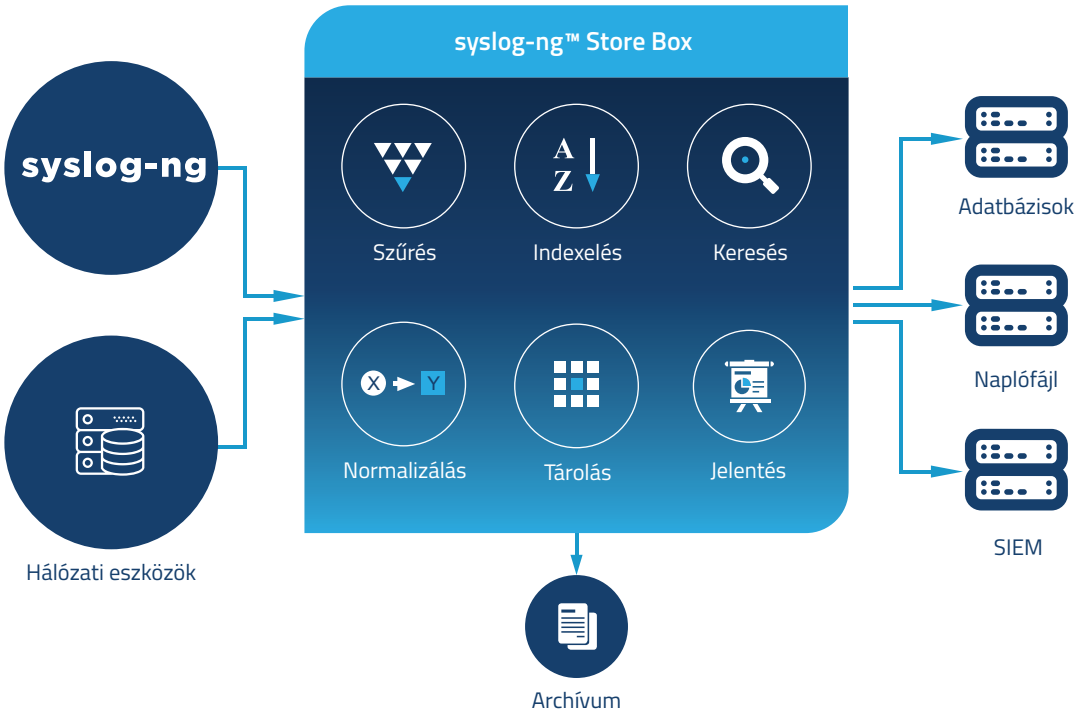
Az SSB a syslog-ng Premium Edition-t használja naplógyűjtő alkalmazásként. Több mint 50 platformra érhetők el telepítő fájlok, beleértve a legnépszerűbb Linux disztribúciókat, illetve a UNIX és Windows kereskedelmi verzióit is. Konfigurációtól függően a syslog-ng PE akár 650.000 naplóüzenetet is képes begyűjteni másodpercenként.

A syslog-ng Store Box indexelő motorját nagy teljesítményre optimalizálták. A konfigurációtól függően egyetlen SSB képes másodpercenként akár 100,000 naplóüzenetet összegyűjteni és indexelni, akár huzamosabb ideig is. "Client-relay" konfigurációban telepítve egyetlen SSB akár több mint tízezer forrásból is képes naplókat gyűjteni.

Keresés, hibaelhárítás és jelentéskészítés

Az SSB szabad szöveges keresőjével másodpercenként Ön több milliárd bejegyzésben kereshet az intuitív webes felhasználói felületen keresztül. A helyettesítő karakterek és logikai változók lehetővé teszik bonyolult lekérdezések és mélyre ható vizsgálatok elvégzését is. Az anomáliák gyorsabb észlelésének érdekében az SSB automatikus keresési funkcióval rendelkezik. Az SSB képes a bejövő naplóadatokon kereséseket futtatni, és riasztást küldeni, ha kritikus eseményt észlel.

A felhasználók könnyedén készíthetnek egyedi jelentéseket, eleget téve olyan megfelelési kötelezettségeknek, mint például a PCI-DSS, az ISO 27001, a SOX vagy a HIPAA.



Szűrés és normalizálás

Az SSB rugalmas szűrési lehetőségeket kínál az üzenetek meta adatai és tartalma alapján. Erre a nagyforgalmú környezetekben keletkező „üzenetzaj" csökkentése, valamint az adatok könnyebb kereshetősége és elemzése miatt lehet szükség. A PatternDB™ valós időben képes osztályozni a bejövő naplóadatokat tartalmuk alapján, és képes kinyerni előre definiált adatelemeket a strukturálatlan naplóüzenetekből. Ezzel lehetővé válik a különböző formátumú naplófájlokból származó adatok aggregálása keresések, illetve elemzések céljából. A parszoló és újraíró képességek lehetővé teszik a naplóüzenetek átalakítását és normalizálását a különböző szűrők és a PatternDB™ eredményei alapján, ezzel tovább segítve a hatékony keresést és elemzést.

Biztonságos naplóadat kezelés

Az SSB képes Transport Layer Security (TLS) titkosítással fogadni és továbbítani a naplófájlokat, így minden érzékeny adat védve marad. A TLS protokoll X.509 tanúsítványokkal azonosítja a hosztot és a szervert.

Az SSB az adatokat tömörítve, titkosítva és időpecséttel ellátva tárolja, a hozzáférést pedig kizárólag az erre felhatalmazott felhasználókra korlátozza.

A hitelesítési, engedélyezési és auditálási beállítások részletes hozzáférés-kezelést biztosítanak, így Ön a felhasználó csoporttagsága alapján korlátozhatja a hozzáférést a konfigurációhoz és a tárolt naplófájlokhoz egyaránt. Az SSB integrálható az LDAP és Radius felhasználói adatbázisokkal.

Tárolás és továbbítás

Az SSB segítségével nagy mennyiségű adat tárolható, automatizált archiválási szabályok alkothatók, és biztonsági mentések készíthe-tők távoli szerverekre. Az SSB 3500 hardver eszköz akár 12 terabájt adatot is képes tárolni, de a virtuális SSB eszköz ennél nagyobb tárkapacitás kezelésére is képes. Az SSB automatikus adatarchiválást biztosít a távoli szerverekre. A távoli szervereken levő adat hozzáférhető és kereshető marad: több terabájtnyi audit trail érhető el az SSB webes felületén keresztül. Az SSB hálózati meghajtóként használja a távoli szervert, a Network File System (NFS) vagy a Server Message Block (SMB/CIFS) protokollon keresztül.

A naplófájlok külső elemzőeszközökre is továbbíthatók, illetve REST API interfészen keresztül is kinyerhetők. A RESTful interfészhez HTTPS protokollon keresztül lehet hozzáférni. Ez azt jelenti, hogy bármilyen programozási nyelv használható az SSB integrációjához, amely rendelkezik RESTful HTTPS klienssel, mint például a népszerű Java és Python nyelvek.

Keresés egyszerre több logspace-ben, eszközön vagy helyszínen

Az SSB logspace-nek nevezett virtuális tárolókban gyűjti és indexeli a naplóüzeneteket. Ez lehetővé teszi a szervezetek számára, hogy a naplóikat tetszőleges kritériumok alapján elkülönítsék, és felhasz-nálói profilok alapján korlátozzák a hozzáférést hozzájuk. A multi-logspace keresési funkcióval Ön egyszerre több logspace-ben is kereshet, akár ugyanazon az SSB eszközön, vagy egy távoli eszközön. A több eszközön való egyidejű keresés lehetővé teszi a szervezetek számára, hogy skálázzák a naplókezelésüket, további eszközök költséghatékony hozzáadásával.

Licencelés és támogatás

A terméklicenc az eszköz hardware konfigurációjának és a napló-üzenet források (Log Source Host-ok) számának függvénye. Az adatfeldolgozás sebességre vagy a tárolási mennyiségre semmilyen korlát nincs, így a projekt költség-tervezése egyszerű. Az SSB megvásárlásával a felhasználó letöltheti, és kliens vagy relay módban használhatja a syslog-ng Premium Edition-t (PE), több mint 50 szerver platformon. A terméktámogatás - akár 7*24 órás is - évenként megújítható. A megvásárolt támogatási előfizetés feljogosítja a vásárlót a szoftver frissítésekre.

Magas rendelkezésre állás

Az SSB magas rendelkezésre állású konfigurációban is telepíthető. Ebben az esetben két, azonos konfigurációjú SSB egység (egy master és egy slave egység) működik egyidejűleg. A master egység minden adatot megoszt a slave egységgel, és ha működése leáll, a slave egység azonnal aktívvá válik, így a szerverek folyamatosan hozzáférhetők maradnak. Az SSB hard-ware redundáns tápegységgel rendelkezik.

Hardware specifikációk

Termék	Unit	Redundáns tápegység	Processzor	Memória	Hasznos kapacitás	RAID
SSB 3000	1	Nincs	Intel Xeon E3-1275 3.60 Ghz (4 Core)	2 x 16 GB	6 TB	LSI MegaRAID SAS 9361-4i
SSB 3500	1	Van	2 x Intel Xeon Silver 4110 2.1 Ghz 8 Core	8 x 8 GB	12 TB	LSI MegaRAID SAS 9361-16i +

Virtuális Gépek

SSB-VA	Virtual Appliance	VMWare ESXi/ESX	Microsoft Hyper-V	Amazon Web Services	Microsoft Azure

ONE IDENTITY™

A One Identity-ről

A One Identity segít a cégeknek a jogosultság és hozzáférés-kezelést (Identity and Access Management, IAM) jól csinálni. Jogosultság szabályozást (identity governance), hozzáférés-kezelést, kiemelt-felhasználó kezelést és jogosultságot, mint szolgáltatást (identity as a service) tartalmazó egyedi termék-portfóliója támogatja a szervezeteket üzleti lehetőségeik teljes kihasználásában, mindezt biztonsági béklyók nélkül, mégis védelmet nyújtva a fenyegetések ellen.