BALASYS

One Identity syslog-ng Premium Edition

Nagyvállalati szintű naplókezelés

ELŐNYÖK

Nagyteljesítményű napló gyűjtés

Üzenetvesztés nélküli továbbítás

Valós idejű szűrés, parszolás, újraírás és normalizálás

Minta-összehasonlítás és korreláció

Adatdúsítás kulcs-érték párokkal, külső adatbázisból

Saját parszer és sablon készítési lehetőség Pythonban

Biztonságos továbbítás a TLS használatával

Hamisíthatatlan, titkosított adattárolás

Telepítő készletek több mint 50 platformra, Windowsra is

Windows eseménynaplók gyűjtése kliens program telepítése nélkül

Közvetlen adatküldési képesség Apache Hadoop, Kafka, Elasticsearch és MongoDB-be

Központi konfigurációkezelés a Puppet segítségével

Egyszerű felügyelet vállalati integrációval

ÁTTEKINTÉS

A syslog-ng™ Premium Edition biztosítja a naplóadatokat, amelyek elengedhetetlenek ahhoz, hogy megértse, mi történik az IT környezetében. Legyen szó felhasználói tevékenységről, teljesítménymutatókról, hálózati forgalomról vagy más naplóadatokról, a syslog-ng képes összegyűjteni és centralizálni a kapcsolódó naplófájlokat. Így Ön megszüntetheti az adatsilókat, és biztosíthatja IT-környezetének teljes átláthatóságát.

Skálázható naplókezelés

Konfigurációtól függően egy syslog-ng szerver több mint félmillió naplóüzenetet képes begyűjteni másodpercenként több ezer naplóforrásból. Egyetlen syslog-ng szerver több mint 5000 forrás-gépről gyűjthet naplóüzeneteket. Ha client-relay konfigurációban telepítik, egyetlen syslog-ng naplózó szerver több tízezer forrásból is képes naplóadatokat gyűjteni.

Biztonságos naplóadatok

A titkosított adatátvitelnek és adattárolásnak köszönhetően a naplók nem hamisíthatók, így sértetlen marad az adatok integritása. A TLS titkosítás megakadályozza, hogy harmadik fél hozzáférjen a naplóadatokhoz. A syslog-ng Premium Edition képes a napló-üzeneteket titkosított, tömörített, és időpecséttel ellátott, biztonságos bináris fájlokban tárolni, így minden érzékeny adat csak a jogosult személyek számára hozzáférhető, akik rendelkeznek a megfelelő titkosítási kulccsal.

1. Ábra: Rugalmas architektúra

Megbízható adatok elemzéshez, incidensvizsgálathoz vagy törvényi megfeleléshez

Mivel a helyi pufferelést, a kliens oldali feladatátvételt (Client Side Failover), és az alkalmazás szintű nyugtázást is támogatja, a syslog-ng egyetlen üzenetet sem veszít el az adattovábbítás során. Ha a központi naplózó szerver leáll, vagy a kapcsolat megszűnik, a syslog-ng a helyi lemezen tárolja a naplófájlokat. Mikor a hiba elhárult, és a kapcsolat helyreállt, a syslog-ng automatikusan továbbítja a naplókat a szervernek, ugyanabban a sorrendben, ahogyan rögzítette azokat.

A syslog-ng Preimum Edition támogatja a Reliable Log Transfer (RLTP™) protokollt, amely lehetővé teszi az alkalmazás szintű üzenetnyugtázást. A szerveren működő syslog-ng alkalmazás nyugtázza a syslog-ng kliensről küldött napló üzeneteket így biztosítva, hogy hálózati meghibásodás esetén se vesszenek el üzenetek.

Elemző eszközök optimalizálása

Erőteljes szűrő, parszoló, újraíró és osztályozó képességeinek köszönhetően a syslog-ng képes átalakítani a naplóüzeneteket már a távoli gépeken, így csökkentve a naplóelemző eszközökre (pl. SIEM) küldött naplóadatok mennyiségét és komplexitását, csökkentve az ilyen eszközök teljes tulajdonlási költségeit.

A PatternDB funkció képes valós idejű adatkorrelációra, vagyis a naplóadatok összevetésére előre meghatározott adatsémákkal. A rugalmas konfigurációs nyelv pedig lehetővé teszi, hogy a felhasználók komplex, mégis robosztus napló feldolgozó rendszereket hozzanak létre egyszerű szabályok alkalmazásával a távoli gépeken.

Rugalmas napló továbbítás

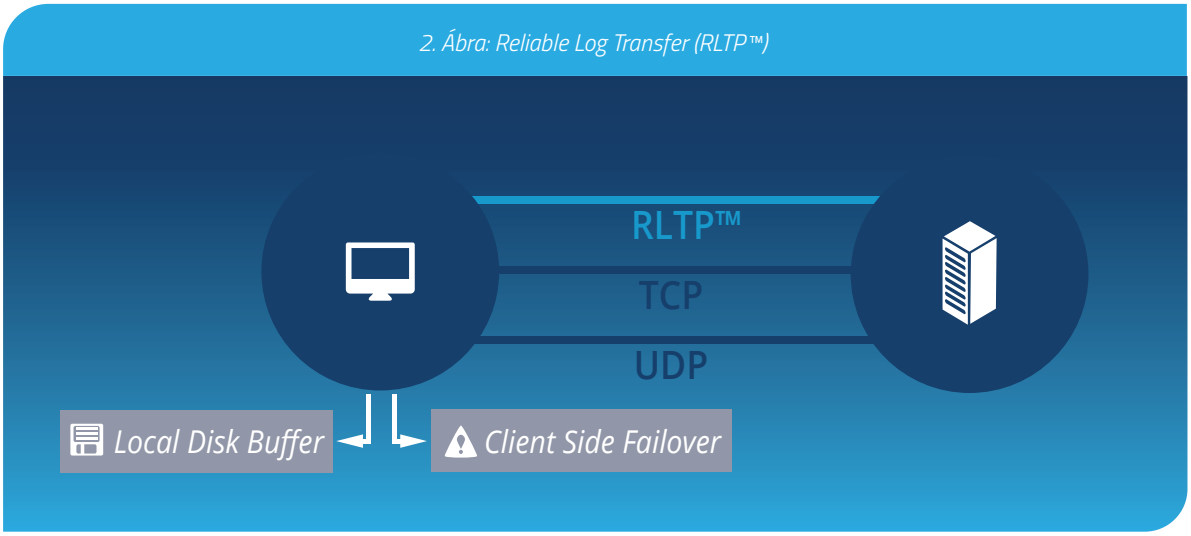
A syslog-ng számos forrásból képes naplóüzenetek gyűjtésére és rugalmas továbbítására, több célhelyre is. A syslog-ng Premium Edition képes begyűjteni és feldolgozni a naplóadatokat bármilyen eszközről syslog protokollon, SQL adatbázisokon, Microsoft Windows platformon, továbbá JSON formátumú üzeneteken vagy plain text formátumú szövegeken keresztül. Ezen kívül képes a többsoros naplóüzenetek feldolgozására is, mint például az Apache Tomcat üzenetek.

Számos nagy szervezetnek egyszerre több naplóelemzési esz-közre is el kell küldenie a naplóadatokat. A legtöbb log elemző és SIEM megoldás képes fogadni syslog üzeneteket. Azonban a syslog-ng alkalmazás képes a naplókat közvetlenül továbbítani SQL adatbázisokba, az Elastisearch-be, a MongoDB-be, az Apache Kafka, és Hadoop Distributed File System (HDFS) csomópontokra is, sőt használja a Standard Network Management Protokollt (SNMP) és a Simple Mail Transfer Protokollt is az egyéb célhelyekre való továbbításhoz.

Karbantartási és telepítési költségek csökkentése univerzális napló gyűjtéssel

A syslog-ng számos különböző hosztra telepíthető ágensprogramként, és képes továbbítani a naplóüzeneteket akár több elemzőeszköz vagy adatbázis felé is, így szükségtelenné teszi egyszerre több ágensprogram telepítését a hosztokon. A syslog-ng Premium Edition bevizsgált telepítői több mint 50 szerverplatformra érhetők el, ezzel is csökkentve a telepítéshez és karbantartáshoz szükséges időt.

2. Ábra: Reliable Log Transfer (RLTP™)



Központosított konfigurációkezelés

A syslog-ng támogatja a Puppet konfiguráció menedzsment szoft-vert, amely lehetővé teszi a syslog-ng telepítését csomag-tárból, a syslog-ng frissítését egy újabb verzióra, a syslog-ng törlését egy gazdagépről, illetve a syslog-ng PE konfigurációs fájl frissítését a távoli gépen. Ezen felül biztonsági másolat létre-hozása is lehetséges a syslog-ng konfigurációs fájljairól, illetve rollback is végrehajtható, amennyiben szükséges.

Licencelés és támogatás

A terméklicenc a napló források (Log Source Host-ok, LSH) számán alapszik. A feldolgozott és tárolt adatok mennyiségére, és feldolgozási sebességére semmilyen korlát nincs, így a pro-jekt költségtervezése egyszerű. A syslog-ng Premium Edition megvásárlása feljogosítja a felhasználót, a bináris telepítő fájlok letöltésére több mint 50 szerver platformra. A terméktámogatás – akár 7*24 órás is – évenként megújítható.

ONE IDENTITY™

A One Identity-ről

A One Identity segít a cégeknek a jogosultság és hozzáférés-ke-zelést (Identity and Access Management, IAM) jól csinálni. Jogosultság szabályozást (identity governance), hozzáférés-ke-zelést, 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.