

Termékismertető

Sentinel Log Manager

A Novell professzionális naplókezelési megoldása lehetővé teszi, hogy a különböző szerverek és hálózati eszközök által generált nagy mennyiségű, eltérő formátumú naplófájlt hatékonyan tárolja és elemezze. A naplóadatok könnyen és gyorsan visszakereshetők, így a kritikus eseményekről rövid időn belül kellő mennyiségű hasznos információ állhat rendelkezésre, a beépített riportkészítési képesség pedig segítséget nyújt az áttekintéshez és az előírásoknak való megfeleléshez.

Minél több a naplóadat, annál jobb?

A naplófájlokat megfelelően tárolni, a releváns naplóbejegyzéseket megkeresni és értelmezni hagyományos módszerekkel komoly erőforrásokat igényel. Elképzelhető, hogy mire egyes naplóbejegyzések vizsgálatára szükség lenne, azok már kigördülnek a megtartásra kijelölt időablakból, vagy nem tartalmazzák a szükséges részletességgel az adatokat, esetleg hatalmas archivált fájljokból kell őket egyenként előkeresni és fáradságos munkával korrelálni.

A Sentinel Log Manager leveszi ezeket a terheket az IT szakemberek válláról. Folyamatosan gyűjti a naplóadatokat a különböző szerverekről és hálózati eszközökről, valós időben feldolgozza, egységesíti, kereshetővé teszi őket, és gondoskodik az összegyűjtött nagy mennyiségű adat hatékony hosszútávú tárolásáról. Végre eljöhét tehát az az idő, amikor káros következmények nélkül növelheti naplófájljai részletességét és jóval hosszabb ideig megőrizheti azokat, így amikor egy kritikus eseményt kell elemezni, több hasznos információ állhat a rendelkezésére. Természetesen az eredeti naplóbejegyzések is teljes terjedelmükben megőrzésre kerülnek, utólag is bármikor lehetőség van részletekbe menő vizsgálatukra, és így a megfelelőségi követelmények is könnyűszerrel teljesíthetők.

Az igazság pillanata: a keresés

Hiába gyűjtött össze és tárolt hatékonyan bármennyi naplóadatot, ha a kritikus pillanatban nincs gyorsan kéznél az információ, amelyre épp szüksége van. A Sentinel Log Manager modern és kifinomult AJAX-alapú keresőfelületével az egyszerű szövegrészlet-kereséstől a bonyolultabb szempontokig könnyedén és gyorsan összeállíthatja a keresési kritériumokat, az egyes adatmezőkre kattintva pedig további szűrőket kapcsolhat be. A rendszer a régebbi, archivált adatokban is épp oly zökkenőmentesen keres, mint a közelmúltban begyűjtött naplóbejegyzések között, ráadásul nem csak a helyi naplószerver adatbázisában, hanem minden további erőfeszítés nélkül bevonhatja a cégénél található többi Sentinel Log Manager szerver által tárolt adatokat is. Ily módon globális kiterjedésű, elosztott informatikai rendszerek esetében is átfogó képet kaphat a felhasználói tevékenységekről, eseményekről, esetleges anomáliákról, azok térbeli és időbeli összefüggéseiről.

Riportkészítés egyetlen kattintással

Ha már megtalálta a keresett adatokat, illetve a keresés során összeállította az ehhez szükséges kritériumokat és szűrőket, mindezt egyetlen kattintással riport-sémává alakíthatja, melyet később bármikor újra felhasználhat.

■ Megoldás

- Személyazonosság-kezelés és biztonság
- Logmenedzsment
- Biztonsági események kezelése (SIEM – Security Information and Event Management)

■ Termékek

- Sentinel Log Manager

Fontosabb képességek:

- naplófájlok és események automatikus összegyűjtése, normalizálása
- nagy teljesítményű, valós idejű feldolgozás
- gyors keresés tetszőleges szempontok szerint
- elosztott keresés az összes Log Manager szerveren
- jelentéskészítés egyetlen kattintással
- PCI-DSS, HIPAA, SOX, és egyéb szabványos riport-sémák
- biztonságos naplótovábbítás TLS/SSL titkosítással
- optimális tárhelygazdálkodás 10:1 arányú adattömörítéssel és a tárhely-igény előrejelzésével

Fontosabb előnyök:

- gyorsan bevezethető, rugalmas, jól skálázható naplókezelési megoldás
- a beépített jelentéskészítés biztosítja a megfelelést a PCI-DSS, HIPAA, SOX, és más előírásoknak
- nincs speciális hardverigény, akár virtuális alkalmazás formájában is telepíthető
- szabványos adatformátum, amely más eszközökkel is tovább kezelhető, nem láncol hozzá egy gyártóhoz
- könnyen továbbfejleszthető a Novell Sentinel-rel teljes értékű SIEM megoldásra



"A hardveres megoldásokat szállító cégek magas összegeket kértek volna a telepítésért és a karbantartásáért, továbbá folyamatos szoftverlicenc-díjakat is kellett volna fizetnünk. A Novell Sentinel Log Manager megoldásával viszont nem volt szükség semmilyen új hardverre — mindössze annyit kellett tennünk, hogy üzembe helyeztünk egy Linux-alapú virtuális alkalmazást"

Paolo Barna, Menedzser, Üzemeltetési és Biztonsági Rendszerek, SONY Italia

www.novell.hu

A beépített PCI-DSS, HIPAA, SOX, és egyéb szabványos riportok mellett így többletmunka nélkül egyedi riportokat is készíthet.

Kiküszöböli a hagyományos naplókezelés gyengeségeit

A Sentinel Log Manager grafikus felületén gyorsan és egyszerűen be lehet állítani az adatforrásokat, továbbá képes a syslog naplóforrások automatikus felismerésére is. Rövid időn belül üzembe állítható és máris kezdődhet a használata. A "Sentinel Link" technológia segítségével képes a naplófolyamokat más rendszerek felé továbbítani, így könnyebben integrálható meglévő környezetbe. A piacon egyedülként TLS/SSL titkosítással forgalmazza a naplóadatokat, így biztosított azok integritása, illetve hogy nem kerülhetnek illetéktelen kezekbe. Természetesen más naplókezelő rendszerek is ígérnek nagy teljesítményt, de amint tényleges feldolgozásra kerül sor, a teljesítményük zuhanni kezd. Ezzel szemben a Sentinel Log Manager valóban képes akár készülékenként 7500 EPS (esemény per másodperc) teljesítménnyel is nemcsak adatgyűjtést, hanem normalizálást is végezni, és újabb egységekkel tovább skálázható szinte a végtelenségig.

Hosszútávú adatmegőrzés hosszútávú elköteleződés nélkül

Miközben számos más naplókezelő megoldás túlárazott egyedi hardverelemek vásárlását kényszeríti az ügyfelekre és speciális adatformátumokat használ, a Sentinel Log Manager bármilyen, a piacon szabadon megvásárolható adattárolási megoldással – akár a már meglévőkkel is – együttműködik. A naplófájlok tárolásánál 10:1 arányú adattömörítést alkalmaz, ami együtt a tetszőlegesen olcsó tárolási és szervermegoldások használatával óriási megtakarításokat eredményez. A szabványos adatformátumnak köszönhetően pedig cége bármikor szabadon rendelkezhethet az összegyűjtött naplóadatokkal, azok szükség esetén más szoftverekkel is tovább kezelhetők.

A Sentinel Log Manager nyomon követi és kimutatja a tárhelyhasználatot, illetve a növekedés ütemét, így a szükséges tárhelybővítés előre megtervezhető.

Üzembeállítási és továbbfejlesztési lehetőségek

A Sentinel Log Manager üzembe állítható fizikai szerveren, 500, 2500, illetve 7500 EPS teljesítményű licenccel, a szükséges teljesítménynek megfelelő hardverkonfiguráción (ld. lentebb). Ebben az esetben a SUSE Linux Enterprise Server 11 operációs rendszer 64 bites verziója a támogatott platform.

Virtual Appliance formátum

Amennyiben cége virtualizációs infrastruktúrával rendelkezik, virtuális alkalmazás formájában pillanatok alatt egy működő Sentinel Log Manager rendszerhez juthat. Ennek feltétele a VMware ESX(i) 4.0+, vagy a Xen 3.1.1+ virtualizációs környezet.

Továbbfejlesztés

Amennyiben a logmenedzsment rendszert a későbbiekben a belső elvárások, a külső fenyegetés, vagy az iparági előírások miatt valós idejű kiértékeléssel és riasztással egy teljes körű SIEM megoldássá szeretné továbbfejlesztetni, ezt könnyen megteheti a Sentinel Log Manager-hez integrálódó Novell Sentinel termékkel.

Változatok és rendszerkövetelmények

■ 500 és 2500 EPS licenc

Maximálisan 1000 eszköz kezelése 500 ill. 2500 esemény per másodperc feldolgozási teljesítménnyel. Javasolt hardverkonfiguráció: 1 db négymagos Intel Xeon E5450 vagy 2 db kétmagos Intel Xeon L5240 CPU, 4GB RAM, hardveres RAID1 tömb 256MB cache-el, 2 db 1TB-os 7200rpm HDD-ből.

■ 7500 EPS licenc

Maximálisan 2000 eszköz kezelése 7500 esemény per másodperc feldolgozási teljesítménnyel. Javasolt hardverkonfiguráció: 2 db négymagos Intel Xeon X5470 CPU, 8GB RAM, hardveres RAID5 tömb 512MB cache-el, 6 db 450GB-os 15k HDD-ből.

Keresse meg a Novell helyi megoldásszállítóját, vagy hívja a Novell helyi képviselőjét az alábbi számon:

Novell Kft.

MOM Park, SAS torony
1124 Budapest, Csörsz u. 45.

Tel: +36 (1) 489-4600

Fax: +36 (1) 489-4601

iroda@novell.hu

www.novell.hu