

- **GfiEventsManager**



## Központosított log-menedzsment és eseményelemzés

A szerverek és munkaállomások eseményeinek, naplóállományainak vizsgálata, a konfigurációs változtatások nyomon követése és ellenőrzése, a bekövetkező hiba- és biztonsági események értékelése a heterogén hálózatok egyik legnagyobb problémája. Bár az informatikai- és üzembiztonság megköveteli a naplók elemzését, a megnövekedett napi logmennyiség manuális vizsgálata ma már nem megoldható, hiszen sem idő, sem pedig elegendő erőforrás nem áll rendelkezésre. A logkezelés problémájának megoldását a többszörösen díjnyertes GFI EventsManager jelenti, amely megkönnyíti és automatizálja az események feldolgozását és leveszi ezt a terhet a rendszerüzemeltetők és biztonsági szakemberek válláról.

Legyen szó Windows-eseményekről, állományok hozzáférés-naplójáról, tűzfal- és router-logokról vagy akár W3C és SNMP eseményekről, a GFI EventsManager egy központi adatbázisba gyűjti a logokat, elvégzi a szükséges elemzéseket, és amennyiben gyanús eseményt vagy hibát észlel, biztonsági riasztásokat küld az üzemeltetőknek.

- **Hálózati biztonság egyszerűen**

A GFI EventsManager behatolás-detektáló rendszerként (IDS) képes felügyelni a hálózatban bekövetkező biztonsági eseményeket azáltal, hogy folyamatosan ellenőrzi a rendszerek biztonsági naplóit. Észreveszi az esetleges behatolási kísérleteket vagy a rendszereket érő támadásokat anélkül, hogy költséges és nehezen üzemeltethető IDS-megoldást kellene a hálózatba telepíteni.

- **Hiba-monitoring és rendszerfelügyelet**

A GFI EventsManager használatával nagymértékben leegyszerűsíthető a rendszerfelügyelet. A naplóállományok azonnali vizsgálatával észlelhetőek a hibás működésre utaló események, így az üzemeltetők akár a hiba bekövetkezése előtt értesítést kaphatnak a várható bekövetkezésről. Az ISA, IIS, Exchange és SQL szerverek felügyelete mellett az üzemeltetők monitorozhatják az SMTP vagy MAPI rendszereket, a diszkek hibás működését vagy akár a diszk- vagy processzorkapacitás csökkenését.

- **Megfelelés a nemzetközi szabványoknak és elvárásoknak**

A központi log-gyűjtés és archiválás mellett az események automatikus feldolgozása számos nemzetközi elvárásban szerepel. A GFI EventsManager bevezetésével a vállalat megfelelhet a PCI Data Security Standard, a Sarbanes-Oxley Act, a Gramm-Leach-Bliley Act, a HIPAA, FISMA, USA Patriot Act, TurnbullGuidance 1999, UK Protection Act és az EU DPD elvárásainak is.

- **Események megértése**

Az EventsManager segítségével valóban képet kaphat az üzemeltető, hogy mi történik az egyes eszközökön és a hálózatban. Az események értelmezése számos rendszer esetében nehézkes, gondoljunk csak a Windows események és üzenetek megértésének problémáira. Az EventsManager azonban nem csak begyűjti az eseményeket, hanem minden üzenet mellé tájékoztatást is ad az üzenet pontos jelentéséről, így az üzemeltetőknek nem szükséges hosszasan keresgélni az interneten a jelenség okáról.

- **Központosított tárolás és archiválás**

Legyen szó akár sok száz monitorozandó rendszerről, az EventsManager egy központi SQL adatbázisban tárolja a begyűjtött logokat, így az egyes rendszerekről akár törölhetőek a naplóállományok, a bekövetkezett események a vállalati biztonsági szabályzatnak megfelelően megőrizhetőek vagy archiválhatóak. A szabályzatnak megfelelő log-archiválásról az EventsManager ütemezhető eseménymentési eljárásai gondoskodnak.

## ▪ Analízis és riasztások

Az EventsManager nem csak begyűjteni és archiválni képes, de számos beépített szabályrendszer segítségével fel is dolgozza az eseményeket. Legyen szó nagyméretű ICMP csomagok többszöri ismétlődéséről, nem megengedett kommunikációról, munkaidőn túli felhasználói aktivitásról, fájlok hozzáféréseiről vagy akár felhasználók létrehozásáról vagy jogosultságváltozásáról, a GFI EventsManager a beállításnak megfelelően email, SMS vagy hálózati üzenet formájában értesíti az üzemeltetőket a gyanús eseményekről.

## ▪ Eszközök támogatása kliensprogramok nélkül

A GFI EventsManager kliensnélküli feldolgozórendszerként minden olyan eszközt támogat, amely Windows-eseményeket, syslogot vagy SNMP üzenetet generál. Számos (CISCO, 3Com, HP, IBM, CheckPoint, Alcatel, Dell, Netgear, Juniper, Arbor, Allied Telesis, Oracle, Symantec) eszközhöz rendelkezik gyári MIB értelmezőfájlokkal, de természetesen más gyártók MIB állományainak importálására is lehetőség van. A teljes SNMP-támogatás mellett az EventsManager a syslog üzenetek egyéni feldolgozására, meződefiníciókra, szűrésekre is lehetőséget nyújt.

## ▪ SQL szerver audit

A GFI EventsManager képes az SQL szerverek (2000, 2005, 2008, MSDE és Express) monitorozására és ellenőrzésére. Felügyeli a hozzáféréseket, az SQL lekérdezések futását, a jogosulatlan hozzáféréseket, adatbázis vagy rekordváltozásokat, törléseket vagy más adatbázis műveleteket. Pontos riportot ad az SQL szerveren belüli folyamatokról, így egyszerűen és könnyen auditálhatóak az adatbázisszerverek.

### ▪ Előnyök:

- Windows események megértése, értelmezése
- Nagysebesség. adatfeldolgozás, akár 6 millió esemény/óra teljesítmény
- Valós idejű figyelmeztetések és értesítések
- Központosított log-gyűjtés és -tárolás
- Szabályrendszer alapú log-menedzsment
- Profilalapú eseménybegyűjtés
- Hálózat- és biztonsági riportok
- Zajok és nem releváns információk kiszűrése
- Grafikus státuszmonitor
- Ütemezett és automatikus riportolás, akár emailben is

### ▪ Rendszerkövetelmények:

- .NET Framework 2.0
- Microsoft Data Access Components 2.6 vagy későbbi verzió
- SQL szerver hozzáférés, MSDE/ Server 2000 vagy későbbi verzió

### ▪ Erősségek

- - Syslog, Windows events, SNMP események központosított begyűjtése és archiválása
- - Tűzfalak, routerek, switchek, IP telefonok, szerverek, munkaállomások eseményeinek automatikus értékelése
- - Problémák azonosítása, valós idejű figyelés és riasztások
- - Gyors és költséghatékony monitorozás és rendszerfelügyelet
- - Megfelelés a nemzetközi elvárásoknak (SOX, PCI DSS, HIPAA, stb.)
- - A leggyorsabb feldolgozási sebesség (akár 6 millió esemény/óra)
- - Gyári szabályrendszer a leggyakoribb eszközökhöz (Cisco, Juniper, 3Com, HP, IBM, CheckPoint, stb.)
- - SQL szerver (2000, 2005, 2008, MSDE, SQLExpress) felügyelet és audit
- - Windows 2008 szerver és Vista támogatás

