



GFI EventsManager

Ereignis-Überwachung, -Verwaltung und -Archivierung

Systemereignisse, die täglich in sehr großer Zahl anfallen, bieten Netzwerkverantwortlichen wertvolle Informationen, mit denen sie Konfigurationsänderungen und administrative Aktionen überwachen sowie Systemfehler und potenzielle Sicherheitsverletzungen erkennen können. Ohne Unterstützung durch spezielle Tools ist es jedoch nicht möglich, relevante Daten aus tausenden von Ereignissen effizient zu erfassen. Je größer das Netzwerk, desto wichtiger eine Lösung, mit der sich Events in heterogenen Netzwerken zuverlässig kontrollieren, verwalten und archivieren lassen.

GFI EventsManager 8 überwacht, verwaltet und archiviert Ereignisse aller Art, ob W3C- und Windows-Ereignisse oder Syslog-Meldungen und SNMP-Traps von Geräten wie Firewalls, Routern und Sensoren. Durch die Unterstützung von Hardware der 20 weltweit größten Hersteller und von individuellen Geräten kontrolliert die Sicherheitslösung eine breite Anzahl an Produkten. Kritische Ereignisse zu Systemzustand und Betriebsstatus jedes einzelnen Geräts werden umgehend gemeldet und Daten zur weitergehenden Analyse erfasst. Darüber hinaus lassen sich Aktivitäten von Mitarbeitern im Unternehmensnetzwerk nachvollziehen, z. B. Änderungen der PC-Konfiguration und Dateizugriffe während der Arbeit. Auch erlaubt es GFI EventsManager, gesetzliche und branchenspezifische Compliance-Vorgaben wie SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standard) oder HIPAA (Health Insurance Portability and Accountability Act) leichter einzuhalten.

- Informationssystem- und Netzwerksicherheit: zum Aufspüren von Eindringlingen und Sicherheitsverletzungen
- Überwachung des Systemzustands: für proaktives Server-Monitoring
- Einhaltung gesetzlicher und branchenspezifischer Sicherheitsvorschriften: zur Umsetzung unterschiedlichster Sicherheitsvorgaben
- Forensische Sicherheitsanalysen: für schnelle Ursachenforschung bei Problemen

Vorteile

Warum GFI EventsManager zur Verwaltung und Analyse von Ereignisprotokollen?

- Ermöglicht die zentrale Erfassung von Syslog-, W3C- und Windows-Ereignissen sowie der SNMP-Traps von Firewalls, Servern, Routern, Switches, Telefonanlagen, PCs u. v. m.
- Steigert die Netzwerk-Uptime und erlaubt eine rasche Problemerkennung durch Echtzeit-Warnungen
- Fördert eine effiziente, kostensparende Überwachung und Verwaltung des gesamten Netzwerks
- Bietet SQL-Server-Auditing für Microsoft SQL Server 2000, 2005 und 2008 sowie MSDE und Microsoft SQL Server Express
- Liefert eine einzigartige Skalierbarkeit zum Scannen von bis zu sechs Millionen Ereignissen pro Stunde
- Kompatibel zu Microsoft Windows Vista und offiziell zertifiziert für Microsoft Windows Server 2008

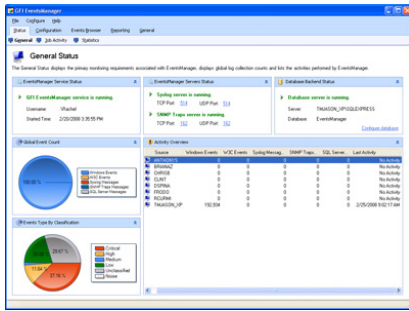
■ Zentralisierte Ereignisprotokollierung

Ereignisprotokolle werden automatisch erstellt und erweitert, ob von Hintergrundprozessen oder durch Anwenderaktionen. Die Speicherung der Dateien erfolgt jedoch oft an verschiedenen Orten. GFI EventsManager sichert alle erfassten Ereignisprotokolle in einer SQL-Datenbank, ob lokal oder entfernt. Backups der Protokolle nach einem festgelegten Zeitplan sind ebenfalls möglich.

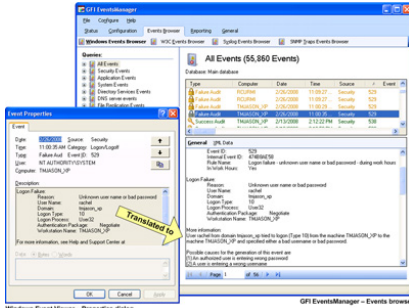
■ Analyse von Ereignisprotokollen (SNMP-Traps, Windows-Ereignisprotokolle, W3C-Protokolle und Syslog)

Zur Aufgabe von Netzwerkadministratoren zählt unter anderem, mit zahlreichen kryptischen Einträgen überfüllte Sicherheitsprotokolle zu analysieren. GFI EventsManager hilft ihnen beim netzwerkweiten Kontrollieren und Verwalten von Event-Logs, um relevante Ereignisse aus Windows-Ereignisprotokollen, W3C-Protokollen oder Syslog-Meldungen unterschiedlichster Netzwerkquellen herauszufiltern. Die Unterstützung von SNMP Version 3 (Simple Network Management Protocol) ermöglicht die Überwachung und Meldung von Zustand und Betriebsstatus unterschiedlichster Netzwerkelemente wie Router, Sensoren und Firewalls.

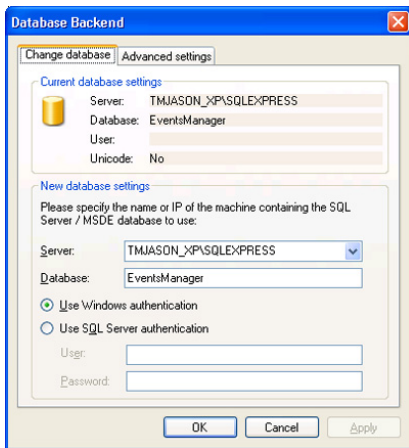
GFI EventsManager



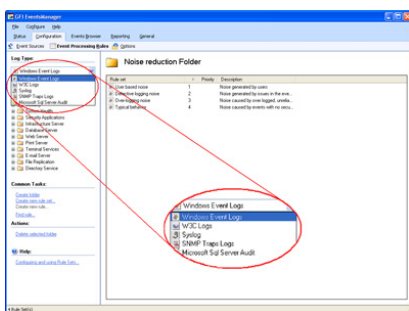
Verwaltungskontrolle



Verständlichere Ereignisprotokoll-Einträge

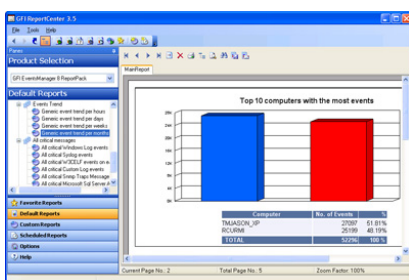


Zentralisierte Ereignisprotokollierung



Unterstützung mehrerer Protokolltypen (Windows-Ereignisprotokolle, W3C, Syslog, SNMP-Traps, Microsoft SQL Server-Audit)

GFI EventsManager ReportPack



Top-10-Bericht zu Computern mit den meisten Ereignissen

■ "Certified for Windows Server® 2008" und Unterstützung von Microsoft Windows Vista

GFI EventsManager ist offiziell für Microsoft Windows Server 2008 zertifiziert und jetzt auch unter Microsoft Windows Vista lauffähig. Das neue Protokollformat beider Plattformen wird ebenfalls erfasst und gemeinsam mit anderen Formaten einheitlich dargestellt, um Systemverantwortlichen einen einfacheren Gesamtüberblick über alle Systeme hinweg zu bieten. Weiterhin unterstützt werden Microsoft Windows 2000, XP und 2003.

■ Granulare Ereigniskontrolle

GFI EventsManager unterstützt die Überwachung einer großen Auswahl an Plattformen und Hardware. Unterschiedliche Protokolltypen mit Windows-Ereignissen, Syslog-Meldungen, W3C-Events und SNMP-Traps von Netzwerkelementen werden zentral gesichert und analysiert. Administratoren ist es möglich, relevante Daten von Windows-Computern und Drittgeräten mit einer hohen Granularität zu erfassen und Informationen auch auf Ebene erweiterter Tags zu verarbeiten. Über die weitergehende Bearbeitung kann dann umgehend auf Grundlage der vorliegenden Ergebnisse entschieden werden – ohne zusätzliche Datenverwaltung.

■ Unterstützung neuer Hardware (MIB-Datei-Import)

Viele Hersteller stellen für ihre Hardware MIB-Dateien (Management Information Base) bereit, die spezielle Geräteeigenschaften definieren und eine Erkennung und Verwaltung der SNMP-Traps zahlreicher Produkte ermöglichen. GFI EventsManager wird mit MIB-Definitionen folgender Hersteller ausgeliefert: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis u. a. MIBs für neue Geräte lassen sich problemlos importieren.

■ SQL-Server-Auditing

GFI EventsManager unterstützt SQL-Server-Auditing für alle kostenpflichtigen und kostenfreien Versionen von Microsoft SQL Server 2000, 2005 und 2008 sowie MSDE und Microsoft SQL Server Express. Mit dem Auditing wird die Authentizität der SQL-Server-Daten sichergestellt. Administratoren können SQL-Aktivitäten verfolgen und protokollieren, darunter das Ausführen von SQL-Anweisungen, Änderungen an Datenbanktabellen und Zugriffsversuche ohne entsprechende Befugnis.

■ Verständliche Erklärungen zu Windows-Ereignissen

Ereignisprotokolle sind aufgrund ihrer teilweise kryptischen Einträge nur schwer zu analysieren. GFI EventsManager überträgt die Ereignisangaben in eine verständliche, präzise Form und bietet klare Lösungsvorschläge.

■ Hochleistungs-Scan-Engine

GFI EventsManager überzeugt mit einer Scan-Engine, die selbst eine große Anzahl von Ereignissen – bis zu sechs Millionen pro Stunde – in kürzester Zeit erfassen, verarbeiten und bewerten kann. Das modulare Konzept erlaubt es, zusätzliche Funktionen und Plug-ins hinzuzufügen, ohne direkte Änderungen an der Engine vorzunehmen.

■ Echtzeit-Warnungen

Wird ein unerlaubtes Eindringen ins Netzwerk oder ein anderes schwerwiegendes Ereignis festgestellt, kann GFI EventsManager Warnungen verschicken. Als Gegenmaßnahmen lassen sich Aktionen wie das Starten von Skripten einleiten oder Mitarbeiter per E-Mail, Netzwerknachricht oder SMS (per E-Mail-zu-SMS-Gateway/Dienst) alarmieren.

■ Erfassung von im WAN verteilten Ereignisinformationen in einer zentralen Datenbank

Ereignisinformationen, die von mehreren, im gesamten Netzwerk verteilten GFI EventsManager-Instanzen erfasst und verarbeitet wurden, lassen sich in einer Datenbank zentralisieren. Tausende über mehrere Standorte verteilte Workstations und Server können ohne Beeinträchtigung von Bandbreite oder Speicherkapazität somit mühelos überwacht werden. Zusätzlich ist es möglich, Ereignisse bei Bedarf schnell per Backup zu sichern oder wiederherzustellen. Die Größe der Datenbank lässt sich im Rahmen der automatischen Wartung durch den Export von Ereignissen regulieren.

■ Regelbasierte Verwaltung von Ereignisprotokollen

Nutzen Sie vorkonfigurierte Regeln zur Protokollanalyse, mit denen Ereignisse unter Berücksichtigung festgelegter Bedingungen herausgefiltert und klassifiziert werden. Standardregeln lassen sich individuell verändern, zudem können Sie neue, auf Ihre Netzwerkinfrastruktur zugeschnittene Regeln erstellen.

■ Fortschrittliche Funktionen zur Ereignisfilterung

Leistungsfähige Filter erlauben ein schnelles Durchsuchen und übersichtliches Anzeigen erfasster und gesicherter Ereignisse unter Beibehaltung sämtlicher Originaleinträge des Datenbank-Backends. Farbliche Hervorhebungen und die integrierte Ereignissuche helfen beim gezielten Auffinden von Ereignissen.

■ Scan-Profil für Ereignisprotokolle

Mit Hilfe von Scan-Profilen lassen sich Gruppen mit Regeln zur Ereignisprotokoll-Überwachung erstellen, die auf einen oder mehrere Computer anzuwenden sind. Über Scan-Profilen können Vorgaben zur Ereignisprotokoll-Verarbeitung zudem zentral angepasst werden. Sie haben auch die Möglichkeit, Regelgruppen allein für die Arbeitsplatzrechner einer einzelnen Abteilung zu erstellen. Richten Sie darüber hinaus ergänzende Profile ein, deren spezielle Ereignisprotokoll-Regeln jeweils nur für Einzel-Computer gelten sollen.

■ Berichte zu wichtigen Sicherheitsereignissen im Netzwerk

Ein integriertes Berichtmodul erlaubt die Erstellung neuer Reports oder die Anpassung von Vorlagen für:

- Kontoverwendung
- Kontoverwaltung
- Richtlinienänderungen
- Objektzugriffe
- Anwendungs-Management
- Drucker-Server
- Windows Ereignisprotokoll-System
- Ereignistrends

■ Unterstützung bei Einhaltung des PCI DSS und anderer branchenspezifischer Sicherheitsvorgaben

Seit September 2007 müssen Unternehmen, die im Zahlungsverkehr mit Kreditkartendaten arbeiten, ungeachtet ihrer Größe die strengen Sicherheitsvorschriften der weltweit wichtigsten Kreditkartenunternehmen einhalten: den PCI DSS (Payment Card Industry Data Security Standard). Die kontinuierliche Erfassung von Ereignisdaten ist wesentliche Voraussetzung für PCI DSS-Compliance: Ereignisprotokolle erlauben eine detaillierte Nachverfolgung aller Vorgänge bei der Bearbeitung von Kreditkartendaten. Zur Einhaltung der PCI DSS-Vorgaben ist somit eine leistungsfähige Lösung zur Ereignisprotokoll-Verwaltung erforderlich – wie GFI EventsManager.

■ Weitere Leistungsmerkmale

- Entfernt irrelevante Ereigniseinträge, die den Großteil der protokollierten Daten ausmachen
- Erlaubt Eindringlingserkennung und Versand von Warnungen rund um die Uhr
- Ermöglicht die Überwachung des GFI EventsManager- und Netzwerkstatus per integrierten Status-Monitor
- Bietet eine Berichterstellung nach Zeitplan und die Verteilung von Berichten per E-Mail

■ Sie befinden sich in guter Gesellschaft ...

Viele führende Unternehmen haben sich bereits für GFI EventsManager entschieden, unter anderem: Primerica, Pepsico France, Royal & Sunalliance USA Inc., ATP, Ceridian Canada u. v. m.

Systemanforderungen

- .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 oder später
- Zugriff auf MSDE/SQL Server 2000 oder später

Auszeichnungen



Ihre Testversion steht unter <http://www.gfi.de/de/eventsmanager/> zum Download bereit!

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com