



GFI EventsManager

Monitorización, administración, y archivo de sucesos

El elevado volumen de sucesos de sistema que se genera diariamente es una valiosa fuente de información para los administradores de red para ayudarlos a monitorizar cambios de configuración, acciones administrativas, identificar errores de sistema y brechas de seguridad sospechosas. Esta es, sin embargo, una tarea abrumadora sin las herramientas apropiadas. Cuanto más grande es la red, mayor es su necesidad de una solución que le permita monitorizar, administrar y archivar miles de sucesos generados por dispositivos a través de redes heterogéneas.

GFI EventsManager 8, galardonada solución de monitorización, administración y archivo de sucesos, soporta una amplia familia de tipos de sucesos como W3C, sucesos Windows, Syslogs y, en la última versión, traps SNMP generados por dispositivos tales como cortafuegos, enrutadores y sensores. Proporcionando soporte para dispositivos de los 20 principales fabricantes del mundo así como dispositivos a medida, GFI EventsManager le permite monitorizar una amplia familia de productos hardware, generar informes sobre el estado operativo de cada uno y recoger información para el análisis. También puede seguir la actividad de los empleados en la red tales como cambios hechos en sus PCs, archivos accedidos durante el día, cumplimiento legal y regulador tal como SOX, PCI DSS, HIPAA y mucho más.

- Seguridad del sistema de información y de la red: Detecte intrusos y brechas de seguridad
- Monitorización de la salud del sistema: Monitorice proactivamente sus servidores
- Cumplimiento legal y regulador: Una ayuda para cumplir con las regulaciones
- Investigaciones forenses: Un punto de referencia cuando algo va mal.

Beneficios

¿Por qué utilizar GFI EventsManager?

- Centraliza los sucesos Syslog, W3C, Windows y SNMP Traps generados por cortafuegos, servidores, enrutadores, switches, sistemas telefónicos, PCs y más
- Incrementa el tiempo de actividad e identifica problemas mediante alertas en tiempo real
- Monitorización y administración de toda la red rápida y económica
- Auditoría SQL Server para SQL Server 2000, 2005, 2008 y también MSDE y SQL Express
- Rendimiento sin igual de escaneo de sucesos de hasta 6 millones de sucesos por hora
- Certificado para Windows Server 2008; Soporta Windows Vista

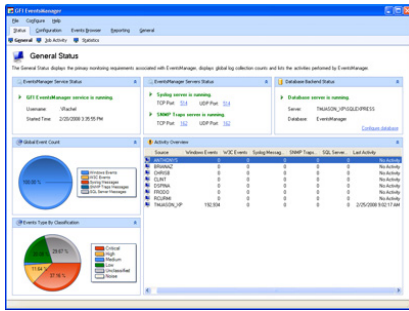
■ Registro de sucesos centralizado

Los registros de sucesos son contante y automáticamente generados por los usuarios o por procesos automáticos/de segundo plano y a menudo son almacenados en lugares distintos. GFI EventsManager almacena todos los registros de sucesos capturados en una base de datos SQL que además puede ser remota. También puede configurar copias de seguridad programadas de sus registros de sucesos.

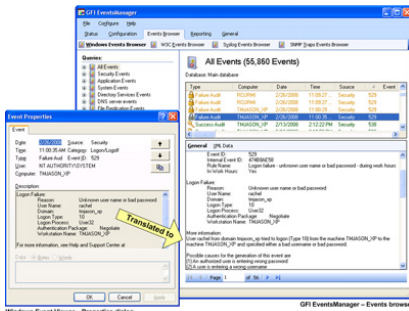
■ Análisis de registros de sucesos incluyendo SNMP Traps, registros de Sucesos Windows, registros W3C y Syslog

Como administrador de red usted ha experimentado los crípticos y voluminosos logs que hacen abrumador el proceso de análisis. GFI EventsManager es una solución de procesamiento de registros que proporciona control y administración en toda la red de registros de sucesos Windows, registros W3C y eventos Syslog generados por sus recursos de red. GFI EventsManager ya soporta Protocolo Simple de Administración de red (SNMP) versión 3 que es el idioma hablado por los dispositivos de bajo nivel como enrutadores, sensores, cortafuegos, etc. Mediante SNMP los usuarios pueden ahora monitorizar una completa familia de dispositivos hardware en sus infraestructuras con la habilidad de generar informes sobre el estado operativo de cada dispositivo.

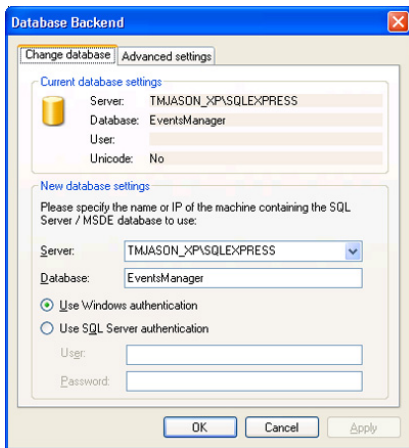
GFI EventsManager



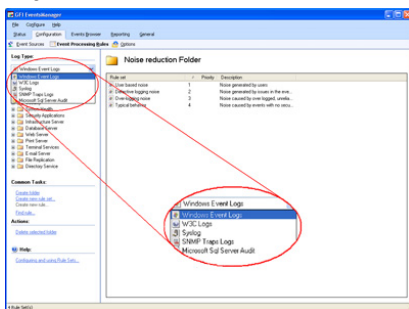
Consola de administración de GFI EventsManager



Hace fáciles de comprender los crípticos registros

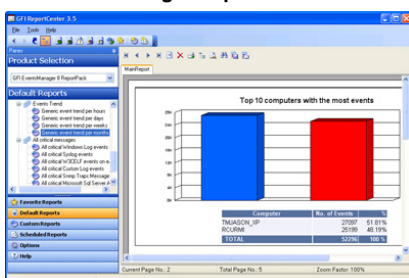


Registro de sucesos centralizado



Soporte de varios tipos de registro (registros de sucesos Windows, W3C, Syslog, SNMP Traps, Microsoft SQL Server audit)

GFI EventsManager ReportPack



Informe que muestra los 10 eventos más generados por los equipos

■ Certificado para Windows Server 2008; Soporta Vista

GFI EventsManager ha conseguido el estado 'Certificado para Windows Server 2008' y se puede instalar en, y recoger sucesos de Windows Vista y Windows 2008. Aunque estas nuevas plataformas utilizan un formato diferente de registro, GFI EventsManager presenta los sucesos de varios sistemas operativos de la misma forma, permitiendo al usuario acostumbrarse a una estructura común, irrespectivamente de la plataforma monitorizada. GFI EventsManager también soporta Windows 2000, Windows XP y Windows 2003.

■ Control granular más profundo de sucesos

GFI EventsManager le ayuda a monitorizar una mayor familia de sistema y dispositivos mediante el registro y análisis centralizado de varios tipos de registro incluyendo sucesos Windows, Syslog, W3C y ahora SNMP Traps que son generados por recursos de red. Los administradores puede recoger información de equipos Windows y de dispositivos de terceros con un mayor nivel de granularidad y además procesa la información del nivel extendido de etiquetas y basa la decisión sobre qué hacer en el acto, sin mayor gestión de información.

■ Soporte de nuevos Dispositivos

Administrar SNMP Traps para una miriada de dispositivos requiere la capacidad de comprender el 'idioma' que utiliza cada fabricante para definir sucesos. Las información de definiciones y dispositivos están contenidas en los archivos de definición Base de Información de Gestión (MIB) que son proporcionados por los fabricantes. GFI EventsManager se entrega con definiciones MIB de los siguientes fabricantes: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis y otros. GFI EventsManager también es capaz de importar archivos MIB de nuevos dispositivos tan pronto como están disponibles.

■ SQL Server Auditing

GFI EventsManager soporta ahora auditoría de servidor SQL de todas las versiones comerciales y gratuitas de SQL Server incluyendo 2000, 2005, 2008, MSDE y SQL Express. La auditoría permite al usuario seguir y generar informes sobre la actividad del servidor SQL tales como: Ejecución de instrucciones SQL, alteración de tablas de BD, intentos de acceso a información sin los necesarios privilegios, etc. Esto puede asegurar que la información de los servidores SQL es auténtica y por lo tanto fiable.

■ "Traduce" los crípticos sucesos Windows

Los crípticos logs hace del análisis de registros un proceso prolongado. GFI EventsManager "traduce" las a menudo crípticas descripciones de los sucesos para proporcionar claridad, explicaciones concisas y sugerencias de acción.

■ Motor de escaneo de alto rendimiento

GFI EventsManager incorpora un motor de escaneo de sucesos totalmente rediseñado que está afinado para alcanzar el máximo rendimiento. Los tests demuestran que es capaz de escanear y recoger hasta 6 millones de sucesos/hora. Es más, su metodología basada en plug-ins permite que sean integradas características y módulos sin interferir con el código existente.

■ Alertas en tiempo real

GFI EventsManager puede enviarle alertas cuando se detectan sucesos clave o intrusiones. Puede activar acciones tales como ejecución de secuencias de comandos o envío de alertas a una o más personas por correo electrónico, mensajes de red y notificaciones SMS enviadas mediante una pasarela o servicio de correo-a-SMS.

■ Recoga datos de sucesos distribuidos por una WAN en una base de datos central

Usted puede recoger los sucesos de instalaciones GFI EventsManager de varios sitios y localizaciones de su red en una base de datos central utilizando la funcionalidad del módulo Operaciones de Base de Datos. Esto le permite a usted monitorizar fácilmente miles de estaciones y servidores a través de la red sin impactar en el uso del ancho de banda ni del almacenamiento. Se integra y centraliza sucesos recogidos y procesados y le permite copiar/restaurar sucesos bajo demanda. Mediante operaciones en base de datos puede administrar el tamaño de la base de datos – sin necesidad de intervención manual – no sólo para la centralización sino también para poder exportar sucesos y copiarlos según se necesite.

■ Gestión de registros de sucesos basado en reglas

GFI EventsManager se entrega con un conjunto de reglas de procesamiento de registros preconfiguradas que le permiten filtrar y clasificar sucesos que cumplan condiciones particulares. Puede utilizar estas reglas predefinidas sin realizar configuración alguna o puede escoger personalizar estas reglas o crear reglas a medida que se adecúen a su infraestructura de red.

■ Características avanzadas de filtrado de sucesos

El potente filtrado de GFI EventsManager tamiza los registros de sucesos almacenados y le permite examinar los sucesos requeridos sin eliminar ningún registro de su base de datos. También puede destacar selectivamente sucesos específicos utilizando un color o la herramienta integrada de búsqueda de sucesos.

■ Perfiles de análisis de registros de sucesos

Los perfiles de análisis le permiten configurar el conjunto de reglas de monitorización de registros de sucesos que serán aplicadas a equipos concretos o a grupos de equipos y proporcionar una forma centralizada de ajustar las reglas de procesamiento de registros de sucesos. También puede configurar un conjunto de reglas que sólo se aplica a estaciones de trabajo de un departamento concreto. Además puede crear perfiles complementarios diferentes que proporcionen reglas adicionales y más especializadas de registros de sucesos en un equipo en función del equipo.

■ Vea informes sobre información clave de seguridad que están ocurriendo en su red

El generador de informes de GFI EventsManager, que se entrega con el producto, le permite crear o personalizar informes, incluyendo informes estándar, tales como:

- Informes de uso de cuentas
- Informes administrativos de cuentas
- Informes de cambios de directiva
- Informes de acceso a objetos
- Informes administrativos de aplicaciones
- Informes de servidor de impresión
- Informes de sistema del registro de sucesos Windows
- Informes de tendencias de eventos

■ Ayuda a cumplir PCI DSS y otras regulaciones

A partir de Septiembre de 2007 todos los negocios que manejen información sobre usuarios de tarjetas – sin tener en cuenta el tamaño – tienen que cumplir completamente los estrictos estándares de seguridad redactados por las principales empresas de tarjetas de crédito. El registro de información es clave para cumplir los requerimientos PCI DSS ya que los registros proporcionan seguimiento retrospectivo de todas las actividades de un entorno de información de titulares de tarjetas de crédito y por lo tanto, un sistema integral de administración de registros, como GFI EventsManager, le proporcionaría la funcionalidad que necesita para ser ayudado en el cumplimiento de PCI DSS.

Requerimientos del sistema

- .NET Framework 2,0
- Microsoft Data Access Components (MDAC) 2,8 o superior
- Acceso a MSDE / SQL Server 2000 o superior

Premios



Descargue su versión de evaluación de <http://www.gfihispana.com/es/eventsmanager/>

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