



GFI EventsManager

Monitoraggio, gestione e archiviazione degli eventi

L'enorme volume di eventi di sistema generato quotidianamente costituisce una fonte preziosissima di informazioni al fine di aiutare gli amministratori di sistema a monitorare modifiche di configurazione e azioni amministrative, e a identificare errori di sistema e violazioni di sicurezza sospette. Tuttavia, si tratta di un'operazione ingestibile senza strumenti adeguati. Più grande è la rete, maggiore è l'esigenza di una soluzione che consenta di controllare, gestire e archiviare i migliaia di eventi che vengono generati dai dispositivi di vari tipi di reti.

GFI EventsManager 8, soluzione pluripremiata di monitoraggio, gestione e archiviazione eventi, è compatibile con una vasta gamma di tipologie di eventi, quali quelli W3C, Windows, Syslog e, nell'ultima versione, con le SNMP trap generati da dispositivi come firewall, router e sensori. Fornendo il supporto di dispositivi distribuiti dai 20 maggiori produttori mondiali e di dispositivi personalizzati, GFI EventsManager consente di controllare un'ampia gamma di prodotti hardware, di creare rapporti sullo stato di salute e operativo di ognuno e di raccogliere dati a fini di analisi. È possibile rintracciare l'attività dei dipendenti sulla rete, ad esempio le modifiche sui PC, i file cui accedono nel corso della giornata, rispettare le conformità legali e normative quali il D.P.R. 513 del 10/11/1997, Legge SOX, PCI DSS, HIPAA e molto altro.

- Sicurezza del sistema informatico e della rete: in quanto rileva intrusi e violazioni di sicurezza
- Monitoraggio stato di salute del sistema, dato che controlla i server attivamente
- Conformità a leggi e normative, in quanto è un ausilio per ottemperare alle normative in materia di conservazione di registrazioni
- Indagini legali, poiché rappresenta un punto di riferimento per quando qualcosa va storto.

Benefici

Perché adoperare GFI EventsManager?

- Perché centralizza gli eventi Syslog, W3C, Windows e SNMP trap generati da firewall, server, router, commutatori, centralini telefonici, PC e altro
- Migliora il tempo di operatività (uptime) della rete e individua problemi attraverso gli avvisi in tempo reale
- Monitoraggio e gestione rapidi e convenienti dell'intera rete
- Controllo del server SQL per SQL Server 2000, 2005, 2008 e anche per MSDE e SQL Express
- Per le prestazioni di scansione degli eventi - senza rivali - scalabili fino a oltre 6 milioni di eventi all'ora
- Certificato per Windows Server 2008. Compatibile con Windows Vista

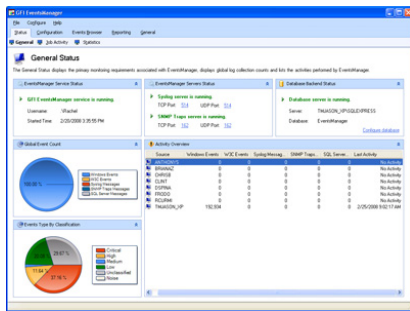
■ Registrazione centralizzata degli eventi

I log di eventi sono generati continuamente e in modo automatico da un utente o da un processo automatico o in background, e i log sono spesso archiviati in diverse locazioni. GFI EventsManager archivia tutti i log di eventi acquisiti su un unico database SQL, che può anche risiedere in remoto. Inoltre, è possibile configurare backup pianificati dei propri log di eventi.

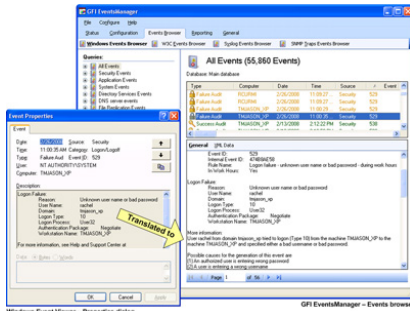
■ Analisi di log di eventi, compresi SNMP Trap, log di eventi Windows, W3C e Syslog

In veste di amministratore di rete, ci si sarà sicuramente trovati di fronte a log voluminosi ed enigmatici, che avranno scoraggiato il processo di analisi degli stessi. GFI EventsManager è una soluzione di elaborazione dei log che offre il controllo e la gestione, su tutta la rete, dei log di eventi di Windows, di W3C e di eventi Syslog, generati dalle risorse della propria rete. GFI EventsManager supporta anche la versione 3 di Simple Network Management Protocol (SNMP), cioè il linguaggio adoperato da dispositivi di basso livello come router, sensori, firewall, ecc. Tramite il protocollo SNMP, gli utenti possono ora monitorare una gamma completa di dispositivi hardware sulla loro infrastruttura, nonché creare rapporti sullo stato di salute e operativo di ogni dispositivo.

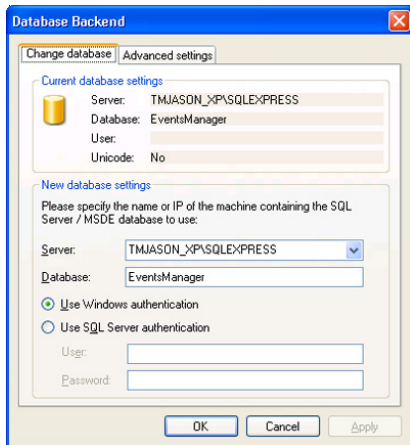
GFI EventsManager



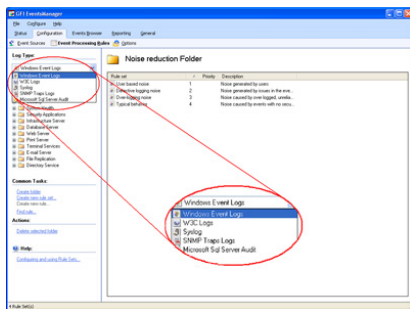
Console di gestione di GFI EventsManager



Migliore comprensione dei log cifrati/enigmatici

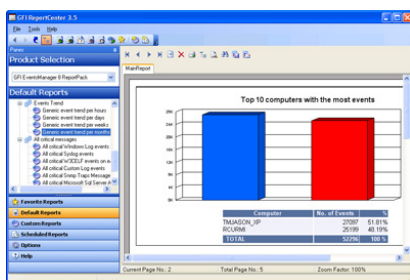


Registrazione centralizzata degli eventi



Compatibilità con più tipologie di log degli eventi (Windows, W3C, Syslog, SNMP Trap e controllo Microsoft SQL Server)

GFI EventsManager ReportPack



Rapporto che illustra i primi 10 computer che generano eventi

■ Certificato per Windows Server 2008. Compatibile con Vista

GFI EventsManager ha ottenuto lo status di "Certificato per Windows Server 2008" e può essere installato su sistemi Windows Vista e Windows Server 2008, dei quali è anche in grado di raccogliere gli eventi. Benché queste nuove piattaforme adoperino un formato di log diverso, GFI EventsManager presenta gli eventi dei vari sistemi operativi con la stesse modalità, permettendo così all'utente di abituarsi a una struttura comune, indipendentemente dalla piattaforma controllata. GFI EventsManager è compatibile anche con Windows 2000, Windows XP e Windows 2003.

■ Controllo granulare degli eventi più profondo

GFI EventsManager aiuta a controllare una gamma più vasta di sistemi e dispositivi, attraverso la registrazione e analisi centralizzate di vari tipi di log, compresi eventi Windows, Syslog, W3C e, adesso, SNMP trap, che vengono generati dalle risorse di rete. Gli amministratori possono raccogliere informazioni dai computer Windows e da dispositivi di terzi con un livello di granularità maggiore, elaborare informazioni a un livello di tag più ampio e decidere immediatamente come utilizzare le informazioni, senza la necessità di gestirle ulteriormente.

■ Compatibilità con nuovi dispositivi

La gestione di SNMP Trap per una miriade di dispositivi richiede la capacità di capire il "linguaggio" adoperato da ciascun produttore per definire gli eventi. Le definizioni e informazioni sul dispositivo sono contenute nei file di definizione Management Information Base (MIB) forniti dai produttori. GFI EventsManager comprende le definizioni MIB dei seguenti produttori: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis e altri. GFI EventsManager è inoltre in grado di importare i file MIB di nuovi dispositivi non appena questi si rendono disponibili.

■ Controllo di SQL Server

GFI EventsManager supporta ora il controllo del server SQL per tutte le versioni commerciali e gratuite di SQL Server, comprese 2000, 2005, 2008, MSDE e SQL Express. Il controllo consente all'utente di rintracciare e creare rapporti su attività del server SQL, ad esempio: l'esecuzione di istruzioni SQL, la modifica di tabelle DB, i tentativi di accedere ai dati senza i privilegi necessari, ecc. In questo modo si garantisce che i dati dei server SQL sono autentici e affidabili.

■ "Traduzione" degli eventi di Windows dal significato "enigmatico"

Log enigmatici allungano il processo di analisi. GFI EventsManager "traduce" le descrizioni spesso enigmatiche degli eventi, convertendole in spiegazioni e consigli chiari e concisi sugli eventuali provvedimenti da adottare.

■ Motore di scansione dalle prestazioni elevate

GFI EventsManager incorpora un motore di scansione degli eventi completamente riprogettato, del tutto sintonizzato per offrire le massime prestazioni di scansione. Test dimostrano che è in grado di eseguire la scansione e raccogliere fino a 6 milioni di eventi all'ora. Inoltre, la sua metodologia "plug-in" consente l'integrazione di ulteriori caratteristiche e moduli, senza che si verifichino interferenze con il codice esistente.

■ Avvisi in tempo reale

GFI EventsManager è in grado di inviare avvisi quando individua eventi critici o intrusioni. Si possono attivare azioni quali script o inviare avvisi ad almeno un soggetto tramite email, messaggi di rete e notifiche SMS inviate tramite un gateway o servizio "email verso sms".

■ Raccolta, in un singolo database centrale, dei dati degli eventi distribuiti su una WAN

È possibile raccogliere in un database centrale tutti i dati di eventi di installazioni GFI EventsManager presenti in più sedi e locazioni della rete, ricorrendo alla funzionalità Database Operations (Operazioni su database). Così, è possibile monitorare con facilità migliaia di stazioni di lavoro e di server su tutta la rete, senza che ne risenta l'utilizzo di larghezza di banda e/o di memoria. Il componente integra e centralizza gli eventi raccolti ed elaborati, consentendo di eseguire il salvataggio in back-up o di ripristinare gli eventi su richiesta. Grazie alle operazioni di database si può gestire la dimensione del database stesso, senza dover intervenire manualmente, non soltanto attraverso la centralizzazione, ma anche grazie alla possibilità di esportare gli eventi e salvarli in backup a seconda delle necessità.

■ Gestione dei log di eventi basata su regole

GFI EventsManager è provvisto di una serie preconfigurata di regole di elaborazione, che consente di filtrare e classificare eventi che soddisfano determinate condizioni. È possibile adoperare tali regole predefinite senza eseguire ulteriori configurazioni oppure si può scegliere di personalizzarle o crearne di nuove, per adeguarle all'infrastruttura della propria rete.

■ Funzioni avanzate di filtraggio degli eventi

Il potente filtro di GFI EventsManager "passa al setaccio" i log di eventi registrati e consente di sfogliare quelli desiderati senza eliminare alcun record dal terminale database. È inoltre possibile evidenziare in modo selettivo eventi specifici, adoperando un colore o lo strumento di ricerca integrato.

■ Profili di scansione dei log di eventi

I profili di scansione consentono di configurare la serie di regole di monitoraggio degli eventi da applicare a un computer o gruppo di computer, e forniscono un modo centralizzato per mettere a punto l'ottimizzazione delle regole di elaborazione dei log di eventi. Si può anche impostare una serie di regole da applicarsi unicamente alle stazioni di lavoro di un determinato reparto. Questo software offre altresì la possibilità di creare profili complementari distinti, che forniscono regole supplementari e più specializzate, computer per computer.

■ Visualizzazione dei rapporti sulle principali informazioni di sicurezza che si verificano sulla rete

Con il generatore di rapporti di GFI EventsManager, incluso nel prodotto, è possibile creare o personalizzare i rapporti, compresi quelli standard, quali:

- rapporti sull'utilizzo dell'account
- rapporti sulla gestione dell'account
- rapporti sulle variazioni dei criteri
- rapporti sull'accesso agli oggetti
- rapporti sulla gestione delle applicazioni
- rapporti sul server di stampa
- rapporti sul sistema dei log degli eventi di Windows
- rapporti sull'andamento degli eventi

■ Ausilio nell'ottemperanza alle norme PCI DSS e ad altri regolamenti

A decorrere dal settembre 2007, tutte le aziende che gestiscono dati di titolari di carte di credito, indipendentemente dalle dimensioni delle aziende stesse, sono tenute all'osservanza di rigide norme di sicurezza emanate dalle maggiori società di carte di credito mondiali. La registrazione dei dati è fondamentale per rispettare i requisiti PCI DSS, poiché i log (registri) forniscono "audit trail" di tutte le attività eseguite in un contesto di dati di titolari di carte di credito; di conseguenza, un sistema completo di gestione dei log come GFI EventsManager fornisce le funzionalità necessarie per ottemperare alle norme PCI DSS.

■ Altre caratteristiche:

- rimozione degli eventi di disturbo (noise) o irrilevanti che rappresentano una grossa proporzione di tutti gli eventi di sicurezza
- monitoraggio e avvisi in tempo reale e continui
- controllo grafico dello stato di GFI EventsManager e della rete grazie al monitor di stato interno
- pianificazione dei rapporti e distribuzione automatica via email.

■ Molti altri ci hanno scelto...

Molte aziende importanti hanno scelto GFI EventsManager. Ecco solo alcuni esempi: Primerica, Pepsico France, Royal & Sunalliance USA Inc., ATP, Ceridian Canada e molte altre.

Requisiti di sistema

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

Premi



Scaricate la copia di valutazione da <http://www.gfi-italia.com/italia/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