

GFI Events Manager

Мониторинг, управление и архивация лог-файлов по всей сети

Сетевое управление файлами регистрации событий – нет необходимости в специалистах!

Лог-файлы – ценный инструмент для мониторинга сети, которые часто используются в недостаточной мере из-за их сложности и объема. По мере роста организации ей требуется более структурированный подход к управлению лог-файлами и их хранению. Недавнее исследование, проведенное институтом SANS, обнаружило, что 44% системных администраторов не хранят файлы регистрации более одного месяца.

ПРЕИМУЩЕСТВА



- **Централизованная обработка, мониторинг и архивация лог-файлов формата Syslog, W3C и Windows, созданных брандмауэрами, серверами, маршрутизаторами, коммутаторами, телефонами, ПК и др.**
- **Настройка с помощью мастера упрощает управление и обслуживание**
- **Непревзойденная система обнаружения событий, которая поддерживает обработку более 6 миллионов событий в час**
- **Предварительно настроенные правила обработки различных типов лог-фалов для эффективной классификации событий и управления ими**
- **Автоматизированный мониторинг событий в режиме 24/7 и сигнализация**
- **Мощное средство создания отчетов для эффективного мониторинга сетевой активности.**



Эффективное управление файлами регистрации событий поможет вам:

- Обеспечить безопасность IT-инфраструктуры компании
- Просто и удобно осуществлять мониторинг исправности системы
- Соответствовать международным стандартам (SOX, PCI DSS, HIPAA)
- Расследования

Сетевой анализ событий, относящихся к безопасности

GFI EventsManager собирает данные от всех устройств, использующих лог-файлы Windows, W3C и Syslog и применяет лучшие в отрасли правила и способы фильтрации для обнаружения ключевых данных. Это позволяет отслеживать, когда сотрудники используют переносные устройства, поднимают трубку, чтобы позвонить домой, включают ПК, что они делают на ПК и к каким файлам они обращаются в течение рабочего дня. GFI EventsManager может уведомить администратора в режиме реального времени, если возникает критическое событие, относящееся к системе и к безопасности, и предлагает корректирующее действие.

Простой анализ журналов регистрации событий по всей сети

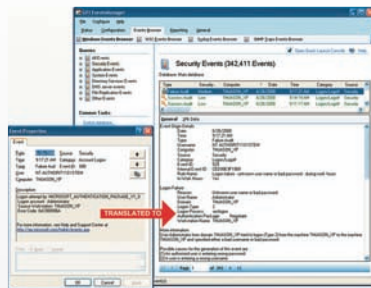
Как сетевой администратор, вы имели дело с непонятными и пространственными файлами регистрации, которые превращают анализ в сложный и трудоемкий процесс. GFI EventsManager представляет собой решение по обработке регистрации событий, обеспечивающее сетевой контроль и управление журналами регистрации событий Windows, журналами регистрации W3C и журналами Syslog, создаваемыми сетевыми ресурсами. GFI EventsManager содержит интеллектуальный процессор обработки событий, обрабатывающий журналы регистрации и предоставляющий информацию централизованным, простым и удобным способом.

«Перевод» непонятных лог-файлов Windows

Анализ журналов регистрации – это долгий процесс. GFI EventsManager «переводит» непонятные описания событий в ясную, краткую форму.



Панель управления GFI EventsManager



Упрощает понимание криптованных лог-файлов

Единое централизованное хранилище лог-файлов

Операционные системы, СУБД, сетевые устройства генерируют тысячи лог-файлов ежедневно, которые хранятся в различных местах по всей сети. GFI EventsManager сохраняет все полученные файлы регистрации в единой базе данных SQL, которая может быть удаленной. Можно также настроить запланированное резервное копирование лог-файлов.

Высокопроизводительный механизм обнаружения

GFI EventsManager включает полностью пересмотренный механизм обнаружения событий, тонко настроенный для достижения максимальной производительности. Исследования показывают, что он способен сканировать и собирать до 6 миллионов событий в час. Более того, его структура, основанная на дополнительных модулях, предлагает дополнительные возможности, а модули можно интегрировать без воздействия на существующий код.

Уведомления в режиме реального времени

GFI EventsManager способен отправлять уведомления при обнаружении ключевых событий или вторжений. Вы можете выполнять такие действия, как выполнение сценариев или отправка уведомления одному или нескольким сотрудникам по электронной почте, сетевым сообщениям и SMS.

Расширенная поддержка лог-файлов различных типов

GFI EventsManager обрабатывает различные лог-файлы, включая журналы регистрации Windows, события Syslog и W3C. Это позволяет собирать больше данных от различных аппаратных средств и программных систем, наиболее распространенных в типичной корпоративной сети.

Сбор данных о событиях, распределенных в WAN, в единую центральную базу данных

Модуль операций над базой позволяет собирать данные от GFI EventsManager'ов, установленных на различных узлах вашей сети в единую централизованную базу. Это дает возможность легко контролировать тысячи рабочих станций и серверов, без нагрузки на использование памяти и пропускную способность. Это платное дополнение объединяет и централизует собранные и обработанные события и позволяет выполнять резервное копирование/восстановление по требованию. Через операции над базой данных можно управлять размером базы данных – без необходимости ручного вмешательства – не только с помощью централизации, но и также с помощью экспорта событий и их резервного копирования при необходимости.

Системные требования

- .NET framework 2.0
- Microsoft Data Access Components (MDAC) 2.6 or later
- Access to MSDE / SQL Server 2000 or later



Для получения более подробной информации и бесплатной демонстрационной версии продукта, пожалуйста посетите <http://www.gfi.ru>

Генеральный дистрибьютор GFI в России и СНГ:

**CONTROL
LINE**

117574, Москва, Одоевского, 7-2-240
+7 (495) 799-1920
www.gfi.ru
info@gfi.ru