

Windows® IT Pro


Comparative Review

GFI Software EventsManager 7.1

GFI Software's GFI EventsManager 7.1 monitors and archives Windows event logs, syslog output, and World Wide Web Consortium (W3C) log file information. GFI EventsManager is an agentless, server-based product and includes a large number of predefined filters, facilitating a quick implementation. Event filters let you configure real-time notifications for select high-priority events, and GFI EventsManager suggests remedial actions for many events. A new add-on utility consolidates the event information that GFI EventsManager servers collect at various company locations into a single database to help you manage database size and record retention. The separately installed GFI EventsManager ReportPack included in the license comes with a variety of predefined reports and enhances your ability to report on events that GFI EventsManager collects.

To collect Windows EVT and W3C logs, the Event Retrieval Engine logs on to the remote system and uses standard Remote Procedure Calls (RPC) and the ETW API to retrieve event data by the schedule that you set. An Event Receiving Engine on the server acts as a syslog host to collect syslog information directed to it. GFI EventsManager will process events against a set of rules and provides the option to archive the events to a SQL Server database. Another option lets GFI EventsManager unconditionally archive all events for all specified logs on selected servers without invoking rules. When you call for the use of rules, GFI EventsManager will filter out uninteresting events and alert you to selected events. Alerting actions include notification via email, Short Message Service (SMS), and Network Messaging (Net Send). You might also run a script or program to perform some remedial action.

Rules let you specify which event criteria will cause GFI EventsManager to select an event for further processing. Rules can be organized into named rule sets for easy management and application. Monitored computers can also be organized within named groups. An event log scanning profile is a named set of rules and other configuration settings that you might apply to monitored computers or groups of computers. You can also apply several scanning profiles to a computer or a group, meaning you can augment profiles that apply to many or all systems with scanning profiles customized for a particular application or server. You can also browse and report on collected events stored in the database by using predefined or custom queries and event filters.

Overall, I was impressed by GFI EventsManager and ReportPack. It's apparent that the designers had both ease of implementation and ease of use in mind when creating these products. The key area I felt GFI EventsManager fell short in is its lack of support for remote workstation installation of the GUI console. I recommend GFI EventsManager for anyone whose log management needs are limited to Windows event logs, syslog output, and W3C log file information. 

InstantDoc ID 95955

John Green

(john@nereus.cc) is the president of Nereus Computer Consulting.

by **John Green**



SUMMARY

GFI EventsManager 7.1

PROS: Many predefined events to facilitate implementation; a well designed, easy to navigate GUI console; many predefined display filters that can be easily augmented with custom display filters

CONS: The GUI console can't be installed remotely, so you must use a remote desktop product for remote administration; has a facility to log all events to the database but not to archive raw EVT files

RATING: 

PRICE: Starts at \$800 for three nodes

RECOMMENDATION: Choose if you need to manage Windows event logs, W3C format log files, and syslog output.

CONTACT: GFI Software • <http://www.gfi.com>

Copyright © 2007 by Penton Media, Inc.

