

EventTracker Pulse

Log Collecting, Alerting and Analysis

Overview

For IT personnel, understanding what is happening in the enterprise network is critical to delivering dependable service to end-users. Event logs put out by your hardware, operating systems, applications and network infrastructure provide a basis for that understanding but without the ability to automate the collection of the logs and help with analysis, event logs can quickly overwhelm even the most sophisticated IT staff. To be successful, you need a solution that first automates the collection of all the events and provides real-time alerting on critical events, then stores and enables in-depth forensic analysis of the event data.

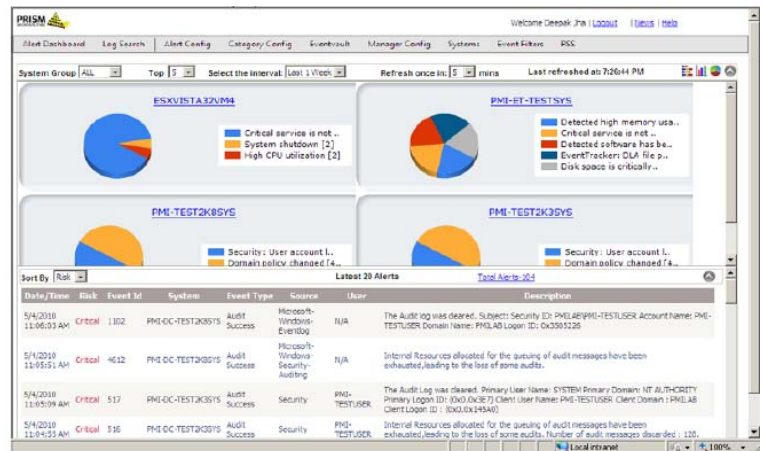
That solution is EventTracker Pulse.

EventTracker Pulse is an affordable, easy to install, log collection, alerting and analysis engine. EventTracker Pulse provides a software-only, agent-optional framework that centrally monitors and manages events generated by all Windows systems as well as syslog and syslog-ng systems and devices. EventTracker Pulse is invaluable for departmental and system admins to gain visibility into systems and components that they are responsible for, as well as for IT security personnel as a security alerting and forensics tool.

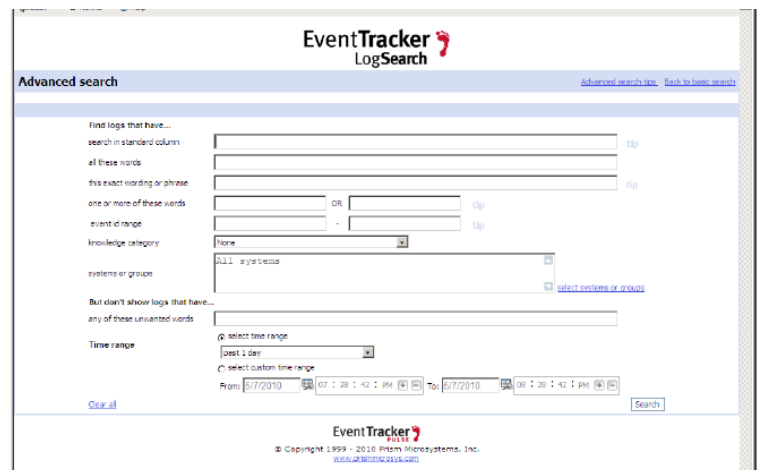
EventTracker is available on a cost-effective subscription basis and can be installed on any Windows platform.

EventTracker Pulse Helps:

- Diagnose system issues before they turn into service-disrupting incidents
- Detect security incidents before costly breaches occur
- Answer the questions: What happened (is happening?) When did it happen? Who or what caused it?



Alert Console



Advanced Search

EventTracker Pulse Framework

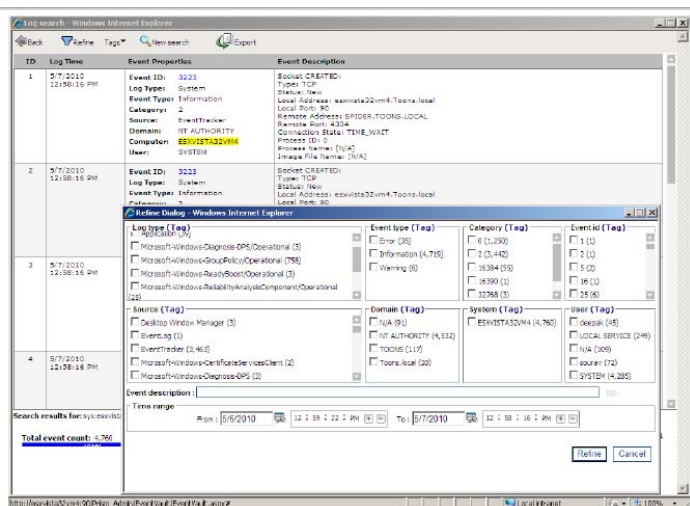
- Support for Windows domain-based and domain-less Network configurations
- Powerful, unlimited rule-based real-time alerting
- Central Security Policy Manager allows remote management of system security policies
- Agent optional – Both agent-based and agentless options available
- Event Warehousing – Ability to archive events for unlimited years in a compressed (>90% compression), tamper-proof archive
- High-speed indexed search with the ability to export results for further analysis
- Optional encrypted, compressed and guaranteed delivery of events
- Automatically backs up and clears the Windows event logs when needed
- Monitoring of any syslog or syslog ng compliant log
- Extensible Knowledge Architecture with built-in support for over 20,000 Event IDs
- Dependable access to the log data from any web-browser

Minimum System Requirements

- 2.8GHz Pentium-based machine
- Windows 2003 Server
- >1GB RAM

Event Storage

- Approximately 120GB disk space per 50 systems per year



Search Results with Refine

Features

Real-time Alerting

- Supports unlimited number of rule-based alerts
- Configurable graphical views of alert groups (systems, types, importance, etc)
- Customizable event criteria including event-fired remedial actions for any defined event
- Out of the box alerts for the most common predefined alert conditions
- Configurable alert prioritization based on event and resource importance as well as vulnerability

Log Search

- High-speed indexed search against all logs
- Search within Search with unlimited refinement
- Over 1000 prepackaged search queries
- Ability to export search results to excel

Unlimited Log Collection

- Highly flexible agent-optional architecture
- Built in syslog, syslog ng receivers
- Supports both UDP or TCP transport
- Optional encrypted delivery of events
- Centralized provisioning of agents from the EventTracker Pulse Console.
- Ability to also poll systems to retrieve logs on a periodic basis
- Support for a mix of agent and agentless systems

Secure Storage

- Optimized, high performance event warehouse included
- Requires no DBMS license
- All logs sealed against tampering with SHA-1 checksum
- Highly compressed (>90% compression)
- Logs can stored on any storage device available on the file system
- No limitation on amount of stored logs

Knowledge

- Integrated access to the EventTracker KB with over 20,000 log definitions
- Includes support for thousands of devices and applications
- Easily extensible by the end-user

8815 Centre Park Drive— Columbia, MD 21045

Toll Free: 877.333.1433 Main: 410.953.6776 Fax: 410. 953.6780

www.eventtracker.com