TOOLBOX

Monitor Your Networks

Greg Steen

EventSentry

www.eventsentry.com

System and network administrators always seem to be looking for a better monitoring solution. By better, I mean more stable, more cost-effective, more scalable, and loaded with more features. NETIKUS.NET aims to deliver a better monitoring solution with the latest version of EventSentry. The application allows you to track most of your vital stats, such as event log entries, disk space, performance, services, installations, and processes. The result is a product well worth considering for your toolbox.

EventSentry uses a Welcome Wizard to get you up to speed quickly; it gives you a quick overview of the application's terminology and feature-set, and provides the suggested steps for implementing the monitoring solution in your environment. EventSentry allows you to divide your monitored systems into different computer groups and specify actions based upon membership to those groups. This is helpful in larger deployments where, for example, you may want to define different monitoring tasks for different departments or handle monitoring of internal application servers differently than Web-servers.

Monitoring services are defined as packages within the application and you can easily assign packages to individual systems, groups, or all monitored systems. The packages are further divided into three groups: filter packages (which are event log filters used to specify which events to process), health

packages (which represent system health monitoring tasks, such as status and disk space), and tracking packages (which are for events that are monitored over time). EventSentry even supports an environmental monitor for measuring the temperature and humidity around your machines as well.

EventSentry provides numerous types of notification, with support for e-mail, databases, Syslog, SNMP traps, text files, and executable scripts and applications. EventSentry also has Web reporting features that let you easily share event log data, tracking data, performance indicators, and service information, which can be viewed with a standard Web browser. You can provide a custom search URL for linking unknown events to, for instance, MyEventlog.com, the Microsoft Knowledge Base, or a custom reference you may have already put together.

The tracking packages require a database for gathering and aggregating data; the application supports both MySQL and MS-SQL. EventSentry includes one default tracking package that tracks all processes, logon/logoff events, and print jobs tracked by the filter packages. The application also includes a default set of filter packages, and additional packages are available from the EventSentry Web site.
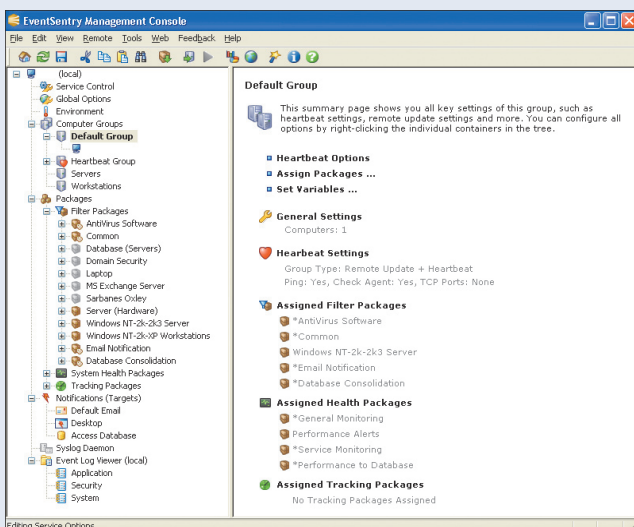
The default filter packages are varied, with event log filters that cover antivirus notifications, database events, Exchange events, various hardware issues, and so on. A particularly handy feature that is fairly new to EventSentry is the Sarbanes-Oxley filter. This filter deals with a number of the event audits that are required to comply with the Sarbanes-Oxley legislation.

The system health packages monitor the general health of your servers. EventSentry includes default settings for monitoring disk space, system resources (CPU and memory performance), and applications and services.

The Remote Update feature allows you to install or update the client agents on your computer groups from a remote host. Remote installation of the client agent does require you to have both the default administrative share (ADMIN$) enabled and the Remote Registry Service running on your host system—and this may not be an option for all infrastructures.

EventSentry's included monitoring packages are customizable and some tailoring of the defaults settings is necessary for handling your needs. The result is a feature-rich yet flexible product that can get you monitoring without breaking the bank.

Price: Based on number of hosts. Starts at $69.00 (direct) for one full license.