

OS Event-Log Monitoring

Automate event-log monitoring and catch potential problems before they occur

Consistently monitoring the Windows event logs should be an integral part of any network-management plan. In a perfect world, you'd review the logs every day and attend to significant events immediately. Unfortunately, network administrators are busy and often don't have time to check logs—a dilemma that can result in network crashes.

Shrinking budgets, staff cutbacks, and management requiring everyone to do more with less have forced drastic changes on the business environment. Network administrators need ways to work smarter. For example, if you had time to regularly review event logs, you could practice proactive network management. The tools in this issue's Buyer's Guide help you manage event logs so that you can work smarter.

When a given event occurs, most OS event-log monitoring tools notify you by pager, email, pop-up box, or through Microsoft Systems Management Server (SMS). Look for a solution that features flexible notification so that you can be notified by pager when crucial events occur and by email or another method when less crucial events occur. You probably don't need to know whether a print job was successful, but you must know as soon as possible if the Microsoft Exchange Server Store Service suddenly fails. Look for tools that let you define notifications by event type, category, and keyword.

Event trend analysis is a troubleshooting feature you should look for. When researching a particular event, you want to be able to easily discover whether the event occurred in the past. Although you can set filters in the Event Viewer to

capture past events, often these events are overwritten and their history is lost. Look for a tool that automatically stores events so that you can analyze this data later. When you have trend-capturing capability, you can use a utility that determines the time interval between specific events as a troubleshooting tool. For example, when Active Directory (AD) events occur on a regular basis, you can analyze the time span between events to help troubleshoot AD or other synchronizing type of errors. Sometimes synchronization errors occur over a time span longer than 24 hours, thus the time interval between errors isn't obvious.

Another useful feature is the ability to annotate the event log. When you have this capability and similar events occur in the future, you won't have to reinvent the wheel. You can simply refer to your notes and quickly solve the recurring problem by using the solution you devised earlier.

The event-log monitoring tools in this guide are especially useful when you have many servers spread across a WAN. Then, you can receive fast notification about events and address them before a situation becomes a problem. Ideally, you shouldn't have to install the tools on each server, but this varies depending on the tool.

If you had time to regularly review event logs, you could practice proactive network management.

When you're ready to invest in an OS event-log monitoring tool, make sure you can access your servers remotely on a secure channel. That feature will let you solve many events remotely or at least temporarily fix the problem until you can get into the office. Installing Windows 2000 Server Terminal Services in Administrator Mode on Windows Server 2003 and Win2K is a powerful remote management solution.

All of the products in this Buyer's Guide let you monitor the Event Viewer by using the "management by exception" model, so you can set alerts for crucial events that have the potential to crash the server or cause network disruptions. Find a product that fits your company's requirements. Some tools specialize in monitoring events, while other tools offer a complete network-management package. Use these tools to work smarter instead of harder and to keep close tabs on the health of your network.

ALAN SUGANO

(asugano@adscon.com) is the president of ADS Consulting Group, which specializes in networking, custom programming, Microsoft .NET Web development, and SQL Server development.

EDITOR'S NOTE

The Buyer's Guide summarizes vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to <http://www.winnetmag.com/buyersguide>.

InstantDoc ID 40712

Contact Information	Product Name	Price	Description
Aelita Software 614-336-9223 800-263-0036 http://www.aelita.com	InTrust	Contact vendor for pricing	Consolidates event, performance, and other audit data across multiple directory services, applications, and systems; performs monitoring, security assessment, capacity planning, and performance optimization; features an optimized repository-based solution for long-term archival of data; provides automatic notification of events that might signal system problems or attempted intrusions; alerts you through email, pager, network message, or SNMP traps; can customize more than 1000 predefined reports
Alchemy Lab 818-789-1644 http://www.alchemy-lab.com	Alchemy Eye	\$299	Monitors Windows 2003, Windows XP, Win2K, and Windows NT event logs; in the event of network errors, the program can issue cell phone or pager alerts
BMC Software 713-918-8800 800-841-2031 http://www.bmc.com	PATROL Express	Starts at \$400 per server	Remotely monitors the performance and availability of servers, applications, and network devices; doesn't require agent installation for the systems you want to monitor; checks on performance and the availability of Web transactions
	PATROL for Microsoft Windows Servers 3.0	\$815	Monitors Windows services and processes, CPU and memory usage, and available disk space; issues alerts or takes recovery action when problems are detected; can be configured to monitor the Windows event log for any event that isn't automatically monitored
Converse Software 650-579-6637 http://www.conversesoftware.com	NimBUS	\$500 per server	Monitors all Windows event logs and non-Windows log files; scans the event log for information according to predefined monitoring criteria; search facilities speed the criteria definition process and reduce implementation time; notifies administrators through email, pager, or SMS message; reporting capabilities feature a Web-based interface that you can customize to reflect event-log status; also monitors Windows performance counters, processes, and services
Dorian Software Creations 678-222-3443 866-682-3646 http://www.doriansoftware.com	Total Event Log Management Solution	Starts at \$89.99 per server	Event Alarm module monitors events and provides notification through email, pager, or pop-up message; Event Archiver module archives selected logs for further auditing; Event Analyst module provides reporting and filtering capability and enables internal compilation and trending; the modules together work locally or remotely and monitor six event logs and syslogs; supports Microsoft IIS
elQnetworks 508-358-7601 http://www.elqnetworks.com	SyslogAnalyzer 2.0	\$495 per 10 managed systems	Browser-based Windows and UNIX event-log analysis and reporting software generates reports and provides insight into server system events and potential problems; provides a centralized mechanism to consolidate event logs from distributed systems running on Windows and UNIX platforms
Engagent 425-485-8754 877-820-7980 http://www.engagent.com	Event Log Sentry	\$195 per server	Features a consolidated view of event logs with detailed filtering of events stored in Microsoft SQL Server; triggers notifications and runs external applications as a response to events; automatically clears and archives event logs; features a specialized viewer to simultaneously show multiple archived log files; provides centralized management of audit policies and event-log settings
Exceedio 888-210-7459 http://www.exceedio.com	Exceedio System Monitor	\$39.95 per year per system	Hosted event-log monitoring service that doesn't require a database, mail services, or configuration; you install a lightweight agent on the systems that you want monitored, and the agent securely sends system and event information to Exceedio's centralized monitoring server; you receive event notification, management, diagnosis, and resolution across all of your systems through a Web-based interface; the service gathers resolution suggestions from previously resolved events and from third-party resources

Contact Information	Product Name	Price	Description
Gravity Square 425-637-1443 http://www.gravitysquare.com	GSI Event Log Gatherer 1.5	\$40 per monitored server	Consolidates multiple-server event-log data into one repository; builds Web reports and notification criteria according to selectable event-log parameters; lets you perform system administration through a Web browser
Heroix 617-527-1550 800-229-6500 http://www.heroix.com	Heroix eQ Management Suite	\$595	Supports application, system, and network monitoring; features local and remote monitoring of all Windows event logs, customizable notification, the ability to annotate log-related events, optional automatic corrective actions, and automatic self-configuration; lets you customize and extend capability without writing code; includes resource trend-alerting capabilities and a Web-based interface
Infopulse sentry.sales@infopulse.ro http://www.sentry-pro.com	Sentry Pro	\$239	Monitors all event sources such as event logs, syslog, services, and performance logs; notifies you about crucial events that require correctivemeasures; lets you set conditions for security, systems, directory services, DNS servers, file-replication services, and event logs that third-party software applications create
Ipswitch 781-676-5700 http://www.ipswitch.com	WhatsUp Gold 8.0	\$795	Identifies network events such as security breaches and system and application errors; features network discovery and graphical mapping of network topology; SNMP threshold monitoring tracks system and network performance bottlenecks; features real-time alerting through email, pager, SMS, and program executable; lets you customize notifications; generates reports
IS Decisions info@isdecisions.com http://www.eventtrigger.com	EvenTrigger 1.61	\$175 for a computer license	A real-time event-log monitoring tool with filter-based notification functions; runs as a Windows service; can generate pop-up or email messages; can start processes or scripts or can insert events into an OLE DB database; supports Windows 2003, Win2K, and NT systems
Microsoft 425-882-8080 800-426-9400 http://www.microsoft.com	Microsoft Operations Manager (MOM)	\$349 for a base processor license; \$349 for an Application Management Pack processor license	Provides enterprise-class operations management with comprehensive event management, proactive monitoring and alerting, reporting, and trend analysis; the built-in Application Management Pack provides a product support knowledge base for applications and services in a Windows-based IT infrastructure
Netikus.net 877-485-3975 http://www.eventsentry.com	EventSentry	Starts at \$159	A Windows 2003, Win2K, and NT application that supports complex filter schemes to divert events to multiple, customizable targets; features several notification types, including SMTP, file, ODBC, syslog, network, process, and desktop; includes built-in event-log viewer with log annotation and syslog daemon features
NetIQ 408-856-3000 888-323-6768 http://www.netiq.com	AppManager Suite	Based on the number and type of managed systems and applications; agents start at \$600, consoles start at \$2500	Monitors all Windows event logs, domain controller (DC) logs, and any application log; supports Windows 2003, Win2K, NT, UNIX, and Linux OSs; notifies you remotely through email or pager or locally through management console; integrates with frameworks and Help desk systems
	Security Manager	Contact vendor for pricing	Performs real-time monitoring and notification through email or pager; provides correlation, analysis, reporting, and automated response to suspicious activity through the security console; consolidates distributed event logs; provides a customizable knowledge base that can link to third-party knowledge sources
NRG Global 213-383-6745 866-797-5623 http://www.nrgglobal.com	Sysload 4.6	\$100	Monitors all Windows event-log files and any text-based log file, including files with unknown filenames; lets you use command line or script-based reactions to events; sends notification through email, pager, visual dashboard, and corrective actions; Log Analyzer module is standard with syslog monitoring and performance management agents

Contact Information	Product Name	Price	Description
Objective Software 416-707-9414 http://objsoftinc.com	EventMaster	Contact vendor for pricing	Manages workstations and servers; routes and delivers collected events according to your filter criteria; Web interface controls processing events and enables the immediate delivery of important messages through email or the Web
Omnitrend 860-673-8910 http://www.omnitrend.com	ServScan	\$599	Monitors all Windows standard and custom event logs from a central location; doesn't require a client piece; sends alerts through email, pager, SMS, and network messaging; can customize notifications to individual events and time of day; logs all notifications for later review; lets you import logs to a database
Opalis Software 416-253-9383 888-672-5471 http://www.opalis.com	OpalisRobot	\$995	Monitors logs and performs automatic corrective action; sends notification with log details and forwards to other management tools; uses message codes to capture log details such as log name, event ID, and source; when software detects a message, it replaces codes with specific details to reduce the need to create multiple rules
OSA Technologies 408-436-6333 http://www.osatechnologies.com	OSA Server Manager	Contact vendor for pricing	Provides hardware, OS, and application monitoring and management; also features process, disk, and memory monitoring; monitors hardware by using the Intelligent Platform Management Interface (IPMI) standard for hung or thrashing OS situations
Prism Microsystems 410-953-6776 http://www.eventlogmanager.com	EventTracker	\$140 per server; \$31 per workstation	Monitors Windows, UNIX, Linux, and SNMP devices; you install the console on a Windows machine and receive events from monitored systems; you can deploy the EventTracker Agent to monitor Windows systems; the console receives syslog and SNMP traps stored in an ODBC database and generates alerts; includes filtering, correlation, and reporting capabilities
RGE 317-745-3398 http://www.ipsentry.com	IPSentry	\$148	Can monitor and filter event logs for user-defined events; alerts you through email, pager, or syslog or by launching an application when it finds specified events; you can use a free version of IPSentry to monitor two separate system logs
TNT Software 360-546-0878 877-546-0878 http://www.tntsoftware.com	ELM Enterprise Manager 3.1	\$415 per server	Provides real-time event collection and consolidation, health and performance monitoring, service and process monitoring, log-file monitoring, enhanced cluster monitoring, end-to-end monitoring, and data collection for Exchange; also provides query-based monitoring of SQL Server; supports Windows Management Instrumentation (WMI), TCP port monitoring, and TCP/IP application-based monitoring of SNMP, syslog, HTTP, HTTP Secure (HTTPS), SMTP, POP3, FTP, and Ping
	ELM Log Manager 3.1	\$325 per server	Automates a variety of the administrative functions required for monitoring and managing event logs, log files, SNMP traps, and syslog messages from Windows-based servers and workstations and TCP/IP systems and devices; features a multilayered architecture
Tools4ever 516-482-4414 866-482-4414 http://www.tools4ever.com	MonitorMagic	Starts at \$599	An agentless monitoring solution that features a Web interface; supports all event logs and provides centralized event-log consolidation and event archiving into Microsoft Access and SQL Server; also features event-log annotation; provides extensive notifications