Monitoring Windows Workstations - Seven Most Important Events

White Paper

8815 Centre Park Drive
Columbia MD 21045
877.333.1433

Publication Date: Apr 23, 2007

ABSTRACT

Monitoring event logs from workstations provides two important benefits a) Save money by adopting a proactive approach to supporting end users (enhanced productivity), and b) Enhance overall security of your organization. The sheer volume of data that must be analyzed, however, renders manual monitoring completely impractical. On the other hand, if you don't monitor workstations at all, you are exposed to security risks, higher cost of administration, lost productivity and user frustration. Rather than adopt an all or nothing position, these documents suggest a middle ground with automation to help justify the cost/benefit.

Why Monitor Workstation Event Logs?

Monitoring event logs from Windows workstations provides two important benefits:

- Save money by adopting a proactive approach to supporting end users (enhanced productivity)
- Enhance overall security of your organization.

The sheer volume of data that must be analyzed, however, renders manual monitoring completely impractical. On the other hand, if you don't monitor workstations at all, you are exposed to increased security risk, higher cost of administration, lost productivity and user frustration.

Two main reasons why many organizations don't monitor workstation are:

- Too much work and administrative effort to monitor hundreds of workstations.
- Cost/benefit (ROI) is not justified

Indeed both reasons are valid if you monitor all events on all workstations. This should not, however, take you to the other extreme of not monitoring any events from any workstation at all. A practical and acceptable medium ground is recommended in this White Paper - monitor a small subset of critical events from workstations such that cost and benefits are justified. This approach yields three main benefits:

1. Annual cost of managing and supporting user can be reduced from 10 to 25%
2. It enhances the overall security of an organization
3. Improves your internal IT control

Security logs provide reams of valuable information, but it's up to you as the administrator to collect, analyze and assess the information provided. This is next to impossible in a large environment given the sheer volume of information. Furthermore, manually parsing log files looking for events is not a timely or practical solution. When the security of your network is at risk, you require access to critical information immediately - not whenever you finally find the time to view your logs.

EventTracker (www.eventLogManager.com) has simplified monitoring workstation by providing a preconfigured ruleset for workstations to enable concentration on the most important events. These include:

- User logon/logoff;
- Logon failures;
- Disk space utilization;
- Service/ start and stop;
- Runaway process monitoring;
- Software install/uninstall monitoring and
- USB disk inserts/removal.

Seven Critical Events

Event	Purpose	What to monitor	Operation
1. User logon/logoff	Monitoring user logon/logoff increases IT control. Can detect an insider threat.	Windows event id 528, 538	Weekly automated task: - Generate and review report of logon-logoffs by users and by group of computers - Generate graph to monitor "off hours" log on activities
2. Logon failures	Intrusion detection, security enhancement, help desk support	Windows event id 529, 530, 531, 532	Daily task: Review the automated logon failure report by user and by computer to ensure security.
3. Monitor disk space	Operations, help desk	EventTracker agent generates threshold defined for disks	Daily task: Review all the disks in your workstation farm which are above 80% full.
4. Monitor Service Start and Stop	Operations, help desk, security Your workstation security and operation is compromised because your critical services are not started –(e.g. Virus checking)	EventTracker agent monitors all the services	Daily task: Review all stopped services on all workstations Weekly task: Review total downtime generated by the services
5. Monitoring runaway process	- Operations, help desk - Trap and identify all the process and services which start consuming over 50% CPU and over 100MB of RAM	EventTracker monitors runaway process	Real-time alert: Notify system administrator right away for runaway process. System administrator should identify and stop runaway process. Weekly task: Review all the runaway processes such that you can remove the task or get the fix from the application vendor
6. Monitor Software install/uninstall	IT controls, Patch management, operations	EventTracker agents monitors software install/uninstall	Daily Task: Review all the software installed on workstations and identify unwanted installed

			software which violates company policy and licenses Weekly task: Generate patch management report to make sure that your workstations are up to date
7. Monitor USB disk inserts	Security Monitor users who mount USB drive or DVD/CD drives and copy files	EventTracker agents monitors USB drive inserts and device chang	Daily task: Review report for USB drive activities

The EventTracker Solution

The EventTracker solution is a scalable, enterprise-class event management, analysis and auditing system for SYSLOG/SYSLOG NG systems, Windows and SNMP devices. EventTracker enables a “defense in depth”, where data can be collected, correlated and analyzed from the perimeter security devices down to application logs. Event logs are a critical trail of information about the usage, health and status of the computer systems that store sensitive data, the applications that contain the data, and the users that access the data.

To prevent security breaches, Event Log data becomes most useful when interpreted in near real time and in context. Context is vitally important because often the critical indications of impending problems and security violations can only be learned by watching patterns of events across multiple systems. EventTracker provides real-time capability that can proactively alert security personnel to an impending security breach.

EventTracker provides a robust solution that centralizes the management of events on your network and allows you to easily extract valuable business intelligence.

EventTracker provides the following benefits

- A centralized server that consolidates all Windows, SNMP V1/V2, legacy platforms, SYSLOGs received from routers, switches, firewalls, critical UNIX servers (Red Hat Linux, Solaris, AIX etc), workstations and various other SYSLOG generating devices.
- Automated archival mechanism that stores network activities over an extended period to meet auditing requirements.
- Real-time monitoring and parsing of event logs to analyze user activities such as logon failures, failed attempts to access restricted information.
- Alerting interface that generates custom alert actions via email, pager, beep, console message, etc.
- Event correlation modules to constantly monitor for malicious hacking activity. In conjunction with alerts, this is used to inform network security officers and security administrators in real time. This helps minimize the impact of breaches.
- Various types of network activity reports, which can be scheduled or generated as required for any investigation or meeting audit compliances.
- Role-based, secure event and reporting console for data analysis.
- Built-in compliance workflows to allow inspection and annotation of the generated reports.

About Prism Microsystems

Prism Microsystems, Inc. delivers business-critical solutions to consolidate, correlate and detect changes that could impact the performance, availability and security of your IT infrastructure. With a proven history of innovation and leadership, Prism provides easy-to-deploy products and solutions for integrated Security Management, Change Management and Intrusion Detection. EventTracker, Prism's market leading enterprise log management solution, enables commercial enterprises, educational institutions and government organizations to increase the security of their environments and reduce risk to their enterprise. Customers span multiple sectors including financial, communications, scientific, healthcare, banking and consulting.

Prism Microsystems was formed in 1999 and is a privately held corporation with corporate headquarters in the Baltimore-Washington high tech corridor. Research and development facilities are located in both Maryland and India. These facilities have been independently appraised in accordance with the Software Engineering Institute's Appraisal Framework, and were deemed to meet the goals of SEI Level 3 for CMM.

For additional information, please visit http://www.prismmicrosys.com/.