

Improving Server Reliability with Windows Event Log and Automated Event Notification

Implementing automated event notification can reduce a flood of events to a trickle and ensure administrators see all critical events within seconds. Those seconds can often make the difference between correcting a problem before users and customers are affected or suffering a major outage.

Using Windows Event Logs

Most system and network administrators quickly turn to Windows event logs to investigate and troubleshoot performance problems on Windows servers. An administrator can easily see key events recorded in the system, security, and application logs and diagnose the source of a problem using the Windows Event Viewer.

Event logs can provide extremely detailed information about the current state of a server. In practice, however, today's administrators can't afford to constantly view the event logs on every server. Plus, manually monitoring logs tends to be reactive and may result in overlooked errors and warnings.

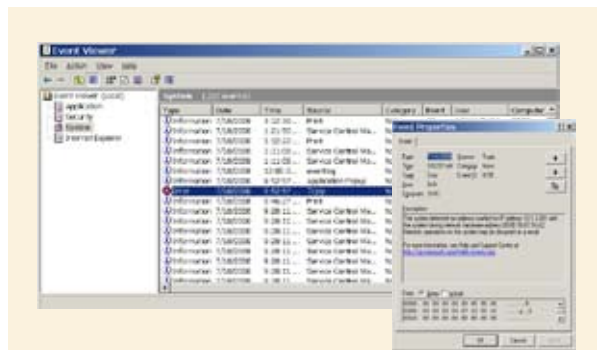


Figure 1: Windows event logs provide critical information troubleshooting sever problems

Implementing Automated Event Notification

Many administrators rely on automated event notification tools to filter events and send notification messages via email or some other media. Automating events enables administrators to catch problems early and significantly improve server reliability.

- The system log contains events associated with the operating system and server hardware. For example, if a disk drive experiences a buffer error, or an interface card detects a bad packet, an event is recorded in the system log.
- The security log records events such as invalid logon attempts and file creation and deletion.
- The application log contains events logged by programs, for example a database program may record an event for an invalid query attempt.

Automated event notification can be especially helpful when troubleshooting a persistent problem. For example, suppose a server reports a warning event, and your research finds three possible causes and related fixes. Initially, you implement the most likely fix, but you need to know whether it actually solved the problem. By creating a notification rule for the specific event, you'll receive a notification should the problem reoccur, and you can immediately apply the next fix.

When implementing automatic notification, you should consider the structure of your support organization. For example, you could configure a set of rules where "Warning" events are sent to a level 1 support desk and "Error" events are routed to a server, security, or application specialist. Also, when troubleshooting, specialists will want to create rules to notify them of specific events as they isolate and correct problems.

There are a number of free Windows event notification tools available to help you manage event logs. EventSentry Light, for instance, filters Windows event log messages and sends an alarm message by email (http://www.eventsentry.com/downloads_downloadnow.php). For basic event log filtering, try Event Log Explorer at <http://www.eventlogxp.com/>.

You can also try Snare Agent for Windows, which forwards Windows event log messages to a syslog server (<http://www.intersectalliance.com/projects/SnareWindows/index.html>). For a more robust event notification, you might consider WinEvent Logger Pro, a shareware tool that retrieves Windows event log messages, processes events according filtering rules, and sends notification messages by email, SMS, HTTP-SMS, syslog, SNMP and pager (<http://www.theonesoftware.com/>).

Leveraging an Integrated Dashboard

Although “point tools”, like those above, do a good job for their intended purpose, deploying an integrated, top-down solution with built-in capabilities such as automated event notification can significantly improve system availability and reliability while freeing administrators from hands-on tasks such as manually monitoring event logs.

dopplerVUE visually integrates server metrics, alarms, and Windows events into a single view. You can select any combination of WMI, SNMP MIB-2, and ICMP metrics, thus allowing you to monitor all aspects of a server from one application.



Figure 2: dopplerVUE lets you monitor all aspects of server performance from a single integrated view

New in dopplerVUE Release 1.2, the onboard Windows Event Log Monitor uses built-in and custom filters to collect Windows events. For example, you can routinely collect all “Error” and “Warning” events for a server using a built-in filter. Then, to troubleshoot a SQL Server login problem, you can add a custom filter to collect only those events with Event ID 17055 (login failed for user).

Configuring a notification rule in dopplerVUE for collected Windows event log data is easy: select the event filters that define the events for the rule, the servers (network elements) to monitor, and the actions to perform whenever a particular event occurs. For example, you might configure a rule that displays alarm and sends an email whenever dopplerVUE collects an “Error” and “Warning” events from the system log.

About dopplerVUE

dopplerVUE is a powerful yet easy to use network management solution for managing up to 5000 network elements. To see how dopplerVUE can solve your network management needs, visit to www.dopplerVUE.com. For more information call 888-dvue-now (888-388-3669).

© 2008 SYS Technologies. All Rights Reserved. All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturer.