Spamming the event log doesn't make things any better

April 4, 2006

Raymond Chen

A common suggestion is that if a problem is detected which the system automatically recovered from but which an administrator might be interested in knowing about, then an event log entry should be created. Be careful, however, not to abuse the event log in the process. If the problem is not security-related and it can occur, say, more than a few times a day, then generating an event log entry may do more harm than good. The event log has a maximum log size (default 512KB on Windows XP), and when the log fills, older log entries are discarded to make room. If you generate a lot of events, you can end up filling the event log with your events, pushing out all the other events that the administrator might have been more interested in. Even worse, the administrator may have disabled automatically discarding old event log entries, in which case the system will generate error messages once the event log fills.

Network administrators make it a habit to go through the event logs of the machines on their network looking for unusual activity. If you fill the event log with chatter, this makes it harder for them to spot the real problems.

Raymond Chen

Follow