

## Important Facets of IT monitoring and Event Correlation

In the world of Information Technology (IT) Management where acronyms and technologies seemingly reproduce exponentially, it is a necessity to be able to separate out the real important issues from the underlying noise. When it comes to monitoring, what really matters is the ability to drill through the noise and determine what in your business is either currently being affected, or what will become affected soon.

There are two basic types of monitoring, fault management (which uses a push model), and network management (which traditionally uses a pull model). Fault management systems use a push model and receive packets of information without requesting it in the form of SNMP Traps, Notifications, and Informs. The senders of this information (the various equipments located on the network), do so whenever they feel that there is something noteworthy, and especially when there is a problem that they are experiencing, whether it be something they themselves are undergoing or something that a neighbor may be reporting to them. One advantage of these fault systems is the breadth of information that is available, as well as the fact that the information simply comes to the SNMP manager. The disadvantage to these types of systems are that typically once the information is sent, it is "too late", and the problem has already happened. It is generally a "reactive" type of monitoring. At this point, the network administrator or engineer must come to the rescue, either with software tools such as a MIB Browser or real hardware tools such as a screwdriver and a hard-drive.

Traditional Network management and monitoring systems use a pull model, and periodically (typically every 5 minutes), poll the systems in the network for specific statistics and information which may be used later on to correlate data or to run historical reports. The advantage of these types of systems is that they are "proactive", and allow the admin to make decisions based on the statistics collected and the reports that they can run.

The combination of the fault and network monitoring allows an administrator to have a much more holistic view of the network. Advanced systems can do event correlation to match some of these real-time faults and SNMP traps with data collected from the polling engines, and then real-life business decisions can be made. For example, if a system determines by analyzing historical data that the amount of free space on a hard-disk has decreased more rapidly as of late, and there is a fault that comes in from the online ordering system stating that it cannot take orders online anymore, a correlation engine can determine that the reason may in fact be because the hard-disk has finally filled up and this is preventing the ordering system from fulfilling orders. An even better system would look at trends over time and send a message to a network administrator before the hard-disk fills up, telling them that they have just a couple of days left before this potential problem could happen.

In conclusion, network and fault management are two of the most crucial facets of your IT monitoring paradigm. There are other important facets of IT to manage, like applications and configuration, but both of these fall underneath the umbrella of network and fault in some cases as well. A really good correlation system must have at least basic configuration knowledge, including components of each system monitored as well as the connective and topological layout of the network and systems.

### About the Author

For more info about [SNMP Traps](#) or especially [Fault Management](#) please visit this website <http://www.oidview.com>

Source: <http://www.tntarticles.com>