



### **Monitoring Your IT Environment**

**Jeffrey S. Bardin, CTO**

**Treadstone 71**

Does your IT staff monitor your environment? If they say they do, what is it that they monitor? Do they provide you, the customer, a view into what they see? Do they provide you with metrics and reporting in both static and proactive/real-time forms? When something breaks, do you have a comfort level that IT will catch the error, and do they have the processes and procedures in place to quickly mobilize to solve the problems?

Not that long ago, IT departments were the exclusive arm of the chief financial officer, driven by the needs of accounting and finance, and not necessarily seen as a vital part of the company's structure. Today, technology is absolutely critical to the daily functions and flow of the company. In actuality, it is not the technology that is core to their business, but the availability and use of the data. IT customers today expect 100% availability of their applications, databases, connectivity, servers, and storage devices, and rapid and consistent response times with a proactive flair < absolutely no excuses as they gain access to data. If IT does not monitor each functional area in the technology stack, how can they be expected to provide an adequate level of uptime?

Many IT departments are finding this level of monitoring < that drives reliability, scalability, and responsiveness to their customer base < much too big a burden to bear. IT budgets continue to rise as these requirements force companies to re-engineer legacy infrastructure and move to current Internet technologies. Most are understaffed and many lack adequate skills. There is an overall reluctance to invest, and internal politics may hinder quick IT turnaround to meet corporate objectives.

Most monitoring solutions today measure various attributes of hardware and software such as CPU uptime, network traffic, e-mail flow, pinging of routers, switches, HTTP, HTTPS, FTP, DNS lookup, file systems space utilization, swap space, memory utilization, and application services. Many IT shops measure these attributes, but few aggregate the data for correlation, performance, and trending analysis. Most only use the data in a reactive mode when something goes wrong. To even come close to the nirvana of 100 percent availability, an integrated solution that detects failures and delivers metrics, staff to address the problem identification, root cause analysis, and problem resolution, and the process flow for mobilizing and supporting all the above is required. With military precision, these mechanisms must occur in parallel, working together like a well-oiled machine to reach the ultimate goal of constant data availability for the customer.

This integrated solution need monitor internal LANs and WANs, as well as monitoring customer firewalls, intrusion detection systems, and virtual private networks for service affecting faults and service degradation. Critical LAN and WAN parameters need to be

monitored against performance thresholds. Data for server hardware monitoring, system status, system health, pre-failure monitors, performance, and environmental factors must be collected and stored. Operating system statistics, logging, and the forwarding of filtered event data < for review and possible immediate corrective action or future capacity planning > needs to be collected and stored.

Applications must be monitored for overall health, security, access, performance, and capacity. Databases need to be monitored for table space availability, status, fragmentation, service state, table page locks, and extents to automatically allocate addition table space. Events and faults must be recorded and displayed visually and via multiple alarm vehicles (e-mail, page, phone, fax, automated trouble ticket creation, and wireless). Remote hands access to servers for out-of-band management must be in place to view blue screens, replay the boot process, and to turn the server on and off. Centralized management and monitoring solutions need to be available and used to integrate and correlate the on-going management, health, and performance monitoring information. This information can be used to predict future failures, providing the ability to take proactive measures against bottlenecks or deviations outside pre-defined benchmarked levels.

Can your IT shop deliver such a solution? Do you have a solution that delivers pre-processing and filtering of events, alarms to reduce information overload and minimize time-to-repair, intelligent polling that optimizes network bandwidth and minimizes agent queries. How about providing a full range of automatic corrective actions, including responding to a single event, a sequence of events, persistence of a condition, and taking multiple actions as the result of a single event? Do you have a staff in place that is highly trained in problem identification, root cause analysis, problem resolution and change management with a customer focus? What is the IT process to collect, analyze, diagnose, develop potential solutions to the problem, select the proper solution, gain customer acceptance for such, and then actually solve the problem?

As much as 80 percent of system downtime is spent identifying a problem prior to even formulating a solution. Is there a method in place to measure these processes for accuracy, actual utilization, and potential improvement? Do your customers have access to daily, weekly, and monthly reports that cover overall resource health, such as network utilization, Web, application, and database response time? Is the ability there for your customers to view comparison and trending reports that are meaningful to them in non-technical lingo? Do they have the ability to generate real-time reports on demand? Do your customers have the ability to watch you watching them?

Does your IT staff provide you with reports covering these industry standards: mean time to notify (MTTN), the average time between alarm detection and NOC notification; mean time to respond (MTTR), the average time between opening of a trouble ticket and initiation of problem resolution; mean time between failures (MTBF), the average time between component and system failures; mean time to repair (MTTR2), the average time required to repair an urgent issue?

If you do not have such an integrated solution, you must ask yourself several questions: Is

my current infrastructure capable to provide such a solution? What is the cost to build this infrastructure and how much time do I have to do so? Are the costs of such an improvement so great that it is not practical? Has my IT environment become so complex that I am headed for availability issues, customer dissatisfaction, and escalating support costs? Have the investments in my IT infrastructure been for naught since they are not available when you need them? What is my core business function < is it information technology? How important is the availability of my data? What other options do I have?

If you find the answers to the above questions less than favorable, it may be time to look at a service provider whose sole focus is to consistently deliver exceptional customer service through affordable solutions that include performance, speed, reliability, scalability, accuracy, and best-of-breed integrated monitoring offerings. A managed service provider who can comprehensively and proactively deliver centralized monitoring, correlation analysis, and reporting of applications, network, security, databases, storage, service, and hardware performance on a 24x7 basis.

In the current business environment, you must be aware of the service provider's financial viability. You must be cognizant of its past. Did it build its business model during the dot-com era of spend at all cost to be first to market? Is the provider already suffering its own legacy issues? Has its focus been on collocation and is it now struggling to move to the managed service space? Does it have a plan for future technological development? Is the provider moving ahead or standing still < treading water until the shakeout is over? Is it willing and able to learn about my business? Is it organized in such a way that it's able to understand that service is measured by the customer? The provider must be able to measure the whole and not just parts with its monitoring solutions. Performance must be measured from the customer inward.

Unplanned outages will occur. The information technology environments of today cannot meet 100 percent availability, but that does not preclude us from striving to achieve that level. Proactive monitoring, data collection, correlation analysis, reporting, problem identification, root cause analysis, and resolution are the foundation that needs to be in place as we move to full fledged service level management, which is a whole subject unto itself better saved for another day.

Jeffrey S. Bardin, CTO  
Treadstone 71  
[jbardin@treadstone71.com](mailto:jbardin@treadstone71.com)