

Moving Past Static Performance Alarms

nGenius Analytics Product Review



Jim Metzler
Ashton, Metzler & Associates
jim@ashtonmetzler.com

Introduction

In an IT Impact Brief published in February 2006, I stated my belief that one of the most important ways that infrastructure and management organizations can demonstrate their business value is to show what they do to enable their company's key applications and business processes. I then included in that brief some market research that I had conducted in an attempt to create a reality check on how companies currently deploy and respond to network and application performance alarms. That research indicated that there is a clear gap between the current approach to using network and application performance alarms and what is required to proactively manage a network and the applications that transit the network. Some of the indications of that gap are:

- Less than a third of companies set a performance threshold on applications
- Two-thirds of companies ignore the vast majority of alarms
- Only a quarter of companies utilize rules programmed into their tools to analyze the severity of alarms
- The most likely person to recognize that there is a performance problem with an application is an end user

This review is intended to discuss the automated detection of anomalies by the use of analytics. Analytics is a rapidly developing component of network management that is intended to remove the limitations imposed by the current generation of network and application performance alarms. As with much of my research and writing, I interviewed a user of the technology to gain additional insights. For this review, the interviewee was a manager of network performance at a major Telco. That interviewee will be referred to in this review as The Telco Manager.

Analytics

According to Wikipedia, the term analytics refers to the branch of logic dealing with analysis. Over the last few years the term has been used in a wide range of contexts. One of these contexts is business analytics. Business analytics refers



to sophisticated forms of business data analysis. For example, business analytics lets companies combine demographic and behavioral data with sales information to determine how best to leverage the relationship that they have with their customers.

Another context is Web analytics. Web analytics refers to the measurement of the behavior of visitors to a website. One common application of Web analytics is to identify which landing pages encourage people to make a purchase.

In the context of IT, analytics can be used to measure a variety of things, including server performance; i.e., CPU or memory utilization. This review will focus on network analytics.

nGenius Analytics Product

One of the primary goals of the *nGenius Analytics* product is to automatically detect any abnormal behavior in terms of how a network is performing relative to a wide range of network characteristics, such as utilization. Another goal of the *nGenius Analytics* product is to identify the application that caused the anomaly to occur.

According to The Telco Manager, having the *nGenius Analytics* product focus on utilization is appropriate as he feels that a change in utilization is the first sign that there is a problem on the network. He stated that one of the main reasons his organization has started to use the *nGenius Analytics* product is because they have a lot of unknown applications running on their network and the combination of the *nGenius Analytics* product and the *nGenius Performance Manager* allows them to identify which application is using a given port.

Referring back to the [February 2006 IT Impact Brief](#) on network and application performance alarms, one of the factors that limits an IT organization's ability to effectively utilize performance alarms is the difficulty of establishing values for the various thresholds that makes sense over time. For example, as was identified in the February brief, roughly two-thirds of IT organizations set thresholds at a high-water mark to ensure that they only see severe problems. This approach essentially guarantees that the majority of problems are ignored until they reach a critical state.

However, if the IT organization is looking either to be more proactive in terms of identifying issues or if they are just trying to troubleshoot a problem, they may well lower the threshold. This approach guarantees that they will be inundated with alarms. Alternating between the two approaches leads to the worst of both worlds - either virtually all issues are ignored until productivity is impacted, or else the IT organization receives so many alarms it cannot respond to them all.

The *nGenius* Analytics product automatically adjusts the level of the thresholds based on sophisticated statistical models of network usage, and can do this for both physical and virtual circuits. For example, consider a circuit that supports 9 DLCIs. The *nGenius* Analytics product would look for anomalies in the utilization of each one of these individual DLCIs, as well as in the utilization of the link in aggregate.

Because of this approach, the *nGenius* Analytics product also has the capability to help manage quality of service classes (QoS). To exemplify this, consider a hypothetical company that has five service classes ranging from the most stringent (real-time traffic) to the least stringent (best-effort traffic). The *nGenius* Analytics product has the capability to analyze each of these service classes and identify anomalies in each class.

The Telco Manager described a situation in which they had set a performance threshold on a T1 link at 70% utilization and were getting a performance alarm every fifteen minutes. When they set the threshold to 90% they got far fewer alarms, but still the problem persisted. When they applied the *nGenius* Analytics product they were able to quickly identify which application was causing the problem.

Based on this sequence, the next step would typically be to drill down in *nGenius* Performance Manager to discover the source and destination address of the users for the application utilization increase. Or it might be necessary to look back into the history for the behavior characteristics of that application, including who has been using it and what the normal patterns of performance happened to be.

Often, the root of the problem will be traced to a configuration change or version update, a recreational use of the network, or perhaps a change in the mix of surrounding traffic and factors that was the "last straw". Having the diagnosis of the specific business service driving the anomaly in traffic patterns, along with the users of that application, makes it easy to implement corrective actions early to avoid costly interruptions and degradations in application services and employee productivity.

One of the primary functions of the *nGenius* Analytics product is to identify network behavior that differs significantly from previous network behavior. To accomplish this function, the product accepts data from NetScout's Common Data Model as well as from NetFlow. However, one of the strengths of the *nGenius* Analytics product is that the basic algorithm that the product is based on is capable of detecting anomalies based on analyzing data from any data source.

Another strength of the product is that it does not have a preconceived notion of how the network should behave. For example, some tools assume that the network performance corresponds to a well-known pattern, such as a bell curve. In contrast, the *nGenius* Analytics product monitors the network and develops a model based on the actual traffic and not a theoretical model.

The Telco Manager stated that the alarms that he gets from the *nGenius* Analytics product are meaningful. He attributes this in part to the fact that the *nGenius* Analytics product has learned his environment and knows what normal usage is.

The process implemented within the *nGenius* Analytics product is comprised of two steps - the computation step and the comparative step. One of the key components of the computation step is the concept of an analysis window. An analysis window is the length of time over which data is analyzed.

The *nGenius* Analytics product supports seven analysis windows. They are .5 hour, 1 hour, 2 hours, 4 hours, 6 hours, 12 hours, and 24 hours. Assume for the sake of example that a data point is generated every 5 minutes. Then the .5 hour analysis window has six data points, and every five minutes a new data point is added, and the oldest data point is aged out.

During the computation step, the *nGenius* Analytics product is looking to identify either a spike in utilization or a longer-term steady increase. In this context, a spike refers to a change that is both brief and distinct. Note that the shorter analysis windows are more appropriate for identifying a spike, while the longer analysis windows are more appropriate for identifying longer-term drift.

The result of the computation that is done during this step is seven values that are referred to as window values. Each window value is compared to the history of relevant window values in order to detect an anomaly such as a spike or drift.

For example, the most recent window value for spikes for an analysis window of .5 hour is compared to other window values for spikes with an analysis window of .5 hour and a probability distribution (p-value) is determined. The p-value is the probability that the given window value would occur. So, if the spike was not very large, the p-value might be 0.3. This means that over time 30% of spikes with an analysis window of .5 hour have been less than the current value, and 70% have been greater. Common sense would dictate that it would not be reasonable to generate an alert for an event like this. As part of the comparative step the p-value of each new window value is compared to other p-values. Common sense would dictate that if the p-value was highly unusual then it is reasonable to generate an alert.

Once an event is detected for a segment and/or virtual circuit(s), the *nGenius* Analytics product examines the unicast, multicast and broadcast traffic behavior. The *nGenius* Analytics product then determines which application(s) caused the event to occur. The results are then added to the diagnosis information and reported together with the alarm to the dashboard as well as to other designated event consoles. For example, integration with both HP OpenView and IBM Tivoli NetView has been recently certified.

Conclusion

IT organizations must change their approach to application management. Perhaps the most compelling factor necessitating that change is the point made in the introduction to this review. That point being that the most likely person to recognize that there is a performance problem with an application is an end user. Given that enterprises continually rely more and more on IT to support key business operations, it is difficult to believe that IT organizations will be perceived as being successful over the next few years if they continue to feature such a reactive approach to application management. It is also clear that while static performance alarms do offer value, the use of these alarms has not enabled IT organizations to take a proactive approach to application management.

The use of analytics is not new. What is new is the application of analytics to networking. Because network analytics has the ability to automatically detect abnormal network behavior, it has the potential to be an important tool to enable IT organizations to more proactively manage application performance.

For more information on this topic and others like it

[CLICK HERE](#)

or visit www.netscout.com



You can find out more about performance alarms in Jim Metzler's Impact brief:

Network and Application Performance Alarms
- What's Really Going On?



NetScout Systems, through its *nGenius*® Performance Management System, offers large organizations cohesive views into application services delivered over today's complex, global networks, helping IT professionals optimize network and application performance and prevent misuse of critical enterprise resources. Based on granular, flow-based

performance information gathered across the enterprise, the *nGenius* System delivers key performance management functions, including application and network monitoring, capacity planning, troubleshooting, and user experience assurance, in a single integrated solution.

For more information visit www.netscout.com.