ExtraHop Networks Offers New Application Performance Option With NAPM Approach

Issues

There is no denying that high-performing, highly reliable networks are becoming increasingly important. In this age of growing application diversity, server virtualization and Cloud adoption, when workloads and services are moving flexibly between systems and locations in dedicated, hybrid, and outsourced infrastructure models, one of the few constants is that networks must keep everything in contact and provide the communications element which allows all the parts to work together as a whole. Despite this, the productivity and agility that organizations look to their IT organizations to provide is primarily embodied not within the network, but rather within the applications and services that the network is entrusted to deliver. IT operations teams recognize this link and are looking for context-aware monitoring techniques that can provide insight into application traffic and transactions to reveal quality, health, issues, and problems. A number of approaches have been brought to market to address this need, but have fallen short either due to a lack of complete visibility or a lack of analytical depth or sophistication. New and innovative approaches are needed to close the gap between infrastructure and application performance visibility, and to provide actionable intelligence focused on the true center of IT's value to host organizations – applications and services.

IT teams seek monitoring techniques that can provide direct contextual insights into application and transaction traffic.

Context

Fortunately, infrastructure technologies (including the network) continue to mature and stabilize and become more and more reliable and resilient. This is a good thing, because the rate of change in the application layer shows no sign of slowing and thus is never likely to achieve the same levels of predictability. Infrastructure technology maturity is allowing operations teams to move beyond basic availability concerns and focus increasingly on the more challenging objectives of optimal performance. And further, since the ultimate goal of IT is to deliver highly reliable, high performing applications, infrastructure operations must tune all monitoring and management activities towards optimization on an application-by-application basis.

With applications constantly changing, aggravated by an increasingly fluid and virtualized computing layer, operations teams must take advantage of the less-variable parts of the infrastructure to establish instrumentation and visibility. The network represents such an opportunity. The network connects servers, storage, and end users, and will be traversed multiple times by any and every application of consequence today. From the network viewpoint, it is possible to measure how each and every application transaction is performing, not only in isolation but also all together, in the mix, where all players must coexist peacefully. This is immensely helpful in understanding the full context of application performance and all of the potential factors that may contribute to any degradations or disruptions.

To date, there have been many attempts to deliver application-aware performance monitoring from the network perspective. Network Performance Management (NPM) was a first attempt, monitoring

©2011 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

activity via agents on each network device and collecting that data for central reporting and analysis. The original RMON standards were intended to deliver application awareness, but created an unacceptable load on network devices and thus were scaled back to the point that application details were lost, and only aggregate traffic data remained available from most devices. From another direction came Application Performance Management tools (APM), which worked by installing agents on servers (and sometimes clients) to look deeply into how each application was performing. APM solutions provided rich understanding of application-layer components, but were expensive to deploy and could not supply any details on performance-affecting factors within the delivery infrastructure. These two viewpoints were helpful, but were commonly deployed by different teams and rarely were directly correlated, hence gaps remained between data sets and operational monitoring viewpoints, resulting in inefficient and ineffective processes for both planning and troubleshooting efforts.

A promising step forward came with the arrival of Application-Aware Network Performance Management (ANPM) solutions. This category employed a set of technologies that recognized and leveraged the fact that application details could be gleaned from the network perspective. While a few were based on the use of active/synthetic test agents, most of these solutions either grew from the use of network device flow records (i.e. NetFlow, sFlow, jFlow, cflow) or the use of packet inspection probe appliances. The probe appliances are, in reality, an evolution of the original RMON initiatives, re-implemented in a way that offloads the analysis computation load from network devices, and flow records are a new, lighter-weight alternative for network devices to document the application sessions and transactions flowing through them.

Existing attempts to deliver the full picture of application transaction performance fall short by leaving out key data or failing to bridge organizational boundaries

ANPM approaches helped to deliver better application awareness across the full delivery infrastructure, and provided a couple of very important advantages over NPM and APM alternatives. Most notably, flow records provided quick visibility into exactly where applications are showing up from a topology perspective and details on exactly what is driving the loads on each device. However, the depth of application detail included in flow records is limited and the approach is not a true real-time monitoring method. Packet-based monitoring goes beyond flow records to understand response time, recognize and correlate network-layer errors, and provide much more complete resolution in terms of application types and transactions, including the ability to support packet-by-packet analysis of activity. Unfortunately, while providing much more business-oriented information than NPM, ANPM solutions have predominantly been employed by networking teams as a means for "self-defense" and reactive troubleshooting, leaving broader IT operations teams unsupported.

NAPM – A New Paradigm for Performance Monitoring

All of these efforts have been helpful and have allowed leading organizations to greatly improve the prioritization of operations practices, but they have not yet directly bridged the divide between application support and network operations. To make matters worse, vendors offering NPM, APM, and ANPM solutions have made big promises regarding breadth and depth of performance visibility, claiming they provide everything needed to solve every performance issue (at least the ones that really matter). Yet few if any have been able to fully deliver on those promises, and many an operations team has spent vast sums on procuring, deploying, and customizing these solutions only to find that they still need help.

Into this divide, a new category of solutions is emerging, bringing the best of transaction and application monitoring and analysis from the APM world and applying it using ANPM-like instrumentation and visibility techniques. Network-based Application Performance Monitoring (NAPM) is more than just a

©2011 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

new twist on an old approach – it is a hybrid solution that bridges the divide and provides a common set of performance monitoring analysis, which can be used directly by both Applications Support and Network Operations teams.

In order to succeed where others have failed, NAPM solutions need to meet a number of criteria in order to close the gaps. First, they need to provide full visibility across the stack – applications and services at Layer 7, but also the details (and errors, specifically) that can happen down in the network layers (L2, L3, and L4) and directly impact performance. Second, NAPM systems must provide true real-time recognition of performance issues, meaning alerting as well as immediate analysis, so issues can be recognized and identified as soon as they occur rather than during after-the-fact analysis. Next, NAPM solutions must be easy to deploy, configure, and adapt to a dynamic application mix, with as much automation as possible in helping operators keep pace with change. NAPM solutions must also deal with very high speeds in core networks – 10Gbps line-rate monitoring is an absolute must, as is a growth path for the higher speeds to come. Finally, NAPM solutions must support large, distributed environments, while also including easy-to-use dashboards and reports that can facilitate collaboration and share findings and results with a broad, sometimes non-technical, audience.

A prime example of an NAPM solution is the Application Delivery Assurance system offered by ExtraHop Networks. Built around high performance network-attached instrumentation appliances, the ExtraHop solution performs packet-level inspection of application traffic and reveals not only who is using which application, but more precisely what is happening within each step and call of application transactions, in true real-time. This brings focus on what matters most to organizations – the activity and health of specific application transactions and activities – directly into view, while also providing the context to understand the delivery infrastructure side of the equation.

ExtraHop's NAPM approach represents a hybrid method, leveraging the best of existing performance management techniques

The ExtraHop solution offers a design that benefits from lessons learned in high-end Application Delivery Controllers solutions (F5, specifically), which translates into deep understanding of application traffic behavior and a pre-disposition for high scalability. The solution provides true real-time application transaction analysis and alerting up to a sustained 10Gbps across the full stack – Layers 2 through 7. The system was also designed from the ground up for ease of deployment, automated recognition and adaptation to new and changing applications, and a rich graphical user interface for dashboards and reporting. The new EH1000v virtual appliance released in mid-2011 adds significant flexibility for deploying the solution, both for monitoring intra-hypervisor, VM-to-VM traffic as well as remote deployments – even into Cloud settings.

Within the application layer, each organization will have elements in common with others in the marketplace, but also many that are specific. There are also unique combinations of transaction metrics that can be related directly to business processes and success indicators. ExtraHop has addressed this customization need with an innovative scriptable framework, called Application Inspection Triggers, which can be used to build those organization-specific business performance indicators based on the rich transaction data intrinsic to the solution.

©2011 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

EMA Perspective

As much as networks are essential, applications are king, and all IT infrastructure technologies exist to serve the king. All management technologies must evolve to span domains and understand how the greater systemic whole is working together to deliver that which IT was built to provide – applications and services. Along the way, scale and complexity are major hurdles. Kudos to anyone who can look these challenges in the eye and laugh, and then deliver a solid, valuable answer. ExtraHop is doing this in a unique way – standing in the middle of the traditional network and application support worlds and delivering value to both operational teams.

IT teams are constantly looking for ways to align their operations with business needs. It's a race that they will never stop running. When it comes to application performance management and monitoring, this means that their management tools, technologies, and practices must be selected, deployed, and applied in context of application and service transactions. And this is what ExtraHop helps them to achieve with a simple and elegant approach.

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter (http://twitter.com/ema_research). 2312.080811

©2011 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com