Multi-Layer Performance Management

Co-Deploying ExtraHop Networks and NetScout Systems Solutions

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for ExtraHop Networks by Jim Frey, EMA Managing Research Director
December 2011
# Multi-Layer Performance Management:
Co-Deploying ExtraHop Networks and NetScout Systems Solutions

## Table of Contents

- Executive Summary ................................................................................................................. 1
- Priorities for Application Performance Management.......................................................... 1
- The NetScout Systems ANPM Solution ..................................................................................... 2
- The ExtraHop NAPM Solution ............................................................................................... 3
- Parallel Deployments in Practice – Three Case Studies ........................................................ 3
  - Case Study #1: Financial Transaction Clearinghouse ............................................................ 4
  - Case Study #2: High-Tech Manufacturer .............................................................................. 4
  - Case Study #3 – Large Investment-Services Organization .................................................. 5
- EMA Perspective ....................................................................................................................... 6
- About ExtraHop Networks ..................................................................................................... 6
Executive Summary
As part of an effort to align with business priorities, the focus of IT operations is shifting steadily and deliberately towards application performance. Performance monitoring and troubleshooting tools are essential elements in this endeavor, and those being deployed to leverage the network viewpoint can supply direct application awareness and transaction visibility. Along the way, many IT shops have found that the best answer involves the use of a combination of tools to meet the complementary needs of top-down, application-oriented performance monitoring with deep packet inspection forensics. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) paper examines three case examples where ExtraHop Networks solutions have been deployed for real-time application performance visibility and triage alongside NetScout® Systems solutions for forensic analysis of complex performance issues and behaviors.

Priorities for Application Performance Management
IT teams across organizations of all size and all sectors are increasingly turning their focus towards a rapidly converging area of management discipline – Application Performance Management (APM) and, more specifically, performance of application transactions. This shift is occurring for many reasons, both technical and business, but primarily because more and more organizations are embracing the fact that applications are the life’s blood of day-to-day processes and value-add. Once this threshold is crossed, there is no option other than to train all efforts upon making sure that those critical applications are not only reliably available but are performing in a way that keeps business operations humming smoothly.

Along with the increased focus on APM comes a new set of requirements for management tools, technologies, and practices. Many such requirements have existed for some time, but they are all taking on a new sense of urgency. First among these requirements is the need for accurate and current visibility – across distributed architectures and across the various layers of technology that must be working together smoothly to effectively deliver applications and transactions. Good visibility also affords another very important byproduct – the information needed for rapid problem identification and, consequently, rapid restoration following an outage or degradation. This critical insight can even provide the early clues needed to predictively and proactively address emerging issues before they breach the threshold of serious business impact. Finally, all of the operational information being gathered needs to be formatted and presented in a way that is consistent with the priorities placed upon each application or group of applications, otherwise known as the much-sought-after alignment between business and IT.

All of those IT teams out there going through this transition are not the only ones who have recognized the increasing focus on and demand for advanced APM. Management-tools vendors are also recognizing the need to address this critical set of requirements. These solution providers recognize the challenges in front of them, in particular the technical challenge of providing truly comprehensive visibility. Many are dealing with incomplete performance data sets or with solutions that have been tuned to the narrow needs of specific constituencies within development or operations organizations.

One of the more advantageous positions for observing and measuring application and transaction performance is from the network.
Multi-Layer Performance Management: Co-Deploying ExtraHop Networks and NetScout Systems Solutions

One of the more advantageous and promising positions from which application and transaction performance can be observed and measured is the network. Since most all applications and streams of transaction activity share common network links, this viewpoint can be used to recognize not only current activity of any individual application, but also all of the other activity going on concurrently in the shared infrastructure. This approach is particularly useful in recognizing the interactions between the various systems and end users and the influences created by the shared delivery media that is today’s modern IP network. And when choosing to leverage the network viewpoint, the most definitive technique for performance monitoring is based upon inspection of the application/transaction flows directly down to the network packet level.

Of those solution providers approaching application performance from the network perspective, two different and yet complementary approaches have emerged. One has its roots in deep analysis and recognition of activity from the bottom up, starting with the lower layers of the network and extended to recognize applications through packet inspection up into Layer 7, the application layer. This approach is commonly known as application-aware Network Performance Management, or ANPM. The other approach focuses much more intensely upon the application layer itself, or from the top down, adding to that some details about what is happening in the lower layers of the network. This latter approach is commonly known as Network-based Application Performance Management, or NAPM.

While both of these approaches aim to deliver visibility and deep awareness of application and transaction activity, many IT organizations have found substantial value in deploying the two together. The remainder of this paper illustrates examples of how real IT users are deploying the ExtraHop Application Delivery Assurance system from ExtraHop Networks, a fast-growing NAPM provider, in parallel with products from NetScout Systems, the largest industry provider of ANPM solutions. In particular, a high-tech manufacturer, a financial clearinghouse, and a large investment services organization have all chosen this approach and found great value in parallel deployments.

The NetScout Systems ANPM Solution

NetScout Systems offers what are arguably the networking industry’s best-known packet-based performance monitoring solutions, now approaching 30 years in the marketplace. At the core of NetScout’s Unified Service Delivery Management ANPM solution are packet collection and analysis instrumentation appliances known as nGenius® InfiniStreams®. The InfiniStream excels at high-rate streaming storage of packet sequences for forensic analysis while also generating real-time performance monitoring metrics and metadata. Advanced APM analysis capabilities are provided through the use of add-on nGenius Intelligence modules that run on the InfiniStream platform and/or through the nGenius Performance Manager and nGenius Service Delivery Manager products, which combine to act as a central reporting/console system. In aggregate, the solution is designed to provide rich forensic packet analysis capabilities for serious network performance troubleshooting, while also providing real-time performance monitoring, alarming, and reporting if the full product suite is employed.

While deployment approaches and criteria do vary, most common are those where the NetScout technology is deployed by the Network Operations team primarily as a safety net, turned to by operators when troubleshooting is required. Legacy Sniffer® product technology that is part of the NetScout
solution has been substantially enhanced over the years to deliver deep, rich, and detailed analytic capabilities for recognizing application types, activities, and interactions across the network stack.

Networking professionals contacted during this case study project indicated that the NetScout products were deployed within their core networks and/or at ingress and egress points to their datacenters. The pros relied specifically on the NetScout products when they needed to understand details regarding protocol interactions, transaction sequences, and network node relationships specifically tied back to particular protocols or addresses. None of the pros consulted in this study were using the NetScout system for sustained monitoring or real-time, application-oriented visibility.

The ExtraHop NAPM Solution

The Application Delivery Assurance NAPM solution offered by ExtraHop Networks is deployed in a manner quite similar to the ANPM example provided above. The ExtraHop system is connected at a key point in the network where concentrations of application and transaction flows occur, either on the core backbone or at the edges of the datacenter. The solution is different, however, in that it does not focus on sustained streaming capture of packets; rather the prime objective is high-volume packet inspection for generating, displaying, and reporting of real-time application and transaction metrics. The user interface is designed to provide broad, intuitive, and immediate visibility into the flow of applications and application transactions across the network.

Given the ExtraHop system’s focus on applications and application transactions, a different constituency is commonly involved in acquiring the products. Networking pros will commonly be directly involved in acquisition and deployment, but Application Development and Support personnel are often a primary proponent and consumer of the resulting system. ExtraHop has focused on providing extensive details within their solution that go well beyond simply what applications are active to reveal specific application transaction types and application error occurrences, so that issues occurring within the uppermost layers of the network, between application systems or within application transactions, can be recognized as quickly as possible and dealt with accordingly before they impact the business.

Networking professionals contacted during this case-study project indicated that they had deployed ExtraHop systems in essentially the same locations as the NetScout products. These IT pros all looked to the ExtraHop system as a primary interface for IT Operations, depending on the solution to monitor real-time application performance and triage and troubleshoot issues. Problems that became apparent through the ExtraHop console were easy to recognize visually and were easily tied directly to business priority because they are all presented on a specific application-by-application basis.

Parallel Deployments in Practice – Three Case Studies

Many IT teams are finding great value in having both of these systems – NetScout’s ANPM and ExtraHop’s NAPM – deployed in parallel. The mix has proven in many cases to be a powerful combination for accomplishing real-time performance monitoring coupled with the details needed to resolve issues quickly regardless of where they occur in the stack. Following are three specific examples based on EMA conversations with Operations pros who have chosen the parallel deployment approach.
**Case Study #1: Financial Transaction Clearinghouse**

This organization has been built entirely around electronic financial transactions and, as such, places significant importance on the speed and reliability of those transactions. With 1600 employees, two datacenters, and direct private network connections to their clients, they would be considered, by most measures, a mid-sized enterprise. The Network and Telecom group manager has deployed ExtraHop systems and NetScout InfiniStreams on the same links within the two datacenters. His team uses the ExtraHop solution to quickly triage and troubleshoot application performance problems and the NetScout solution as a backup when deep packet-based forensics is necessary. Neither system is used today for sustained monitoring; however, there are regular situations where each has proved crucial in efficient problem recognition and resolution.

“For example, we recently had an FTP application that was failing to move files properly,” said the network manager. “We first thought it was a network congestion problem, such as a backup that was contending for the same links or storage locations. We used the ExtraHop system to assess and eventually dismiss this based on studying the FTP application behavior, including error messages, and everything else going on around it during the time slices of the failures. We then jumped into the NetScout system to dig into the controls and protocols, and found that the receiving server was returning errors due to lack of available disk space.”

“We have found the ExtraHop system to be most effective for top-down problem isolation,” the network manager explained. “ExtraHop is like the CT scan, giving us a quick view of the overall landscape. When we need to go deep, the NetScout system is the place to go.”

**Case Study #2: High-Tech Manufacturer**

This organization is of similar size to case #1, with approximately 2000 employees worldwide; however, as a high-tech manufacturer dealing with stringent supply chain and inventory management objectives as well as complex channels to market, communications and ERP applications are mission critical. The global IT infrastructure manager handles all network and telecomm technologies as well as the full span of communications tools worldwide. His team has deployed the ExtraHop system in both of the company’s datacenters and uses a NetScout InfiniStream deployed on the same links in the larger datacenter. The ExtraHop system is being used for sustained application performance monitoring, and the NetScout products provide deep, packet-based forensics when needed.

“We were looking for ways to make the network team more directly relevant in supporting our key applications, such as Oracle,” said the infrastructure manager. “The ExtraHop system does this really well, giving us great overall traffic visibility into the datacenter and graphing/displaying it in a single consolidated view. If the problem is in the application layer, such as SQL errors, we can find that and isolate it directly within the ExtraHop system. If the problems are deeper, we turn to the NetScout tools.”

“For example, we’ve had a couple of Microsoft Exchange issues recently that show how they are different,” the infrastructure manager continued. “In one case, an Exchange server was bogged down by lots of I/O. The ExtraHop system saw this, but wasn’t the best for getting into the details on where..."
traffic was coming from for the specific problem ports; the NetScout tools could do this really fast. In another case, we saw traffic between our Exchange server and our BES (Blackberry Enterprise Server) bogging down. There, the problem was that Exchange was throttling back BES connections due to load and generating lots of connection errors. This was easy to recognize in the ExtraHop system but would be really hard to find with the NetScout tools.”

Case Study #3 – Large Investment-Services Organization
This organization is larger than the other two profiled here and delivers investment and trading services to clients worldwide. Over the past few years, they have placed growing emphasis on a new set of Web-based applications that provide direct services access to their broad and diverse clientele. As the primary external touch point among an increasing number of their customers, these Web applications are deemed to be mission critical. The associate director of network management handles more than just networks – his team also looks after the systems that host those critical Web-based apps. His team deployed ExtraHop systems in the DMZ at each of the organization’s three datacenters, while having previously deployed dozens of NetScout InfiniStreams throughout the core and access networks, coupled with multiple nGenius Performance Manager servers.

The ExtraHop system provides real-time visibility and proactive early warning for the cross-domain Monitoring team. The Networking team also uses the ExtraHop system for troubleshooting application performance issues – mostly for problem isolation. The NetScout system is used as a forensic backup, primarily by the Network Engineering team, turned to when issues require retroactive analysis and reconstruction of context and conditions.

“Our monitoring group is something of a nexus,” said the associate director. “They need to see as much detail as possible across the infrastructure, organized around our critical Web apps. Often they end up bringing the network and application developers together when an issue comes up. The ExtraHop system provides us with live dashboards that we use to figure out activity baselines, so we can recognize when operational indicators are outside of the norm. For example, we recently saw a strange situation where an application that normally ran balanced between two datacenters – one hot/live and the other as secondary – driving identical full loads of traffic from both sites. It hadn’t caused any noticeable issues yet, but the extra load and congestion was immediately clear from the ExtraHop dashboard. As it turns out, the Applications team decided to change the configuration, so we had to then make some changes in the network to accommodate the additional load.”

“The NetScout system plays a different role,” he continued. “It is our go-to platform when we need to do deep analysis, particularly if we’re trying to look back in time. For example, our Customer Support team has trained up several analysts that work on specific customer-reported issues. They will pull packet traces directly from the InfiniStreams to do detailed session and transaction reconstruction while investigating the issue. This is a premium, targeted service that our customers really appreciate, and we couldn’t do it without the forensic store that the NetScout system provides.”
EMA Perspective

There are a number of conclusions that can be drawn from the examples illustrated in this report. First off, as many IT pros find time and time again, a best-of-breed approach to meeting specific needs is a well-known and well-accepted strategy. Instead of seeking a single, all-encompassing solution requiring a long and expensive deployment, the organizations interviewed found that adding the ExtraHop solution to their existing NetScout deployment was a cost-effective approach that quickly delivered significant incremental and complementary value.

Second, it is impossible to place too much importance on having the tools at hand that are needed to protect today’s mission-critical applications and assure that they are continuously operating at peak performance. The ExtraHop and NetScout solutions complement one another well, with the ExtraHop system providing clear and crisp real-time views into application performance across all tiers of the application environment. In the organizations interviewed, the ExtraHop system delivered top-down starting points that helped IT operations teams to understand real-time performance and quickly triage performance problems. NetScout provided deep forensics capabilities, yielding critical details that were at times necessary to resolve more-complex issues.

Lastly, the success that ExtraHop is experiencing by addressing the joint needs of application and infrastructure operations is strong evidence that the historical walls are coming down and collaborative solutions that build bridges by focusing on the common goal of application and transaction performance are real and viable today. Whereas NetScout products are predominantly used by Network teams, the ExtraHop system, with its applications focus, is commonly used by a broader audience and readily serves as a basis for facilitating collaboration across the entire IT organization.

About ExtraHop Networks

ExtraHop Networks is a leading provider of network-based application performance management (APM) solutions. The ExtraHop Application Delivery Assurance system performs the fastest and deepest analysis in the industry, achieving real-time transaction monitoring at speeds up to a sustained 10Gbps in a single appliance and application-level visibility with no agents, configuration, or overhead. The ExtraHop system quickly auto-discovers and auto-classifies applications and devices, delivering immediate value out of the box. ExtraHop Networks provides award-winning solutions to companies across a wide range of industries, including ecommerce, communications, and financial services. The privately held company was founded in 2007 by Jesse Rothstein and Raja Mukerji, engineering veterans from F5 Networks and architects of the BIG-IP v9 product. Follow us on Twitter @ExtraHop. For more information, visit www.extrahop.com.
About Enterprise Management Associates, Inc.

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 line of business users, IT professionals and IT vendors at [www.enterprisemanagement.com](http://www.enterprisemanagement.com) or [blogs.enterprisemanagement.com](http://blogs.enterprisemanagement.com). You can also follow EMA on [Twitter](http://twitter.com) or [Facebook](http://facebook.com).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2011 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

**Corporate Headquarters:**
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
[www.enterprisemanagement.com](http://www.enterprisemanagement.com)

2378.121411