NETSCOUT

| WHITE PAPER |

Nabbing Performance Suspects in AWS Cloud-Based Apps Through Visibility

An Intellyx White Paper for NETSCOUT by Jason English

Whodunit?

You don't have to be an expert performance engineering sleuth to notice when a site or app you are using seems 'out of breath.' The delay may cost you a few extra seconds of load time after a click, or it may manifest itself as the endlessly spinning 'disk of death.'

The causes of these interruptions may seem a mystery, but the results are well known. In a retail setting, users can start to lose enthusiasm and abandon their carts within 2-5 seconds of lag time. For a banking or insurance company, a compromised network can be a board level issue. And if your company uses SaaS or cloud-based software for work, you will definitely experience work delays and missed deadlines due to a procrastinating business system.

Companies undergoing a digital transformation increasingly move parts of their applications and data to a hybrid IT infrastructure, which includes cloud services like AWS, to gain the benefits of elastic scaling and dynamic flexibility. But that doesn't address several mysterious performance and security problems.

Let's investigate and find out what clues we can track with greater visibility.

What Are the Usual Suspects Affecting Performance of AWS Cloud-Based Apps?

Suspect: The Development Process?

New development patterns are emerging, as companies seek to become more responsive to customer demand. The Agile revolution accelerated development, but also brought fragmentation, especially within large enterprises. Scaling causes uncertainty when semi-autonomous teams may provision their own labs and meet business requirements on independent iterative cycles.

Getting beyond yesterday's waterfall approaches and requirement tracking tools leads to newer project approaches and a portfolio of open and proprietary toolsets to support them. This creates borders to visibility between teams, departments and partners as to what is really being promoted to production.

Clues to Close the Case: Look for patterns of interdependency at every detected deployment to see if there are upstream or downstream release impacts that can ultimately hamper user experience.

Suspect: AWS Itself?

Whether you are running applications entirely on AWS, or, more likely, using them as one part of your hybrid IT strategy, you can't simply fault the cloud. AWS is taking performance tuning as far as they possibly can, beyond what any company would be able to do by itself, given the massive traffic and storage load they are subject to on a daily basis.

Still, the devil is in the details. AWS may host applications and data in different geo regions, which often talk to outside app services and data sources. Since even the fastest fiber can't carry data faster than light, even data moving within the cloud provider can get held up for large cumulative amounts of time as it is routed around the world. There may be potential for network flow improvement here.

Clues to Close the Case: Ensure packet-level tracing across a networked transaction, and don't just settle for round-trip response time as an indicator. Try to break down the 'stops' in each transaction as a performance budget and look for variations across sessions.

Jason "JE" English is Principal Analyst and CMO at Intellyx. Drawing on expertise in designing, marketing and selling enterprise software and services, he is focused on covering how agile collaboration between customers, partners and employees accelerates innovation.

A writer and community builder with more than 25 years of experience in software dev/test, cloud computing, security, blockchain and supply chain companies, JE led marketing efforts for the development, testing and virtualization software company ITKO from its bootstrap startup days, through a successful acquisition by CA in 2011. He co-authored the book Service Virtualization: Reality is Overrated to capture the then-novel practice of test environment simulation for Agile development. Follow him on Twitter at @bluefug.

Suspect: A Lack of Appropriate Security Visibility?

Many applications do a great job of solving for the "known knowns" of perimeter security: preventing and detecting unauthorized access attempts and DDoS attacks seeking to knock down the front door.

But what do you do when the 'front door' is potentially renewed and changing as dynamic application instances are added? Every new service integration and API can introduce new data sources to your app, which may execute actions within applications. Add in feeds from 5G networks, mobile and IoT devices, and the attack surface grows exponentially. And what about internal employee misuse of the network – perfectly authorized users that are responsible for almost half of the world's data breaches?

Clues to Close the Case: Enterprises will always need perimeter security from the IaaS provider, with, intrusion detection, load balancing and strong authorization controls. But in a hybrid IT model, you also need network level perception of malicious data types and behaviors. For instance, the NETSCOUT Atlas security suite can create "smart data" from TCP/IP traffic directly, and profile it against an updated feed of hundreds of known malicious or negligent packet behaviors.

Suspect: The Ui or Network Response Time?

APM (application performance management) tools have evolved with the cloud to measure performance at the user interface and even responsiveness at the service composition layer. This would work fine if your entire application was a self-contained island.

Even if AWS is hosting most of the application environment, and files and images are served rapidly from a CDN, any significant ongoing business interest always has some systems of record, apps and data in an on-premises or managed data center, and user sessions will need to share data with external services.

Clues to Close the Case: Seek comprehensive visibility into the interdependencies and network traffic happening across the network of the entire Hybrid IT environment, in order to track down any culprits that would never appear in a standard APM tool.

The Intellyx Take: An Application Is an Entire Network

You can't catch a suspect you can't see. There are already many good solutions for diagnosing integration, performance and security issues on the market for applications that run on cloud-based services like AWS.

What the clue performance sleuths often miss is that a modern hybrid IT application actually crosses several organizational borders of responsibility, and its entire network is much broader and amorphous in deployment than its cloud footprint in AWS belies.

User expectations for a fast, functional and flexible experience has never been higher. Time to eliminate those borders and shine a light on whole-network visibility.

For example, NETSCOUT for AWS enables more informed business decisions by removing the barriers associated with mining high-volume wire data in the AWS cloud. NETSCOUT accomplishes this by enabling real-time analyses of all data traversing the AWS infrastructure and on-premise data centers across large enterprises. Enterprise data hidden within dynamic cloud workloads transforms into timely and valuable insights with the NETSCOUT solution to truly close the case.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

NSWP_005_EN-1901 08/2019