slashdotmedia
Pure Technology. Pure Engagement.
sourceforge Slashdot free(code):

ExtraHop

10 Ways Wire Data Can Help You Conquer IT Complexity

November 2013

The need for IT business intelligence is well-known, but equally important is the need for IT operational intelligence. That is, the ability to see and know everything that is happening in your IT environment right now, at any moment.

That is a very tall order considering that today's IT environments have unprecedented levels of scale, complexity, and dynamism. Virtualization and software-defined networks (SDN) are adding to that complexity. But armed with operational intelligence, IT teams can better collaborate, fix problems, and provide support for application rollouts, migrations, upgrades, compliance audits, and other key IT initiatives.

Where IT Operational Intelligence Comes From

IT operational intelligence can be gleaned from four primary data sources:

- **Machine data**, such as log files, SNMP and WMI
- **Code-level instrumentation**, which is what traditional application performance management (APM) is based on
- **Service checks** that provide some insights on whether applications are up or down and how well they are performing
- **Wire data**, or the data-in-motion that definitively describes all communications between systems

Wire data is the record of everything that is happening in your IT environment in real time. It provides an unmatched, in-depth view into the performance, availability, and security of your environment, including issues that you otherwise might not know about. However, this great source of operational intelligence has historically been untapped.

Wire Data Is Elusive Prey

Like anything of great value, wire data does not come easily. The sheer size and speed of all the data running through your IT environment on a constant basis makes wire data difficult to catch in its entirety. In just one day, a large organization can easily create petabytes of raw wire data in a number of application protocols and formats. And, like machine data, wire data is unstructured. Wire data is also high-velocity, generally at 10Gbps in data centers, and faster still in cloud environments.

There are significant challenges to analyzing it at scale, especially in the messy reality of today’s datacenters. IP fragmentation, out-of-order packets, and microbursts are some of the challenges when reassembling the packets into flows and sessions. The biggest challenge, however, is that the sheer volume of wire data requires powerful packet processing capabilities to keep up at line rate.

A solution that can analyze and act on wire data will result in a variety of operational benefits for your organization.

Conquering IT Complexities

Following is a list of 10 ways that wire data can help you conquer IT complexities.

1. Trolling and Polling – A wire data solution can automatically detect application and infrastructure performance issues based on communications over the wire. Some solutions may only offer "polling" capabilities, such as a scripted SNMP process that periodically "polls" the system to ask if it is doing any retransmissions, for example. Polling will catch problems at the time the poll is being conducted, whereas "trolling" looks for evidence of problems on a continual basis.

2. Application-Level Performance Metrics – Traditional agent-driven solutions will monitor the performance of your CPU, disk, and memory. To fully understand what is happening in your IT environment, you'll want to measure all Layer 7 application communications—which wire data solutions will do. The benefits of a wire data solution include the ability to receive reports on your ICA latency, SQL statements, and DNS records without having to run agents on your systems.

3. Big Data Analysis – The data flowing through your system is immense in volume. Historically, there has not been an easy way to extract specific pieces of wire data and feed it into Big Data analysis platforms such as MongoDB or Splunk. A robust wire data solution can tap into data defined by Layer 7 protocols (SQL, HTTP, NFS, MySQL, etc.) and send it to Splunk, where it can be used for generating Big Data analysis. By adding customized triggers in the parsing engine, you can select unique pieces of data from the transaction payload, such as order IDs or global unique identifiers (GUIDs).

4. Spotting Data Theft – A great advantage of triggers is the ability to help you identify when data is being stolen from your back-end databases, a particularly vulnerable place to theft entry. Some of the most sensitive data that an organization stores may be located on back-end database servers. By paying attention to the queries that are being run against these databases, you can quickly spot when queries are being made by unknown or untrusted sources.

5. Database Monitoring – Wire data analysis can also help you monitor your database performance without having to run profilers, and enable you to obtain reports on table performance, processing time by client or server, total queries by client or server, and processing time by query.

6. Parsing Data – By integrating a robust wire data solution with MongoDB, Splunk, or another Big Data analysis solution, you can mine that data for business intelligence purposes. For example, you are able to do specific queries and receive tables and indexes that show how those queried topics are performing. You can generate reports by User ID, database, client Subnet, Client IP address, database server, database table, and individual stored procedure.

7. Catching DNS Failures – A robust wire data solution can look for DNS lookup failures as they happen. DNS failures can be reported by Client IP, DNS server, or Subnet. Gaining better control of DNS resolution will

increase the speed of logins. Very frequently, DNS errors are overlooked as a source of slow performance, especially if those issues are intermittent or affect a subsection of users.

8. Query Behavior Monitoring – In the event that applications are interacting poorly with your database, you want a record of that behavior. A robust wire data solution will perform that function, first by spotting the unusual behavior, and then by tracking logon sources, time of queries, length of query times, and nature of the queries.

9. Faster Launch Times – A robust wire data solution should not only enable you to improve the rate of launch times on your hosted applications, but also help you produce meaningful reports that enable you to analyze what is happening. You can generate reports that include average launch times by User Name, Client Name, Client IP, Customer Subnet, Application, and XenApp Server.

10. Better Cookies – A non-intuitive benefit of a wire data solution is the ability to better track cookies and assess the value of each cookie. While wire data may be thought of as an unconventional way of analyzing cookies, the ability to have wire data in real time makes the process much easier and quicker.

Why Choose a Wire Data Analytics Platform?

To manage today's increasingly complex IT environments, IT teams need operational intelligence to know what's happening at any moment. Wire data fills this need and has recently been made accessible through robust solutions that can analyze production traffic at line rates. Equipped with this data source, IT teams can conquer IT complexities that are not easily addressed by other approaches.

About ExtraHop

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop Operational Intelligence platform analyzes all L2-L7 communications, including full bidirectional transactional payloads. This innovative approach provides the correlated, cross-tier visibility essential for application performance, availability, and security in today's complex and dynamic IT environments. The winner of numerous awards from Interop, TechTarget, and others, the ExtraHop platform scales up to 20Gbps, deploys without agents, and delivers tangible value in less than 15 minutes. To learn more, go to http://www.extrahop.com