Visibility and Operational Intelligence for the Cloud Era

Using Splunk to Extract Business Value from Data in Hybrid IT Environments

research. analyze. neovise.

Perspective Report

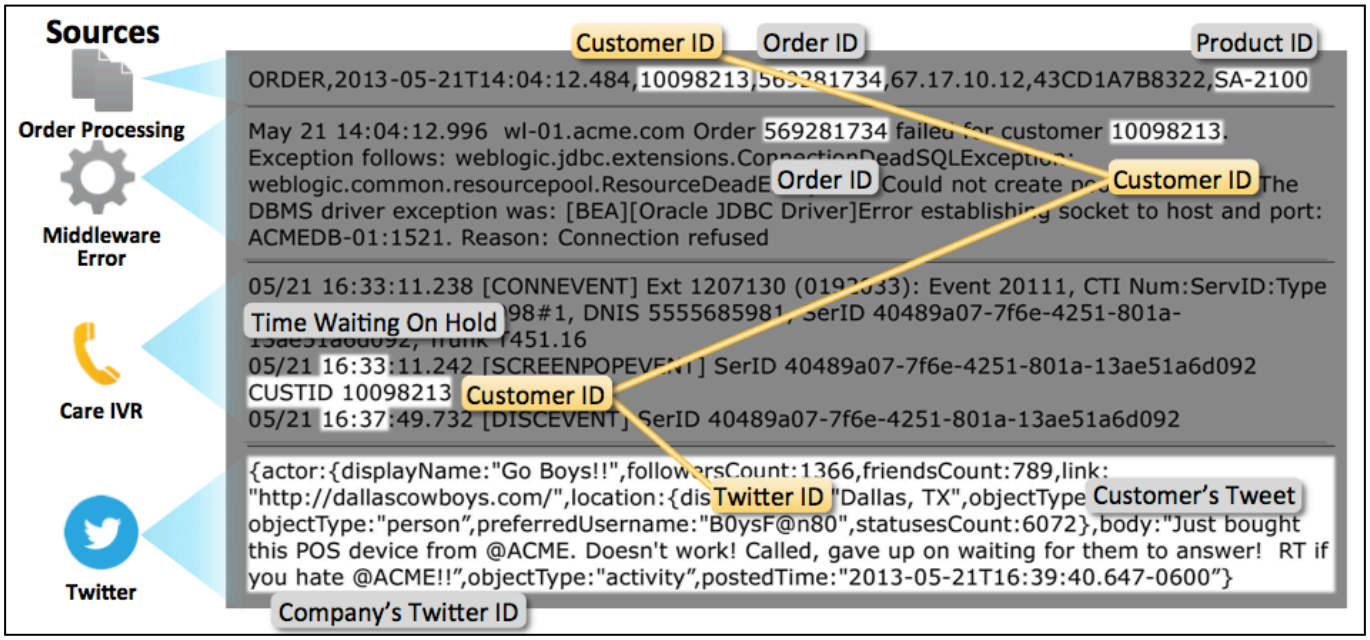
Published March 10, 2014

The Business Value of Data

We all understand that data has value. For instance - within a business environment - customer data, competitive data and financial data are all valuable to the business in some way. While this idea seems quite obvious, it is less clear how data actually becomes valuable.

It turns out that *raw* data is not very valuable at all. It generally needs things like transformation, processing and context to gain value. These steps are analogous to the way raw materials move through a value chain and eventually become more valuable finished products. The specific steps in a data value chain could include: data collection, metrics creation, analysis, insight and action. Taking an action that results in business value is the culmination of transforming raw data into business value.

Consider a real world example, illustrated by the following diagram:



A customer of ACME Inc. purchased a product that failed to work as expected. When he attempted to get support through the company's interactive voice response (IVR) system, he spent several minutes on hold. Giving up in frustration, the customer complained about his experience with ACME to 1,366 Twitter followers. By using Splunk to process all this data from disparate systems – including Twitter, the customer care IVR, WebLogic middleware, and the order processing system – ACME was able to quickly find and fix the technical problem in the customer care system, as well as track down the customer and resolve his concerns.

Cloud and Hybrid Environments Add Complexity

The example above describes one common scenario where data analysis can produce business value, but it only hints at the complexity of today's IT systems. In the cloud era, enterprises run more of their applications in cloud environments, taking advantage of improvements in flexibility, scalability, agility, and economics. As a result, businesses collect and process raw data from many additional sources outside their traditional IT environments. These include infrastructure as a service (IaaS) environments, software as a service (SaaS) environments, web applications and services, and more.

Without a solution like Splunk, data visibility and analysis becomes difficult as businesses expand their IT footprints from relatively simple on-premises infrastructure to these highly distributed environments. Since each part of a hybrid IT environment has unique mechanisms for exposing underlying data, enterprise IT organizations rely on a diverse array of tools for data collection and analysis. For instance, they might have one specialized tool for collecting server data, another for collecting network data, and still others for collecting application data. Of course, most of these tools were designed to work in on-premises environments and fail to support data collection from various types of cloud environment.

"Without a solution like Splunk, data visibility and analysis becomes difficult as businesses expand their IT footprints from relatively simple on-premises infrastructure to these highly distributed environments."

Using multiple tools to collate, normalize and analyze all this data is extremely problematic. IT organizations often stitch together scripts and use other homegrown solutions to gather and view their data. With greater effort, they can use even more tools to analyze the data, generate insights and ultimately make decisions. But these ad hoc solutions typically lack the flexibility, speed, and power that businesses need to produce real value from their data.

Taming Hybrid IT Environments with Splunk

Splunk is a powerful analytics solution that helps businesses get more value from their data. It helps users draw time and transaction-based correlations among distributed data, perform sub-searches to see where results are repeated, and use lookups to correlate their machine data with external sources, adding more context and meaning. Splunk is also massively scalable, so customers have flexibility in deciding the scope of their analysis. They can choose to analyze data strictly on premises or run Splunk across all their data centers and cloud infrastructures.

Splunk can analyze data from virtually any source within hybrid IT infrastructures, including the systems powering cloud services. This deep data analysis is the key to deriving business value from highly distributed data. By correlating the events taking place throughout all the various components in their extended IT environments, Splunk helps customers better understand their data and deliver more value to their business, end users, partners and customers.

Capabilities:

- Splunk can collect and analyze data from all connected systems, whether they are local, remote, physical or virtual, so customers with hybrid infrastructure can see and analyze all their distributed data.
- With distributed and/or hybrid IT environments, it can be difficult to pinpoint how data in one place correlates with data in another. Customers can use Splunk to draw time-based and transactional-based correlations between data stored on-premises, in the cloud, or in web environments, so it's easy to correlate related activities and processes taking place in different locations, even when they seem related.
- Splunk is available in a variety of deployment forms. Customers can deploy Splunk Enterprise on-premises, in the cloud, or wherever they need to gain extra data visibility. They can also take advantage of Splunk Cloud, the software as a service (SaaS) form of Splunk Enterprise, to access data analytics anywhere they have an Internet connection.
- Splunk also serves as a development platform for analytics applications. It lets developers define their own models for analyzing and correlating data so they can isolate the value they want. Splunk apps can also integrate with other applications, so analysis and correlations can be done in a more focused, case-specific context.

Benefits:

- Splunk provides customers with a complete view of the data and data relationships within their hybrid IT environment, helping them see where problems are occurring, where improvements can be made, and where value can be added.
- By helping customers correlate data from virtually any source – including cloud-based services – Splunk makes it easy for organizations with hybrid infrastructures to draw actionable insights and add value to the business.
- By allowing developers to build useful analytics applications with Splunk as their platform, Splunk turns data into a more valuable resource. With Splunk applications, developers can align analytics with overarching business goals and integrate with other applications to deliver more valuable information.

Neovise Perspective

The increased use of public clouds and distributed, hybrid IT environments makes it difficult to conceptualize all the moving pieces, much less capture data from all the right sources, perform analysis and draw meaningful correlations. Enterprises today need tools like Splunk that provide increased visibility and operational intelligence for applications running in these highly distributed environments. Real-time analytics and time-based correlations from Splunk not only reveal deep operational insights related to application availability and quality of service (QoS), they can also help businesses understand critical information about their customers' behavior.

Perhaps the most important consideration for prospective customers is the fact that Splunk is a generalized platform, making it useful in far more scenarios than typical data analytics solutions:

1. Splunk monitors and analyzes everything from customer clickstreams and transactions to network activity and call records – all from any data source, whether on-premises or in the cloud. It also scales to meet the demands of web-scale data.
2. Splunk supports several deployment options. Splunk Enterprise can be deployed on-premises or in the cloud, while Splunk Cloud gives customers a SaaS version they can access via the Internet. Customers can also scale analytics across multiple Splunk deployments to get visibility and intelligence for all their data.
3. Splunk does not parse or normalize the data it gathers, which would predefine and limit what could be done with the data. Instead, Splunk uses a "schema on the fly" approach, allowing data to be formatted and structured as users interact with it.
4. Splunk is a platform that enables developers to define the context and focus of their analytics by creating specialized applications to suit their exact needs. A variety of applications are available through the Splunk community.
5. Splunk stands out in complex cloud environments by tracking resource consumption and costs, providing real-time insights for rapidly changing infrastructures, and meeting the unpredictable demands of elastic applications.

In the cloud era, understanding data can yield extraordinary business benefits; but to draw valuable and actionable insights, businesses need tools that enhance their visibility and operational intelligence in distributed, hybrid IT environments. Whether it's analyzing cloud data or correlating other types of complex machine data, Splunk provides businesses with an innovative and flexible way to extract more value from their data.

About Neovise

Based on independent research and analysis, Neovise delivers essential knowledge and guidance to cloud-related technology vendors, service providers and systems integrators, as well as business and IT organizations that purchase and use cloud-related services and technology. Our offerings include research, advisory and collateral development services that help our customers—and their customers—make optimal decisions and formulate winning strategies. ***Research. Analyze. Neovise***.

For more information, visit www.neovise.com.