

Cut Your Logs Down to Size

In today's IT world almost every action is logged and stored for some future use, creating a huge pile of data that you have to chop your way through to extract the critical splinters of information you need. You need a tool to help cut that pile down to size and shape the raw data into useful information. Pion from Atomic Labs enables you to turn your log data into a valuable asset that you can use to improve security, compliance, performance and business intelligence. To understand how read on.

Working in real time – Many log files are updated as things happen and the data they contain is often most valuable at the moment that data becomes available. So you need a log processing system that can handle those raw data events in real time. Pion is built on top of an advanced event-driven architecture so the moment the data becomes available Pion will help you to make sense of it.

Sifting through the gigabytes – Often log files contain thousands of informational or unimportant events that must be sifted through to get to the truly important ones. Pion is built for speed and can rapidly filter the critical events from the junk to distill the vital information. Equally important is Pion's ability to aggregate information on the fly to keep running totals or counts that can be accessed for real-time reporting or provide summarized output.

Flexibility – One of the best things Pion can do for your data is to make it flexible through on the fly transformations, reformatting and consolidation. Pion can quickly be taught to recognize and handle any log formats through configurable "codecs". Codecs define how data is formatted in the file for input or output and are definable through Pion's point-and-click interface. These user-defined codecs can be easily shared with other Pion users. Once Pion knows how the data is laid out it can be easily manipulated through the drag and drop interface so that even a non-technical person can easily transform data into any format they choose.

Making the data available and searchable – It's no secret that log files come in every format and language imaginable, so how do you make many different log files usable together? Pion enables you to normalize and transform the data so that no matter what format the log is in you can have a standardized output format available. The normalized data can then be made available to a web service, a log file or put in a database. The most popular approach is to take advantage of Pion's native database output capabilities to load the normalized log data into Oracle, Microsoft SQL, IBM DB2, MySQL Enterprise (and more) where it is immediately available. This is all done in real time so that the data from logs is processed and available extremely quickly. For larger operations Pion has built in mechanisms to optimize data loading so that the database performance doesn't suffer.

Real-time reporting – Pion can deliver real-time high level reports that put the right information in front of the right decision makers to ensure better and faster decisions. The reporting is customizable so that you can take advantage of the many different types of data you might have available to you.

Whether your needs are performance related, real time or just dealing with too many log files Pion can help. Our systems engineers are happy to work with you to figure out how. Drop us a line at www.atomiclabs.com

Case Study - Catching the Bad Guys

Finding the bad guys after a security breach is a critical but often daunting task that law enforcement officials face on a daily basis. Not only is there a ton of data to sift through, most of it is unimportant. As one agent described it, “trying to find the evidence you need in a computer crime is like trying to find a wedding ring in a garbage dump.” One of the biggest challenges is that in addition to all of the historical data, they have new data coming in each second and ideally they would like to catch the criminal in the act. Pion helps by clearing away most of the garbage and putting the remainder in a searchable database that agents can then run their ad hoc queries over. This step is critical because it allows them to interrogate the data to find answers in a way they couldn’t when it was stored in various log files and different formats. Perhaps more important though is Pion’s flexibility. With new technology, new logs and new attacks coming in all the time law enforcement needs to be adaptable. Pion’s XML-based interchange format allows agents and officers to easily exchange the latest formatting information and the newest analysis techniques as they are developed in the field. Pion delivers the speed, effectiveness and flexibility required to keep your transactions safe.

