The Beginnings of IT Insight: Business Activity Monitoring
by
David Luckham

My previous articles describe our inability to manage real time event-driven enterprises, or make grand eCommerce visions happen, or fully utilize new technologies like RFID. This is due to IT blindness, an inability to understand how patterns of low level events in the IT layers of our enterprises will impact high level business goals, policies and processes.

All is not lost. People are beginning to understand the challenge of solving IT blindness. Those who do, view it as a goldmine business opportunity. Gartner lists well over a hundred vendors selling tools that build on top of the current generation of middleware to enable EAI and SOAs, or track the progress of business processes, or predict violations of high level policies, or analyze the impact of overloaded IT resources on executing business transactions. These are some of the things you can do, or claim to do, with just a little IT insight. In fact, Gartner leads the way in categorizing these various tools and applications.

This is a second generation activity building on first generation middleware. It tries to make business sense out of events in the middleware by using a little IT insight. This activity is gathering strength as can be seen by the recently announced proposed standards for a Common Event Infrastructure (CEI). This is a first step towards standards for middleware to support event processing. If middleware supports CEI it will be easier for vendors to build tools that tell us which high level business operations will be effected by the events in that middleware — as they happen. And if all the different middleware out there supported the same CEI, well wouldn’t that be nice! We could buy one tool and install it on all of our middleware, maybe.

But first, before we get into what event processing standards ought to contain, let’s take a look at the tip of this IT insight iceberg — something that became noticeable a couple of years ago — Roy Schulte of Gartner named it “BAM”.

Business Activity Monitoring (BAM)
BAM products are a first small step towards helping enterprises overcome IT blindness. This is a very active and expanding area. Gartner listed over 50 vendors of BAM products in 2003 ranging from small start-ups to the big guys, IBM, HP, TIBCO etc. And new vendors are appearing all the time.

If you survey the BAM market you’ll find tools that claim to do some or all of the following:
provide instant insight into how IT events at any system level (e.g., network failures, database access loads, on-line website activity, and changes in metrics on all kinds of resources) will affect the progress of high level business transactions.

permit real-time business level decisions in response to system events—e.g., rescheduling business process instances that have stalled as a result of a credit reporting service slowdown.

automate real-time notification of violation or pending violation of business level policies (e.g., SLAs).

provide statistics on business process performance.

Essentially, BAM attempts to do for business processing what network management tools do for network operations. And since BAM tools are an add-on to the middleware or legacy systems you’ve already got, one sales pitch is that they increase the return on your existing IT investment.

To get an idea of how BAM tools work, let us look at a simplified model. The basic idea is to let you know when events that are significant for your business appear on your IT layer. If you buy one of these products and have it installed on your middleware, here’s typically what happens. You tell the BAM product what events interest you—e.g., signify that a business process is too slow or a security policy is in danger of being violated—and it alerts you when those events happen. If you don’t know what events are significant, most BAM products will have some out of the box list of events they monitor. Some products let you specify what actions to take in response. That’s basic BAM and it usually comes with a colorful dashboard that displays different types of events as they happen.
A basic BAM tool installed on some enterprise’s IT layer is shown in figure 1. This enterprise has a bunch of applications that play critical roles in its business transactions, a website, an entry order system, etc. The enterprise applications communicate by sending messages or events across some middleware layer. For example a workflow engine would service an on-line order from the website by sending messages to the other applications in some sequence. Each message triggers an application to perform a step in processing the order.

Suppose as in Figure 1 the enterprise installs a BAM tool to help track its transactions. The arrows indicate flows of events added by the BAM tool’s components. This BAM tool reads events from the applications but doesn’t interfere with the communication between applications. It feeds the events to activity monitors installed to watch each application. Event feeds are implemented in many different ways. The monitors use the events to measure certain metrics or “statuses” which are all displayed on the dashboard in nice colors. When statuses reach a critical state the colors change and alert events are created.

For example, if the status of the credit card gateway goes red the BAM tool creates an alert to let you know that transactions using that gateway are likely to have problems — depending upon what that metric is. If it is a load metric (e.g., the number of transactions awaiting credit verification) then the transactions will slow down. Some tools will let you write rules that react to these status alerts and take an action you specify. These are often called event-condition-action (ECA) rules. For example, “whenever the Credit Card
Gateway status turns RED, if more than five transactions are waiting for credit verification then notify the network manager”.

What I’ve just described is **basic BAM**. It can be a useful business management tool, helping us to connect some IT layer events with our business transactions and policies. Certainly it is a good step better than being completely IT blind.

Basic BAM uses single events, or very simple collections of events, to trigger rules that notify you of situations on your IT that may affect your business. This is *simple event processing*.

I’ll make one prediction. If you buy a basic BAM tool, and get it to work, it won’t be long before you’ll be asking for more than that tool can do. In my next article I’ll discuss why, and how BAM tools are maturing, and will soon be delivering more IT insight and greater operational control over your business.