May 2012
(c. online)

Simplicity, security drive MQ management trends

By Stephanie Mann

In a world of abundant endpoints and heterogeneous application environments, messaging middleware is becoming increasingly prevalent—and increasingly complex. When it comes to current trends in message queuing (MQ) management, the mantra is clear: simplify, simplify, simplify.

"It's just an explosion in terms of the amount and the scale that you have to deal with," said Kathy McGroddy Goetz, vice president of connectivity and integration product management at IBM. "And you're trying to do it all faster."

The problem is getting attention. Results of the SearchSOA.com Reader Challenges & Priorities Survey indicate that complexity is the biggest roadblock to successful application integration: 64% of respondents said complexity is the top challenge—more than cost, performance and maintenance.

Meanwhile, 65% of respondents said they value ease of integration above all when it comes to application integration and infrastructure software. The survey data also indicates message queuing is today's most widely used integration method.

Industry insiders are taking note of a greater need to monitor message queuing while maintaining security—and without adding more layers of complexity.

Open enterprise pushes new features, security risks

Some of today's newer MQ management product features reflect demands for self-service, data and event management, and secure messaging. In addition, capabilities like low-latency messaging and faster file transfer systems bring new management challenges. As more companies create open APIs and expose their services, there is a call for new ways to connect to things beyond the four walls of the enterprise.

All of this contributes to more complex middleware infrastructure.

"Many of our customers have built up an infrastructure of messaging middleware and they're using it to integrate all their applications," explained April Hickel, senior product manager, BMC. "It's got integration with more components; there are more layers involved. They have message brokers; they have hardware appliances."

By adding advanced software agents, troubleshooting capabilities and data analytics, monitoring products aim to facilitate better oversight of multiple middleware components.

For example, BMC's Middleware Management suite—which includes administration, monitoring and transaction tracing products—provides self-service capabilities to enable broader control of middleware environments. Customers can deliver a Web-based interface for monitoring and management straight to application users. That, along with an analytics engine that provides dynamic base-lining and behavior analysis, reflects a user-centric trend.

As companies continue to open up services to Internet users, outside partners and suppliers, it is becoming more important to monitor who is accessing services—and to determine how the user experience can be improved.

"Regardless of how our infrastructure is working," said BMC Lead Solution Manager for application operations Jody Hunt, "it's the end-user's perception of the application [that matters]. A lot of times, their perception is colored by the front-end infrastructure, the actual pulling out of all these endpoints."

But opening up the enterprise and expanding management capabilities heighten MQ security risks. That risk is compounded when companies undergo mergers and acquisitions or use disparate middleware monitoring and management products together, said Charley Rich, vice president of product management, **Nastel**. "[A new feature] we've added is a single security model," he noted. "In one place, you can control all of your access to all the different middleware your company has."

Higher security features have also been added by other vendors. In 2010, IBM announced a WebSphere Advanced Message Security product, now available as an integrated capability within the WebSphere MQ server.

Endpoints or pain points?

According to Goetz, a key driving trend in MQ management is the proliferation of endpoints. More point-to-point connections mean more points of access and more events to respond to.

It also means more governance is on the horizon.

"SOA is really a core foundational thing, and it's about good design," she said. "People are afraid of [governance], but it's so critically important in this day with barriers being knocked down and trying to manage within and beyond the enterprise."

While preexisting monitoring products aim to keep an eye on efficiency and performance, updated features take into account that the high volume of MQ data can make governance difficult. Without proper message monitoring, application architecture can suffer.

"Message queuing is very different from other systems—it's almost like a network," said Rich. "It's asynchronous…it's all disassociated. Yet it is the glue that holds the enterprise application architecture together, which is exactly what you need to make SOA work."

According to Rich, many companies are stuck with middleware monitoring systems that overwhelm them with information, making decision-making a challenge. "Monitoring products are actually contributors to the problem," he noted.

Important MQ information is lost in the fray. To address that pain point, Nastel's core messaging middleware product, AutoPilot, now includes a complex event processing engine as a way of consolidating the "big data" generated by messaging.

Clearly, there is a lot more to systems monitoring than there was in the past. This is due in great part to proliferating middleware diversity. The diversity of tools for managing middleware can be expected to expand. Another big new middleware challenge is looming in the form of multiplying mobile applications and devices that are now tapping into enterprise back-end systems.