



## Configuration Management Soup for the IT Administrator's Soul

As systems and applications become more powerful and flexible, the more difficult it becomes to secure and audit them. This is true because as technologies become more powerful and flexible their configurations become more complex, making configuration management tasks much more detailed and exacting. It is therefore no surprise that IT's most time consuming activities in securing, managing and auditing complex technologies involve configuration management. Deploying new patches involves changing software configurations. Installing an upgrade involves changing a software configuration. Reporting on corporate or regulatory policy compliance involves comparing the actual configuration of systems to an ideal configuration. The list seems never ending. These activities hinge on understanding and controlling technology configurations in an effective and efficient manner. Ptak, Noel & Associates (PNA) interviewed Autonomic Software's customers to determine their key criteria for evaluating configuration management solutions and their experiences using Autonomic Software's solution. PNA found that scalability, flexibility, policy based control, and agent performance were important to the interviewees. This paper outlines PNA's view on those criteria and summarizes the experiences of Autonomic Software's customers.

### *Scalability*

The number of deployed systems and applications keeps growing in leaps and bounds, thus configuration management solutions must scale with this growth. Three factors influence a solution's scalability. First is the ability to aggregate vast amounts of data and provide holistic reporting. For example, most products require multiple management servers to scale to thousands of managed nodes, however, some products have difficulties providing management views and reporting across multiple management servers. The second factor is the speed at which the solution can complete its tasks. Solutions that take days to discover or patch hundreds of systems are not truly scalable. Third is the ability to work across wide-area networks, the solution should accurately discover and efficiently manage all nodes at remote locations.

Autonomic Software customer, BankWest expanded up from an initial 100 node installation to well over 1200 nodes in a short time period. Brian DeLucca, an IT manager at BankWest, commented that the ease of expansion was impressive for two reasons. First, the speed at which the solution delivers comprehensive asset reporting, analysis and patching across the entire enterprise environment. Scanning technology collects very granular information on both servers and desktops and the flexible reporting provides trouble-free creation of very detailed system-level reports and comprehensive bank branch level reports. Secondly, the solution works well with BankWest's Active Directory authentication deployment, which spans multiple domains and is fairly sophisticated due to rapid corporate expansion and regulatory requirements. BankWest had some hurdles with other configuration management solutions being unable to recognize all managed nodes across its network. However, DeLucca noted that Autonomic Software's solution had none of these issues.

BankWest's IT administrators use the solution to package, test and automatically deploy patches and report patch deployment status. DeLucca noted that the solution worked well for both desktops and servers. He estimated that it would take one administrator fully dedicated to system patching to manage the nodes associated with their original Nevada branches.

However, with Autonomic Software in place there are no dedicated patching administrators, even through corporate growth by multiple acquisitions.

Bob Parsons, President of Automated Office Systems (a managed services provider with over 300 customers) is also pleased with the solution's scalability. He noted that the solution works well in several customer scenarios – a single location with thousands of managed systems, distributed over several remote branch offices, and as a hosted solution for clients with as few as 10 managed systems. Parsons was also impressed by how well the solution works in a variety networking situations, as customers with 256K lines, leased lines, or T1 lines all have high satisfaction rates.

### ***Flexibility***

All enterprises have custom applications that must be deployed and managed, however the rate of application change is increasingly exponentially, as is the variety of technologies these applications must use and support. The variety of computing end-points is exploding with mobile devices (such as PDAs and Smart-phones) and smart devices (such as digital video recorders (DVR) and unattended kiosks). Not only must IT manage these new resources, but new business models can hinge on IT's ability to actively control the configurations of these devices. In addition, software development can occur in weeks rather than months, this allows software vendors to deliver new applications and patches with increasing regularity. Administrators can no longer ignore these releases as regulatory compliance and controlling security vulnerabilities are now imperative for business operation. Configuration management solutions architected to easily expand management to new devices, operating systems and custom applications, without requiring significant solution upgrades or redeployments, have a distinct advantage.

Parsons explained that his customers often have unusual project requirements that test the flexibility of management solutions. For example, a banking customer required a solution to deploy and patch custom mainframe 3270 applications. Autonomic Software not only created custom deployment templates for the client, but had the solution debugged and tested for high performance inside of six weeks. This is not the only unusual use of Autonomic Software's technology. For example, a telecommunications company quickly adapted the solution to control the configuration of custom set-top devices deployed in consumer homes.

### ***Policy based control***

Using policy based configuration management is particularly important in cases where users or multiple IT administrators have some control over system configurations. For example, if a hundred people were given the same desktop at 9am, by noon every system would have a different configuration. Similarly, every IT application server may be initially deployed with a standard configuration, yet application managers and developers typically tweak those configurations to resolve problems or optimize performance of a particular application, resulting in different application server configurations in seemingly no time at all. Some of these configuration changes are harmless, impacting neither security nor compliance, but others pave the road to data theft, resource hijacking, service meltdowns, or failed audits.

Automatically recognizing those differences dramatically reduces system administration headaches. For this reason, PNA believes configuration management processes should evolve from simply

reporting system configurations to actively applying configuration policies. Having a report stating that 300 desktops have Oracle client software installed is good background knowledge, but that the report itself does little to help IT from the standpoint of continuous compliance or security. However, having definitive proof that every Oracle client is automatically patched according to approved policies creates a computing environment that is continuously protected and easily auditable for compliance.

The difference here is that instead of preventing any and all changes to a system's configuration, system configuration is checked against policy and violations are remediated automatically. These configuration policies can relate to anything: software patches, security related best practices, regulatory compliance rules from government or industry agencies, or business policies to ensure corporate confidentiality. What is important is the use of a policy checking and automated remediation approach to managing configurations.

In addition to automated policy checking and remediation, DeLucca uses Autonomic Software to identify systems not in routine contact with the management server, these red flags help administrators be proactive in controlling system configurations. DeLucca also appreciates the ability to schedule patches according to policy, for example they could push five patches to 100 systems after 9pm. If desktops were turned off during the scheduled time, when the system comes back online the scheduled patches are automatically deployed, thereby ensuring a continuously protected environment.

Parsons is fond of saying that it only takes one misconfigured or unpatched system to create a gaping security hole. Therefore his MSP customers are encouraged to create policies to ensure that patches are automatically applied and that known configuration issues are automatically remediated. He noted that his customers typically have a wide variety of patching and configuration policies based on machine types, operating system versions or business use. Autonomic Software's small footprint and fast patch deployment ensure that policy enforcement is not disruptive to customer's business activities. In addition, IT managers are alerted to non-compliance and remediation actions, which simplifies auditing and improves security.

### ***Well-behaved agents***

Management agents have been much maligned in recent years for being fat (hogging system and network resources), lazy (unable to do more than report metrics) and difficult (unreliable behavior and requiring extra maintenance effort). Therefore any management solution with agent technology must demonstrate the agent's utility, good performance and stability. In other words, demonstrate its ability to take action on the system, validate its low consumption of system or network resources, and prove it adds no instabilities to the system being managed.

DeLucca's past experience with performance and stability problems lead to a "no agents" rule-of-thumb for his management solutions. However, he made the exception for Autonomic Software after the solution breezed through their extensive testing process. He notes that in the three years since, there has never been a problem with the patch distributions, unexpected system crashes during the patching process, or communication between the agent and the controllers failing. Parsons reported similar experiences, explaining that customers who had quickly decommissioned other solutions because of negative experiences with agent behavior.

Yet these same customers were satisfied with the performance of Autonomic Software's agent technology.

### **Conclusion**

Configuration management can no longer be a passive reporting task. The technology is too complex and there are too many patches, security issues, and compliance audits for IT to ignore. IT administrators must take active control over their system's configurations if they are to keep up with all of these demands on their time. Yet configuration management is a complex, time consuming and error prone task – unless IT administrators have intelligent, policy-based automation tools. Autonomic Software's customers found their answer to these challenges.

---

This document is subject to copyright. No part of this publication may be reproduced by any method whatsoever without the prior written consent of Ptak, Noel & Associates.

All trademarks are the property of their respective owners.

While every care has been taken during the preparation of this document to ensure accurate information, the publishers cannot accept responsibility for any errors or omissions.

PNA conducted telephone interviews with Autonomic Software customers in November 2007.

---

### **About Ptak, Noel & Associates LLC**

With a belief that business success and IT success are inseparable, Ptak, Noel & Associates works with clients to identify, understand and respond to the implications of today's trends and innovations on the future of IT Operations.

[www.ptaknoelassociates.com](http://www.ptaknoelassociates.com)

---

### **About the Author**

**Jasmine Noel** has 10 years experience helping clients understand how the adoption of new technologies affects IT management. Noel served previously as director of systems and applications management at Hurwitz Group, where she formulated and managed the company's research agenda. She was also a senior analyst at D.H. Brown Associates, where her responsibilities included technology trend analysis in the network and systems management space. Noel is regularly quoted in publications such as ComputerWorld, eWeek, and NetworkWorld. She also has contributed articles to several leading publications on various IT management topics. Noel holds a bachelor of science from the Massachusetts Institute of Technology and a master of science from the University of Southern California.

[jnoel@ptaknoelassociates.com](mailto:jnoel@ptaknoelassociates.com)