AccelOps' Unified Infrastructure Management Examined

How network and security administrators can monitor performance, availability and events with just one application

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for AccelOps

August 2012

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

AccelOps' Unified Infrastructure Management Examined

How network and security administrators can monitor performance, availability and events with just one application

Table of Contents

Executive Introduction 1

Managing a More Dynamic and Complex World 1

Adopting the Right Technology 2

AccelOps Today 2

AccelOps in Depth 2

Some Additional Recent Enhancements 3

Two Customer Perspectives 4

American Wing of a Global Manufacturing and Retail Company 4

A North American Retailer for Home Supplies 5

EMA Perspective 6

About AccelOps 6

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

AccelOps' Unified Infrastructure Management Examined

How network and security administrators can monitor performance, availability and events with just one application

Executive Introduction

Enterprise Management Associates (EMA) has had a solid, three-year history tracking AccelOps' growth and talking to AccelOps' deployments. EMA dialogs have shown that AccelOps customers are enjoying unique benefits in terms of time to value, scope of value, and cohesiveness in performance and security management thanks to the company's premium on pragmatic innovations. Recently, AccelOps has experienced more accelerated growth and introduced new functionality relevant to cloud, product administration, and monitoring for performance and security should bring yet further value to its customers.

This report provides a current view of AccelOps' capabilities in industry context, including interview excerpts with three AccelOps customers.

Managing a More Dynamic and Complex World

IT organizations are faced with a series of seemingly contradictory and impossible requirements. These include *doing more with less,* managing ever increasing complexity, and dealing with an accelerating degree of change and change-related interdependencies that impact infrastructure, security, applications and other IT services. Moreover, IT organizations are finding themselves increasingly at the very heart of much-needed business transformations towards greater efficiencies and improved responsiveness.

Security is in itself an area of increasing concern. The threat landscape has matured to the point where many common attacks may well be characterized as "industrialized," with attackers packaging sophisticated crimeware toolsets with the commercial-grade values of legitimate off-the-shelf software, from levels of features to dedicated support. At the other end of the spectrum are adversaries with the skills, resources – and patience – to craft highly targeted attacks against selected victims. This class of threat is noted for its subtlety and success at evading detection and remaining entrenched at a target for months or years.

Add to these factors the changes affecting IT itself, as rising levels of mobility create open doors for security breaches, and as accelerating change in infrastructure and cloud adoption further expose new levels of vulnerability. These factors not only increase the complexity of IT, but can lead to additional security exposures as well. Attackers often exploit a vulnerability in one aspect of IT to gain access to a sought-after target – which, in turn, may enable deeper levels of access to more sensitive, and often less well protected, assets.

All this demands that IT organizations perform more holistically. EMA data consistently supports the fact that IT organizations that operate with cross-domain management capabilities routinely outperform those IT organizations that still limit themselves to siloed views. According to multiple EMA studies, cross-domain management improves service quality, accelerates IT operational efficiencies, enhances corporate respect, and even leads to significantly better odds for increasing IT budget dollars.

IT organizations that operate with cross-domain management capabilities routinely outperform those IT organizations that still limit themselves to siloed views.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Adopting the Right Technology

So, what should you look for in a cross-domain management solution?

Strong analytic resources is one of the answers. For instance, EMA data from the 2011 research report, *Operationalizing Cloud* revealed that organizations with cross-domain performance analytics were 1.8 times more likely to reduce management complexity, 1.7 times more likely to free up resources for strategic projects, and 1.9 times more likely to improve service resilience when adopting some form of virtualization or cloud computing.

In parallel, technology selection priorities in *Optimizing Cloud for Service Delivery* (EMA Research Report, 2012) stressed security and compliance along with faster time to value. In fact, the six most important criteria were as follows:

1. Security, risk or compliance capabilities
2. Low cost
3. Management or performance capabilities
4. Ease of implementation
5. Ease of Use
6. Extensibility and integration features

Trying to combine analytic strengths with cross-domain breadth, and fast time to value is clearly a lot to ask for. But there are a few true innovators in the market today seeking to step up to that challenge. And one of the clear leaders, with a unique balance between service and infrastructure performance, security, and change-impact awareness, is AccelOps.

AccelOps Today

Founded in 2007, AccelOps has developed a solution that combines strong infrastructure, security and service management in a single cohesive package. It is, according to its own words, helping to "change the narrative around IT infrastructure monitoring" and Security Information and Event Management (SIEM) away from point-tool deficiencies towards a more integrated, and ultimately service-aware vision.

AccelOps also does this by delivering fast time to value, and in a manner supportive to the habits of many IT practitioners in both the NOC and the SOC, who are often perplexed by many purportedly "advanced solutions" that end up sitting on the shelf due to complexity and lack of role-aware support.

AccelOps in Depth

The AccelOps Virtual Appliance is easy to deploy and delivers actionable information within hours. Out of the box, it offers a wide spectrum of device monitoring and reporting capabilities that are easy to extend and customize as required. The "scale-out architecture" and solid multi-tenant capabilities enable the product to operate with equal efficiency in Managed Service Provider environments and large enterprises. Customers can simply add virtual machines to the AccelOps cluster to boost its parallel computation performance and maintain high availability.

The AccelOps Virtual Appliance is easy to deploy and delivers actionable information within hours.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

- **Monitoring, Discovery and Topology:** AccelOps' automated discovery capability enables its customers to achieve fast time to value and cohesive insights across SOC, NOC and services. The solution's monitoring capabilities go well beyond SNMP and ping sweeps to include SSH, Telnet, SOAP, syslogs, network flow, WMI, Microsoft RPC, Cisco SDEE, Checkpoint LEA, JDBC, JMX, HTTP and ARP tables, among other sources, so that security, infrastructure and service issues can be understood in context with each other. Recently AccelOps has enhanced its monitoring for Cisco Unified Computing Systems (UCS), Oracle databases, Microsoft SQL servers, custom JDBC and JMX requirements.
- **Analytics:** AccelOps provides built-in and customizable sets of analytics rules to support of availability, performance, security and change management best practices. Its analytics engine uses an XML language to parse data, an XML query language for mining the parsed data, and statistical profiling for anomaly detection. Its analytics capabilities also include correlation, predictive trending, self-learning heuristics, with support for extensive log file pattern descriptions, to enable more proactive alerts and diagnostics for the NOC, SOC and service management. In terms of security, this centralized capability can help organizations overcome one of the most consistently frustrating obstacles of security management – the siloed nature of security tools that often fail to correlate events across technology silos. The more holistic view of security-relevant information provides a more complete picture of suspicious activity, enabling both security and IT operations teams to respond more effectively.
- **The Service View/Capturing Dependencies in Context:** AccelOps offers *the* most automated performance-centric application-dependency mapping solution in the industry. EMA has confirmed its accuracy and relevance for both performance and security monitoring through numerous customer interviews. AccelOps combines this with a compelling capability to link applications together in a business service and set policies around that service in container-like fashion. New devices or applications relevant to that service can be added simply by adding them to the business service folder. All this is complemented by a Business Service Dashboard—suitable for executive as well as practitioner (drill-down) use.

Some Additional Recent Enhancements

As AccelOps continues to evolve its solution, it is worth noting some additional recent enhancements:

- **Amazon EC2 Monitoring:** By deploying an AccelOps collector inside the Amazon EC2 Cloud, rich application-level metrics and logs can be assimilated at near-real-time intervals. These complement more basic system information metrics published via the Amazon AWS API.
- **Geo-location in events:** AccelOps allows users to create and query rules based on geographical attributes by offering an IP geo-location database so that every public IP address in an event can be associated in real time with a city, state, organization, latitude/longitude location, etc.
- **National Vulnerability Database (NVD) integration:** AccelOps now offers a pre-populated Intrusion Prevention System (IPS) Vulnerability map with more than 45,000 entries to detect IPS false positives. The Vulnerability map is integrated with the National Vulnerability Database to differentiate false positives from attacks against known vulnerabilities, identify known exposures and alert both IT operations and security teams when exposures in IT are being targeted. This further helps to prioritize vulnerability remediation – a substantial challenge given the thousands of vulnerabilities in any IT environment – and identify where countermeasures may be most effective.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

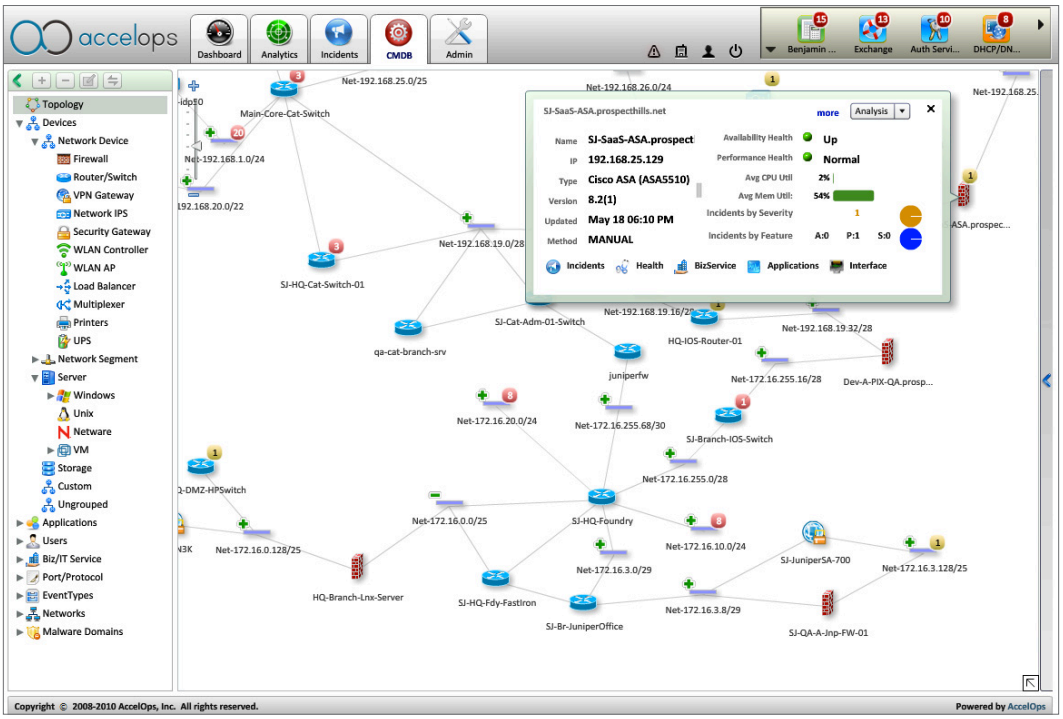

Figure 1: Dashboard Insights unite security and infrastructure concerns in service context

Two Customer Perspectives

American Wing of a Global Manufacturing and Retail Company

What is your environment like?

We are a large, global, manufacturing and retail environment and some of our applications are targeted at customer purchasing and so their performance and responsiveness is really key. Our overall IT team just for the U.S. is about 130 to support about 1,300 employees as well as many thousands of customers. We are all experienced – there are no juniors – so we have to work very efficiently. Everyone has shared responsibility, so the networking team has to be flexible enough to address security issues as well.

How did you get involved with AccelOps?

Originally we were looking for a replacement for Cisco MARS (Monitoring, Analysis and Response System) in security. We needed an improved Intrusion Prevention System, including support for wireless. I invited AccelOps in, as they did both Security Information and Event Management (SIEM) and network monitoring. We saw that AccelOps could potentially allow us to consolidate our tool sets and move away from various siloed tools across the IT team. We had BMC Patrol for monitoring servers and CA Spectrum and Cisco LMS for network management, for example. There was no central tool that all the teams used. So we needed a Manager of Managers instead of the hundreds of products we did use. Everyone got tired of logging into a million different interfaces before they could even get started with their day.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

What do you like best about AccelOps?

We are still early on in the deployment. But one of the first values I've seen from AccelOps is its ability to harvest data from log files. We were using LogLogic to do that, but AccelOps querying capability is much richer. And the network team likes AccelOps' capability to discover firewalls which can often block out access to critical servers and other devices. AccelOps tells us where the firewalls are so we know where we have to make a rule change. Right now our focus is on infrastructure management and security, but we plan to migrate to get application dependency information in the future.

A North American Retailer for Home Supplies

What is your role and your organization?

I am an engineer and a storage analyst and I work for a group that takes care of infrastructure requirements overall – including networking, servers, storage – pretty much everything outside of desktops.

How did you come to choose AccelOps?

We were looking for a solution that would allow us to function more effectively as a team. Compliance also had a role in it, as they needed something to support their security requirements. We wanted a tool that not only did log aggregation, but also did monitoring, and support root cause analysis.

We were using Orion from Solar Winds, but it was too basic and didn't have what we needed in log aggregation. We looked at Splunk, but they were too expensive. AccelOps offered the breadth we needed, and offered us a relatively smooth go-forward deployment.

What is the scope of your deployment?

We've been in deployment for about eight or nine months. We have two hot data centers in the Mid-West and we bounce between them. AccelOps monitors both of these and reports back to a single instance that does our alerting. Right now we have exactly 578 devices – 103 network devices, 453 servers, 11 storage devices, and four environmental devices, such as power supplies.

How many stakeholders are currently using AccelOps?

Overall there are about twelve. A little less than a third focused on security in Compliance, and the rest of us focused on infrastructure.

What are some of the things you like most about AccelOps?

Definitely the holistic view – and the integration with Compliance – for security and infrastructure monitoring. This breadth of function is allowing some tool set consolidation as well. We really don't have to look to another tool. The alerting is extremely granular and I like the ability to archive events. And the ability to schedule reports is good – we didn't have that before. In the future we expect to bring in more of an applications view with support for our executives.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

EMA Perspective

While the customer comments in the core of this report should speak for themselves, it may be worth noting perspectives from several other AccelOps customers that EMA has spoken to in the past. These reflect deployments focused on broad-based requirements for managing and optimizing change in both a performance and security context:

- *Accelops is doing a good job of supporting our migration towards a more fully virtualized infrastructure.*
- *We depend on AccelOps' capabilities for autodiscovery to make sure that we know what the assets are in our data center with100% accuracy.*
- *The AccelOps dashboard is great – good tabs, good search options and good presentation. A great way to drill into data as we try to understand the impacts of changes made to the infrastructure and to overcome the technology silos that often stymie security management.*

In summary, AccelOps has shown both significant strengths in supporting bottoms-up requirements for NOC and SOC practitioners seeking more effective and more cohesive ways of working, as well as more top-down concerns for strategic initiatives ranging from data-center consolidation, to broad-ranging service management optimization. AccelOps has even added more effective real-time support for CMS and CMDB deployments.

AccelOps has shown both significant strengths in supporting bottoms-up requirements for NOC and SOC practitioners as well as more top-down concerns for strategic initiatives.

However, it should be clear that some of AccelOps' strengths come from intentional design limitations. For instance, the AccelOps Virtual Appliance is not currently optimized for assimilating data from other management tools, but is fine-tuned to discover, monitor and analyze metrics based on its own data collection capabilities. Nor does AccelOps pretend to be a true Application Performance Management solution with granular transaction awareness. As such it is meant to be a complement to more transaction-centric solutions.

However, what AccelOps has already achieved is both substantial and impressive. And perhaps above all, it is a demonstrably usable and pragmatic solution in spite of the breadth and scope of its capabilities. As such, EMA expects to see AccelOps grow as an increasingly successful company in its own right – both in mid-tier and up-market environments. EMA also looks to AccelOps to become a provocative industry catalyst for much needed change towards a true cross-domain way of working compelling at once to both practitioners and executives.

About AccelOps

AccelOps provides a new generation of integrated security, network, and data center monitoring and management software for dynamic and virtualized data centers. Based on big data scale-out architecture and patent-pending distributed real-time analytics technology, AccelOps automatically analyzes and makes sense of behavior patterns spanning server, storage, network, virtualization and applications to rapidly detect and resolve problems. AccelOps works across traditional data centers as well as private and hybrid clouds. Its unmatched delivery of real-time and proactive security and operational intelligence allows organizations to be more responsive and competitive as they expand the IT capabilities that underpin their business. For more information, visit www.accelops.com. Follow AccelOps on Twitter: @accelops and blog: http://www.accelops.com/blog/

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2523.082212