accelops

SOLUTION BRIEF

Next-Gen SIEM: 5 Ways to Faster, Better Data Center Monitoring

The AccelOps software's ability to integrate, automate and learn, coupled with its contextual intelligence and real-time analytics acts a force multiplier that results in a faster, more effective IT monitoring solution.

- Ensure key business application Service-Level Agreements (SLAs)
- Protect networks from threats
- Real-time alerts for anomalous activity
- Meet compliance requirements

Increasing IT Complexity

Virtualization has been the catalyst for elastic data center resources, synchronized across private and/or public cloud infrastructures. This provides organizations the agility to scale data center resources supporting specific business applications as performance needs change.

Ever-increasing network speeds and "connect from anywhere" mobility solutions provide access to business applications from virtually anywhere in the world. While this significantly improves knowledge worker productivity, it also increases end-user expectations. Users now expect "always-on" availability, as well as dependable, low-latency application performance, whether in the office, from home or on the road.

With this mobility boom also comes security challenges to protect business information assets. For businesses that must adhere to compliance regulations, cloud-based services and application mobility further exacerbates security and availability challenges.

Doing More with Less

"Do more with less" is certainly an often overused, yet very relevant expression as it applies to most IT departments today, especially in smaller organizations. While technology demands continue to accelerate, budgets and staff have not. As a result, resource-constrained IT staffs are expected to manage the administration and maintenance of servers, storage, networks, firewalls, intrusion detection and prevention systems, email system, databases, business applications, user access rights management, cloud services and more. Using separate, siloed management and monitoring tools to keep track of IT resources is inefficient and is simply not an option in today's fast-moving environments.

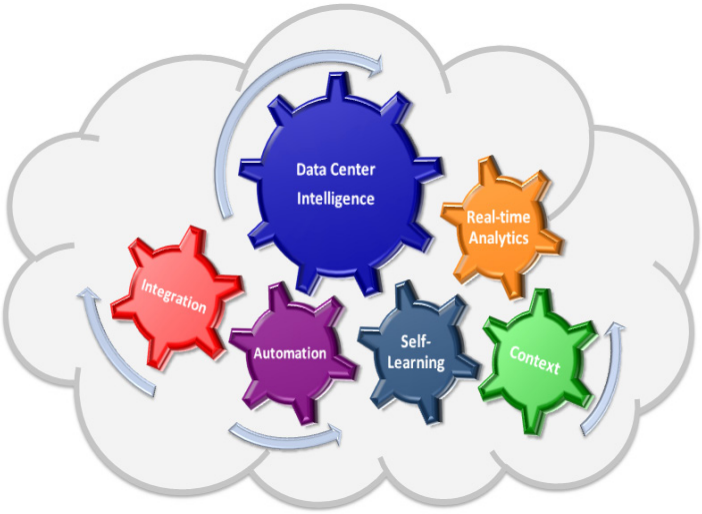
What's needed is a solution that increases IT department efficiency and productivity – an IT operations force multiplier. AccelOps does this by providing an integrated, intelligent monitoring application that automatically discovers your environment, baselines traffic patterns and uses pre-defined rules to proactively alert on performance-impacting events – in real time. By appending events with additional contextual intelligence, such as user identity, device type and geo-location information, AccelOps helps users quickly identify and rectify problems. As a force multiplier, it amplifies your efforts.

AccelOps Monitoring Application Force Multipliers

- Integration – Security, performance and availability monitoring
- Automation – Device discovery
- Self-learning – Traffic activity baselining
- Contextual Intelligence – User identity, device types and geographic location
- Real-time Analytics – Incident and event alerting

1. Integrated Monitoring – "Single Pane of Glass"

To improve IT monitoring efficiency, AccelOps combines Security Information and Event Management (SIEM) with performance and availability monitoring from a single pane of glass. The AccelOps monitoring application spans all elements of the data center, including servers, storage, virtualized resources, networks, security devices, users and applications. The solution provides unified real-time visibility into all data center resources, both physical and virtual, accelerating problem identification and resolution.



AccelOps' monitoring application is an IT operations force multiplier

2. Automated Discovery and CMDB – Complete Infrastructure Awareness

The AccelOps monitoring application runs on a VMware virtual appliance. After a simple installation and a few hours, the solution automatically discovers your entire IT infrastructure – servers, storage, virtualized servers and storage, networks, security devices, applications and users, including user identity. The discovery process is agentless, employing a variety of protocols, including SNMP, SSH, WMI, LDAP, JMX, JDBC and VM-SDK. The application automatically categorizes IT resources by type and populates a Configuration Management Database (CMDB). By periodically running device discovery, you can easily identify new devices, network or server configuration changes and maintain an up-to-date network topology.

To further improve IT efficiency, AccelOps provides complete infrastructure awareness to correlate incidents and events directly to the specific affected devices and user services. Using a drag-and-drop user interface, users can link physical and virtual infrastructure resources to the business and business services, such as Exchange, CRM, ERP, database, Accounts Payable and more.

This provides a means to track application and infrastructure resources, understand interdependencies, monitor key performance indicators, track SLA metrics and proactively monitor business service delivery. In the event of a service disruption or degradation, this consolidated business service view enables you to focus only on the resources that deliver that service, expediting problem identification and resolution.

3. Self-learning – Activity Monitoring and Real-time Alerts

After the automated device discovery and population of the CMDB, AccelOps begins collecting log information, device statistics, network flow data and resource utilization. The system self-learns the interrelationships between data center devices and automatically produces detailed Layer 2 and Layer 3 network topology maps. The system then self-learns and tracks network behavior, traffic baselines, server CPU utilization, storage used/unused capacity and application workload patterns. Previous generation SIEM and performance monitoring tools required hours of manual characterization and programming of thresholds into multiple monitoring tools. AccelOps' self-learning reduces time, effort and human errors in baselining the infrastructure for automated monitoring.

The 2 A.M. Phone Call

Pat Gilman manages a three-person IT group supporting a non-profit federal credit union. With more than 10,000 members, the organization manages assets in excess of $100 million. As is true with many credit unions, the majority of its members choose the online-only option for managing accounts, saving substantially on monthly fees. And, of course, the majority of customers check their accounts, transfer funds and pay bills during non-business hours – customers now expect 24 x 7 banking.

One night, Pat received an urgent phone call from Customer Support that more than a dozen credit union customers were unable to complete transactions. She asked for additional information and was told the complaints were all concerning the online bill payment service.

From her home office, Pat brought up the AccelOps monitoring application, selected the bill payment business service from AccelOps' Biz Service Dashboard menu, and quickly identified a non-functioning Ethernet switch whose ports connected the billing application servers to the network attached storage array. She then rebooted the switch remotely, tested the bill payment application, called back Customer Support, and alerted them that the problem was resolved.

More than 250 built-in security threat and performance-impact detection rules generate alarms and alerts to notify IT when activity falls out of bounds. These rules maybe modified or IT can create custom rules to accommodate business-specific activity patterns. Anomalous activity examples include excessive port scans, excessive logon failures, password lockouts and authentication failures during off-business hours or from unusual IP addresses.

4. Contextual Intelligence – Expedite Forensics and Automate Compliance

"Context" is additional data attributed to an event that adds more information about the event. For example, a log-on failure to a server is an event. The log for that event will include the IP address of the device that attempted the login. If the monitoring application is integrated with Active Directory, the identity of the actual user will be known, even if that person tried to log in fraudulently as an administrator. This provides additional context about the failed login attempt. The group(s) to which the user belongs and access privileges add even more context.

AccelOps also integrates a geo-location database in its monitoring solution. This provides city, state, country, latitude and longitude location metadata and is also appended to logs and events.

The enhanced context adds intelligence to help IT expedite forensic activities. The ability to correlate users with events is also a critical component in compliance reporting and meeting compliance requirements. AccelOps' suite of compliance reports takes advantage of this contextual intelligence to automate the compliance process.

In summary, contextual intelligence provides more specific and granular criteria to identify potential security threats and anomalous behavior. This not only provides a higher degree of detection but also minimizes false positives.

5. Real-time Analytics – Faster, More Reliable Incident Detection

A patented real-time analytics engine anchors the AccelOps monitoring application. AccelOps collects, parses and stores events, logs and metrics in a high-performance, flat file database. Collected metrics include device health and performance, Virtual Machine (VM) performance and health, and network flow data. The application cross-correlates this information across security, performance, availability and change management domains. From this, AccelOps' analytics capability supports both real-time alerts for any out-of-bounds conditions and forensic analysis of historical records.

Real-time alerts increase IT response time to security threats or application service-impacting events. A high-performance search engine returns results from a simple text-based search or a complex, multi-variable structured query of billions of records within seconds to accelerate problem identification and reduce mean time to repair (MTTR).

Putting It All Together

The AccelOps next-generation integrated security, performance and availability monitoring application allows you to:

- Find and fix problems faster
- Reduce IT monitoring complexity
- Enhance IT management efficiency
- Increase application availability and end-user satisfaction
- Meet compliance requirements

AccelOps includes more than 1,500 predefined dashboards and reports, all of which may be customized for your unique business environment. Reports may be run automatically on a scheduled basis and emailed to distribution lists, greatly simplifying IT workflow.

About AccelOps

AccelOps provides a new generation of integrated security, performance and availability monitoring software for today's dynamic, virtualized data centers. Based on patented distributed real-time analytics technology, AccelOps automatically analyzes and makes sense of behavior patterns spanning server, storage, network, security, users, and applications to rapidly detect and resolve problems. AccelOps works across traditional data centers as well as private and hybrid clouds. The software-only application runs on a VMware ESX or ESXi virtual appliance and scales seamlessly by adding additional VMs to a cluster. Its unmatched delivery of real-time, 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.

AccelOps, Inc.
2901 Tasman Drive, Suite 100
Santa Clara, CA 95054
USA

Web: www.accelops.com
Tel: 1 (408) 490-0903
Email: sales@accelops.com

accelops

© Copyright 2012 AccelOps, Inc. All rights reserved. AccelOps and the AccelOps logo are trademarks of AccelOps, Inc. All other product names referenced are used for identification purposes only and belong to their respective companies. The information contained herein is subject to change without notice. | Rev. 113012