Enabling Efficient Data Center Monitoring

How IT Organizations See the Big Picture of Their Infrastructure Using AccelOps’ Unified SIEM, Performance and Availability Monitoring Software
Virtualization, cloud computing, unified computing systems and mobile devices have changed the dynamics of today’s data centers. The goal of optimized computing has blurred the boundaries between network, server and storage. A data center is now any collection of CPU, memory, network and storage resources, on-site or in the cloud, and applications are deployed by selectively choosing from existing sharable resources.

This enormous flexibility comes at a price as the increase in interdependencies can cause several things to break simultaneously. For example, a security vulnerability in a virtualization layer may result in the virtual machines running on that physical machine to fail. A temperature issue in one part of a server rack may result in multiple machines failing simultaneously. There is an urgent need to holistically monitor the data center from a service availability perspective.

Ensuring optimal infrastructure performance and data availability is a critical data center mandate. However, assuring service delivery and reliability becomes increasingly difficult as virtualization, distributed and mobile access, cloud-based applications and outsourced service technologies fuel operational complexity. Not to mention stringent compliance regulations coupled with escalating resource constraints that IT organizations must continually contend.

Overburdened data center and IT teams have responded by evolving processes and building out workgroup specialties such as networks, operations, applications, security and help desks that serve to scale management. Unfortunately, this can also produce departmental silos, reduced IT responsiveness and reduced service capacity. Further, IT expansion often drives the procurement of specialized tools designed to manage the infrastructure from a component, rather than a service perspective.

The growth in data center and IT complexity, potential blind spots and inefficiencies due to operational silos, and disparate IT management tools – or in some cases, the lack of tools in some organizations – contribute to service delivery risks, outages and degradation. It diminishes an effective means to monitor and optimize service levels, manage change, quickly find and resolve the root cause of problems, and automate compliance efforts. Virtualization and cloud technologies also contribute to operational control and reliability issues.

Integrated Data Center Monitoring Required

To meet today’s business demands for greater IT efficiency and responsiveness, IT organizations must be able to see and manage all aspects of security, performance, availability and change in their entire IT infrastructure, both on-premise in traditional data centers and virtually in the cloud. This requires a fully integrated approach to capture, correlate and manage operational data, consolidate core IT management functions, and automate service definition and Service-Level

---

“During our evaluation of both RSA Envision and AccelOps, it was clear that AccelOps would help us realize our ‘Single Pane of Glass’ vision and eliminate multiple tools. AccelOps was up and running in under three hours. Once deployed, AccelOps’ powerful discovery capabilities helped us find things in our environment we didn’t even know about.”

Russell Butturini
Senior Information Security & Infrastructure Architect, Healthways
Agreement (SLA) tracking. Until now, available IT management tools have either been too expensive, very labor-intensive or lacking in required integration.

AccelOps’ powerful, all-in-one software application helps data center administrators and IT staff to monitor and enhance service levels, optimize resources and reduce business risk. AccelOps combines discovery with an auto-populated Configuration Management Database, data aggregation, correlation, real-time analytics, data management and reporting to create a fully integrated dashboard into IT operations and services.

Integrated functionality includes:

- Security Information and Event Management (SIEM)
- Performance and availability monitoring
- Business Service Management and service mapping
- Availability Management / Service-Level Agreement
- Change Control / Automated Configuration Management Database (CMDB)
- Event / Log consolidation with cross-correlation
- Identity, access and location management with directory service integration
- Network visualization and enterprise search
- Compliance and governance automation (HIPAA, PCI, SOX, COBIT, FISMA and GLBA reporting)

**Siloed IT Management Tools are Insufficient**

To fully understand the necessity of holistically managing a data center and IT, consider the following scenario: A remote branch office worker reports a slow application. Is the application really overloading the host or is the database server not responding fast enough? Is there another application on the same server that is competing for resources? Are the networks in-between ok? Is the storage network between the database server and the storage ok? Are the supporting network infrastructure services such as DNS, Domain Controllers responsive? Did someone recently make a change to network devices or the applications or databases? Did the change occur from a known admin account and workstation? Is the virtualization server in the process of moving the virtual host containing the application or the database server from one physical machine to another? Are there known unpatched security vulnerabilities on the server? Are any workstations showing abnormal traffic flow? If it was caused by a security vulnerability, how did it get into the network, who is the attacker and who else got affected?

In many cases, the problem is indeed one of the above. Sometimes however, another user is downloading a large file or watching streaming media that is clogging up a shared router interface and the problem automatically goes away when the other user is done. The question is how quickly can problems be pinpointed, prioritized and resolved to maintain service levels with the best use of IT staff and technology resources.

Siloed IT management tools cannot correlate the data effectively or fast enough, and the real problem of inferring the true root cause is often left to the user. Even
after the root cause is identified, getting to the true identity and current location of the offending user or host is another matter, since this information is spread across different management domains, e.g., OS logs, router configurations, VPN logs, etc. This lack of automation and real-time alerts affects the organization’s capacity to keep an IT infrastructure healthy with minimal service level disruption and degradation.

The AccelOps Approach

AccelOps provides a new generation of integrated security, performance, availability and change 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 delivers a seamlessly integrated, unified and service-oriented platform for the collection, monitoring, precise drill-down, root-cause analysis, and detailed reporting on all IT events/logs and performance metrics that cuts through networks, systems, applications, vendors and technology boundaries. It provides IT organizations the full context at their fingertips in any given time, and the necessary confidence and control in service delivery.

CMDB Automation Across the Organization

Mapping the infrastructure landscape and relationship in the CMDB are prerequisites for any data center and IT management solution.

AccelOps completely automates the CMDB building process via a bottoms-up approach:

- Automatic discovery of networks, servers, applications and users
- Automatic categorization into specific functional device groups, such as firewalls, storage, virtualized servers, databases and into user groups such as administrators
- Automatic identification and maintenance of component relationships: layer 2 and 3 topology maps, virtual to physical host mappings, wireless AP to controller, and n-tier application traffic flows, applications to infrastructure mappings
- Automatic identity and location mappings: network identities such as workstation IP, MAC addresses are continuously mapped to user identities such as domain/server/VPN accounts and corresponding locations such as wired switch ports, VLAN IDs, wireless access points and VPN gateways
Automatic configuration and software details mappings: network device and server configurations and software details are captured and versioned to detect changes.

The bottoms-up approach in CMDB automation gives data center and IT staffs a pragmatic way to quickly realize the benefits of change management while removing the burden of data collection across organizational barriers.

Real-Time Analytics and Correlation for Efficient Root-Cause Analysis

Without correlation and analytics capabilities, a CMDB would not be complete for any data center and IT management solution. The rich infrastructure relationship information in CMDB needs to be correlated with the current events and performance metrics to provide proactive measures for identifying exceptions, vulnerabilities and problems ahead of time, and to accurately pinpoint root causes to minimize service disruption.

AccelOps can detect network services and profile network traffic from network flows and firewall logs. An advanced analytics engine detects patterns in data over a rolling time window taking into account very complex patterns. This includes combined patterns of network, system, application and user activity. The built-in analytics engine can be easily extended using XML-based definitions.

AccelOps contains more than 1,500 built-in reports and more than 250 rule classes, which cover scenarios such as:

- Host scans, port scans, fixed-port host scans, denied scans and other traffic anomalies from firewall and netflow logs
- Network device and server logon anomalies
- Network access anomalies from VPN, domain controller and wireless logons
- Web server and database access anomalies
- Rogue workstations, PDAs, WLAN APs etc. from DHCP logs
- Account lockouts, password scans and unusual failed logon patterns
- Botnets, mail viruses, worms, DDOS and other zero-day malware from DNS, DHCP, web proxy logs and flow traffic

Reports can be placed on a dashboard to view in near real-time. Rule thresholds can be static or dynamic based on statistical profiles. SQL-like aggregation and sorting on more than 1,000+ parsed attributes is supported. And adding custom parsers to AccelOps software does not slow down your system, unlike other vendors. The solution ships with a bevy of built-in and customizable device support and analytics, including most top-tier vendors. Exposure to pre-defined analytics and an intuitive graphical interface to write searches and rules ensures a nominal learning curve.

Unified treatment of all data along with the rich contextual metadata from discovery allows the user to search and write accurate problem detection rules that span performance, availability, security and change aspects. Scenarios include zero-day malware from unpatched machines, suspicious database log-ons,
unusual geographical sources of web server traffic, slow network scans and sudden increase/decrease of application traffic.

**Service Discovery and Impact Analysis to Align IT with Business**

Rather than monitor only the health and security of the data center, network IT infrastructure and cloud environment separately and on a component-by-component basis, AccelOps allows data center, service provider and IT organizations to truly manage them from a service perspective for the ultimate goal of improving IT service delivery.

AccelOps defines a business service as a smart container of relevant devices and applications serving a business purpose. From that point on, all the monitoring and analysis can be presented from a business service perspective. It is possible to track service-level metrics, efficiently respond to incidents on a prioritized basis, record business impact and provide business intelligence on IT best practices, compliance reporting and IT service improvement.

Any query or report can use that business service as a filter, i.e. What changes have happened in my business service? Are there any security, performance or availability issues with my business service? What features are not working in my business service?

What is also novel about AccelOps is how easily a business service can be defined and maintained. Because AccelOps automatically discovers the applications running on the servers as well as the network connectivity and the traffic flow, the user can simply choose the applications and respective servers and be intelligently guided to choose the rest of components of the business service. This business service discovery and definition capability in AccelOps completely automates a process, which would normally take more labor and considerable effort to complete and maintain.

With the understanding of service, IT executives and staffs can answer questions such as:

- How can we gain insight into IT service achievement?
- How can we proactively manage our infrastructure and more efficiently respond to incidents and threats from a service perspective?
- What are the vulnerabilities and risks in our infrastructure?
- Where can we make improvements?
- Are my technology investments yielding expected results?
- When and where can performance and availability problems and service interruptions be avoided and which issues have greater service consequences?
- Which technology, deployed application, patch or potential chokepoint is affecting uptime?
- What resources can be further optimized, either by consolidation or adding capacity?

“We tried every product we could get our hands on… Now with AccelOps, everything about our environment is in that one single pane of glass – whether it’s our virtualization, storage or classic systems and network management infrastructures. This really helps IT talk in a way that business understands.”

Todd Thomas
Chief Information Officer, Austin Radiological Association
AccelOps offers “single pane of glass” security, performance and availability monitoring across all data center resources – physical or virtual – on-premise, remote and in the cloud.

- Where can we reduce capital expenditures, redeploy resources and improve efficiency?

These questions can be fulfilled through more than 1,750 built-in reports and rules coupled with comprehensive analytics. Behavioral or statistic profiling rules and best practices reports can be tuned and applied to satisfy a variety of security, availability, performance and compliance monitoring requirements and can create compensating controls.

AccelOps solution offers a customized view so executives can see a cross-departmental view. In addition, the unique virtual appliance based clustered, multi-tiered and hybrid storage architecture separates the storage from the computation and the hardware from the software.

This allows the user to:

- Utilize AccelOps’ all-in-one, integrated solution for security, performance and availability monitoring, built from the ground up, not with bolted-on products or modules
- Keep migrating the software to less expensive, faster, newer hardware to improve performance without losing any data
- Take advantage of robust failover capabilities of virtualization management servers to gain higher availability for the AccelOps solution
- Right-size the AccelOps virtual appliance’s memory, CPU and disk size to your environment
- Utilize the virtual appliance infrastructure to scale to meet your needs
- Use VMware’s higher availability or disaster recovery services

The Solution

The hybrid data management architecture is comprised of a proprietary “flat-file-based” database for storing event data and an embedded, commercial-grade relational database for storing CMDB data. This approach allows better compression and faster event handling (data insertion and query rates) that equates to greater scale, productivity, efficient data storage and a more engaging user experience.

AccelOps has a multi-tiered, clustered, scale-out architecture that can be run on multiple virtual machines to facilitate parallel computation. This allows the user to instantly increase performance by adding hardware without expensive data migration procedures.

Finally, AccelOps’ user interface is built using Adobe Flex RIA framework that allows for a more engaging desktop application experience, yet runs from a browser offering anywhere, anytime accessibility.
AccelOps brings to market a uniquely integrated data center and cloud service management solution that allows IT to see the trees, as well as the forest – harnessing the value from an organization’s existing operational data and fortifying the successful adoption of cloud computing.

Yet it provides a cost-effective, extensible and scalable IT application. Given the solution’s functional depth and breadth, the holistic approach allows organizations to be more efficient, enhances service reliability, supports cloud service transparency and makes business service management practical and tangible.

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.