

Enabling Datacenter and Cloud Service Management for Mid-Tier Enterprises

Overcoming the IT Service Management Syndrome

Companies rely on datacenter and IT to provide mission-critical services, like e-mail, Web, and voice. However, assuring service delivery and reliability becomes increasingly difficult, as the necessary growth in data center virtualization, distributed and mobile access, cloud-based applications, and outsourced service technologies fuel operational complexity. Datacenter and IT organizations respond by evolving processes and building out workgroup specialties such as networks, operations, applications, security and help desk that serve to scale management. Unfortunately, this can also produce departmental silos, reduced IT responsiveness and blurred service capacity. Furthermore, enterprise expansion often drives the procurement of specialized tools designed to manage the infrastructure from a component, rather than a service perspective.

The growth in datacenter 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 mid-tier IT 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. The adoption of cloud computing can extend operational control and reliability issues.

To improve service reliability, organizations must be able to see and manage all aspects of performance, availability and security related to that service. This requires a fully integrated approach to capture, correlate and manage operational data (be it on-premise or cloud-based), consolidate core IT management functions, and automate service definition and SLA tracking. Until now, available IT management tools have either been too expensive, very labor intensive, or lacking in required integration.

AccelOps puts the “who, what, where, when, why, and how” at the operator’s fingertips to monitor and enhance service levels, better optimize resources and further reduce business risk. AccelOps combines discovery, data aggregation, correlation, out-of-the-box analytics, data management and reporting to yield a single pane of glass into datacenter and IT operations and services. Integrated functionality includes:

- + Business Service Management and service mapping
- + Performance Management / Network Behavior Analysis
- + Availability Management / Service Level Agreement
- + Security Information Event Management
- + Change Control / Automated 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

Why Silo-ed IT Management Tools Do Not Suffice

To fully understand the necessity in holistically managing datacenter 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 is caused by a security vulnerability, how did it get into the network, who is the attacker and who else got affected?

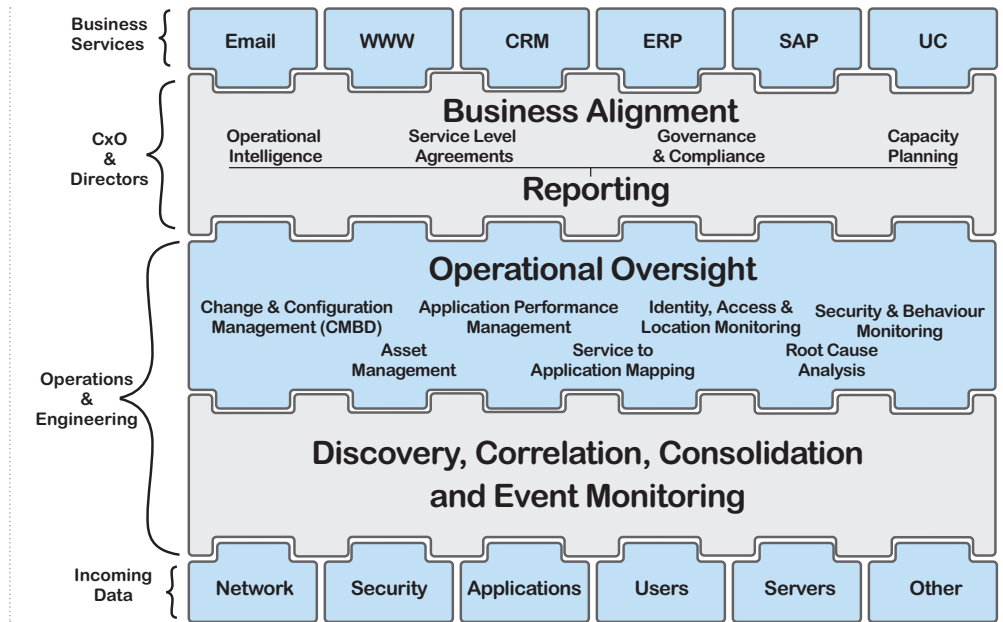
In many cases, the problem is indeed one of the above. Sometimes however, another user is downloading a large file or watching streaming media that is clogging up a shared router interface and the problem automatically goes away when the other user is done. The question is, how quickly can problems be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

Silo'd 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 visibility affects the organization's capacity to keep an IT infrastructure healthy with minimal service level disruption and degradation.

The AccelOps Approach

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 datacenters, managed service providers and IT organizations the full context (who, what, where, when, why and how) at their fingertips in any given time, and the necessary confidence and control in service delivery.

Building the full context requires understanding the infrastructure components, their relationships, the meaning of current events to them by analytics and correlation, and being able to align their meaning and impact to higher level business services and applications.



CMDB Automation for Instant Success in Change Management

Mapping the infrastructure landscape and relationship in CMDB are prerequisites for any datacenter and IT management solution. AccelOps completely automates the CMDB building process via a bottom-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 bottom-up approach in CMDB automation gives datacenter and IT organization a pragmatic way to quickly realize the benefits of change management while removing the burden of data collection across organizational barriers.

Innovations in Analytics and Correlation for Proactive Management & Efficient Root-Cause Analysis

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

This is accomplished by the AccelOps' powerful analytics and correlation engine powered with three major innovations: (a) XML based language for parsing data and (b) XML based search and rule language for mining the parsed data and (c) a profile and anomaly detection engine that can detect anomalies on any problem dimension. The languages are versatile enough for dealing with a wide range of IT operational data such as events/logs, network flows and performance metrics from networks, servers and applications. Being XML based, the language enables users to rapidly add support for custom applications and share with the community. The XML files are compiled in at run time to give the same level of performance as hand-written code. The search and rule language supports a diverse range of analytics from simple searching for textual patterns in the raw data to complex rules that trigger when abnormal event patterns is detected.

Rule thresholds can be static or dynamic based on statistical profiles. SQL-like aggregation and sorting on more than 340 plus parsed attributes is supported. 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 logons, 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 only monitor the health and security of the datacenter, network IT infrastructure and cloud environment separately and on a component-by-component basis, AccelOps allows datacenter, service provider and IT organizations to truly manage them from a service perspective for ultimate goal of maintaining and 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. 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 many people 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?
- + Where can we reduce capital expenditures, redeploy resources and improve efficiency?

These questions can be fulfilled through more than 700 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.

As a SaaS and virtual appliance offering, AccelOps solution is built from ground-up for multi-tenancy support, where different organizations can have their own customized view and higher-level management can have 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:

- + Choose the best-of-breed storage platform
- + Keep migrating the software to cheaper, 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

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 datacenter 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, flexible and scalable IT management software solution packaged for mid-tier enterprises. 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.

See how AccelOps can help your IT accelerate business at www.accelops.net.



AccelOps, Inc.
2905 Stender Way, Suite 49
Santa Clara, CA 95054
t 408.490-0903
f 408-970-9666
sales@accelops.net