

I D C T E C H N O L O G Y S P O T L I G H T

Taming IT Management Chaos

January 2009

Adapted from *Datacenter Automation: Accelerating Market Maturity Through Investment in IT* by Tim Grieser, IDC #213868

Sponsored by EMC

Traditional IT management methodologies are focused on managing individual devices and subsequently created IT silos, each with its own staff, tools, and methodologies for managing its piece of the infrastructure. However, over the past 10 years, IT infrastructure architectures have dramatically shifted from hardwired, private corporate networks to highly distributed, IP-based systems that are flooded with new types of traffic from virtual machines, video, and voice. At the same time, IT budgets are not growing at a rate that is commensurate with actual business requirements. This shift, compounded by smaller IT budgets, has caused traditional IT methodologies to break down and fail to meet the demands of managing today's dynamic IT environments. Traditional methods are contributing to the cost and difficulty of managing IT infrastructure. This Technology Spotlight focuses on the following areas:

- *Why the traditional approaches to change and configuration management are less effective in today's environments*
- *How managing change and IT compliance through automation will allow IT departments to save time and money and greatly reduce the risk of unplanned outages*
- *Why there is a need for integrated, top-down management solutions rather than bottom-up point solutions*

This paper should provide readers with a better understanding of why management practices need to shift from individual device orientation toward a more integrated, cross-domain management approach.

Traditional Approaches to IT Management

The device-oriented approach that IT has embraced over the past 20 years is no longer sufficient for managing the technically complex, quick-changing IT environments of today. The widespread and fast-paced adoption of virtualization, Web-based applications, and wireless device access, as well as globalization, have all rendered traditional tools and methods outmoded. The challenges facing IT managers include the following:

- Lack of complete visibility across all IT components and their dependencies
- Difficulty in identifying the root cause of problems when they happen
- Mean time to repair and mean time to restore are taking too long
- Lack of integration across tools
- Staying compliant across servers, applications, networks, and storage
- Setting the right key performance indicators (KPIs) and tracking trend data
- Managing virtualized services

The device-oriented approach created pockets of expertise that evolved into IT silos of knowledge and information. Each silo has its own set of tools for monitoring and managing its domains. These tools allow the users not only to monitor but also to perform changes to the devices and the services they monitor. Because these standalone tools work in isolation, it is very difficult to effectively coordinate activities among groups and correlate symptoms to their root cause, and it is next to impossible to enforce policies across IT groups.

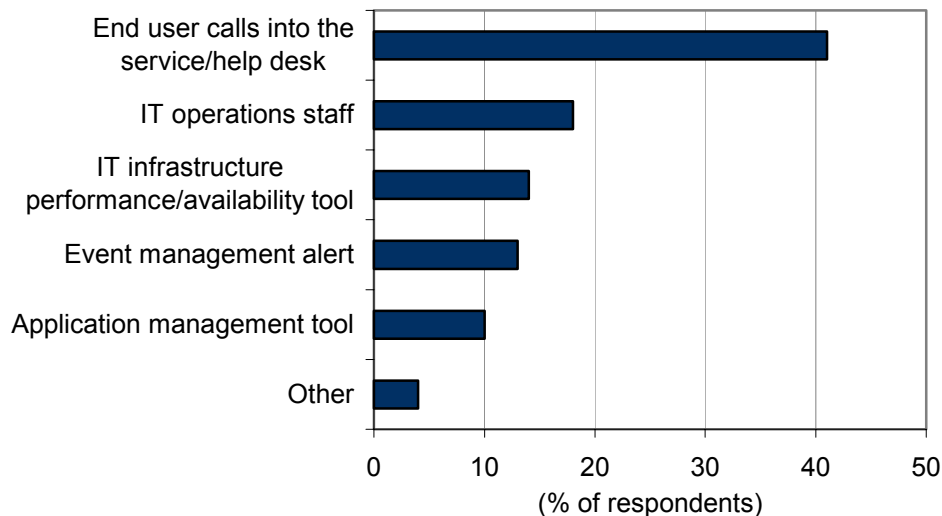
As IT infrastructures (applications, servers, networks, and storage) grow in size, they also grow in complexity, and change becomes a constant. Uncontrolled change greatly improves the chance for errors and potential service outages. For example, if the IT person in charge of a set of virtual machines decides to make a change to the user-group permissions and makes a mistake, effectively blocking an entire user group from gaining access to a particular server, that is a problem created through configuration error. Without an audit trail, finding that error is more difficult and subsequently more time-consuming.

Component monitoring tools are very good at gathering information. KPIs that provide alarms only when basic thresholds are exceeded are not good enough anymore. Too often, monitoring lights are green, while performance is steadily degrading. As Figure 1 illustrates, over 40% of IT managers surveyed stated that their first point of notification when a service was disrupted or was experiencing degradation in performance was *not* from existing IT monitoring tools but rather from end users calling the help desk. What and how IT departments are monitoring needs to change. Only KPIs that incorporate and correlate data from multiple silos will provide the business intelligence to enhance the operations going forward.

Figure 1

IT First Points of Notification When Service Degradation Occurs

Q. What is your first point of notification when a service disruption/degradation occurs?



n = 78

Source: IDC, October 2007

Consequently, IT managers are frustrated with their inability to proactively anticipate and tackle problems before they impact users or customers. The lack of communication or integration between tools means there is no way to create real KPIs that mirror real business processes. The management process and tools have not kept pace with the changing environment, making it impossible for IT organizations to effectively do their jobs and/or measure where they may be falling short.

Server, application, and network device configurations must be managed with an understanding of the interdependencies between them. Without this understanding, it becomes impossible to predict the true impact of making configuration changes.

Managing Change Through Automation

Ad hoc moves, adds, and changes in the corporate infrastructure have become the norm. Of the IT organizations IDC recently surveyed, 77% believe that the number of changes made to their infrastructure will increase by 10% or more in 2009. If change is not effectively managed and implemented, erroneous change deployments and poor configuration practices will cause service degradation and increase maintenance cost and downtime to the network.

The manual configuration of individual components or services is a time-consuming, labor-intensive process that is prone to error. Individual point solutions are locked away within each IT silo and do not share information. IT organizations place "lack of coordination among IT groups" as the major challenge in providing effective change, configuration, and release management.

Tasks such as change management can be done more effectively through automation. Automation solves the dilemma of how change is executed, tracked, and verified. Automation improves accuracy, reduces errors, and drastically reduces the time it takes to perform these tasks. Over half of the respondents surveyed feel very strongly that automation is important for reliable and cost-effective change and release management.

Automation is a way to establish and enforce policies as well as provide remediation and an audit trail. An audit trail is a way to track changes for reporting compliance, as well as for troubleshooting problems when they occur.

Automation also reduces the need to hire more administrators, even as infrastructure, virtualization, and the amount of change all increase. Automation has begun to deliver business process impact, driving the discussion within IT organizations of how critical business processes can operate more effectively through the use of automation solutions versus manually developed, error-prone scripts. The vast majority of IT organizations surveyed — 84% — view automation as a top investment priority.

Integration

The pressure for IT to operate with greater efficiency will only increase. To be more proficient, IT must have a complete picture of what is happening across the IT infrastructure. That can be realized only through the horizontal integration of tools, personnel, and processes. Disparate point solutions do not scale. A top-down, integrated management approach is needed. This approach would enable departments to share data and information across domains and build logical connections between KPIs that map to real business processes. Analytics can be applied to take it one step further and prioritize IT response based on event correlation to critical business processes and applications.

Successful integration requires a strong foundation, grounded in a common model, and that requires the following steps:

- **Step 1** — The physical integration of the tools
- **Step 2** — The integration of personnel
- **Step 3** — The integration of all the components and their dependencies that make up a business service into a configuration management database (CMDB)

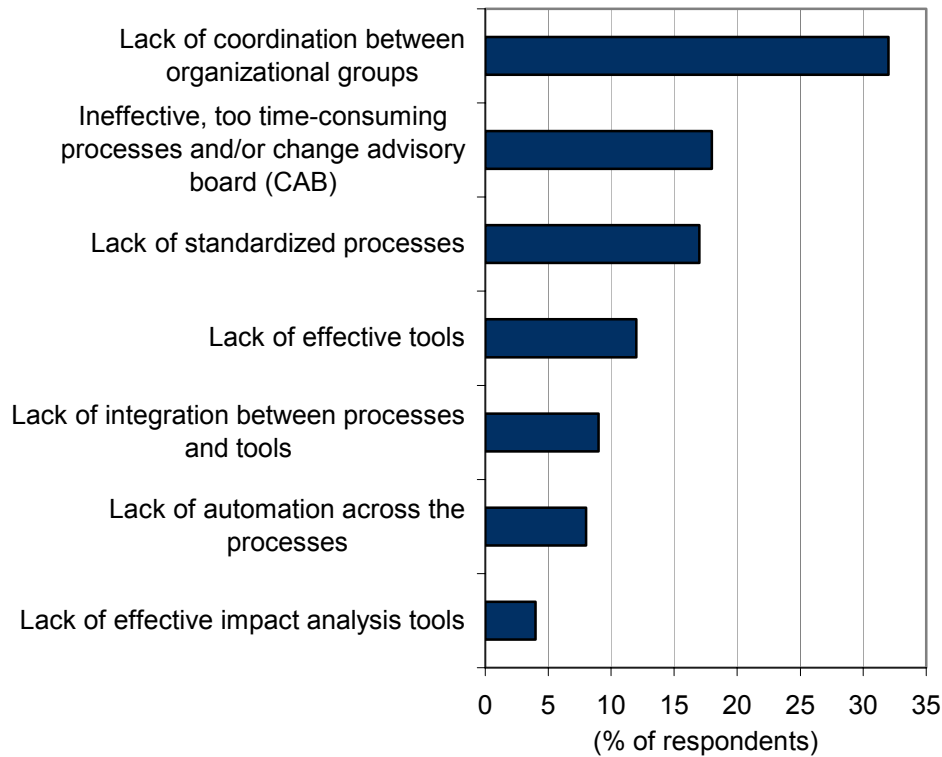
The need for individual expertise does not go away. However, that knowledge needs to be better leveraged across the IT organization. A CMDB provides a structured data scheme of all assets and maps their relationships and dependencies to a business process. The exercise of populating the CMDB will help organizations better understand the critical path between components and processes and help with priorities and troubleshooting as well as aid in the reduction of mean time to repair.

In Figure 2, respondents to an IDC survey listed the challenges they face with change, configuration, and release management. The biggest challenge is a lack of coordination among disparate IT groups. An integrated solution can help bridge this divide.

Figure 2

Change, Configuration, and Release Management Challenges

Q. *What is your major challenge in providing effective change, configuration, and release management? (Choose one.)*



Source: IDC, August 2008

Considering EMC Technology

EMC Corporation is looking to bridge the gap between IT domains and is delivering integrated management solutions that share a common set of information across domains. EMC offers a set of products that provide automated change and configuration management across server, network, and applications. This integrated solution consists of five major components:

- EMC Smarts
- EMC Server Configuration Manager (SCM)
- EMC VoyenceControl
- EMC Application Discovery Manager (ADM)
- EMC Configuration Analytics Manager (CAM)

EMC Smarts provides a strong root-cause analysis and monitoring solution for problem management across the IT infrastructure. Smarts integrates with both VoyenceControl and SCM to provide a more complete end-to-end picture of what has changed in the infrastructure. This integration enables network and server changes to be fed into and viewed from the common Smarts Service Assurance Manager (SAM) console.

EMC SCM is an automated change, configuration, and compliance management solution for both physical and virtualized server environments. Features include the following:

- Support for multiple server platforms and desktop compliance (Windows desktops, servers, Unix and Linux servers)
- Out-of-the-box compliance toolkits (including SOX, PCI, HIPAA, FISMA, and many others)
- Integration with EMC VoyenceControl, EMC Smarts, and EMC ADM
- Active Directory and virtualization support (including VMware ESX server)
- Automated change and configuration management
- Remediation
- Patch management

EMC VoyenceControl is a model-based automated compliance, change, and configuration solution for managing network infrastructure. Features include the following:

- Provides a joint PCI DSS solution with RSA enVision, EMC Smarts, and EMC SCM
- Discovers and models network relationships
- Links network compliance with remediation
- Prevents unauthorized device access
- Provides detailed audit and compliance reports

EMC ADM is an agentless discovery and dependency mapping product for the application and host infrastructure. Features include the following:

- Hybrid passive/active discovery of the application and host configurations
- Dependency mapping that enables visualization of which application and hosts are communicating and connected with each other
- Integration with EMC SCM, EMC Smarts, and EMC Infra
- Ability to track changes over time
- Ability to track relationships between the physical and virtual environments (supporting VMware ESX server)
- Ability to enable change impact analysis and populate CMDBs (including EMC Infra and BMC Atrium)

EMC CAM makes more effective use of KPI information as a whole. CAM applies analytics to KPIs to measure and capture changes over time. CAM is fed data from both EMC SCM and EMC VoyenceControl. It allows the creation of a single services model for monitoring, analyzing, planning, and forecasting compliance and IT service levels. It creates an abstracted cross-domain view at a higher level of a service. It provides the ability to quickly view compliance of both network and server devices. Managers can use this tool to build reports that show compliance trending over time.

The integration of these solutions provides a unified modular architecture that provides insight into the relationships and dependencies of applications, servers, and network devices in the IT environment. This solution enables collaboration across domains and ensures that everyone is working from the same conceptual view of resources. A common management model makes certain that managed resources are exposed in consistent format. Finally, the solutions are virtualization ready and aware.

This approach enables EMC customers to ensure best practices and regulatory compliance across multiple domains. The addition of EMC CAM, a Web-based dashboard for viewing KPIs across network and server domains, provides a strategic integration point for EMC SCM and EMC VoyenceControl and enables users to view compliance over time and to correlate over 80,000 different configuration variables and their trends over time.

Challenges

One challenge EMC faces is the deeply entrenched use of point solutions across IT domains. IT departments are often tightly wedded to these point tools and are reluctant to use others. Also, interdepartmental politics make it difficult to redefine IT boundaries. Fortunately, EMC has recognized this challenge by offering integration points to many third-party solutions to supplement their capabilities rather than force customers to rip and replace everything.

EMC's integrated solution must appeal to multiple IT disciplines, as well as to different levels of IT users — from engineers to management. The tools need feature sets that are attractive to both groups. For the technology to succeed, all users have to be on the same page.

For their part, IT organizations need to be open to working with different tools and across staff; otherwise, they will not reap the full benefits that an integrated solution such as EMC's has to offer.

Conclusion

The growing dependency of the business on the network means that IT departments are under great pressure to execute at peak levels of performance. The reduction of network downtime and the consistent delivery of business-critical applications are vital factors in IT's ability to ensure maximum business productivity. Ad hoc moves, adds, and changes can introduce errors into the IT infrastructure that result in performance degradation or unplanned and unnecessary downtime. The following are some key points for organizations to keep in mind when they are considering automation solutions:

- Perform an internal audit of existing tools and solutions to better understand the needs of each individual IT group and to find common points of integration
- Look for change and configuration management solutions that integrate into a common system management console to provide greater visibility and impact of change across the network, server, and application infrastructure
- Benchmark the time it takes to execute change and configure tasks on various devices with current methods to better understand the time and personnel savings through automation
- Look for solutions that allow the creation of policy and apply automated, continuous policy analysis and remediation that is based on a unified model of the infrastructure
- Look for solutions that support existing or planned virtualization platforms
- Look for tools that provide detailed reporting and KPIs including trend analysis over time

The implementation and enforcement of change management through automation will greatly reduce the risk of downtime through configuration errors and will also enable IT to work at a higher level of efficiency and improve cross-group collaboration.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC. For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com