The Mandate for Lights-Out IT Management

By Jim Metzler, Cofounder, Webtorials Editorial/Analyst Division

Introduction

Businesses on a worldwide basis are under increasing competitive pressure to become more agile and so are looking to their IT organizations to help them respond to these pressures by continuing to provide new value added services and applications. As a result, IT organizations have been adding a wide range of new functionality to the IT infrastructure including:

- Wireless LANs to enable additional mobility
- Quality of Service (QoS) to enable differentiated services
- Network optimization techniques such as caching, compression and protocol optimization
- Security functionality such as firewalls as well as Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS)
- Network Attached Storage (NAS) and Storage Area Networks (SAN)
- Server Load Balancers (SLB) and Application Delivery Controllers (ADCs)
- Virtualized servers, desktops and storage

At the same time that the IT infrastructure is becoming more complex, the role of the network manager is changing. Until recently, the typical network manager focused almost exclusively on the availability of networks. However, recent market research[1] indicates that there is a growing trend to have network managers be responsible for the performance of networks as well as for other components of IT including servers, security and applications.

Today the IT organization consumes as much as 80% of its resources maintaining the status quo.[2] This percentage has been increasing over time and unless significant steps are taken it will continue to increase as more functionality is added to the infrastructure. As the percentage of IT resources that are consumed by maintaining the status quo increases, the ability of the IT organization to provide new value added services demanded by the business decreases.

One of the ways that IT organizations can reduce the percentage of IT resources that are consumed maintaining the status quo is through automating tasks such as change and configuration management as well as event, incident and problem management. In addition to freeing up needed resources, automating change and configuration management can improve availability. In a survey that Webtorials recently gave to 150 IT professionals, forty-two percent of the survey respondents indicated that ineffective change and configuration management caused the majority of their network outages.

One of the factors that have traditionally reduced IT operational efficiency is the technological and organizational stovepipes that often characterize the IT organization. As such, another important step that IT organizations can take to be more productive is to reduce the number of network management tools they use by implementing tools

---

[1] The 2008 Application Delivery Handbook, Jim Metzler, http://www.webtorials.com/abstracts/Kubernan2008handbook.htm

[2] Gartner Says Eight of Ten Dollars Enterprises Spend on IT is "Dead Money" http://www.gartner.com/it/page.jsp?id=497088

that can perform a wide range of functions. The importance of taking this step is reinforced by the fact that as previously described; the typical network manager is taking on a wider range of responsibilities.

The goal of this brief is to identify how IT organizations can successfully automate the management of an increasingly complex IT environment.

Lights-Out IT Management

Lights-Out IT Management refers to the automation of both problem identification and problem resolution. The successful implementation of Lights-Out IT Management is built upon an integrated system that provides three key management functions: find, configure and monitor.

Find: Particularly in large IT organizations, it is difficult if not impossible to track all of the components of the IT infrastructure (i.e., networking equipment, servers, storage and applications) using manual methods, as these methods are both time consuming and error prone. As a minimum, what is needed is the ability to automatically discover all of the IT infrastructure elements.

IT infrastructure elements such as network switches and routers are important unto themselves. These elements, however, are typically used to provide resources for services such as a VLAN (Virtual LAN) or a VPN (Virtual Private Network). As a result, what is also needed is the ability to discover services and to be able to perform deep subcomponent discovery in order to understand the relationships between deployed services and the subtending infrastructure elements, down to the level of individual ports and interfaces.

Configure: IT organizations are continually modifying their processes. Given this, a successful implementation of Lights-Out IT Management should allow IT organizations to easily modify their processes over time but must not require that they modify them as part of the implementation of the tool. As a result, a Lights-Out IT Management tool must allow the IT organization to configure a wide range of devices using a broad range of approaches; i.e., GUIs, CLI, etc. Configuration should include exposing capabilities as automation tasks at both device and service level.

As previously mentioned, successful Lights-Out IT Management requires a focus on services such as VLANs. Because these services are typically comprised of multiple devices, a Lights-Out IT Management tool must enable an IT organization to automatically configure a service and all of the subtending IT infrastructure elements.

Monitor: Monitoring can be done either passively or actively. Using a passive approach, an infrastructure element such as a network switch would inform the management tool of a problem. Using an active approach, the management tool would interrogate infrastructure elements and would determine the health of the individual components and/or the associated service. Since both approaches have their advantages and disadvantages, an effective solution requires both. In order to enable automated remediation, it is necessary that the monitoring tool capture a level of information that is granular enough to enable root cause analysis down to the subinterface level.

Historically, the functionality described in the preceding paragraph would involve multiple IT disciplines using multiple tools. However, in order to support the expanding role of the network manager and to reduce the negative impact of technological and organizational stovepipes, it is important that all of these capabilities are available on a single system that features a customizable user interface.

Another critical success factor relative to implementing Lights-Out IT Management is the use of a Configuration Management Data Base (CMDB). A CMDB is a repository of information related to all the components of an information system. IT Infrastructure Library (ITIL) coined the term CMDB [3]. ITIL has also created a detailed description of a number of important IT processes (i.e., problem management, configuration management, incident management) with a set of comprehensive checklists, tasks and procedures that can be tailored to any IT organization.

[3] http://www.itil-officialsite.com/home/home.asp

In the ITIL context, a CMDB represents the authorized configuration of the significant components of the IT environment. A key goal of a CMDB is to help an organization understand the relationships between these components and track their configuration. A CMDB also stores contextual information about IT assets, finance, and organizational structure. A CMDB is a fundamental component of the ITIL framework for an effective configuration management process. CMDB implementations often involve integration with other systems, such as Asset Management Systems.

Implementing Automation

Increasing complexity and the growing focus on end-to-end services makes it imperative that management solutions providing automation are capable of supporting existing and future multi-vendor environments comprised of a wide variety of IT infrastructure elements, including applications, servers, routers/switches, and specialized network appliances. Automation is best applied where performing the management tasks manually is repetitious, time-consuming, and prone to human error. The remainder of this section provides an overview of where automation can be best applied to improve operational efficiency and effectiveness for key management functions.

1. **Configuration Management:** Minimizing the need for manual configuration of IT infrastructure elements reduces the operational workload and helps to eliminate human errors that can affect the reliability and security of the network. An automated configuration management system discovers the infrastructure elements and stores their configuration and associated business data in a CMDB, which can be used as the basis for generating both physical and logical perspectives of the entire IT infrastructure and the services it supports. As new elements or services are brought on-line, or changes are made to the configuration of the infrastructure, configurations can be automatically downloaded from the CMDB to ensure consistency and accuracy.

   As noted, IT infrastructure elements (i.e., switches, routers, access points, firewalls, IDSs, IPSs, Windows servers, Linux servers, clients, printers, etc.) are typically combined into network services such as VLANs and VPNs. As such, an effective Lights-Out IT Management tool must be able to assist in the rapid creation and/or modification of network services such as automating the creation and/or modification of a VLAN across multiple switches and switch ports.

   The CMDB can also be leveraged to enforce policies related to software updates, authorized device access, and configuration changes. Maintaining a documented audit trail of actions taken by operational personnel, including addition, removal and modification of Configuration Items (CIs) reduces errors and helps automate the processes required for regulatory compliance.

2. **Event Management:** Event management systems are required to maximize network and service availability by reducing the downtime of critical devices and subsystems. Event management systems typically provide error detection and some degree of error analysis, together with alarm generation. Automated event management systems can proactively monitor IT infrastructure elements for conditions that may lead to fault events and can use automated event correlation and root cause analysis to determine the precise nature and location of the faults that do occur. Effective root cause analysis relies heavily on the service dependencies that are discovered, as well as an accurate physical and logical topology of the network, such as one derived from a CMDB. Furthermore, in addition to raising alarms, the automated event management system can use the results of the event detection and analysis processes to trigger automated remediation actions.

3. **Service Level Management:** Management at the service level is essential to ensure user satisfaction with services such as VoIP or video conferencing, as well as meeting Service Level Agreements (SLAs) for user access to ERP, CRM, and other business-critical application services. Automated service level management involves proactive monitoring of service level metrics such as availability, as well as service and application response times. Results from service level monitoring can be used to trigger actions and to create SLA violation events that can be automatically fed into the fault management system for diagnosis and resolution. Automated integration of service level management, fault management systems, and trouble ticket systems can help minimize service downtimes or SLA violations.

4. **Security Management:** Automated security management includes continual monitoring of the security configuration and status of the various elements of the network to ensure that security policies are not being violated. Security audits can be automated as regularly scheduled scans or as responses driven by various security events. Security events can also by automatically correlated with other network events to minimize the number of false positives requiring management attention. Validated security events can then trigger automatic responses, such as reconfiguration of security devices, server reconfiguration, patch deployments, or revocation of user access privileges.

As the preceding discussion indicates, the value of Lights-Out IT Management is enhanced by the elimination of the stovepipes that separate configuration management, fault management, service level management, and security management. The best overall approach is a unified network management automation system. This system should integrate multiple management functions and facilitate enhanced functionality and automation by ensuring a common understanding of the infrastructure and its services and by leveraging a common pool of data in a CMDB regarding the history, status, and behavior of the network.

Summary and Call to Action

In order to be regarded as being successful, IT organizations must continually provide new value added services and applications. Being able to add these new services and applications is increasingly difficult as the IT environment becomes ever more complex and a growing percentage of the IT organization's resources are consumed just maintaining the existing environment.

Automating key network management tasks is one of the steps that IT management can take in order to free up the resources required to develop and implement new services and applications.
When evaluating automated management tools, IT organizations should look for:

- An integrated system that supports find, configure and monitor functions
- Support for a customizable user interface
- Multi-vendor, multi-element, multi-domain support
- Service-level awareness and reporting
- Support for virtualized environments
- Support for physical and logical network topologies and root cause analysis
- Integrated functionality across the Fault, Configuration, Accounting, Performance, Security (FCAPS) model and Service Level Management
- The ability to assist in the rapid creation and/or modification of a service
- Support of a sophisticated CMDB
- A high degree of automation within each function and across functions
- Ease of integration with other network management tools

A Word from the Sponsor – Dorado Software

Dorado Software is a leader in IT infrastructure management software to find, configure and monitor converging IT assets, including networking, servers, storage, and security devices. Dorado Software's Redcell™ portfolio automates IT infrastructure lifecycle management from visibility, proactive monitoring, change detection and remediation, troubleshooting, OS/file and patch updating, service provisioning, to reporting on everything. For more information about Dorado Software, visit http://www.doradosoftware.com or send an email to info@doradosoftware.com.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

Webtorials Briefs
Vol 2, Number 9

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.